UNIVERSITÀ DEGLI STUDI DI PAVIA

DIPARTIMENTI DI GIURISPRUDENZA, INGEGNERIA INDUSTRIALE E DELL'INFORMAZIONE, SCIENZE ECONOMICHE E AZIENDALI, SCIENZE POLITICHE E SOCIALI, STUDI UMANISTICI

CORSO DI LAUREA INTERDIPARTIMENTALE IN

COMUNICAZIONE, INNOVAZIONE, MULTIMEDIALITÀ

IL CASO SONY E LA PROTEZIONE DELLA PROPRIETÀ INTELLETTUALE: LEZIONE PER IL FUTURO DELLA CYBERSECURITY

Relatore:

Chiar.mo Prof. FABRIZIO SANNA

Correlatore:

Chiar.mo Prof. EMANUELE TUCCARI

Tesi di laurea di

ALESSIA TARANTINO

ANNO ACCADEMICO 2023/24

INDICE

IL CASO SONY E LA PROTEZIONE DELLA PROPRIETÀ INTELLETTUALE: LEZIONE PER IL FUTURO DELLA CYBERSECURITY

INTRODUZIONE

Negli ultimi decenni, l'avvento delle tecnologie digitali ha trasformato radicalmente la nostra società, ponendo nuove sfide in termini di sicurezza informatica. La crescente interconnessione tra dispositivi e la dipendenza dalle infrastrutture digitali hanno reso la cybersecurity un tema centrale per governi, aziende e individui. Questa tesi si propone di analizzare in modo approfondito il concetto di cybersecurity, esplorandone le radici storiche, i modelli di sicurezza, le normative in vigore e l'impatto concreto attraverso l'analisi di un caso emblematico, quello dell'attacco informatico alla Sony del 2011.

Nel primo capitolo, verrà fornita una definizione del concetto di cybersecurity, evidenziando l'importanza di investire in questo settore per proteggere dati sensibili e infrastrutture critiche. La storia della sicurezza informatica verrà ripercorsa attraverso un'analisi dell'evoluzione delle minacce, partendo dalle prime forme di hacking fino agli attacchi più sofisticati dei giorni nostri. Il capitolo si soffermerà, inoltre, sull'origine di Internet e sull'impatto che ha avuto sulla sicurezza globale, con un focus sulle prime vulnerabilità emerse con la diffusione delle reti informatiche.

Il secondo capitolo approfondisce i principi fondamentali della sicurezza informatica. Verranno esaminati i modelli di sicurezza più utilizzati, come il modello CIA (Confidentiality, Integrity, Availability) e il modello DREAD, confrontandone le caratteristiche e l'efficacia nella valutazione delle minacce e dei rischi informatici. Sarà analizzato, inoltre, il ruolo dei Security Operations Center (SOC) e dei Network Operations Center (NOC), due elementi chiave per il monitoraggio e la protezione dei sistemi informatici. L'obiettivo di questo capitolo è fornire una comprensione strutturata delle strategie di difesa impiegate per mitigare i rischi cyber e garantire la sicurezza delle infrastrutture digitali.

Nel terzo capitolo, si discuterà dell'importanza delle regolamentazioni in materia di sicurezza informatica. Verranno illustrati i principi fondamentali del GDPR e il loro impatto sulle strategie aziendali per la protezione dei dati. Saranno analizzate anche le prospettive future, come

l’evoluzione dell’User and Entity Behavior Analytics (UEBA) e del machine learning nella difesa cibernetica. Inoltre, verrà approfondita la tutela della proprietà intellettuale, aspetto fondamentale per garantire l’innovazione e la competitività globale. Questo capitolo mira a fornire una visione chiara delle normative vigenti e delle migliori pratiche per la gestione della sicurezza informatica a livello internazionale.

Infine, il quarto capitolo, analizzerà uno degli attacchi informatici più significativi della storia recente. L’attacco alla Sony PlayStation Network ha messo in luce le vulnerabilità dei sistemi aziendali e l’importanza di adottare strategie efficaci di prevenzione e mitigazione delle minacce. Verranno esaminati nel dettaglio le dinamiche dell’attacco, l’impatto sui dati degli utenti e le misure adottate da Sony per il ripristino della sicurezza. Inoltre, si discuteranno le implicazioni più ampie di questo evento per la cybersecurity globale e per le aziende multinazionali, sottolineando come le minacce informatiche possano compromettere la fiducia dei consumatori e la stabilità economica.

I. CYBERSECURITY: UN VIAGGIO NELL'ANONIMATO DIGITALE

1. DEFINIZIONE DEL CONCETTO DI CYBERSECURITY

Prima di esplorare il mondo della cybersecurity, è fondamentale fare un passo indietro e comprendere come siamo giunti a parlare di sicurezza informatica. Dobbiamo analizzare come l'evoluzione tecnologica abbia trasformato profondamente la società, portandoci a confrontarci con sfide e opportunità che hanno radicalmente influenzato il nostro modo di vivere e lavorare. Per questo, non si può affrontare il tema della cybersecurity se non risaliamo prima alle origini di Arpanet, la rete pionieristica che ha gettato le basi per l'infrastruttura digitale moderna. Arpanet (Advanced Research Projects Agency Network) nacque nel 1969 ed era una rete di calcolo ad uso militare creata dal dipartimento di difesa degli Stati Uniti D'America creata in piena guerra fredda per resistere ad un ipotetico attacco nucleare. Infatti, il loro obiettivo era quello di ostruire una grande rete americana che mettesse in comunicazione i calcolatori delle forze armate di tutto il territorio, possibilmente resistente ad un attacco nucleare sovietico. Il gruppo progettuale lavorò per diversi anni per far si che si potesse far dialogare tutti i calcolatori con un unico linguaggio comprensibile da tutte le macchine, ma con scarsi risultati. La *DARPA (Defense Advanced Research Projects Agency)* "agenzia intergovernativa volta a studiare soluzioni tecnologiche all'avanguardia da utilizzare in ambito militare.[1]", finanziò l'Università di Stanford dando vita ad una rivoluzione: cioè, quello di creare un insieme di protocolli di comunicazione per l'interconnessione di calcolatori eterogenei, dando il via all'*Internet Protocol Suite* che ben presto sarebbe diventata la più grande rete di calcolatori. Coloro che diedero inizio nel 1973 ad una nuova procedura di trasmissioni furono Robert Kahn e Vinton Cerf, due informatici statunitensi. Questa procedura di trasmissione consisteva in due protocolli: il protocollo *TCP (Trasmission Control Protocol)* e il protocollo *IP (Internet Protocol).* I due protocolli furono incorporati e diedero vita al binomio *TCP/IP*. Questo protocollo consisteva in un insieme di regole che permette ai diversi dispositivi di comunicare tra di loro in modo ordinato e senza errori. Il protocollo IP fa si che ogni dispositivo in rete sia identificato in modo univoco da un numero detto indirizzo IP. Questo protocollo, quindi, permette di individuare con precisione il mittente e il

[1] **LOGUERCIO L**, *Darpa, che cos'è e che cosa sta facendo l'agenzia statunitense a cui si ispira EneaTech* , 2021, https://www.economyup.it/innovazione/darpa-che-cose-e-che-cosa-sta-facendo-lagenzia-statunitense-a-cui-si-ispira-eneatech/

destinatario di un messaggio tramite il loro indirizzo IP. Una volta chiarito chi è il mittente e chi è il destinatario tramite l'indirizzo IP, il protocollo *TCP/IP* suddivide il messaggio in parti più piccole chiamati "pacchetti" e le invia. I pacchetti non viaggiano secondo l'ordine che avevano in partenza; infatti, uno dei compiti del TCP e proprio quello di controllare che i pacchetti siano trasmessi in modo affidabile e vengano riordinati all'arrivo, verificando che la trasmissione del messaggio avvenga in modo corretto tra i due corrispondenti. Nasce così il concetto di rete informatica: tutti i calcolatori collegati alla rete *ARPANET* (chiamati nodi) erano autonomi ed indipendenti, e nel caso di un attacco nucleare che avesse distrutto un nodo della rete, avrebbe fatto sì che tutte le altre macchine da calcolo avrebbero potuto continuare ad operare senza problemi. Arpanet veniva ormai considerata una possibile arma strategica contro l'Unione Sovietica, in particolare per l'archiviazione di informazioni cruciali in ambito militare. Con il passare del tempo Arpanet cominciò ad essere troppo impegnativa e anche economicamente costosa per essere solo utilizzata in ambito militare. Infatti, divenne estremamente attraente per i centri di ricerca universitari statunitensi, tanto è vero che Arpanet con il passare degli anni ottenne sempre di più un notevole apprezzamento nell'ambito della ricerca universitaria. Questo comportava che Arpanet nato come progetto che puntava esclusivamente a scopi militari diventava un progetto che allargava i suoi orizzonti ad altri interessi. Ormai l'utilizzo della rete aveva preso il sopravvento, soprattutto nella metà degli anni 80 con la nascita dei personal computer. Il 30 Aprile 1986 nell'Italia ci fu il primo collegamento realizzato dal Centro Nazionale Universitario di Calcolo Elettronico dell'Università di Pisa con destinazione la Pennsylvania. Nel 1991, l'ingegnere britannico Tim Berners-Lee, ricercatore presso il CERN di Ginevra, sviluppò un sistema rivoluzionario che consentiva di navigare tra diversi contenuti multimediali interconnessi tramite collegamenti ipertestuali. Questo sistema, che avrebbe poi preso il nome di World Wide Web, offriva un modo nuovo e più accessibile per usufruire delle informazioni online. Berners-Lee introdusse anche il protocollo di rete HTTP, che garantiva la disponibilità costante dei materiali online. Nello stesso anno, venne pubblicato il primo sito Internet, segnando una tappa fondamentale nello sviluppo del web moderno. In quegli stessi anni, Internet divenne accessibile al pubblico, permettendo a chiunque di contribuire con nuovi contenuti e svilupparne le potenzialità. Durante gli anni '90, si assistette a una crescita esponenziale della rete, accompagnata da numerose innovazioni che trasformarono radicalmente la società. Il modo di comunicare, lavorare e socializzare subì cambiamenti profondi. Grazie a Internet, le distanze si accorciarono drasticamente: entrare in contatto con persone lontane non richiedeva più giorni, ma solo pochi istanti. Numerose furono gli eventi che segnarono la società moderna come: la nascita nel 1994 del motore di ricerca Yahoo, un anno dopo viene lanciato il primo sito dedicato alle aste online chiamato eBay. Inoltre, nel 1997 si cominciò a parlare di cloud computing per la prima volta. Sempre nello stesso anno, a settembre, venne registrato

il dominio google.com, segnando l'inizio di uno dei più importanti motori di ricerca al mondo. Nella primavera del 1999 fece il suo debutto Napster, il primo programma di file sharing, che rivoluzionò la condivisione di file musicali. Nello stesso anno fu fondata PayPal, una startup innovativa che offriva servizi di pagamento digitale e trasferimento di denaro online. Nel 2004, con la nascita di Facebook, si aprì una nuova era per i social network, destinata a trasformare le dinamiche sociali e di comunicazione. Fu così che Internet che divenne profondamente legata alla nostra società tanto che ogni piccola distorsione poteva provocare forti ricadute economiche ma allo stesso tempo può avere ripercussioni importanti nella sicurezza delle nazioni e dei paesi. Per questo man mano che la rete si espandeva, la sicurezza è diventata una priorità cruciale. Dati e comunicazioni, un tempo limitati a pochi nodi sicuri, necessitavano ora di protezione su scala globale. L'avvento e la diffusione di Internet hanno dunque creato l'esigenza di salvaguardare informazioni sensibili, impedendo accessi non autorizzati e assicurando la tutela della privacy. Le prime minacce informatiche avvennero già durante gli anni 70 e 80 andando a colpire le vulnerabilità dei primi sistemi informatici, infatti, proprio nel 1988 Arpanet fu colpita dal primo attacco hacker. La storia dell'hacking, di cui il termine riguarda "è l'uso di mezzi non convenzionali o illeciti per ottenere l'accesso non autorizzato a un dispositivo digitale, un sistema di elaborazione o una rete informatica[2]", ha assunto nel corso del tempo diverse connotazioni, variando in base al contesto storico e all'uso specifico. Il termine "hacker" risale ai primi anni 60 all'interno del *Tech Model Railroad Club (TMRC)* del Massachusetts Institute of Technology (MIT) di Cambridge. Fu proprio in questo contesto che il termine "hacker" iniziò a diffondersi per la prima volta. Non nasceva con una connotazione negativa, ma bensì veniva utilizzato per indicare coloro che possedevano delle competenze informatiche di alto livello, non comuni tra tutti i componenti. Queste competenze portavano ad un approccio innovativo e soprattutto portava ad una risoluzione dei problemi dei vari sistemi informatici. Proprio in quegli anni però, emerse un articolo sul giornale studentesco del MIT dove questi individui considerati dei geni informatici avevano causato disservizi telefonici nel tentativo di collegare le reti tra l'università di Harvard e il MIT. Questo portò a fare una distinzione di hacker: l'hacker "buono" (white-hat) e quello "malintenzionato" (black-hat). L'intenzione non era quella di distinguere gli individui leali da quelli criminali, ma piuttosto a differenziare le loro azioni che, pur essendo per fini sperimentali potevano creare inconvenienti e soprattutto seri danni. La società odierna si stava affacciando alle prime minacce informatiche in grado di mettere in pericolo interi sistemi informatici. Questi seri danni venivano creati proprio da software malevoli, i cosiddetti malware. I malware "cercano di invadere, danneggiare o disattivare computer, sistemi informatici, reti, tablet e dispositivi mobili, spesso

[2] **IBM**, *Che cos'è l'hacking informatico*? https://www.ibm.com/it-it/topics/cyber-hacking

assumendo il controllo parziale delle operazioni di un dispositivo[3]". Il primo malware che apparse nella storia non aveva però scopi dannosi, ma aveva l'obiettivo di capire quanto i programmi riuscivano ad autoreplicarsi. Ed è quello che sperimentò nel 1971 Bob Thomas ingegnere della BBN Technologies, una delle case fondatrici di Arpanet. Questo malware prende il nome di Creeper che in italiano ha vari significati: dalla pianta rampicante a qualcosa che striscia. Insomma, Bob Thomas utilizzò questo termine per dimostrare come un programma sia capace muoversi tra computer interconnessi e non per indicare qualcosa che si insinua come un verme per infettare il sistema informatico. Questa prima versione di worm replicava sui vari schermi un messaggio con scritto un usuale messaggio: " *I'm the creeper, catch me if you can*". Il messaggio invitava l'utente a "prendere" il worm in maniera ironica prima che il messaggio lasciasse il dispositivo per raggiungerne un altro. Il 2 Novembre 1988 fu lanciato l'attacco che avrebbe cambiato per sempre la storia di Internet e soprattutto della cybersecurity. Fu considerato uno dei peggiori attacchi informatici della storia, il primo nel suo genere ad essere diffuso tramite la rete, ma fu anche il primo caso a suscitare un forte clamore mediatico. Questo attacco hacker venne chiamato "Morris worm" e prende il nome dal suo creatore e cioè uno studente statunitense Robert Tappan Morris. Il Morris worm può essere considerato una pietra miliare nella storia del cybercrimine. Sebbene nell'intenzione del suo creatore fosse solo uno strumento utile a misurare la vastità della rete Internet dell'epoca si trasformò in una vera e propria catastrofe. I risultati dell'esperimento furono ben diversi da quelli che Morris aveva previsto e le conseguenze provocarono notevoli danni economici. Morris decise di sviluppare un programma in grado di replicarsi e installarsi autonomamente su tutti i computer connessi alla rete con sistema operativo Unix. Questo worm sfruttava le vulnerabilità di sendmail, un server di posta elettronica, e di Finger, un protocollo Unix per lo scambio di informazioni. Il "worm" che tradotto significa "verme", veniva chiamato così per la capacità di insinuarsi nei sistemi in modo discreto, rubando poca memoria agli altri processi. Esso, inoltre, a differenza di altri virus non aveva bisogno di comandi esterni per eseguire le operazioni e propagarsi, ma era in grado di farlo autonomamente. Questo malware una volta entrato nel sistema crea diverse copie di sé. Usando le sue abilità informatiche Morris si collegò ad un computer del MIT così da far partire il suo virus da quel dispositivo. Il worm iniziò a propagarsi molto rapidamente anche per via della scarsa attenzione alla sicurezza da parte degli utenti a quei tempi. Il virus era progettato in modo che possa reinstallarsi anche su computer in cui è già presente, così da rendere molto più difficile la neutralizzazione. È proprio questo a portare ad una propagazione incontrollata del worm. Nell'arco di 24 ore il 10% della

[3] **ALWAREBYTES**, *Che cos'è il malware?* https://www.malwarebytes.com/it/malware?srsltid=AfmBOoo0aaUwVWS44pjZUL3ERrLSrdmZ9ILsK4l35ZJk7_8HV3POB4F7

rete, ovvero circa 6.000 dispositivi risultato infetti. È una telefonata anonima al New York Times a rivelare l'accaduto alla stampa che diffonde la notizia in prima pagina dando ampio risalto. Per la prima volta un attacco informatico diventa una notizia talmente rilevante da rubare spazio persino alle elezioni presidenziali di quel tempo. Successivamente il governo degli Stati Uniti istituì il CERT (Computer Emergency Response Team), una squadra di esperti informatici che avevano lo scopo di evitare il ripetersi di simili eventi. La creazione di questi gruppi da parte delle autorità e del mondo accademico rappresentano il muoversi dei primi passi all'insegna dello sviluppo di quella che verrà chiamata cybersecurity o sicurezza informatica. La cybersecurity "(anche detta cyber sicurezza o sicurezza informatica) consiste nell'insieme di tecnologie, processi e misure di protezione progettate per ridurre il rischio di attacchi informatici[4]". Infatti, in un mondo sempre più connesso e sempre più soggetto a vari cambiamenti, la cybersecurity non nasce come un campo statico, ma piuttosto in continua evoluzione, che si adatta costantemente ai nuovi sviluppi tecnologici e soprattutto alle mutevoli minacce informatiche. Esistono differenti categorie di sicurezza informatica, ognuna mirata a gestire minacce e vulnerabilità specifiche come ad esempio: *la sicurezza della rete* che salvaguarda l'integrità, la riservatezza e la disponibilità delle reti informatiche, prevenendo accessi non autorizzati, attacchi e irregolarità; inoltre, abbiamo la *sicurezza delle informazioni* che riguarda quello che oggi abbiamo a che fare ogni giorno e cioè i dati, infatti questa sicurezza riguarda proprio la salvaguardia di tutti i dati, assicurandone la loro riservatezza, l'integrità e prevenendo accessi non autorizzati, furti o alterazioni. Dopodiché abbiamo la *sicurezza degli endpoint* che punta ad assicurare la sicurezza di cosiddetti endpoint e cioè "qualsiasi dispositivo che possa connettersi a Internet, sia fisicamente che in cloud[5]" come i dispositivi mobili e portatili, contro attacchi, malware e accessi non autorizzati. Esiste inoltre, un'altra tipologia di sicurezza è la *sicurezza cloud.* I sistemi basati sul cloud consistono "nella fornitura di servizi di computing, quali software, database, server e reti, tramite connessione Internet. Ciò significa che gli utenti finali sono in grado di accedere a software e applicazioni ovunque si trovino[6]". Questa tipologia di sicurezza si assicura che anche quei dati raccolti o trattati nel cloud siano protetti da attacchi informatici e furti. Un'altra tipologia di sicurezza guarda la *sicurezza delle applicazioni* che si assicura di difendere le applicazioni software dalle vulnerabilità che potrebbero essere sfruttate da hacker, assicurando il loro corretto funzionamento in modo sicuro. Inoltre, la cybersecurity si impegna a proteggere tutte le informazioni sensibili. Il rischio che un hacker possa ottenere accesso a dati personali, causando danni irreparabili agli utenti, rappresenta un motivo

[4] **IT GOVERANCE**, *Cos'è la cyber security?*, https://www.itgovernance.eu/it-it/what-is-cyber-security-it

[5] **SERVICEMATICA**, *Endpoint: cosa sono e perché sono fondamentali per la sicurezza informatica*, 2020, https://servicematica.com/endpoint-cosa-sono-e-perche-sono-fondamentali-per-la-sicurezza-informatica/

[6] **SALESFORCE**, *Che cos'è il cloud computing?*, https://www.salesforce.com/it/learning-centre/tech/cloudcomputing/

cruciale per cui la cybersecurity assicura che solo le persone autorizzate possano accedere a risorse specifiche. Questo obiettivo viene perseguito attraverso l'implementazione di strumenti come l'autenticazione a più fattori. Insomma, la cybersecurity tende a salvaguardare la sicurezza di tutti gli utenti che ogni giorno sono collegati a Internet attraverso milioni di dispositivi definiti "più piccoli" come un device mobile. Infatti, gli utenti spesso credono erroneamente che i loro telefoni cellulari siano immuni agli attacchi informatici, sottovalutando i rischi a cui questi dispositivi sono esposti. Invece, ad oggi i nostri dispositivi mobili risultano essere diventati sempre di più bersaglio del cybercrimine. Ma pensiamo anche a tutte quelle imprese che a prescindere dalle loro dimensioni o dal suo settore sono esposte a minacce informatiche di ogni tipo. Per questo l'adozione e la diffusione di tecnologie digitali hanno sempre di più ampliato la cosiddetta *superficie di attacco*, ovvero l'insieme di punti di ingresso vulnerabili che possono essere sfruttati da attori malevoli per penetrare nei sistemi aziendali. La superficie di attacco detto anche *attack surface* si divide in tre categorie: superficie di attacco fisica, digitale, e di ingegneria sociale. *La superficie di attacco digitale* "espone potenzialmente il cloud e l'infrastruttura locale dell'organizzazione a qualsiasi hacker con una connessione internet[7]". Gli hacker solitamente sfruttano varie scorciatoie per condurre un attacco, tra cui: *password deboli* che fanno sì che aumentino significativamente il rischio che un hacker possa rubare la password e utilizzarla per violare l'account; *vulnerabilità di software, sistema operativo e firmware* che riguardano la vulnerabilità derivanti da errori di codifica, sviluppo nelle applicazioni, software di sistema e firmware esterni. Questo permette agli hacker di infiltrarsi nel sistema e installare malware di ogni tipo. Inoltre, anche *applicazioni o dispositivi non aggiornati* generano vulnerabilità non sorvegliate che i cybercriminali possono facilmente sfruttare. Un altro punto di vulnerabilità possono essere gli *asset esposti a Internet* che possono essere uno strumento di attacco da parte di hacker attraverso un'interfaccia come API (Application Programming Interface) che riguarda "sono interfacce che permettono alle applicazioni di interagire con altre applicazioni[8]". Infine, sempre più imprese subiscono attacchi informatici a causa di utilizzo non consentito di applicazioni e strumenti tecnologici da parte dei dipendenti. Infatti, un altro punto debole esposto ad attacchi informatici è proprio il concetto di *Shadow IT.* Quando si parla di Shadow IT ci si riferisce "all'utilizzo di sistemi, applicazioni, dispositivi o servizi informatici senza l'approvazione del dipartimento IT di un'azienda o organizzazione[9]". Questi dispositivi, costituiscono uno dei vettori di attacco più rischiosi, poiché la loro attività non può essere controllata. La seconda categoria di

[7] **IBM**, *Che cos'è una superficie di attacco?*, https://www.ibm.com/it-it/topics/attack-surface

[8] **AZIONA**, *API cosa sono e come funzionano*, 2021, https://www.azionadigitale.com/api-cosa-sono-e-come-funzionano/

[9] **AXITEA SECUIRTY EVOLUTION**, *Cos'è lo Shadow IT: esempi di "IT ombra, rischi e soluzioni*, https://www.axitea.com/it/blog/cos-e-lo-shadow-it-esempi-di-it-ombra-rischi-e-soluzioni/

superficie d'attacco riguarda quella *fisica* che comprende tutti quei dispositivi a cui è consentito l'accesso che sono presenti fisicamente come ad esempio computer, dispositivi mobili etc. I principali canali di attacco in questo caso sono: *l'adescamento* dove l'hacker, come dice il nome stesso, adesca gli utenti lasciando dispositivi con, ad esempio, chiavette USB infette da malware. Questo potrebbe comportare un inconsapevole rischio da parte degli utenti che si ritrovano a diffondere inconsapevolmente un virus nell'intero sistema. Un altro punto di debolezza potrebbe essere un *utente interno malintenzionato* che potrebbe fornire una chiave di accesso a criminali informatici e permettere loro di rubare informazioni riservate, disattivare i dispositivi e installare software dannosi. Infine, la *sottrazione di dispositivi* che comporta un accesso completo da parte del cybercrime sia ai dati in esso memorizzati che ai database cloud e alle risorse di rete correlate. Un uso incustodito di dispositivi aziendali costituisce dei rischi pericolosi per l'azienda stessa. L'ultima categoria di superficie di attacco riguarda quella *social engineering* che punta a colpire la parte psicologica degli individui più debole. Queste pratiche di manipolazione viene chiamata anche "hacking umano", perché si cerca di persuadere gli utenti a adempiere a delle richieste, puntando ad ottenere l'accesso ad informazioni riservate con all'inganno ma soprattutto attraverso tecniche di manipolazione psicologica. Il *phishing* è il metodo di attacco di ingegneria sociale più conosciuto e attuale. Un attacco phishing "Il suo nome deriva dal verbo inglese "to fish", pescare. Questa tecnica di truffa ricorda l'atto della pesca in quanto l'attaccante lancia un amo, in attesa che la vittima "abbocchi", attraverso ad esempio strumenti come e-mail e messaggi di testo da account che sembrano apparentemente affidabili[10]". Infatti, gli hacker si spacciano per personale facenti parte di un'azienda affidabile, ad esempio, spacciandosi per un funzionario bancario; oppure fingendo di essere persone che la vittima conosce personalmente, come un parente o un amico. Pensiamo quante volte ci ritroviamo di fronte a delle richieste di accesso tramite link, non sapendo che un semplice click può permettere a dei criminali informatici di accedere ai nostri dati personali, e tutto questo puntando alla nostra vulnerabilità e non ai nostri dispositivi. Analizzare in modo accurato questa superficie di attacco è cruciale per comprendere dove e come un'azienda potrebbe essere vulnerabile. Solo con una chiara visione dei vettori di minaccia, ossia i canali attraverso i quali un attacco può essere portato a termine, si possono sviluppare strategie efficaci di mitigazione del rischio. Ma non solo, gli attacchi informatici possono creare forti disagi anche alle cosiddette infrastrutture critiche. Per infrastrutture critiche si intende "un elemento, un sistema o parte di questo che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo a causa

[10] **IT IMPRESA SOLUZIONI INFROMATICHE**, *Phishing: cos'è e come prevenirlo*, 2023, https://www.it-impresa.it/blog/phishing-attack/

dell'impossibilità di mantenere tali funzioni[11]". I rischi che corrono le infrastrutture critiche possono creare delle conseguenze enormi sulla società, influenzando gli elementi essenziali come il benessere fisico, la salvaguardia e la stabilità economica e sociale della popolazione. Alla luce di queste evoluzioni, la cybersecurity è passata dall'essere una necessità principalmente per scopi militari a diventare una priorità imprescindibile in ogni settore della società contemporanea. Con l'aumento esponenziale delle minacce, la protezione dei dati sensibili, la salvaguardia della privacy e la prevenzione degli attacchi informatici sono diventati elementi cruciali per garantire la sicurezza delle reti, delle aziende e degli utenti.

2. L'IMPORTANZA DI INVESTIRE NELLA CYBERSECURITY

Nell'attuale era digitale, la cybersecurity è diventata una priorità fondamentale per individui, aziende e governi. L'incremento di attacchi informatici, sempre più sofisticati, richiede un impegno costante da parte dei professionisti del settore per fronteggiare minacce in continua evoluzione. Gli hacker sono in costante ricerca di nuove vulnerabilità da sfruttare e di metodi innovativi per aggirare le misure di sicurezza esistenti. Di conseguenza, chi si occupa di cybersecurity è costretto a rimanere al passo con i pericoli emergenti, cercando ogni giorno di anticipare le mosse di questi individui senza scrupoli, che mirano a sabotare interi sistemi. Tuttavia, l'evoluzione delle tecnologie e l'introduzione di soluzioni di protezione sempre più avanzate hanno generato anche nuove vulnerabilità. Oltre a colpire singoli utenti e aziende, la criminalità informatica ha esteso i suoi obiettivi, arrivando a minacciare intere nazioni. Si inizia a parlare di *cyberterrorismo*, per indicare il terrorismo che questi criminali intendono diffondere attraverso la rete con l'obiettivo di compromettere l'ordine e la sicurezza pubblica. Il cyberterrorismo si manifesta in due modi: attraverso la propaganda e attraverso l'azione diretta. La propaganda viene utilizzata dagli hacker per attirare gli utenti attraverso dei messaggi che possano raggiungere più utenti possibili, utilizzando tutti i mezzi di comunicazione possibili. La sicurezza pubblica riguarda attacchi che hanno l'obiettivo intaccare ad esempio infrastrutture critiche per poter mettere in subbuglio un intero paese e accaparrarsi dati sensibili. Tutto ciò comporta ripercussioni sempre più gravi che paesi e imprese si ritrovano ad affrontare, e che mettono in evidenza l'importanza di strategie operative dettagliate e di un monitoraggio continuo degli investimenti nell'ambito della cybersecurity. Le aziende detengono grandi quantità di dati a trovarsi a fronteggiare attacchi informatici di notevole entità. Tuttavia, il problema non si limita a loro, ma coinvolge l'intero contesto economico, impattando anche fornitori, clienti e istituti bancari.

[11] **ICT SECURITY**, *Infrastrutture Critiche, cosa sono e come proteggerle*, 2016, https://www.ictsecuritymagazine.com/articoli/infrastrutture-critiche/

Gli attacchi informatici possono comportare costi estremamente elevati: oltre alle spese per la riparazione dei danni e il recupero dei dati, le imprese devono far fronte al calo di produttività, al danno d'immagine e alle possibili ripercussioni legali. L'importanza di investire nello studio e nello sviluppo della cybersecurity spinge le imprese a destinare sempre più risorse al miglioramento della sicurezza informatica, affinché le nuove soluzioni digitali garantiscano i più elevati livelli di protezione. Inoltre, investire nella cybersecurity porta ad un implemento maggiore dei processi aziendali, migliorando quella che è la resistenza dell'impresa e diminuendo le interruzioni causate da attacchi hacker. L'Italia ha avviato diverse iniziative per tutelare la sicurezza informatica. Tra queste spicca il Perimetro di Sicurezza Cibernetica, introdotto nel 2019, con l'obiettivo di garantire un elevato livello di protezione per le reti, i sistemi informativi e i servizi digitali delle amministrazioni pubbliche, degli enti e degli operatori sia pubblici che privati. Questa normativa è volta a prevenire e contrastare possibili attacchi informatici, che potrebbero interrompere operazioni e servizi, compromettendo la sicurezza nazionale. Proprio nel contesto italiano, dominato da PMI con specifiche caratteristiche in termini di dimensioni, processi operativi e settori economici, la sicurezza informatica rappresenta una sfida crescente. Un recente sondaggio condotto da SWG per Confesercenti, focalizzato sulle PMI, ha rivelato che "una PMI su quattro (26%) è stata colpita da problemi relativi alla sicurezza informatica e il 52% destinerà nell'anno in corso risorse per la messa in sicurezza dei propri dati, per un investimento complessivo di quasi 470 milioni di euro[12]". Pertanto, le PMI devono puntare su strategie specifiche, personalizzate in base alle esigenze di ciascun caso. È fondamentale investire nella sicurezza ponendo particolare enfasi sulla formazione e sulla crescita professionale del personale interno. Questo richiede un'attenzione maggiore all'atteggiamento generale all'interno dell'organizzazione, poiché anche un piccolo comportamento inappropriato può compromettere l'intero sistema, aumentando il rischio di intrusioni da parte di hacker e cybercriminali. In aggiunta, uno strumento essenziale per proteggere le informazioni e i dati personali di un'organizzazione è il *backup*. Questo processo prevede la creazione di copie di sicurezza delle informazioni digitali, che vengono conservate in posizioni distinte rispetto ai dati originali. In questo modo, le copie fungono da rete di protezione in caso di perdita o danneggiamento delle informazioni cruciali. Tuttavia, limitarsi a creare copie dei dati non è sufficiente; è necessario anche assicurarsi che le procedure di recupero, analogamente al backup, siano realmente efficaci e che i dati possano essere recuperati con successo quando necessario. Investire nella cybersecurity rafforza la credibilità di un'azienda agli occhi di finanziatori, soci e clienti. Ogni organizzazione deve garantire che i dati siano

[12] **CONFESERCENTI**, *Sicurezza informatica: Confesercenti-SWG, un'impresa su quattro colpita, il 52% potenzierà sistemi di difesa nel 2023*, 2023, https://www.confesercenti.it/blog/sicurezza-informatica-confesercenti-swg-unimpresa-su-quattro-colpita-il-52-potenziera-sistemi-di-difesa-nel-2023/

sempre protetti e intatti. Tra i vantaggi di investire nella cybersecurity, vi è la possibilità di ottenere un vantaggio competitivo rispetto a chi non adotta adeguate misure di sicurezza e quindi rimane più vulnerabile e a rischio. Un ulteriore beneficio è la tranquillità offerta ai clienti, assicurando loro che i propri dati non saranno utilizzati in modo improprio. Inoltre, le organizzazioni puntano ad investire nella cybersecurity proprio per evitare quelli che sono le interruzioni e i ritardi nelle proprie attività lavorative. Quando un'azienda affronta il blocco di un sistema a causa di un attacco hacker, si trova di fronte a una vera e propria paralisi operativa. Anche se il sistema non si arresta completamente, subisce comunque un significativo rallentamento delle attività. Questo comporta anche una breve interruzione che può tradursi in rilevanti perdite economiche e compromettere l'efficienza dell'intera organizzazione. Rallentamenti e blocchi possono infatti abbassare la produttività, portando non solo a una riduzione dei guadagni, ma anche a un calo della soddisfazione dei clienti. Un rapporto Clusit (Associazione Italiana per la Sicurezza Informatica) del 2023 evidenzia come il settore sanitario in Italia sia il settore più colpito nel 2023 da parte della criminalità informatica. Il rapporto dichiara che "gli attacchi sferrati alla sanità sono stati il 17% sul totale, da gennaio a marzo 2023, contro il 12% del 2022[13]". Questo comporta un grave danno non solo di carattere economico o di privacy, ma comportano dei grossi danni sulla salute delle persone. Un esempio di attacco fu quello avvenuto alle strutture ospedaliere che fece tremare l'opinione pubblica e non solo avvenuta il 23 novembre del 2023, quando al Mountainside Medical Center di Montclair ci fu una vera e propria interruzione di rete. La società sanitaria non ha potuto confermare se i dati dei pazienti siano stati compromessi, ma ha agito rapidamente, chiudendo la rete e adottando misure per proteggere le informazioni e i dati sensibili dei pazienti. Anche il sistema sanitario italiano è stato colpito da un grave attacco informatico, che ha coinvolto l'Azienda Socio-Sanitaria Territoriale Fatebenefratelli Sacco di Milano. I dati sensibili dell'ospedale, insieme a informazioni personali dei pazienti, sono stati esposti pubblicamente, causando notevoli disagi. L'attacco ha generato una serie di malfunzionamenti nei sistemi di gestione del pronto soccorso e ha compromesso le normali attività ospedaliere. Milano, tuttavia, non è un caso isolato: anche le ASL di Roma, Savona, Terni e altre hanno subito attacchi hacker, soprattutto attacchi chiamati *ransomware* che sfruttano la crittografia dei dati essenziali e richiedono un riscatto per sbloccarli e ripristinarne l'accesso rapidamente. Questo dimostra che il settore sanitario è particolarmente vulnerabile sul fronte della sicurezza informatica. Da un lato, molte delle tecnologie utilizzate negli ospedali sono obsolete e insufficienti in termini di sicurezza dei dati. Dall'altro, la crescente digitalizzazione della sanità, sebbene offra vantaggi significativi, introduce

[13] **BOOLEBOX**, *Cybersecurity e sanità: minacce, rischi e possibili soluzioni per un settore sempre più nel mirino degli hacker*, 2023, https://www.boolebox.com/it/cybersecurity-in-sanita-minacce-e-difese-possibili/#:~:text=Il%20settore%20sanitario%20%C3%A8%20stato,contro%20il%2012%25%20del%202022.

nuovi rischi e minacce, poiché i sistemi tecnologici integrati possono essere attaccati da più angolazioni. Questo scenario evidenzia l'urgenza di investire nella cybersecurity da parte della società sanitaria italiana, poiché interruzioni prolungate non solo minacciano la privacy dei pazienti, ma possono anche mettere a rischio la loro vita. Tutto ciò ha spinto l'Italia a elaborare una strategia per gestire in modo efficace gli attacchi ai sistemi informatici. Innanzitutto, fronteggiando l'aumento degli attacchi, tenendo conto del grande dispendio di energie e risorse necessarie che comporta contrastarli e prevenirli. Successivamente, attuare azioni che siano allineate agli interessi nazionali, garantendo sempre la protezione delle infrastrutture digitali. Questo può essere realizzato solo attraverso una collaborazione stretta con le istituzioni degli altri Stati, per garantire coesione su un tema cruciale come la cybersecurity. A tale riguardo nel febbraio 2020 i membri *dell'Euro Cyber Resilience Board* (ECRB) hanno avviato un'iniziativa nota come *Cyber Information and Intelligence Sharing Initiative*, volta a diffondere informazioni riguardo quelle che possono essere le minacce informatiche, contribuendo così a proteggere i risparmi dei cittadini europei dagli attacchi dei criminali cibernetici. Gli obiettivi di quest'iniziativa riguardano "la protezione del sistema finanziario attraverso un meccanismo di prevenzione, la rilevazione e la risposta agli attacchi informatici ed infine l'incoraggiamento alla condivisione delle informazioni strategiche, operative e tattiche attraverso una piattaforma automatizzata[14]". La Commissione ha poi pubblicato in seguito una modifica del programma sulla cybersecurity puntando principalmente al monitoraggio e alla condivisione delle minacce cibernetiche, all'implementazione della normativa dell'UE in ambito di sicurezza informatica, alla preparazione per far fronte a emergenze causate da attacchi informatici e alla collaborazione reciproca tra Stati, fornendo anche sostegno ai centri nazionali di coordinamento. La cybersecurity nella società odierna si conferma come uno dei settori strategici con prospettive di crescita durature, spinto dalla continua espansione dei servizi digitali e dall'aumento delle minacce informatiche. La costante evoluzione degli attacchi richiede alle aziende specializzate nello sviluppo di soluzioni di difesa di innovare continuamente, offrendo tecnologie avanzate di rilevamento e protezione. Questo crea una domanda crescente da parte di imprese e istituzioni che, per salvaguardare le proprie infrastrutture e dati, devono investire in modo continuo in sistemi di sicurezza sempre più sofisticati. Le organizzazioni devono adattare la loro struttura operativa al contesto della cybersecurity, trovando un equilibrio tra l'impiego di professionisti esterni, con accesso a piattaforme avanzate e il rafforzamento delle competenze interne nella gestione e nel monitoraggio della sicurezza e dell'adattabilità tecnologica. In passato, questi aspetti venivano spesso trascurati o delegati in modo eccessivo a risorse esterne. Tuttavia, è essenziale che le aziende oggi investano nello

[14] **AZZELLINI G**, *Informazioni cyber e iniziativa di condivisione dell'intelligence (CIISI-UE)*, 2023, https://www.antiriciclaggiocompliance.it/informazioni-cyber-e-iniziativa-di-condivisione-dellintelligence-ciisi-ue/

sviluppo di un solido know-how interno per affrontare le sfide della cybersecurity in modo efficace e autonomo. Infine, possiamo affermare che una profonda consapevolezza su come attenuare l'impatto delle interruzioni, un'attenta analisi delle vulnerabilità in ambito cybersecurity e lo sviluppo della resilienza sono elementi chiave che consentiranno alle organizzazioni di affrontare i rischi dovuti agli attacchi informatici. Per questo, investire in queste aree non solo favorisce un recupero tempestivo, ma permette anche di affrontare future minacce da una posizione di forza, garantendo una solida preparazione per eventuali eventi avversi.

3. CONTESTO STORICO ED EVOLUZIONE DELLE MINACCE INFORMATICHE

Le minacce informatiche sono diventate una realtà inevitabile nella vita quotidiana, colpendo non solo i cittadini privati, ma anche aziende, enti e pubbliche amministrazioni. L'incremento dell'uso di Internet per lavoro, studio e intrattenimento ha spinto i cybercriminali a creare una gamma sempre più sofisticata di attacchi. Anche i *malware*, nel tempo, si sono evoluti: alcuni mirano a sfruttare vulnerabilità temporanee, mentre altri sono stati progettati per colpire debolezze strutturali nei sistemi informatici, ancora irrisolte, che continuano a rappresentare un punto di accesso per gli attacchi dei criminali informatici. Oltre al già citato Creeper, negli anni '80, con l'aumento delle vendite di dispositivi informatici e il progresso delle competenze tecnologiche, nacque *Elk Cloner*, il primo virus per computer. Creato nel 1982 da Rick Skrenta, all'epoca quindicenne, Elk Cloner era progettato per il sistema operativo Apple II e si diffondeva tramite floppy disk. Infatti, questo virus "si diffuse infettando il sistema operativo Apple DOS 3.3 utilizzando una tecnica ora nota come virus del settore di boot[15]". All'epoca, i floppy disk erano ampiamente utilizzati nelle organizzazioni, favorendo la rapida diffusione del virus tra i diversi sistemi. Nel 1983, Fred Cohen sviluppò il primo programma capace di infettare altri software e prendere il controllo completo di un computer in brevissimo tempo. A lui si deve infatti, il primo utilizzo del termine "virus", coniato dal matematico Leonard Adleman. Un altro virus trasmesso tramite floppy disk è stato il *Brain*, un virus informatico di massa creato nel 1986 da due fratelli pakistani, Amjad Farooq Alvi e Basit Farooq Alvi. Le motivazioni dietro la creazione di questo virus rimangono ancora sconosciute. Alcuni ipotizzano che fosse un sistema di protezione anticopia ideato dai fratelli per difendere il loro software, mentre altri ritengono che fosse concepito per "punire" gli Americani, accusati di una pratica "immorale" come la copia illegale di

[15] **RHC**, "*Elk Cloner. Il primo virus informatico della storia*", 2021, https://www.redhotcyber.com/post/dagli-scherzi-agli-apt/

software. Pochi anni dopo ci fu la creazione di un virus che avrebbe distrutto tutti i dati presenti nei vari dispositivi informatici. Questo virus chiamato *Lehigh,* attaccava il file di sistema command.com. Già in quegli anni gli utenti cominciarono ad essere più scrupolosi in termini di sicurezza informatica monitorando la dimensione del file, perché questo sarebbe stato sintomo di un potenziale attacco. Nel 1987 si inizia a parlare di un particolare tipo di virus: i *virus polimorfi.* La caratteristica di essi è che danneggiano i dati compromettendo l'efficienza del sistema innescando anomalie nel sistema informatico, come ad esempio errori di schermata blu. Questi errori, chiamati anche *Blue Screen of Death*, comportano l'arresto delle operazioni mostrando infatti una schermata blu che obbliga gli utenti a riavviare il sistema. Questi virus necessitano di programmi host e sono proprio questi file host che vengono intaccati dal virus o vengono direttamente sostituito con versione infetta. Uno dei più famosi virus polimorfi è il virus *Vienna*. Esso individua i file con estensione .com e ne elimina alcuni nel tentativo di infettarli. Nel 1995 iniziano a diffondersi i primi virus macro che tendono a intaccare documenti e altri file di dati. Uno dei macro-virus era chiamato *Concept* che andava a colpire maggiormente i documenti Word. Sono difficili da scovare perché non funzionano subito se non avviene prima una macro-infetta, da cui danno il via per eseguire una sequenza di comandi. Alla fine degli anni 90 nacquero un altro tipo di malware chiamato *virus di Chernobyl o CIH*. Questo virus è stato creato per distruggere tutti i dati presenti nel computer infettato. Il CIH parte da un file per propagarsi in tutto il dispositivo. È chiamato anche "virus Chernobyl" perché si attiva il giorno della data della catastrofe nucleare avvenuta il 26 aprile 1986. Con la diffusione di Internet nella società odierna la diffusione dei malware non avviene più attraverso floppy disk, ma bensì attraverso e-mail. Infatti, nel 1999 David Lee Smith programmatore di AT&AT, un'azienda statunitense, creò un virus chiamato Melissa. Questo virus venne chiamato con questo nome in riferimento ad una spogliarellista di Miami. Il *virus Melissa* forniva delle password per accedere gratuitamente a siti che fornivano materiale pornografico. Tutto questo avveniva attraverso documenti Word e una volta fatto accesso a queste pagine il virus si espandeva su tutto il dispositivo. Attraverso Outlook, il servizio di posta elettronica, il virus si diffondeva proprio attraverso e-mail che invitava l'utente ad accedere a questi documenti. Un altro virus che si diffuse via e-mail nello stesso anno fu *Happy99*. Questo worm si presentava come allegato in un'e-mail sotto forma di un file chiamato HAPPY99.EXE. Una volta che il dispositivo veniva infettato, il virus si replicava, consentendo l'invio di copie di sé stesso a tutti i destinatari delle e-mail originate dal sistema compromesso. Negli anni 2000 si assistette a un'evoluzione costante dei malware, come nel caso del virus *I Love You*. Questo virus, mascherato da un messaggio che poteva sembrare una dichiarazione d'amore, era in realtà un potente programma dannoso in grado di causare seri danni al sistema, replicandosi e inviando copie di sé stesso a tutti i contatti della rubrica. Nel 2004 la società si ritrovò ad affrontare un virus denominato *SQL Slammer*

che paralizzò la maggior parte delle reti a livello globale mandando in tilt interi sistemi. Il virus Slammer tentava di connettersi alle varie reti in modo da poter scovare le vulnerabilità. Esso appena individuava un server SQL debole si propagava creando sempre copie infette di sé stesso. Sempre in quell'anno cominciò a diffondersi un worm denominato *MyDoom* che fu il primo malware a diffondersi in maniera così repentina sulle reti. Questo malware poteva diffondersi in due modalità: tramite e-mail o sfruttando la rete Kazaa. Nel primo caso, il virus si propagava infettando un dispositivo e poi inviandosi automaticamente agli altri contatti. Nel secondo, individuava la cartella dei file condivisi su Kazaa e da lì si diffondeva rapidamente ad altri computer nella rete. Nel 2007 si iniziò a parlare di un altro malware: i trojan. I trojan sono un tipo di categoria di malware che si nascondono all'interno di programmi o cercano di ingannare gli utenti spingendoli a scaricarli sui propri dispositivi. Infatti, i malware denominati "cavallo di troia" "fingono di essere qualcos'altro, come una versione gratuita di un software importante. Una volta che la vittima scarica ed esegue il trojan sul proprio computer, questo esegue la sua funzionalità dannosa[16]". In questo caso, il trojan era lo Storm Worm, responsabile della creazione di una delle più grandi reti di computer zombie. Un dispositivo viene definito "computer zombie" quando è compromesso da un hacker o infettato da un virus, con l'obiettivo di utilizzarlo per attaccare siti web o inviare e-mail indesiderate. Nel 2010 con l'arrivo di un altro virus informatico chiamato *Stuxnet* si inizia a parlare di guerra cibernetica. Questo virus era stato progettando per fermare la diffusione delle armi nucleari, ma il suo effetto fu completamente opposto: ci fu una vera e propria diffusione delle tecnologie legate alle armi cibernetiche. Proprio in quell'anno le centrifughe utilizzate per l'uranio nella centrale di Natanz in Iran, iniziarono a non rispondere ai comandi funzionando in maniera incontrollata. Questo incidente portò al danneggiamento di tantissime centrifughe provocando vari ritardi nel corso del programma iraniano. Il malware *Stuxnet* era riuscito ad entrare nella centrale di Natanz attraverso una chiavetta USB inserita all'interno dei computer, compromettendo l'intero software della centrale e modificandone il codice. Questo virus non si fermò alla centrale iraniana, ma si diffuse anche fuori. Inoltre, in quello stesso anno un altro malware cominciò a colpire non solo il sistema iraniano ma bensì tutto il Medio Oriente con l'intento di avere accesso alle informazioni private. Infatti, l'obiettivo di questo virus non era quello di creare danni ai sistemi, ma bensì quello di reperire più informazioni possibili e trasmetterli al proprio server. Si inizia a parlare di *cyber-spionaggio*, la tecnica con cui "un utente non autorizzato acquisisce dati classificati[17]". Nel caso del malware trojan, esistono varianti strettamente legate chiamate *RAT (Remote Access Trojan).* Questi consentono agli

[16] **CHECK POINT**, "*Tipi di minacce alla sicurezza informatica*", https://www.checkpoint.com/it/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

[17] **CNS TECH**, "*Cyber-spionaggio: cos'è, e come prevenirlo?*", 2021, https://www.cnsspa.it/cyber-spionaggio-cose-e-come-prevenirlo/

hacker di prendere il controllo anche a distanza di un computer infetto, eseguendo qualsiasi azione senza che l'utente ne sia consapevole. Inoltre, l'hacker può installare ulteriori funzionalità per estendere ulteriormente il controllo sul sistema, sempre all'insaputa dell'utente. Un altro tipo di categoria di malware sono i *ransomware* "che bloccano l'accesso a un computer cifrando i dati in esso contenuti, con l'obiettivo di ottenere un riscatto dalla vittima, per poter accedere nuovamente ai propri dati[18]". Un caso tipico di ransomware che si manifestò nel 2012 fu il *Reveton,* noto anche come "il ransomware della polizia di Reveton". Questo ransomware si presentava alle vittime come un avviso ufficiale, apparentemente emanato dalle forze dell'ordine, che intimava il pagamento di una sanzione per evitare il rischio di avere ripercussioni come ad esempio la reclusione. Questa situazione ha generato terrore e confusione tra gli utenti, poiché la notifica era così credibile da far sembrare autentico l'avviso della polizia, spingendo molti a pagare senza verificare la sua attendibilità. Con il passare del tempo iniziarono a crearsi nuovi ransomware sempre più pericolosi e sempre più specializzati a colpire in maniera accurata i diversi sistemi. Un esempio emblematico di software virus è il ransomware *Cryptoloker.* Questo malware crittografa il contenuto del disco rigido su cui è installato il sistema operativo, bloccando l'accesso e il corretto funzionamento del sistema. L'attacco si diffonde tramite e-mail che si riferiscono a un acquisto effettuato dall'utente in precedenza. Queste e-mail includono un documento, come una ricevuta, che contiene un file dannoso che si installa automaticamente se si tenta di aprirlo. Un'altra categoria di malware è il *Cryptojacking.* Questo tipo di attacco online si infiltra nei dispositivi per sfruttarne le risorse al fine di generare criptovalute, una forma di valuta digitale. Tali attacchi si basano sull'algoritmo Proof of Work dove si richiedeva ai "minatori" di impiegare una notevole quantità di potenza di calcolo per risolvere un problema matematico complesso, con l'obiettivo di prevenire frodi all'interno del sistema. Inoltre, tra le diverse categorie di malware si annovera lo *Spyware*. Questo tipo di malware ha l'obiettivo di infiltrarsi nei computer per acquisire dati personali degli utenti. La sua efficacia dipende dall'utilizzo che viene fatto di tali informazioni: possono essere impiegati dalle forze dell'ordine oppure sfruttati per ottenere dati sensibili, compromettendo la sicurezza di intere organizzazioni. Un esempio tipico di spyware è il *monitoraggio dei cookie*, che consente di tracciare gli utenti su Internet e di conoscere i loro interessi attraverso le loro attività online. I cookie, infatti, servono a conservare e recuperare le informazioni relative all'utente, facilitando così il rilevamento e l'analisi dei comportamenti degli utenti stessi. Questo tipo di monitoraggio diventa particolarmente rilevante nella società attuale, in cui milioni di organizzazioni svolgono gran parte delle loro operazioni nel mondo digitale, gestendo le proprie attività tramite internet. Proprio perché queste attività sono incentrate maggiormente online un loro

[18] **PROOFPOINT**, *Cos'è un ransomware?*, https://www.proofpoint.com/it/threat-reference/ransomware

arresto porterebbe a grosse perdite. Tali interruzioni sono spesso provocate da attacchi definiti *DDoS (Distributed Denial-of-Service)*. Questo attacco veniva sferrato dagli hacker sfruttando quelli che erano i "botnet". Le botnet erano dei malware che permettevano ai criminali di sferrare attacchi ai dispositivi vulnerabili. La loro pericolosità risiedeva proprio nella loro capacità di bloccare e mettere fuori gioco servizi prestazioni che sono fondamentali per gli utenti. Nel caso dei degli attacchi DDoS, le botnet venivano utilizzati per poter avere un numero sempre maggiore di dispositivi infetti e poter scagliare un attacco di questo tipo. Nel caso dell'attacco DDoS avvenuto nel 2018 al servizio GitHub, un servizio di hosting, non vennero utilizzato le botnet ma bensì un sistema di cache come memcached. Questo sistema aveva lo scopo di "ridurre, sostanzialmente azzerandoli, i tempi di accesso al database contestualmente all'utilizzo di applicazioni web dinamiche che fanno uso di banche di dati[19]". Gli attacchi puntarono a manipolare l'indirizzo IP di questa piattaforma e incrementare il suo volume di traffico. Insomma, i danni avrebbero potuto essere disastrosi se non fosse stato per le precauzioni prese dal GitHub per contrastare attacchi di questi tipi. Ad oggi, la situazione delle minacce informatiche è diventato motivo di numerose ricerche statistiche, che hanno fatto sì che le diverse agenzie che si occupano di cybersecurity siano sempre aggiornate sulla situazione delle minacce informatiche nel panorama odierno. Proprio l'agenzia dell'Unione Europea per la sicurezza informatica (ENISA) che "contribuisce alla politica informatica dell'UE accrescendo la fiducia nei prodotti, nei servizi e nei processi digitali elaborandone sistemi di certificazione della cibersicurezza e coopera con i paesi e gli organismi dell'UE contribuendo a prepararsi alle future sfide informatiche[20]", si è occupata di redigere una relazione sulla situazione attuale delle minacce informatiche nella società odierna. Per questo motivo, ENISA ha pubblicato l'ENISA Threat Landscape 2022 (ETL) con l'obiettivo di fornire una panoramica completa delle principali minacce informatiche che colpiscono le società moderne e di identificare gli attori responsabili che mettono a rischio la cybersecurity, insieme alle conseguenze che ne derivano. Il report evidenzia come il 2022 sia segnato da una crescente complessità e da un numero in costante aumento di minacce informatiche. Una delle maggiori preoccupazioni riguarda la sempre maggiore specializzazione di questi attacchi, che dimostrano una conoscenza precisa su come e dove colpire. Inoltre, i loro obiettivi non si limitano più a piccole organizzazioni o individui, ma mirano a scopi economici e strategici di rilevanza internazionale. Le minacce ransomware rappresentano un problema critico, poiché continuano a colpire duramente le organizzazioni, costringendole a proteggersi adottando strategie

[19] **IONOS DIGITAL GUIDE**, *Memcached in breve: funzione e utilizzo*, 2021, https://www.ionos.it/digitalguide/hosting/tecniche-hosting/che-cose-memcached/

[20] **UNIONE EUROPEA**, Agenzia *dell'Unione europea per la cibersicurezza (ENISA)*, 2004, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_it#:~:text=L'ENISA%20contribuisce%20alla%20politica,prepararsi%20alle%20future%20sfide%20informatiche.

più efficaci. L'obiettivo non è solo quello di contrastare gli attacchi, ma anche di prevenirli, migliorando la capacità di risposta e resilienza a queste incursioni. Il malware aveva avuto un breve declino nel 2021 durante il periodo della pandemia, ma ad oggi sta diventando di nuovo una minaccia centrale. Il report mette in luce come il phishing e le sue varianti, parte delle tecniche di ingegneria sociale, abbiano un impatto significativo sulla vulnerabilità degli utenti, spesso ingannati per aggirare i sistemi di sicurezza informatica. Questo evidenzia l'importanza di accrescere la consapevolezza tra gli utenti, affinché siano meglio preparati a difendersi da attacchi mirati a sfruttare le loro debolezze. Inoltre, i dati continuano a essere un bersaglio primario degli attacchi informatici, con lo scopo non solo di sottrarre informazioni sensibili, ma anche di manipolarle secondo gli interessi degli hacker. In particolare, la crescente diffusione dell'Internet of Things (IoT) e delle reti mobili offre ai cybercriminali nuove superfici di attacco, come evidenziato dal più grande attacco DDoS mai registrato in Europa nel 2022. Si tratta dell'attacco del 21 luglio 2022 dove Akamai, "un'azienda specializzata nei servizi di content delivery network (CDN) e sicurezza informatica[21]", è riuscita a contrastare sulla piattaforma Prolexic il più grande attacco DDos mai registrato prima. Inoltre, un fenomeno particolarmente preoccupante è la crescente diffusione della disinformazione e della misinformation, che non solo viene generata su vasta scala, ma è ormai commercializzata come un vero e proprio servizio, noto come *Disinformation-as-a-Service*, dove professionisti vengono proprio remunerati per creare fake news e distorcere le informazioni. L'uso dell'intelligenza artificiale amplifica ulteriormente questo fenomeno, poiché questa tecnologia facilita la creazione di notizie false e ne rende più agevole la diffusione, permettendo di raggiungere con precisione un pubblico mirato. Infine, il report evidenzia un altro tipo di attacco che risulta essere un fenomeno sempre più in crescita, e cioè gli *attacchi alla supply chain*. Questo tipo di attacco "si verifica quando un criminale informatico accede alla rete di un'azienda tramite collaboratori terzi o attraverso la catena di fornitura (la supply chain, appunto)[22]". Attacchi di questo tipo provocano danni significativi, rendendo difficile non solo contrastarli ma anche rilevarli, a causa della loro complessità e capacità di eludere i sistemi di sicurezza. Inoltre, insieme agli attacchi alla supply-chain, un'altra fonte critica che permette ai cybercriminali di sferrare attacchi e colpire le varie infrastrutture è la vulnerabilità zero-day. Come indica il nome, questa tecnica sfrutta le vulnerabilità di un sistema informatico sconosciute ai suoi programmatori, permettendo ai cybercriminali di sfruttare tale debolezza per raggiungere i propri obiettivi. I risultati emersi da questo report dimostrano che la cybersecurity oggi

[21] **ICOS**, *Akamai*, https://www.icos.it/brand/akamai/

[22] KEEPER, *Che cos'è un attacco alla supply chain?*, https://www.keepersecurity.com/it_IT/threats/supply-chain-attack.html#:~:text=Un%20attacco%20alla%20supply%20chain%2C%20noto%20anche%20come%20attacco%20a,la%20supply%20chain%2C%20appunto

deve affrontare sfide estremamente complesse, che vanno ben oltre il semplice aspetto tecnologico, includendo anche la dimensione geopolitica e il contesto sociale in cui si muovono gli attacchi. Per far fronte a questo scenario, le raccomandazioni di ENISA si concentrano su alcune delle necessità di strategie di difesa articolate, tra cui: la gestione delle vulnerabilità, protezione della supply chain e rafforzamento della consapevolezza degli utenti. Tutto ciò ci deve portare a non sottovalutare l'influenza che le minacce informatiche hanno sulle nostre organizzazioni ma anche sui noi stessi. È essenziale, inoltre, analizzare attentamente i dati relativi ai rischi e identificare azioni adeguate ad affrontarli in modo efficace. Questo ci dimostra che adottare un approccio proattivo e strategico nella gestione delle minacce informatiche è fondamentale per garantire la sicurezza delle nostre organizzazioni e la protezione dei nostri dati personali. Solo attraverso un impegno collettivo e una costante vigilanza possiamo costruire un ambiente più resiliente, capace di affrontare le sfide del mondo digitale in continua evoluzione.

II. ANALISI DEI FONDAMENTI E DEI MODELLI DI SICUREZZA: CONFRONTO E APPLICAZIONI NELL'ANALISI DELLE MINACCE E DEI RISCHI

1. PRINCIPI FONDAMENTALI DELLA SICUREZZA INFORMATICA

Il costante progresso del mondo digitale impone alle organizzazioni di adeguarsi per proteggere i propri dati. La sicurezza delle informazioni è essenziale per evitare che vengano sfruttate da cybercriminali per scopi illeciti. Crescono i casi in cui i dati personali fuoriescono dalle organizzazioni a causa di minacce interne, che risultano essere sempre più frequenti. Pertanto, le aziende devono prestare grande attenzione anche alle violazioni interne all'organizzazione, adottando misure efficaci per garantire un controllo completo dei dati, considerando la crescente complessità nella loro gestione quotidiana. Le infrastrutture tecnologiche hanno subito cambiamenti profondi, diventando sempre più articolate. Questa complessità crescente le rende più vulnerabili agli attacchi informatici e sempre più difficili da gestire in modo efficace, aumentando le sfide legate alla loro protezione e controllo. Gli utenti sono sempre più consapevoli dell'importanza di proteggere la privacy dei propri dati personali, spesso condivisi con leggerezza online. Questo ha portato a una

maggiore attenzione nella gestione delle informazioni sensibili, rendendo la tutela dei dati un bene essenziale e una risorsa strategica con un forte impatto economico. Per difendere queste informazioni da minacce come hacker e attacchi informatici, la cybersecurity gioca un ruolo cruciale, garantendo che i sistemi e le reti aziendali siano adeguatamente protetti. La sfida diventa ancora più complessa quando si tratta di dati su larga scala, che coinvolgono intere nazioni, dove il volume delle informazioni è particolarmente elevato. Un accesso non autorizzato o un'appropriazione indebita di questi dati può avere conseguenze disastrose, anche a livello nazionale. La circolazione di tali informazioni richiede un alto livello di riservatezza e deve assicurare che i dati rimangano intatti, senza subire modifiche non autorizzate dal legittimo titolare. Queste informazioni sono fondamentali per le organizzazioni, che si trovano a gestire milioni di dati cruciali per sviluppare strategie competitive, sia a breve che a lungo termine. Oltre alle minacce interne ed esterne, una protezione e gestione efficace dei dati rappresenta un vantaggio strategico fondamentale nell'attuale contesto competitivo. In questo scenario entra in gioco la cybersecurity, il cui lo scopo principale è tutelare i sistemi informatici e, di conseguenza, tutte quelle informazioni vitali per le organizzazioni. La sua importanza non si limita alle aziende, ma si estende a tutte le entità che dipendono dalla sicurezza e dall'integrità dei dati per operare in modo sicuro e continuativo. In un rapporto dell'Osservatorio Cybersecurity & Data Protection del 2023 emerge come le organizzazioni abbiano ulteriormente potenziato le loro misure nella cybersecurity. Infatti, "il 60% delle grandi organizzazioni ha aumentato il budget per la sicurezza informatica, il 54% giudica necessario rafforzare le iniziative di sensibilizzazione al personale sui comportamenti da adottare, mentre il 46% si è dotata di un Chief Information Security Officer (CISO)[23]". Quest'ultima figura si occupa di stabilire una strategia globale per garantire la sicurezza dei dati e mettere in atto programmi per proteggere le risorse informative da quelli che sono le minacce informatiche. È fondamentale che ogni organizzazione implementi una solida "barriera di sicurezza" mirata alla protezione informatica, al fine di ridurre le minacce provenienti da hacker che cercano di infiltrarsi nei sistemi e sottrarre dati sensibili. Vi sono a riguardo dei principi fondamentali che punt ano a difendere le organizzazioni da attacchi hacker. Per proteggere i dati sensibili, la cybersecurity si basa su tre pilastri essenziali che garantiscono una gestione efficace della sicurezza: *confidenzialità*, *integrità* e *disponibilità*, noti con l'acronimo CIA (Confidentiality, Integrity e Availability). Questi principi sono cruciali per assicurare la protezione e la gestione sicura delle informazioni aziendali. Questi tre principi vogliono essere i pilastri per mantenere la sicurezza e l'affidabilità dei sistemi. Ogni misura di sicurezza adottata deve essere valutata in base alla sua capacità di garantire il rispetto di questi tre pilastri, rendendo la triade CIA

[23] **NAMIRIAL FOCUS**, *Sicurezza informatica e privacy dei dati: tutto quello che devi sapere*, 2022, https://focus.namirial.it/sicurezza-informatica/

un elemento imprescindibile nella costruzione di un'infrastruttura di sicurezza solida. Il pilastro della *confidenzialità* riguarda l'idea secondo cui solo gli utenti autorizzati possono accedere a determinate informazioni o a particolari risorse, impedendo che la riservatezza di determinate informazioni sia compromessa da accessi non autorizzati. Infatti, non vengono tutelati soltanto i dati personali ma tutte le informazioni che possono compromettere l'utente titolare di questi dati. Gli accessi non autorizzati vengono prevenuti attraverso l'adozione di tecniche specializzate, *come l'uso della crittografia a chiave pubblica*. Questo strumento funge da "cassa di sicurezza" che opera con un sistema di serratura a chiave, proteggendo al suo interno dati sensibili. La crittografia a chiave pubblica utilizza due chiavi di sicurezza: una chiave pubblica e una chiave privata. Queste chiavi, rappresentate da formule matematiche, consentono di cifrare e decifrare i messaggi. Esistono due modalità di utilizzo delle chiavi a seconda del tipo di crittografia adottata: la *crittografia simmetrica* e la *crittografia asimmetrica* (nota anche come crittografia a chiave pubblica). Nel caso della crittografia simmetrica, viene utilizzata una sola chiave sia per la codifica che per la decodifica. Questa chiave consente di criptare un messaggio, rendendolo segreto e inaccessibile a chi non ne è in possesso e quindi non è autorizzato a visualizzarlo. D'altro canto, *la crittografia asimmetrica* impiega due chiavi distinte: una chiave pubblica per la codifica e una chiave privata per la decodifica, offrendo così un ulteriore livello di sicurezza. Questa modalità di crittografia utilizza le due chiavi per cifrare e decifrare il messaggio. Un altro elemento importante della crittografia a chiave pubblica sono gli algoritmi. Esistono diversi tipi di algoritmi, tra cui *l'algoritmo RSA*. Questo algoritmo "si basa sul concetto di funzione modulare, un'operazione matematica che coinvolge il calcolo di resti in base a un modulo[24]". Infatti, la sua forza risiede proprio nel fatto che è molto complesso invertire il processo, tant'è che rappresenta uno strumento essenziale per la sicurezza dei dati digitali. Il secondo algoritmo di crittografia simmetrica è l'algoritmo DES (Data Encyption Standard). Esso protegge le informazioni utilizzando un principio della cifratura a blocchi. Nell'algoritmo DES "la chiave usata per cifrare è un blocco di 64 bit suddivisa in 8 sottoblocchi di 8 bit ciascuno; l'ultimo bit di ogni sottoblocco è di controllo, di conseguenza i bit liberi che costituiscono in pratica la chiave sono 56[25]". Infine, l'utlimo algoritmo di crittografia a chiave pubblica sono gli *algoritmi con funzione hash crittografica*. Questi algoritmi vengono utilizzati in applicazioni crittografiche come le firme digitali, per verificare che il messaggio sia autentico. Essi "trasformano un dato di lunghezza arbitraria (messaggio) in una stringa binaria (detta "digest") di lunghezza fissa, lunghezza che varia a seconda dell'algoritmo di hash utilizzato[26]".

[24] **INFORMATICA E INGEGNERIA ONLINE**, *Il Segreto della Sicurezza Digitale: L'Algoritmo di Crittografia RSA,* https://vitolavecchia.altervista.org/il-segreto-della-sicurezza-digitale-lalgoritmo-di-crittografia-rsa/

[25] **ZINATO M**, *Il DES l'algoritmo di crittografia moderno più noto: il Data Encryption Standard,* 2006, https://www.html.it/pag/16475/il-des/

[26] **SBARAGLIA G**, *Gestione delle password: cosa sono gli hash e a cosa servono*, 2022, https://www.cybersecurity360.it/outlook/gestione-delle-password-cosa-sono-gli-hash-e-a-cosa-servono/

Un' altra possibile tecnica che può garantire la riservatezza dei dati è sicuramente il *controllo degli accessi.* Esso è un elemento importante per concedere solo l'accesso agli utenti autorizzati ed evitare che soggetti malintenzionati possano accedere. Esistono diverse tipologie di controllo degli accessi, come ad esempio *il controllo di accesso condizionale (DAC)*. Questo strumento permette di gestire l'accesso degli utenti in base alla loro identità e ai permessi associati. Il proprietario della risorsa può così determinare chi può accedervi e quali azioni possono essere eseguite. A supporto di questo controllo, a ogni risorsa è associato un elenco che specifica le autorizzazioni concesse agli utenti. I proprietari delle risorse possono modificare questi elenchi per concedere o revocare i permessi in base alle necessità. La seconda tipologia di controllo di accesso è quello *obbligatorio (MAC).* Questo tipo di controllo accerta che gli identificatori siano associati sia all'utente sia alla risorsa e che siano in linea con le regole di accesso stabilite. Pertanto, l'accesso è consentito solo se i criteri di sicurezza dell'utente sono uguali o superiori a quelli richiesti dalla risorsa in questione, nel rispetto delle normative che disciplinano l'accesso. Gli accessi che riguardano la tipologia di controllo MAC avvengono soltanto se è strettamente necessario; quindi, soltanto quelli che siano necessari affinché l'utente possa svolgere il proprio compito. Un altro controllo importante è il *controllo degli accessi in base al ruolo (RBCA).* Questo sistema di controllo impedisce che dipendenti non appartenenti a ruoli aziendali adeguati possano accedere ai dati sensibili. In effetti, ciò impedisce l'accesso a coloro che non appartengono al settore di lavoro assegnato. L'ultima tipologia di *controllo di accesso è quella in base agli attributi (ABAC).* Questa tipologia di controllo consente che l'accesso è autorizzato attraverso appunto degli attributi. Esso consente che i dati vengano protetti fornendo un accesso mirato a determinati elementi. Un ultimo strumento per assicurare la riservatezza è il *monitoraggio* per identificare e fermare tempestivamente gli accessi non autorizzati. Il monitoraggio è un elemento fondamentale per far sì che qualsiasi organizzazione operi per riconoscere eventuali intrusioni all'interno del sistema. A tale fine molte organizzazioni hanno applicato un Security Operations Center (SOC) che ha la funzione di "migliorare le funzionalità di rilevamento, risposta e prevenzione delle minacce di un'organizzazione unificando e coordinando tutte le tecnologie e le operazioni di cybersecurity[27]". Il SOC è uno strumento utile per rilevare quelli che possono essere accessi non autorizzati utilizzando dei registri in cui vengono raccolte ed esaminate le varie minacce, creando poi avvisi. Con l'aumentare delle minacce da parte di cybercriminali e del loro modo di cercare di infiltrarsi nei vari sistemi, hanno portato le diverse organizzazioni a sviluppare sempre di più un Security Operations Center. Infatti, esso è sempre più implementato nelle organizzazioni per permettere ad esse di sorvegliare e diminuire le probabilità di attacco, facilitando il rilevamento

[27] **SCARPICCHIO M, DOWNIE A, FINIO M,** *Cos'è un SOC?*, 2024, https://www.ibm.com/it-it/topics/security-operations-center

tempestivo delle minacce da parte di hacker. Inoltre, le organizzazioni spesso non dispongono di tantissime risorse per sostenere gli investimenti necessari a garantire la loro sicurezza e crescita. Per questo il ruolo della Security Operations Center è fondamentale per implementare le risorse a disposizione, e per far fronte a una reazione immediata a quelle che sono le ipotetiche minacce. Oltre a ciò, vengono implementati software come la SIEM (Security Information and Event Management). Esso rappresenta uno strumento prezioso per il SOC, consentendo di identificare i punti critici che necessitano di un intervento immediato e di intraprendere azioni sia correttive che migliorative. Ma non solo, oltre alle SIEM le organizzazioni integrano come strumenti software anche il GRC (Governance Risk e Compliance). Il GRC "viene utilizzato per descrivere tutti i processi e le misure che aiutano le aziende a raggiungere gli obiettivi prefissati, a individuare e contrastare i possibili rischi e a rispettare le normative e le regole che si applicano alla loro attività quotidiana[28]". Esso punta infatti, a identificare, ridurre e controllare i potenziali attacchi, promuovendo un utilizzo più ottimizzato delle risorse e aiutando a ridurre i costi operativi. Questi strumenti costituiscono un elemento fondamentale per la gestione della sicurezza delle informazioni, proteggendo le organizzazioni dagli attacchi mirati all'accesso non autorizzato ai dati sensibili. Infine, un processo che può essere implementato dalle organizzazioni per avere un monitoraggio continuo è il VAPT (Vulnerability Assessment e Penetration Testing). Esso individua le vulnerabilità dei sistemi informatici e ne corregge mettendo in atto eventuali misure correttive. Molte organizzazioni ricorrono ai VAPT, proprio per aumentare il livello di sicurezza dei vari sistemi informatici e far in modo che ci sia una diminuzione degli attacchi hacker. Inoltre, un buon monitoraggio può avvenire attraverso una gestione delle patch che punta ad un equilibrio tra la sicurezza informatica e le necessità operative aziendali. Questi "patch" correggono quelle che sono le eventuali vulnerabilità delle organizzazioni. Bisogna sottolineare che questi patch portano a delle inattività che fanno sì che la loro gestione è quella di minimizzare queste interruzioni, rendendo più agevole e veloce il processo di aggiornamento. Infine, il monitoraggio può essere assicurato attraverso la creazione di programmi che favoriscano la formazione del fattore umano. Una forza lavoro consapevole può apportare un contributo significativo alla sicurezza complessiva dell'organizzazione. La componente umana riveste un ruolo fondamentale nell'individuare attivamente potenziali punti deboli nei sistemi aziendali, che potrebbero essere sfruttati per eventuali intrusioni e possibili anomalie nel sistema. Il secondo pilastro della sicurezza informatica è *l'Integrità (Integrity*), ed è un aspetto cruciale perché garantisce che i dati non vengano alterati in modo non autorizzato. Questo principio assicura che le

[28] **SANTEUSANIO L**, *Cos'è il sistema GRC e perché sta diventando sempre più importante,* 2022, https://www.eqs.com/it/polo-di-conoscenza-compliance/blog/gestione-dei-processi-grc/

informazioni siano trasmesse in modo corretto e integro, evitando alterazioni non consentite che potrebbero danneggiare l'organizzazione. La precisione e l'affidabilità dei dati sono essenziali per preservare l'integrità aziendale e mantenere una solida reputazione. L'integrità di queste informazioni può avvenire attraverso delle pratiche specifiche, come *il controllo degli hash.* Infatti, la verifica hash è essenziale proprio per verificare che i dati che sono stati modificati corrispondono agli originali. Infatti, questo strumento permette di valutare se il valore hash dei dati originali corrisponde con quello dei dati trasferiti o archiviati. Se i valori hash coincidono vuol dire che i dati non sono stati alterati. Al contrario, se i valori non coincidono significa che i dati sono stati compromessi. Un'altra tecnica che può garantire l'integrità delle informazioni è l'utilizzo dei checksum. Un checksum "è un valore derivato da un insieme di dati, in genere un file o un messaggio, utilizzato per rilevare errori o alterazioni[29]". Essi vengono utilizzati in combinazione con altri strumenti di sicurezza, come la crittografia, per garantire una protezione più robusta dei dati. Questa strategia viene adottata per mantenere un controllo costante sull'integrità e la sicurezza dei dati, assicurando che diverse misure lavorino in maniera sincronizzata. In questo modo, anche se una misura viene aggirata, le altre rimangono attive per garantire una continua protezione dei dati. In aggiunta, i checksum sono integrati con processi di automazione che riducono il rischio di errori, rendendo i processi più efficienti e precisi. Questi strumenti automatizzati consentono di effettuare controlli di integrità dei dati in modo rapido, sia durante la trasmissione che nell'archiviazione. Un ruolo cruciale per il rispetto dell'integrità dei dati lo giocano anche l'utilizzo dei file system dei vari sistemi operativi che permettono di assicurare l'integrità dei vari file e quindi dei dati. I file system "è un sistema di archiviazione su un supporto di memoria che struttura e organizza in modo specifico scrittura, ricerca, lettura, memorizzazione, modifica ed eliminazione dei file[30]". Essi sono lo strumento che consente di individuare i file in modo accurato, garantendo anche un controllo sugli accessi, determinando le azioni che ciascun utente è autorizzato a compiere. Tutto ciò evidenzia come la società dei big data sia esposta a rischi legati alla vasta quantità di informazioni in circolazione, richiedendo un'attenzione sempre maggiore alle azioni necessarie per salvaguardare l'integrità dei dati. È quindi fondamentale che le organizzazioni adottino misure efficaci per garantire una consapevolezza più profonda dei principi essenziali su cui si basa la protezione dei dati. L'ultimo pilastro della sicurezza informatica che permette alle organizzazioni di proteggersi dalle ipotetiche minacce informatiche è *l'Availability (disponibilità).* La disponibilità riguarda la possibilità di accedere alle informazioni quando gli utenti

[29] **BALLEJIS L**, *Che cos'è un checksum e come usarlo,* 2024, https://www.ninjaone.com/it/blog/cos-e-un-checksum/

[30] **IONOS**, *File system: cosa sono e quali sono quelli più importanti,* 2020, https://www.ionos.it/digitalguide/server/know-how/file-system/

autorizzati ne necessitano, in modo da dare loro la disponibilità appunto, di poter usufruire di informazioni attendibili e immediate. Inoltre, se pensiamo al contesto delle organizzazioni vediamo la disponibilità non solo come accesso alle informazioni, ma bensì anche un elemento portante per assicurare un corretto funzionamento delle operazioni interne ed esterne all'organizzazione. I clienti, infatti, non dovrebbero trovarsi ad affrontare un servizio scadente caratterizzato da possibili arresti durante l'utilizzo del sistema. L'organizzazione deve anche valutare la vulnerabilità del proprio sistema come guasti e interruzioni, identificando le eventuali lacune sistemiche e intervenendo prontamente per risolvere i problemi. L'organizzazione deve inoltre mantenere i criteri inizialmente promessi ai propri clienti, garantendo che il sistema funzioni in modo regolare e continuativo, e soprattutto quando l'utente lo ritiene necessario. La disponibilità consente alle organizzazioni di verificare se i loro servizi soddisfano gli obiettivi per cui sono stati sviluppati e di valutare se le contromisure adottate siano efficaci nel migliorare i profitti dell'organizzazione. Per questo è efficace adottare delle strategie che garantiscono la disponibilità alle organizzazioni, come ad esempio adottando *strategie di ridondanza* per assicurare una sicura disponibilità del sistema. La ridondanza consiste nella replica di parti o funzioni all'interno di un'organizzazione, al fine di garantire la continuità operativa. In caso di guasti o problemi di disponibilità, un componente sostitutivo entra in funzione, assicurando che il sistema continui a operare senza interruzioni. Infatti, lo strumento della ridondanza permette di rendere accessibile un sistema in ogni momento anche nel caso di un guasto. Inoltre, la ridondanza non si limita a garantire l'accessibilità, ma gioca un ruolo cruciale anche nella protezione dei dati attraverso la creazione di sistemi di backup ridondanti. Mantenere una regolarità del servizio e assicurare la sicurezza della rete grazie all'implementazione di strumenti come la ridondanza, consente di preservare la fiducia dei clienti. Questo approccio inoltre, favorisce l'innovazione, offrendo alle organizzazioni l'opportunità di esplorare nuove soluzioni con un rischio ridotto. Integrare uno strumento come la ridondanza nelle organizzazioni non dovrebbe essere un intervento da attuare in un secondo momento, ma al contrario, il sistema dovrebbe essere progettato fin dall'inizio con strumenti come la ridondanza già integrati. Questo consente di monitorare nel tempo quali servizi richiedono maggiormente strumenti come la ridondanza e, in particolare, quanto l'implementazione di tale misura abbia contribuito a migliorare la disponibilità del servizio. Un altro strumento per garantire una continuità operativa che può essere molto utile alle organizzazioni insieme alla ridondanza è l'implementazione del *meccanismo di failover.* Esso "prevede l'utilizzo di sistemi di backup in standby, pronti a subentrare immediatamente in caso di guasto del sistema primario[31]". Questo meccanismo consente al sistema operativo di continuare a funzionare senza

[31] **RACKONE**, *Failover: protocollo di sicurezza per la continuità dei servizi IT – Tecnico informatico ed elettronico*, https://www.rackone.it/glossario/failover/

interruzioni, evitando ostacoli che potrebbero causare disagi all'utente finale. Un piano di failover prevede un intervento immediato non appena si verifica un problema, rilevando eventuali anomalie nel sistema e monitorando costantemente lo stato del suo funzionamento. È molto importante, infatti, rilevare la causa originale del problema per poter intervenire e far sì che si possa ritornare alla piena operatività dei sistemi primari. Per questo Integrando sistemi di failover con strumenti di monitoraggio e altre soluzioni per verificare l'efficienza della disponibilità del sistema, sarà possibile garantire all'utente un'esperienza ottimale. Inoltre, è fondamentale sottolineare l'importanza di eseguire backup sistematici. Questo approccio garantisce la disponibilità dei dati e la continuità operativa, creando copie di sicurezza che assicurano una protezione completa delle informazioni. Grazie all'uso del backup è possibile ripristinare i dati persi e riportare il sistema allo stato operativo originale. Solo una gestione efficace dei dati consente di minimizzare il rischio di errori, come la perdita di informazioni o la possibilità che queste diventino irraggiungibili. Infine, è importante utilizzare anche soluzioni di mitigazione degli attacchi DDos. Questi attacchi portano, oltre a danni in termini economici all'organizzazione anche interruzioni delle operazioni aziendali. In un contesto di attacchi in continua evoluzione, un servizio di mitigazione efficace individua e blocca gli attacchi il più rapidamente possibile dagli attacchi DDos. Poiché la sfera degli attacchi di questo tipo sta diventando sempre più complessa, è essenziale che le organizzazioni investano costantemente nelle capacità di difesa. Per garantire la migliore protezione, sono necessarie tecnologie avanzate in grado di rilevare il traffico malevolo e attuare misure di difesa solide per ridurre rapidamente gli attacchi. Esempi di mitigazione degli attacchi DDos che permettono di proteggere il traffico da questi attacchi sono: servizi di sicurezza basati su CDN, sistemi scrubbing DDos su icloud, difesa dagli attacchi DDoS on-premise (on-prem), protezione dagli attacchi DDoS ibrida e cloud signaling. *I servizi di sicurezza basati su CDN* possono essere un ottimo strumento di sicurezza contro gli attacchi DDos. Quando parliamo di CDN ci si riferisce a un "processo definito "caching" o memorizzazione nella cache, che archivia temporaneamente copie dei file in vari data center dislocati in tutto il mondo, consentendo agli utenti di accedere ai contenuti sul web dai server che si trovano nelle loro vicinanze[32]". Quando le organizzazioni sfruttano la propria CDN come sistema di sicurezza per ottimizzare il traffico HTTP e HTTPS, gli attacchi DDoS rivolti a uno specifico URL possono essere immediatamente bloccati. La differenza di questo sistema di protezione basato su CDN con *i sistemi scrubbing DDos su icloud* è che nel secondo c'è una protezione completa sia su sistemi web che sui sistemi IP. Questo perché lo scrubbing DDos permette che l'operatività dei servizi e delle attività sia

[32] **AKAMAI**, *Che cos'è una rete per la distribuzione dei contenuti (CDN)?,* https://www.akamai.com/it/glossary/what-is-a-cdn

comunque sempre funzionante anche durante un attacco DDos. Implementare questo servizio nel cloud consente di ridurre significativamente gli attacchi diretti alle risorse interne su larga scala. Per quanto riguarda invece *la difesa dagli attacchi DDoS on-premise* è uno strumento di difesa che *viene* attuata per attacchi di piccole dimensioni. Questo tipo di difesa, infatti, prevede che i dispositivi siano installati nel data center di un'azienda e si integrino con i router situati ai margini della rete per fermare gli attacchi dannosi. Questo sistema on-premise, in combinazione con le soluzioni basate sul cloud, crea una protezione ibrida contro gli attacchi DDoS. Infatti, integra soluzioni on-premise in grado di difendere l'infrastruttura di rete da minacce di bassa intensità con l'utilizzo di competenze di un servizio di scrubbing in cloud per affrontare attacchi di grande portata. Infine, come ultimo strumento per mitigare gli attacchi DDos troviamo il *cloud signalling*. Esso si riferisce al procedimento di trasferimento di dati da parte di strumenti on-premise con dati che riguardano l'attacco ai centri di scrubbing nel cloud. Per contrastare le possibili minacce che possono compromettere il sistema, è utile anche *creare dei firewall* che permettono di intervenire per affrontare minacce esterne e controllare il traffico in rete. I firewall controllano i pacchetti provenienti dall'esterno per verificare che siano sicuri prima di consentirne l'accesso alla rete interna. Questo processo è progettato per prevenire possibili attacchi esterni e, soprattutto, per proteggere le stazioni interne da intrusioni da parte di hacker. La sicurezza delle reti dipende dalla capacità dei firewall di garantire che le infrastrutture interne siano sufficientemente robuste. Questo sistema di protezione consente di contrastare diversi attacchi esterni, evitando potenziali interruzioni di servizio e impedendo l'accesso non autorizzato. Tuttavia, i firewall presentano dei limiti: non possono difendere il sistema da attacchi che utilizzano pacchetti che non vengono sottoposti al loro controllo. Per questo motivo, le organizzazioni devono monitorare costantemente tutti i servizi, assicurandosi che vi sia un controllo attivo anche da parte del personale. Il personale interno, infatti, può involontariamente facilitare attacchi hacker, ad esempio condividendo password o fornendo altre informazioni riservate dell'organizzazione, aprendo così una via di accesso agli hacker. In questi casi, anche i sistemi di sicurezza più avanzati, come i firewall, rischiano di essere inefficaci, rendendo vulnerabile l'intera infrastruttura. Inoltre, con l'orientamento sempre più marcato verso la digitalizzazione, le organizzazioni possono adottare gruppi di continuità per garantire un'operatività costante e ininterrotta, proteggendo le infrastrutture critiche collegate alle reti di distribuzione elettrica. Un esempio efficace di questi dispositivi sono i gruppi di continuità UPS (Uninterruptible Power Supply), che contribuiscono a raggiungere tali obiettivi in modo efficiente. Un gruppo di continuità UPS "è un dispositivo, utilizzato per evitare che anomalie o interruzioni nella fornitura di energia elettrica, come cali di tensione e blackout, determini l'interruzione delle attività aziendali, se non addirittura il

danneggiamento di server e altri apparecchi[33]". Questi strumenti, indipendentemente dalle condizioni della rete, assicurano un'energia di alta qualità. Si attivano automaticamente in caso di interruzioni improvvise, sovratensioni o cali di tensione. Grazie a dispositivi di questo tipo, le organizzazioni possono raggiungere obiettivi cruciali di resilienza informatica, garantendo una disponibilità continua dei servizi e un'esperienza senza interruzioni per gli utenti che utilizzano la rete. Quando un'organizzazione presenta delle lacune per quanto riguarda i sistemi interni è facile che si verifichino diversi problemi, tra cui inconvenienti di diverso tipo. Per questo garantire un'elevata disponibilità delle risorse diventa quindi fondamentale per assicurare l'efficienza e il successo dell'organizzazione. In conclusione, possiamo affermare che i tre pilastri fondamentali della sicurezza informatica—riservatezza, integrità e disponibilità—sono strettamente interdipendenti, poiché l'uno non può esistere senza gli altri. Pertanto, un sistema di sicurezza dei dati richiede un approccio integrato che prenda in considerazione tutti e tre questi principi. Incorporando tali valori nelle strategie e nelle procedure di un'organizzazione, è possibile proteggere efficacemente l'accesso ai dati da una vasta gamma di minacce informatiche che le organizzazioni si trovano ad affrontare quotidianamente.

2. TECNICHE DI ANALISI DI MINACCE E RISCHI: IL MODELLO DI CIA E IL MODELLO DI DREAD A CONFRONTO

Un'importante sfida quotidiana per le organizzazioni è mantenere un livello di sicurezza costantemente elevato, senza mai abbassare la guardia contro potenziali attacchi da parte di organizzazioni criminali. Adottare tutte le misure di sicurezza disponibili nella fase strategica è essenziale per creare lo scudo di protezione di cui un'organizzazione ha bisogno. Questo approccio consente di sviluppare continuamente nuove strategie per ridurre la propria vulnerabilità e difendersi efficacemente dalle minacce in continua evoluzione. Un processo che lavora proprio sui rischi che si ritrovano ad affrontare le varie organizzazioni e che affronta le minacce informatiche e i suoi rischi è il *threat modeling*. Questo processo di sicurezza permette di identificare e analizzare i potenziali attacchi, valutando l'impatto che potrebbero avere sull'organizzazione e definendo le azioni necessarie per contrastarli. La vastità delle minacce comporta che questo processo debba essere utilizzato sia al momento della pianificazione, di quella che è la realizzazione dell'organizzazione, sia nel momento in cui il prodotto raggiunge l'utente finale, proprio per avere un piano completo

[33] **NEW INNOVARE PER CRESCERE**, *Gruppi di continuità: cosa sono, a cosa servono e come funzionano,* https://www.newcomm.it/informatica-e-networking/gruppi-di-continuita-ups/

dall'inizio alla fine sui controlli e le contromisure che devono essere implementate. Infatti, individuare quelle che sono le minacce già in fase di progettazione permette all'organizzazione di individuare le lacune presenti e permettere di intervenire in maniera rapida. Per questo il threat modeling garantisce un piano completo, dall'inizio alla fine, per i controlli e le contromisure da implementare, utilizzando un approccio sistematico per far fronte alle minacce informatiche che riguardano un contesto preciso. Il threat modeling intende adottare un approccio sistematico per identificare le minacce legate a una determinata situazione servendosi di alcuni approcci specifici. Il primo approccio a cui fa riferimento il threat modeling è quello incentrato sugli asset. Quando parliamo di asset ci riferiamo "a tutti quei beni materiali e immateriali di proprietà di un'impresa, che non generano direttamente un profitto, ma sono il mezzo per ottenere un guadagno futuro[34]". La gestione dei rischi che corrono questi asset diventa cruciale per il threat modeling, che cerca di individuare le possibili minacce che può intercorrere un determinato asset in un determinata circostanza. Un altro approccio del threat modeling è quello focalizzato sugli attacker. Questo metodo si concentra sull'identificazione dei potenziali hacker e sui tipi di attacchi che potrebbero utilizzare per raggiungere i loro obiettivi. Capire quale sono le probabili mosse che può compiere un hacker in un determinato momento, permette di concentrarsi su quelle che possono essere le vulnerabilità di certi asset. Infine, l'ultimo approccio riguarda la protezione dei software. È fondamentale difendere i prodotti software da potenziali minacce, concentrandosi sui punti deboli che potrebbero consentire l'accesso a potenziali hacker che comporterebbero anche rischi difficili da identificare e risolvere. Certamente, il processo di modellazione delle minacce si differenzia in base alle strategie adottate dalle organizzazioni. Infatti, il threat modeling esamina un componente dell'organizzazione o del software che potrebbe risutare vulnerabile a minacce da parte di criminali informatici. Infatti, quest'analisi valuta il funzionamento del componente in relazione alla visione complessiva dell'organizzazione e ai potenziali rischi che essa potrebbe affrontare. Alcuni tipi di minacce che vengono rilevate con il processo di threat modeling è ad esempio l'accesso non autorizzato. Questo processo, infatti, porta a individuare le fragilità del sistema che possono essere causa di attacco, come ad esempio password che non sono abbastanza complesse e quindi che permettono l'accesso e l'appropriazione di dati da parte di cybercriminali. Ma non solo, anche gli attacchi di escalation dei privilegi risulta essere oggetto di numerosi attacchi attraverso l'accesso ad account e alle informazioni correlate. Anche per questi tipi di attacchi che arrivano a compromettere funzioni chiave dell'organizzazione, il threat modeling può essere uno strumento utile a identificare i modi in cui determinati meccanismi potrebbero essere aggirati da attacchi hacker, aiutando a migliorare la

[34] **AGICAN**, *Cosa si intende per asset di un'azienda,* https://agicap.com/it/articolo/asset-aziendale/

sicurezza dell'intero sistema. Inoltre, il processo di threat modeling punta a proteggere l'organizzazione da quelli che sono i rischi di manipolazione umana provocati dagli attacchi di ingegneria sociale. In questo caso il threat modeling aiuta a prevenire attacchi di questo tipo integrando all'interno dell'organizzazione misure comportamentali adeguate, formando il personale sui rischi di questi attacchi e implementando misure di sicurezza che possano ridurre il rischio di manipolazione. Anche le informazioni che sono sempre di più esposte a minacce di violazione e diffusione da parte di hacker, soprattutto quando si parla di informazioni sensibili, possono causare delle criticità all'interno dell'organizzazione. Per questo il threat modeling cerca di indentificare quelli che possono essere le fragilità di un'organizzazione, per poter realizzare delle strategie di difesa che possano proteggere tutti i dati sensibili da quelle che possono essere delle divulgazioni non autorizzate. I sistemi o i servizi resi inutilizzabili dai sovraccarichi causati dagli attacchi DoS spingono le organizzazioni a utilizzare il threat modeling per analizzare le potenziali vulnerabilità a questi attacchi. Tra le tecniche di mitigazione più comuni vi è il blocco degli IP, che consiste nell'interrompere l'accesso da parte di un indirizzo IP quando viene identificato come sospetto. Infine, le minacce interne, che derivano dalla diffusione non autorizzata di informazioni da parte del personale interno all'organizzazione, sfruttano l'accesso privilegiato per arrecare danno all'azienda o per scopi personali. In questo contesto, il threat modeling svolge un ruolo cruciale, aiutando le organizzazioni a identificare tali rischi e a sviluppare strategie efficaci per proteggere le loro risorse, migliorando la sicurezza e creando un ambiente di lavoro più protetto e affidabile. Questo ci fa capire come il primo step che il threat modeling deve attuare è quello di rilevare le minacce per poter poi applicare le fasi successive. La metodologia utilizzata da questo processo offre approcci diversi per analizzare e ridurre la possibilità di minacce informatiche di un determinato sistema. Una delle possibili metodologie utilizzate dal threat modeling è ad esempio *l'attack tree.* Come dice il nome stesso questa metodologia scompone i diversi passaggi che un hacker potrebbe compiere per colpire determinate vulnerabilità e raggiungere determinati obiettivi. Questo modello cataloga e descrive le diverse minacce proprio attraverso una struttura ad albero dove in cima troviamo l'obiettivo ultimo dell'hacker, dopodiché troviamo i sotto-obiettivi che servono all'hacker per raggiungere i suoi obiettivi e infine, troviamo le azioni sferrate dall' hacker. Un'altra metodologia utilizzata è il *trike* che si occupa di monitorare e valutare la sicurezza informatica attraverso la gestione di quelle che sono le probabili minacce. Essa adotta una prospettiva difensiva opposta a quella degli hacker e indica un'unione delle minacce come un sostituto della metodologia attack tree per far sì che queste minacce non si ripetano. Un ulteriore strumento adottato dal threat modeling è il processo *Pasta (Process for Attack Simulation and Threat Analysis).* Essa si suddivide in sette momenti che punta a contrastare i rischi relativi alle minacce di grossa portata per raggiungere un determinato obiettivo. Questo

processo inizia innanzitutto con lo stabilire gli obiettivi dell'organizzazione e quindi quali risultati l'organizzazione vuole raggiungere; nella seconda fase il processo pasta stabilisce il contesto tecnico e quindi quella che è la sequenza temporale degli obiettivi; la terza fase riguarda la suddivisione del sistema che riguarda l'organizzazione delle applicazione nei suoi elementi trasferibili; la quarta fase riguarda la valutazione delle minacce e l'esaminare quelli che sono i rischi presenti; una volta esaminato le minacce il processo Pasta nella quinta fase compie una valutazione delle vulnerabilità e dei punti critici, identificando le aree da potenziare; la sesta fase riguarda il creare da parte di questo processo di scenari di attacco plausibili e analizzare i risultati; infine, l'ultima fase riguarda quello che è la valutazione del rischio e dell'impatto che ha questo sull'organizzazione, e quindi il modellare delle soluzioni in base proprio a quelli che sono i risultati che si vogliono ottenere. L'ultimo modello da analizzare del threat modeling è il processo *Stride (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service* ed *Elevation of privileges.* Esso venne sviluppato da Microsoft e il suo acronimo intende analizzare delle categorie specifiche di minacce tra cui: *la falsificazione di identità* (*Spoofing*) che riguarda la capacità degli hacker di spacciarsi per altre persone, come ad esempio, fingendo di essere un utente delle poste che intende raggirare l'utente per avere informazioni personali; *l'alterazione dei dati (Tampering)* e riguarda tutti quei dati che non possono essere modificati e si ritrovano invece ad essere modificati da hacker che approfittano di vulnerabilità all'interno di un sistema per poter mettere le mani su determinati dati; *ripudio di un'azione (Repudiation)* si verifica quando un utente malintenzionato nega di aver compiuto un'azione illegale, e il sistema non ha prove sufficienti per dimostrarlo; *divulgazione delle informazioni* (*Information Disclosure)* che riguarda l'accesso da parte di utenti non autorizzati ad accedere a determinate informazioni portando così a diffondere dati sensibili senza il permesso del titolare; *diniego di servizio (Denial of Service)* che puntano a mettere fuori uso il sistema e quindi a renderlo inutilizzabile dall'utente impedendo anche una semplice azione; *elevazione dei privilegi (Elevation of Privilege)* che si manifesta quando l'utente ha la capacità tecnica di eseguire operazioni che non potrebbe svolgere, permettendo ad hacker di sfruttare delle vulnerabilità per poter ottenere il controllo su un determinato sistema. Questo processo porta a valutare bene il proprio sistema all'interno dell'organizzazione, identificando le minacce che rientrano nelle categorie sopra descritte. Dopo aver individuato la minaccia in questione, è fondamentale analizzare la gravità che ha ogni singola minaccia per l'organizzazione e questo può avvenire utilizzando la tecnica *Dread (Damage Potential, Reproducibility, Exploitability, Affected User e Discoverability)*. Questa metodologia utilizza dei punteggi che vengono dati per ogni rischio dovuto ad ogni singola minaccia. Infatti, il risultato di questi punteggi riguarda la vulnerabilità di ogni organizzazione basate proprio sul rischio. Questo rischio è dato proprio dalla possibilità che possa accadere una determinata minaccia e gli effetti che

questa può causare. Il nome di questa metodologia richiama infatti, le cinque tipologie che descrivono un aspetto specifico di una minaccia: la pima tipologia è il *damage potential* che si basa sulla gravità della minaccia nel caso in cui dovesse colpire un determinato sistema; la seconda tipologia riguarda la *reproducibility* che si sofferma su quale può essere la probabilità che la minaccia si ripresenti una seconda volta; Il terzo fattore è l'exploitability, che si riferisce al tempo, all'impegno e alle competenze che servono affinché una minaccia possa essere considerata riuscita; il quarto fattore è l'*affected users* tocca gli utenti e quanti di loro verrebbero colpita da una determinata minaccia; e infine, l'ultimo fattore è il *discoverability* che riguarda quanto può essere semplice per un attaccante scoprire una minaccia. Queste cinque categorie vengono utilizzate nel calcolo numerico che permette di assegnare loro un punteggio, con l'obiettivo di determinare i rischi e i parametri di una minaccia in un determinato contesto. Il parametro di valutazione con cui si calcola il rischio possono essere due, in base ad una determinata situazione e sono: uno schema ridotto con tre livelli di misurazione e uno schema più dettagliato con dieci livelli di misurazione. Ciò che accomuna entrambi gli schemi di calcolo è che dal risultato finale emergono le fragilità che comporta una determinata minaccia, dove se il valore sia dello schema ridotto con tre livelli e sia dallo schema con dieci livelli è alto vuol dire che c'è bisogno di un maggiore intervento; al contrario se il valore è basso vuol dire che c'è minore urgenza d'intervenire. Le organizzazioni hanno quindi, un crescente bisogno di adottare modelli di questo tipo che consentano di gestire efficacemente le vulnerabilità presenti nei sistemi e gestire le potenziali minacce che sfruttano queste debolezze per infiltrarsi e comprometterne la sicurezza. Infatti, grazie a questi modelli ci può essere un'ottima gestione delle minacce e dei rischi che essi comportano. Per questo è essenziale che nell'ambito della sicurezza informatica lavorino insieme sia il modello CIA sia il modello DREAD pur essendo due modelli che hanno degli obiettivi diversi, ma che riescono a dare insieme una visione completa di quella che è la sicurezza informatica per ogni singola organizzazione. Il modello CIA, come abbiamo spiegato nel paragrafo 1, richiama quella che è la protezione dei dati attraverso i tre pilastri della *confidenzialità, dell'integrità* e della *disponibilità.* Questo modello porta a creare dei sistemi solidi e maggiormente protetti, ed è importante per valutare la resistenza di un'organizzazione salvaguardare i dati per proteggerli da quelli che possono essere attacchi hacker attraverso accessi e modifiche non autorizzate o vari bug nel sistema. Proprio per questo il modello CIA vuole rappresentare un quadro difensivo progettato per garantire l'integrità e la disponibilità delle informazioni in ogni situazione. A differenza del modello CIA, il modello DREAD, come visto recentemente, si concentra sull'analizzare le minacce e classificarle sulla base del rischio che esse comportano. Quest'analisi data da questo modello aiuta le organizzazioni a capire l'importanza di intervenire di più o di meno in una determinata situazione. Ciò che differenzia i due modelli, pur potendo essere complementari, è proprio l'obiettivo principale. Il modello CIA vuole

essere un modello difensivo che intende definire i principi su cui un'organizzazione debba costruire una rete di sicurezza robusta, con l'obiettivo di proteggere i sistemi operativi esistenti all'interno dell'organizzazione. Al contrario, il modello DREAD ha un approccio più dettagliato su quelle che sono le minacce e come si classificano, permettendo all'organizzazione di valutare il rischio di una minaccia in corso e determinare quali minacce hanno bisogno di un intervento tempestivo rispetto ad altre. Questo modello non punta a garantire l'integrità di un sistema, ma bensì a stabilire la gravità delle minacce che potrebbero compromettere il sistema di un'organizzazione. Inoltre, la differenza tra i due modelli la troviamo anche nella loro applicazione, in quanto il modello CIA proprio perché riguarda la sicurezza della gestione dei sistemi all'interno di un'organizzazione, è molto spesso utilizzato come modello per verificare se il sistema risulta essere conforme o meno al GDPR, e cioè il regolamento generale sulla protezione dei dati. Infatti, proprio nell'art 32 par. 1 lett. b del Regolamento 679/2016 vengono riconosciuti l'importanza dei tre pilastri della riservatezza, dell'integrità e della disponibilità, ma anche quello della resilienza che viene indicato come quarto pilastro per garantire la sicurezza dei sistemi. Per questo l'art 32 dichiara che tra le misure adeguate ad assicurare la sicurezza del trattamento rientra nella lettera b anche "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento[35]". Questo quarto pilastro della resilienza citato dall'articolo, vuole riferirsi alla "capacità di resistere e di reagire di fronte a difficoltà, avversità, eventi negativi[36]" da parte di un'organizzazione. È importante sottolineare che le organizzazioni si trovano quotidianamente a gestire crisi di vario genere e, sebbene una solida resilienza sia fondamentale, a volte non basta da sola. Tuttavia, queste situazioni possono rappresentare opportunità di crescita futura, offrendo l'occasione di valutare più chiaramente cosa funziona e cosa necessita di miglioramento all'interno dell'organizzazione. Al contrario, il modello DREAD vuole essere uno strumento più pratico rispetto al modello CIA, impiegato per analizzare il rischio e per stabilire quali interventi sono necessari per far fronte alle minacce. Infine, un ultimo fattore che differenzia i due modelli è la struttura in cui sono composti: il modello CIA si concentra su tre principi essenziali, mentre il modello DREAD riguarda cinque categorie di minacce, ed offre una valutazione del rischio più dettagliata andando ad approfondire ogni singola minaccia. Questo valutare in maniera dettagliata ogni singola minaccia da parte dagli analisti comporta anche una diversa interpretazione, essendo che ogni organizzazione è composta da differenti esperti che hanno metriche di valutazione distinte. In sintesi, potremmo dire

[35] **ALTALEX**, *"Art. 32 GDPR - Sicurezza del trattamento",* 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-32-gdpr-sicurezza-del-trattamento

[36] **BUTTI G**, *"Resilienza, contro gli attacchi informatici: linee guida per le aziende",* 2018, https://www.cybersecurity360.it/soluzioni-aziendali/resilienza-contro-gli-attacchi-informatici-linee-guida-per-le-aziende/#:~:text=propriet%C3%A0%20dei%20materiali%20di%20resistere,negativi%20ecc.%3A%20resilienza%20sociale.

che entrambi i modelli sono fondamentali per la sicurezza informatica pur rispondendo a esigenze diverse. Per questo una buona combinazione del modello CIA e del modello DREAD all'interno di un'organizzazione permette di affrontare la sicurezza informatica sia in modo sia proattivo, che permette di impedire in maniera proattiva il verificarsi di attacchi hacker che possano mettere in pericolo dati e informazioni personali; che reattivo, proteggendo le informazioni e rispondendo rapidamente alle minacce emergenti nel momento in cui ci un'organizzazione si ritrova davanti a dover affrontare una determinata minaccia.

3. IL RUOLO COMBINATO DI SOC (Security Operations Center) E NOC (Network Operations Center) NELLA SICUREZZA INFORMATICA

Nonostante l'evoluzione costante della cybersecurity, sostenuta da continui investimenti e innovazioni, essa si trova ad operare in un ambiente sempre più esposto a vulnerabilità e minacce informatiche, rapide e insidiose. Un'azienda che si occupa del progresso e della fornitura di servizi di cybersecurity è l'azienda Sophos. Questa azienda "sfrutta i dati di intelligence sulle minacce, l'intelligenza artificiale e il machine learning dei SophosLabs e di SophosAI per offrire una vasta gamma di prodotti e servizi avanzati, in grado di proteggere utenti, reti ed endpoint contro ransomware, malware, exploit, phishing e un'enorme varietà di attacchi informatici[37]". Essa, ha sviluppato attraverso la ricerca *active adversary report for tech leaders 2023* quello che è l'approccio e i mezzi che hanno utilizzato le minacce informatiche nel 2023. I dati riportavano che l'individuazione delle minacce risultava in media tra gli otto giorni tra l'attacco e la sua identificazione e che i sistemi venivano violati in pochissimo tempo. Nel primo paragrafo abbiamo introdotto il SOC (Security Operations Center), una struttura essenziale per le organizzazioni, in cui esperti di sicurezza informatica si dedicano alla protezione contro le minacce potenziali. Questi specialisti monitorano, rilevano e intervengono tempestivamente per prevenire azioni che potrebbero compromettere la sicurezza digitale dell'organizzazione. Esso però non opera soltanto fronteggiando quelle che sono le minacce esterne, ma gestisce anche il lavoro di sicurezza interna per quanto riguarda gli eventi che possono compromettere la sicurezza da parte delle risorse interne. L'analisi dei dati aziendali da parte di questo organo è gestita in modo da garantire un controllo completo delle informazioni, permettendo interventi tempestivi in caso di intrusioni, sia da parte di hacker esterni sia da parte del personale interno con intenti malevoli. Oltre alla salvaguardia dei dati personali da questi

[37] **SOPHOS**, *"Garantiamo i migliori risultati di sicurezza per le organizzazioni che hanno bisogno di soluzioni concrete"*, https://www.sophos.com/it-it/company#:~:text=Sophos%20sfrutta%20i%20dati%20di,un'enorme%20variet%C3%A0%20di%20attacchi

accessi non autorizzati, il SOC porta l'organizzazione a contribuire a mantenere la continuità dei processi senza che ci siano interruzioni improvvise. Questo contributo del SOC, inoltre, porta a fidelizzare i clienti e far sì che l'organizzazione mantenga una certa reputazione. Le organizzazioni che optano per un SOC interno possono evitare numerosi danni, spesso altamente costosi, sia in termini di impatto reputazionale sia di perdite economiche. Implementare un modello SOC consente loro di adottare misure di sicurezza preventive, preparandole efficacemente a fronteggiare potenziali minacce. Rispetto alle organizzazioni che non decidono di investire in modelli di questo tipo, coloro che usufruiscono di SOC interni hanno un livello di contenimento delle minacce più elevato e soprattutto una minimizzazione delle interruzioni all'interno del sistema. Il monitoraggio di questi sistemi, oltre a ridurre al minimo i rischi d'intrusione e i possibili danni che essi comportano, porta le organizzazioni a rimanere al passo con lo scenario delle minacce in costante evoluzione. Infatti, in questo modello, i veri elementi portanti non sono tanto gli strumenti utilizzati, quanto gli operatori stessi, che li applicano con le loro capacità e competenze. Grazie alla varietà di funzioni all'interno del team SOC, ogni problema può essere affidato agli specialisti più adatti. La scelta di che modelli implementare spetta proprio alle organizzazioni in base alle loro esigenze; quindi, valutare se è preferibile attuare un SOC interno o altri modelli di sicurezza. Proprio per questo con il passare del tempo nasce una nuova forma di difesa che riprende mansioni del SOC in rapporto con gli stakeholder, ed è il *SOC as a service.* Questo modello funge da parametro di controllo dei sistemi sorvegliati, permettendo di individuare ciò che potrebbe mettere in pericolo la sicurezza informatica e intervenire di conseguenza. Il SOC as service offre dei punti forza se viene implementato all'interno di un'organizzazione, come ad esempio, il *potenziamento del team di sicurezza.* Esso avviene perché il personale interno all'organizzazione spesso ha poca esperienza in ambito cybersecurity e soprattutto spesso non ha dimestichezza con le nuove tecnologie correlate. Collaborare con professionisti di un SOC as a Service permette di rafforzare e completare il personale interno che si occupa di sicurezza informatica, riuscendo a colmare queste eventuali carenze. Inoltre, il SOC as a Service contribuisce a innalzare ulteriormente il livello di sicurezza all'interno dell'organizzazione, poiché gli operatori di questo modello possono offrire le competenze necessarie per potenziare rapidamente le risorse di cybersecurity. Questo permette anche di aggiornare le singole organizzazioni: collaborando con un provider di SOC as a Service, l'organizzazione beneficia di funzionalità sempre all'avanguardia. Oltre ai numerosi vantaggi che il modello di SOC as a Service offre, sono varie anche le sfide che ogni giorno un'organizzazione che sfrutta questo modello si ritrova ad affrontare, come ad esempio, *la protezione dei dati aziendali*. Le organizzazioni che scelgono di implementare questo modello devono condividere una quantità significativa di dati sensibili con i fornitori di SOC as a Service. Questi ultimi necessitano di una visione completa dei

sistemi aziendali per individuare le potenziali minacce e attivare tempestivamente le azioni difensive appropriate. Tuttavia, questo processo di condivisione può compromettere la sicurezza dei dati sensibili dell'organizzazione, rendendoli eccessivamente esposti e limitando il pieno controllo che l'organizzazione stessa può esercitare su di essi. Questa poca sicurezza risulterebbe anche avvenire per quanto riguarda quella che è lo scenario normativo. Le organizzazioni, infatti, devono monitorare le linee guida adottate per provare che esse siano conformi alle regolamentazioni attuali. Affidarsi a fornitori di SOC as a Service in questo caso, significa fidarsi che essi svolgano i loro compiti in maniera corretta e conforme alla legge e questa, non è una garanzia che viene sempre assicurata. Un'ulteriore sfida che un'organizzazione si trova ad affrontare implementando servizi di SOC as a Service riguarda *il processo di onboarding.* Questo processo è molto importante nel momento in cui uno degli obiettivi strategici di un'organizzazione è "fornire ai nuovi dipendenti tutti gli strumenti per essere completamente operativi, produttivi e integrati con la struttura e la cultura aziendale, così da garantire l'inclusione nel team e buone performance nel tempo[38]". Il processo di onboarding richiede un percorso complesso; per questo motivo, i provider di SOC-as-a-Service hanno bisogno di tempo per integrare efficacemente i loro strumenti di sicurezza all'interno delle organizzazioni che scelgono di adottare questi servizi. Non tutte le organizzazioni hanno l'esigenza o la possibilità di adottare servizi di questo tipo. Le piccole e medie imprese, ad esempio, spesso non percepiscono la necessità di investire risorse nella sicurezza informatica. Al contrario, le grandi aziende, che gestiscono enormi quantità di dati e risorse, richiedono strumenti come il SOC as a Service per monitorare l'intera infrastruttura e proteggerla dalle minacce. Infatti, investire in modelli come il SOC as service o semplicemente in SOC interni, dipende da molti fattori come, ad esempio, maggiori costi che una piccola organizzazione avrebbe difficoltà a gestire. Per molte organizzazioni invece, sostenere un SOC interno o SOC as a Service rappresenta la strategia più adeguata alle loro esigenze interne. Indipendentemente dalla scelta di quale Security Operations Center applicare, è fondamentale che essi abbiano i mezzi necessari per poter mettere in atto misure di salvaguardia contro le minacce informatiche. Un'altra attività fondamentale per un'organizzazione, oltre alla funzione di sicurezza che svolge il SOC, è la gestione della rete svolta dal *Network Operation Center (NOC)*. I NOC "collaborano direttamente con le organizzazioni per supervisionare i loro complessi ambienti di rete, compresi server, database, firewall, dispositivi e servizi esterni correlati[39]". Essi operano dividendo i singoli problemi in base alle tecnicità del problema che viene assegnato a varie categorie. Le operazioni del NOC non sono svolte sempre dagli stessi specialisti; ciascuno si occupa di aree

[38] **IN RECRUTING**, *Onboarding: cos'è, come farlo e perchè è importante,* 2024, https://www.in-recruiting.com/it/onboarding-definizione-significato/

[39] **IBM**, Che cos'è un NOC?, https://www.ibm.com/it-it/topics/network-operations-center

specifiche, affrontando i problemi che emergono, implementando soluzioni mirate e adottando misure preventive per evitare futuri inconvenienti. I benefici che porta il NOC alle organizzazioni che decidono di implementarlo sono vari: come, ad esempio, l'eliminazione dei tempi di interruzione del sistema che favoriscono un corretto funzionamento di software, di hardware e reti. Essi, infatti, intervengono per far sì che le criticità che si vengono a creare per via di anomalie vengano contrastate, per non ritrovarsi di fronte ad ulteriori problemi che possano crearsi alla rete o ad un software in generale a seguito di queste anomalie. Per questo proprio in quelle aeree che richiedono dei miglioramenti, il NOC attua degli interventi adatti per rendere la rete più robusta attraverso anche un'analisi dettagliata sulla stabilità della rete. Questo per dire che un'organizzazione solida ha bisogno di un NOC per far fronte a malfunzionamenti della rete e di un SOC che difenda le risorse interne da minacce informatiche. Nonostante i loro ruoli e obiettivi distinti, le nuove tecnologie e i moderni sistemi di rete promuovono una cooperazione tra NOC e SOC. Entrambi i team devono infatti essere in grado di gestire i potenziali malfunzionamenti della rete e affrontare le minacce che potrebbero rendere l'organizzazione vulnerabile in determinate aree. Pertanto, il NOC si impegna a garantire che le operazioni siano svolte senza interruzioni, evitando disagi per gli utenti. Allo stesso tempo, il SOC si dedica a proteggere l'organizzazione da potenziali minacce informatiche che potrebbero compromettere le diverse attività. Anche coloro che operano all'interno di questi due modelli operano in ambiti di esperienze diverse insieme alle loro funzioni che vengono eseguiti in ambiti di interessi diversi. Infatti, il Network Operation Center (NOC) impiega il proprio team interno per risolvere problemi di natura infrastrutturale, in particolare quelli legati alle reti e ai dispositivi interni di un'organizzazione. Tutto questo per ottenere una maggior miglioramento del sistema e di tutti i dispositivi che operano all'interno dell'organizzazione. Al contrario, coloro che operano all'interno del Security Operation Center puntano a utilizzare le proprie competenze per salvaguardare l'organizzazione da quelli che possono essere minacce dovute a cybercriminali. Questo porta loro a dover sapere muoversi e cercare di capire come opera il mondo della criminalità informatica e soprattutto, capire se all'interno di un'organizzazione il personale interno può essere la causa scatenante di determinati problemi come, ad esempio, la diffusione di dati sensibili interni dell'organizzazione che possono mettere in pericolo non solo l'organizzazione ma anche gli utenti stessi. È per questo che entrano in gioco gli operatori del SOC, per garantire che l'organizzazione sotto l'aspetto della cybersecurity sia abbastanza solida per poter contrastare le minacce, ma anche a mettere atto misure che portino ad una strategia di difesa che metta in guardia l'organizzazione già prima che la minaccia si sia consolidata. Il far sì che si cerchi di creare una strategia che miri a prevenire richiama anche un processo molto importante che è quello dell'*hardening*. Esso "non è soltanto una misura di difesa reattiva, ma una strategia preventiva che mira a ridurre le opportunità

per gli attaccanti di penetrare nei sistemi[40]". Mettere in atto strategie che possano mettere al riparo non soltanto i dati ma anche gli utenti, può portare a creare delle misure di sicurezza informatica più robuste. Per questo le organizzazioni che utilizzano mezzi come l'hardening, possono portare a riuscire a gestire un attacco in maniera più efficiente rispetto ad altri mezzi meno avanzati che possono portare a una minore presa d'azione della minaccia e delle sue conseguenze. Il SOC si occupa proprio di questo, di garantire una maggiore sicurezza dei sistemi implementando misure che siano preventive al danno e ottimizzare sempre di più la loro struttura, rendendo l'organizzazione più solida da un punto di vista di cybersecurity. Questi due modelli, implementati all'interno di un'organizzazione, porta ad avere un funzionamento delle reti e una risoluzione dei problemi interni solo grazie all'intervento di entrambi i centri operativi NOC e SOC che può avvenire in maniera più efficiente attraverso una loro cooperazione, per avere un risultato ottimale in termini di sicurezza e soprattutto reazioni tempestive di fronte ad eventuali crisi. Inoltre, questi due centri operativi per continuare a dare una notevole sicurezza alle organizzazioni e contemporaneamente far sì che ci sia un miglioramento sul lato della capacità operativa, ha bisogno di rafforzare la collaborazione su alcuni punti comuni, come ad esempio l'attività di controllo e segnalazione di determinati problemi che possono causare seri danni all'organizzazione. Per questo motivo, i due centri operativi devono collaborare in stretta sinergia nella gestione delle segnalazioni di potenziali minacce che si manifestano come interferenze nella rete, così da garantire una piena consapevolezza dell'intera infrastruttura e delle vulnerabilità che la caratterizzano. Avere delle strategie che possano portare a una migliore difesa da parte delle organizzazioni, porta ad avere ottimali controrisposte a determinati incidenti di sicurezza. Ecco che molto spesso si parla di *incident response* all'interno delle organizzazioni, perché sempre di più si ha bisogno che le organizzazioni attuano delle strategie difensive che possano innanzitutto individuare le probabili minacce e poi rispondere bene a quelle che possono essere le conseguenze di un evento dannoso. Infatti, l'incident response è uno dei processi fondamentali all'interno delle organizzazioni, ed è per questo che avere gli strumenti necessari, come anche un gruppo di lavoro adeguato, può portare ad una maggiore capacità nell'affrontare e sostenere gli effetti di eventuali incidenti nel contesto della cybersecurity. Non si potranno sicuramente evitare che le minacce incombano, ma si può far in modo che le conseguenze degli effetti siano meno disastrosi, riducendo al minimo i danni operativi, danni economici e soprattutto i danni all'immagine che potrebbero creare all'intera organizzazione. I vantaggi del pianificare un incident response plan all'interno di un'organizzazione è riscontrare immediatamente

[40] **REDAZIONE RHC**, *Che cos'è l'Hardening: Alla scoperta di una strategia preventiva per la mitigazione delle minacce,* 2024, https://www.redhotcyber.com/post/che-cose-lhardening-alla-scoperta-di-una-strategia-preventiva-per-la-mitigazione-delle-minacce/

i segnali di un attacco hacker e far sì che il team interno metta in pratica tutte le azioni adeguate a contenere il danno. Un team interno solido e ben preparato può essere un'ottima occasione per ridurre significativamente gli impatti derivanti da eventi imprevisti. Esso, inoltre, permette una gestione tempestiva degli eventi, evitando che l'organizzazione debba ricorrere ad altri piani molto più articolati e onerosi. Ovviamente bisogna che ci sia una comunicazione efficace tra i diversi settori dell'organizzazione, proprio per essere compatti nel garantire una risposta rapida ed efficace. In molti casi la pesantezza della minaccia può portare l'organizzazione a non essere abbastanza rapida nel gestire l'evento critico. Per questo è importante trasmettere le informazioni essenziali ai team incaricati di intervenire in caso di emergenza, per contribuire alla risoluzione dell'incidente. Queste informazioni devono essere chiare, strutturate e precise, affinché la trasmissione avvenga in modo corretto ed efficace. Infine, per avere un completo rispetto delle normative e dei regolamenti viene ormai richiesto alle organizzazioni l'utilizzo dello strumento del incident response plan, proprio per dare prova di quelle che sono le azioni che l'organizzazione attuerà per contrastare ipotetiche minacce. Molto spesso l'incident response può risultare per molte organizzazioni un investimento molto costoso e anche non necessario, ma bisogna pensare ai danni che può comportare una determinata minaccia che potrebbero causare danni ancora più irreparabili e soprattutto ancora più costosi. Ritornando ai due strumenti operativi, giocano un ruolo importante all'interno dell'incident response, proprio perché il SOC e in grado di gestire e individuare le minacce che possono essere causa di attacchi da parte di cybercriminali; mentre il NOC si concentra su quelle che sono le anomalie o malfunzionamenti della rete. La sinergia tra i due team, attraverso una comunicazione efficace e una stretta collaborazione, consente di affrontare gli incidenti in modo più rapido ed efficiente, minimizzando l'impatto complessivo. Questi servizi, in termini di sicurezza informatica, permettono anche alle organizzazioni prive di competenze in questo ambito, di poter avere un elevato grado di efficienza a livello operativo. Essi danno la possibilità rispetto a coloro che si trovano sprovvisti di determinati strumenti come il SOC e il NOC di contribuire a ridurre significativamente i rischi di attacchi informatici e di perdita di dati, offrendo soluzioni avanzate e supporto esperto. Infatti, entrambi gli strumenti sono un ottimo incentivo per migliorare le capacità e la gestione dei processi interni. La crescente digitalizzazione sta portando sempre di più le organizzazioni a doversi mettere al riparo dai continui attacchi da parte di cybercriminali che non risparmiano nemmeno le piccole organizzazioni. Per questo ogni dispositivo o database ha bisogno di essere presa in carico dal SOC e dal NOC affinché non siano soggetti ad attacchi di questo tipo. Inoltre, affidarsi ad esperti esterni può portare a non dover sostenere costi interni, per far sì che il personale interno possa acquisire ulteriori competenze tipiche di un esperto SOC e NOC. Oggi con la crescente digitalizzazione e con i milioni di dati che le organizzazioni hanno a che fare, affidarsi ad esperti esterni SOC e NOC può

portare a ridurre ancora di più la perdita e la diffusione illecita di questi dati. Per questo affidarsi a esperti di SOC e NOC può quindi rappresentare un valore aggiunto strategico per le organizzazioni moderne, facilitando una crescita sicura in un contesto in cui le minacce informatiche sono sempre dietro l'angolo e dove l'operatività delle organizzazioni sono sempre più a rischio. Potremmo affermare che è estremamente vantaggioso nella società moderna l'utilizzo di questi strumenti, per migliorare sempre di più nelle organizzazioni la possibilità di rilevare minacce alla sicurezza e di evitare che l'operatività di una determinata organizzazione sia compromessa. Investire nella Security Operation Center e nel Network Operations Center risulta cruciale, perché le conseguenze in ambito legale, economico e reputazionale di un determinata minaccia non possono essere sottovalutate. Potenziare maggiormente la capacità di difesa dell'organizzazione e monitorare l'operatività della rete, migliora la prontezza nella risposta alle minacce da parte di hacker che tentano di mettere sottosopra l'intero sistema operativo e, allo stesso tempo, rappresenta una strategia fondamentale per la crescita aziendale. In definitiva, il NOC e il SOC costituiscono la soluzione ideale per affrontare le sfide che ogni giorno deve affrontare la cybersecurity, offrendo una protezione completa e integrata che sappia rispondere alle esigenze di una società sempre più digitalizzata e in continua trasformazione.

III. NORMATIVE PER LA PROTEZIONE DEI DATI: STRATEGIE E BEST PRACTICE NELLA GESTIONE DELLA CYBERSECURITY

1. PRINCIPI FONDAMENTALI DEL GDPR SULLA PROTEZIONE DEI DATI

Nella società odierna, il web è spesso definito la "miniera d'oro" dell'era digitale, grazie all'enorme valore custodito nei dati. Coloro che possiedono la capacità di estrapolare informazioni rilevanti da queste risorse detengono un potente strumento per comprendere e influenzare il mondo in cui viviamo. Quando analizzati con precisione e combinati in modo strategico, i dati possono generare conoscenze di straordinario valore, con ricadute significative in ambiti come la ricerca, l'innovazione, il business e persino la formulazione di politiche strategiche. Un esempio significativo è rappresentato dalla pandemia di COVID-19 nel 2020, durante la quale le decisioni sanitarie sono state fortemente guidate dall'analisi dei dati. Informazioni come l'andamento dei contagi o i tassi di occupazione ospedaliera si sono dimostrate fondamentali per gestire con efficacia l'emergenza sanitaria, evidenziando il ruolo cruciale dei dati in situazioni di crisi globale. Tuttavia, dati di questa

natura, essendo altamente sensibili, devono essere protetti da usi impropri o divulgazioni non autorizzate. In un contesto sempre più digitale, in cui i dati personali assumono un valore crescente sia per le aziende sia per i malintenzionati, la loro protezione è essenziale. Per evitare che queste informazioni finiscano nelle mani sbagliate, la loro gestione è regolamentata da normative che stabiliscono le modalità corrette per la raccolta, la conservazione, l'elaborazione e la condivisione dei dati personali. Questi regolamenti hanno l'obiettivo di salvaguardare i diritti degli individui, assicurando un trattamento dei dati responsabile e trasparente. Nell'Unione Europea, la normativa di riferimento per la protezione dei dati personali è il *Regolamento Generale sulla Protezione dei Dati (GDPR)*. Ma prima di parlare di come si articola il GDPR bisogna fare un passo indietro e capire come si è iniziato a parlare di questo Regolamento così importante e soprattutto quale è stato il percorso che ha condotto all'adozione del GDPR. Per fare questo bisogna che sia chiaro la distinzione tra due concetti che sono essenziali l'uno per l'altro: la concezione di privacy e la concezione di protezione dei dati. Innanzitutto, la distinzione tra tutela dei dati personali e diritto alla privacy risale al 1890 da due giuristi di Boston, Samuel Warren e Louis Brandeis che delinearono i principi legati alla privacy. In quell'epoca si iniziò a discutere del tema della privacy in risposta alla diffusione illecita di fotografie scattate durante eventi privati, poi pubblicate senza autorizzazione sulla stampa locale. Questi scatti, spesso relativi a feste private, erano accompagnati da dettagli personali sui soggetti ritratti, configurando una chiara violazione della riservatezza. Tale fenomeno evidenziò l'urgenza di introdurre una tutela giuridica per porre fine a queste pratiche lesive. Per contrastare questo fenomeno, Warren e Brandeis pubblicarono un articolo intitolato "*The Right to Privacy*", in cui definirono la privacy come il diritto di essere lasciati in pace e di tutelare la propria sfera personale. I due autori sottolinearono come la divulgazione di informazioni relative a momenti privati potesse causare danni morali, generando un disagio emotivo che influiva profondamente sia sui rapporti interpersonali che sulle attività economiche. L'Europa abbraccia il concetto di privacy proprio con due norme che trattano proprio l'importanza della sfera intima di ogni individuo: *l'articolo 2 della Costituzione Italiana del 1947* che dichiara che "la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale[41]"; l'altro articolo fondamentale è *l'articolo 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU)* del 1950 che cita testualmente che "ogni persona ha diritto al rispetto della sua

[41] **GOVERNO ITALIANO PRESIDENZA DEL CONSIGLIO DEI MINISTRI**, *principi fondamentali*, https://www.governo.it/it/costituzione-italiana/principi-fondamentali/2839#:~:text=limiti%20della%20Costituzione.-,Art.,solidariet%C3%A0%20politica%2C%20economica%20e%20sociale.

vita privata e familiare, del suo domicilio e della sua corrispondenza[42]". Nel 1978 la Germania federale emanava la prima legge che riguardava la protezione dei dati proprio per rispondere alle minacce che la dittatura di quel periodo comportava, soprattutto la possibilità che attraverso l'utilizzo delle informazioni personali del popolo tedesco lo Stato cerchi di rafforzare ancora di più il suo potere autoritario. Due anni dopo un altro documento che sancì il rispetto della vita privata del singolo fu la Convenzione 108 che mirava a tutelare le persone in seguito alla diffusione delle tecnologie che iniziarono a diffondersi a partire dagli anni '60. Questa Convenzione riguarda il trattamento dei dati personali in tutti le sfere, sia nel privato che nel pubblico. Infatti, *l'articolo 1 della Convenzione 108* dichiara che "lo scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano[43]". Nel 1992 con il *trattato di Maastricht* si arriva alla nascita ufficiale della Comunità Europea (CE). Questo trattato sanciva che il Parlamento europeo avrebbe ottenuto la facoltà di richiedere alla Commissione europea di avanzare una proposta legislativa su materie che considera meritevoli di un intervento normativo a livello comunitario. Inoltre, la Commissione nel suo insieme doveva essere approvata tramite il voto del Parlamento, rafforzandone il controllo politico. Inoltre, spettava al Parlamento il compito di designare il Mediatore europeo, incaricato di vigilare sulla correttezza amministrativa delle istituzioni dell'Unione. Il progresso rappresentato da questo trattato risultava insufficiente senza l'introduzione di una normativa europea che garantisse una protezione uniforme dei dati personali. Con l'istituzione dell'area Schengen, che promuoveva la libera circolazione dei cittadini tra i Paesi membri ampliando le libertà di movimento, si assicurava al contempo la sicurezza interna attraverso una gestione condivisa del controllo e della protezione delle frontiere esterne. Di conseguenza, era indispensabile consentire anche la libera circolazione dei dati, eliminando eventuali ostacoli che potessero limitarla. Per far sì che questo potesse accadere bisognava uniformare le normative sulla privacy a livello nazionale, in modo che non accadesse il paradosso di ritrovarsi da una parte Stati con leggi troppo tolleranti e dall'altra parte Stati con leggi estremamente restrittive. Proprio per evitare questo nel 1995 viene adottata la *Direttiva 95/46/CE* che puntava ad allineare le normative in materia di protezione dei dati personali, in modo da avere una tutela piena di uno dei diritti fondamentali del cittadino. La necessità di armonizzare le normative derivava dalla frammentazione delle leggi tra i vari Paesi

[42] **OFFICE ADVICE**, *art.8 – convenzione europea dei diritti dell'uomo (CEDU) diritto al rispetto della vita privata e familiare*, https://officeadvice.it/cedu/articolo-8/

[43] **SAETTA B**, *convenzione 108 del Consiglio d'Europa*, 2018, https://protezionedatipersonali.it/convenzione-108-consiglio-europa

membri dell'Unione, rendendo indispensabile un avvicinamento delle regolamentazioni nazionali, senza però compromettere la protezione dei diritti delle persone. In questo contesto, agli Stati membri veniva riconosciuta una limitata libertà di azione. La direttiva fu concepita con la consapevolezza che, all'epoca, non vi era ancora una piena comprensione dell'importanza della protezione dei dati, né le condizioni per introdurre una normativa unica valida per tutti gli Stati. La scelta di adottare una direttiva mirava a garantire che la protezione dei dati dei cittadini non fosse trascurata, fornendo al contempo obiettivi chiari da raggiungere. Questo approccio lasciava ai singoli legislatori nazionali la libertà di definire le proprie leggi in materia, adattandole alle specificità dei rispettivi contesti, pur rispettando le linee guida comuni stabilite a livello europeo. Nel 2007, il Trattato di Lisbona ha reso giuridicamente vincolante la *Carta dei diritti fondamentali*, che era stata proclamata a Nizza. Infatti, all'interno della Carta de diritti fondamentali troviamo, in riferimento alla protezione dei dati personali, *l'articolo 8* che cita testualmente che "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano[44]". Sarà proprio nel 2016 che si inserirà il regolamento generale per la protezione dei dati personali 2016/679, il *GDPR (General Data Protection Regulation)* che detta regole comuni a tutti e 27 membri dell'Unione Europea. Il regolamento è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 ed è entrato in vigore il 24 maggio dello stesso anno. Tuttavia, la sua applicazione pratica è stata differita di due anni, iniziando ufficialmente il 25 maggio 2018. Questo regolamento è composto da 99 articoli che definiscono le disposizioni giuridiche vincolanti e 173 Considerando che svolgono una funzione interpretativa, fornendo chiarimenti e linee guida per l'applicazione corretta delle norme contenute nel testo normativo. Il GDPR si occupa precisamente della "tutela diritti e le libertà fondamentali delle persone fisiche[45]"; mentre non si applica ai dati delle imprese, delle pubbliche amministrazioni, in generale a tutte quelle che il diritto chiama "persone giuridiche". Il GDPR identifica come dati personali "le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.[46]" Questa definizione ci richiama all'idea che i dati personali possono presentarsi in forme molto diverse, come un'immagine o un audio, un'informazione scritta o un codice identificativo; se sono riferibili direttamente o

[44] **FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS**, *carta dei diritti fondamentali dell'Unione Europea*, 2007, https://fra.europa.eu/it/eu-charter/article/8-protezione-dei-dati-di-carattere-personale#:~:text=1.,fondamento%20legittimo%20previsto%20dalla%20legge.

[45] **USERCENTRICS COOKIEBOT**, *cos'è il GDPR*, https://www.cookiebot.com/it/gdpr/

[46] **GDPR GARANTE PER LAPROTEZIONE DEI DATI PERSONALI**, *cosa intendiamo per dati personali?* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2002896#:~:text=Sono%20dati%20personali%20le%20informazioni,sua%20situazione%20economica%2C%20ecc.

indirettamente a una persona fisica vuol dire che sono dati personali e sono soggetti al GDPR. Non sono dati personali, e di conseguenza non sono soggetti al GDPR, i dati anonimi e i dati pseudonimizzati, cioè quelli che vengono resi anonimi in un secondo momento. Entrambi escludono che si possono risalire all'identità della persona interessata e perciò il GDPR non si applica. Il GDPR non tratta esplicitamente i dati anonimizzati, ma vengono richiamati nel *Considerando 26* il quale definisce che "principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca[47]". Un esempio di dati anonimi sono i dati statistici che molto spesso possono essere anonimi in partenza o anonimizzati in un secondo momento. Diversi dai dati anonimi sono i *dati pseudonimizzati*, che sono analizzati nel GDPR *all'art 4 comma 5* il quale considera "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile[48]". Essi se vengono presi da soli non consentono di risalire all'identità della persona, ma se vengono presi insieme ad altre informazioni allora consentono di risalire all'identità di quella determinata persona, ad esempio è possibile l'associazione di un codice identificativo a dei clienti per proteggerne l'identità, mentre se si associa quel codice identificativo ad altre informazioni come la data di nascita, il sesso in quel caso è possibile risalire all'identità. Per questo se vengono presi insieme ad altre informazioni possono essere considerati dati personali a tutti gli effetti e quindi essere soggetti al controllo del GDPR. I dati personali si dividono in due gruppi: i *dati comuni*; quindi, quelli che permettono l'attribuzione diretta ad un soggetto come il nome e il cognome; o che permettono un'attribuzione indiretta come ad esempio, i dati anagrafici, il codice fiscale, la residenza; nel secondo gruppo troviamo quelli che il GDPR chiama *categoria particolari di dati*, chiamati così perché riguardano aspetti intimi e personali della vita di una persona fisica. Essi riguardano l'origine razziale o etnica, l'orientamento sessuale, le opinioni politiche o i nostri eventuali

[47]**COLLINI M**, *Anonimizzazione dei dati personali: un percorso per orientarsi*, 2021, https://privacygdpr.it/news-privacy-sanita/anonimizzazione-dei-dati-personali-un-percorso-per-orientarsi/#:~:text=Per%20essere%20pi%C3%B9%20precisi%2C%20il,riferiscono%20a%20una%20persona%20fisica

[48]**ACCADEMIA ITALIANA PRIVACY**, *Sicurezza dei dati: pseudonimizzazione o anonimizzazione?* 2022, https://www.accademiaitalianaprivacy.it/dettaglioNews.asp?id=646#:~:text=Il%20dato%20anonimo%20non%20%C3%A8%20definito%20nel%20GDPR&text=%E2%80%9Cdecifratura%20non%20autorizzata%20della%20pseudonimizzazione,possibile%20%E2%80%9Criaccoppiare%E2%80%9D%20le%20informazioni.

trascorsi giudiziari. Inoltre, rientrano nella categoria particolari di dati i dati genetici e i dati biometrici che identificano in modo univoco la nostra persona. Per dati biometrici intendiamo ad esempio, l'impronta digitale che utilizziamo per sbloccare lo smartphone o semplicemente il riconoscimento facciale. L'importanza nel distinguere i dati comuni dalle categorie particolari di dati sta nel fatto che nella seconda categoria il GDPR impone che questi dati non possono essere utilizzati a meno che non ci sia delle eccezioni come il consenso esplicito da parte dell'interessato. Il GDPR intende tutelare tutti questi dati che riguardano gli interessati, facendo sì che vengano salvaguardati quei diritti e quelle libertà essenziali che li riguardano. Inoltre, questo comporta un ambiente più fiducioso perché permette un pieno sviluppo dei mercati attraverso una libera circolazione dei dati. Per questo bisogna che ci sia una particolare attenzione all'importanza di comprendere e applicare la disciplina stabilita dal GDPR in maniera consona da parte dei soggetti coinvolti, e cioè da parte del *titolare del trattamento* che secondo *la legge n. 675/1996 all'articolo 4, par. 1, n. 1* "è la persona fisica o giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le scelte di fondo sulle finalità e sulle modalità del trattamento dei dati, anche per ciò che riguarda la sicurezza[49]"; ma non solo, anche da parte del *responsabile del trattamento* che nel GDPR è disciplinato *all'articolo 4. par. 1, n.8* che definisce il responsabile del trattamento come "la persona fisica, giuridica, PA o ente che elabora i dati personali per conto del titolare del trattamento[50]". Infine, un'ultima figura che deve essere sottostare alla disciplina del GDPR è *l'interessato,* la cui definizione viene disciplinata nel GDPR all'articolo 4, par. 1, n. 1 dove dichiara che esso "è la persona fisica alla quale si riferiscono i dati personali[51]". Spesso gli utenti non percepiscono pienamente le conseguenze legate all'utilizzo di dispositivi connessi a Internet, soprattutto in termini di sicurezza e privacy dei propri dati personali. Infatti, in tali situazioni, interviene *l'Autorità di controllo*, incaricata di gestire le segnalazioni ricevute e di vigilare sulle violazioni del Regolamento Europeo e delle leggi nazionali sulla protezione dei dati. Tuttavia, la sua competenza è limitata ai casi che coinvolgono uno stabilimento situato nel territorio del proprio Stato membro o che abbiano un impatto rilevante esclusivamente sui cittadini di quello Stato. Ad esempio, in Italia il ruolo di Autorità di controllo viene

[49] **GDPR GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**, *Titolare, responsabile e incaricato - Individuazione del 'titolare del trattamento'*, 1997, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30915#:~:text=675%2F1996%2C%20il%20%22titolare,ci%C3%B2%20che%20riguarda%20la%20sicurezza.

[50] **PONTI C**, *Responsabile del trattamento, chi è e cosa fa: tutto quello che c'è da sapere*, 2022, https://www.agendadigitale.eu/sicurezza/privacy/responsabile-del-trattamento-chi-e-e-cosa-fa-tutto-quello-che-ce-da-sapere/

[51] **GDPR GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**, *Cosa intendiamo per dati personali?*, https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali#:~:text=Interessato%20%C3%A8%20la%20persona%20fisica,Regolamento%20UE%202016%2F679)%3B

svolta dal Garante per la protezione dei dati personali. Inoltre, Il GDPR assegna ad essa anche il compito di sensibilizzare e informare il pubblico sui pericoli connessi al trattamento dei dati personali. È fondamentale, secondo il GDPR, che l'Autorità di controllo assicuri che l'interessato sia pienamente consapevole dei potenziali rischi legati al trattamento dei dati personali, delle normative da rispettare, nonché delle tutele e dei diritti che gli spettano. Oltretutto, il GDPR ritiene che l'attenzione non debba essere posta soltanto dagli interessati, ma anche dai responsabili del trattamento affinché possano comprendere l'importanza del rispetto degli obblighi imposti dal Regolamento stesso. Proprio per far sì che avvenga il rispetto del trattamento dei dati personali il GDPR ha stabilito dei principi fondamentali che ritroviamo all'articolo *5 del Regolamento*. Al *paragrafo n.1, lettera a*., del seguente articolo troviamo il primo principio che riguarda *la liceità, la correttezza e la trasparenza* del trattamento dei dati personali. Per questo il GDPR stabilisce che "i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato[52]". Questo significa che non basta trattare i dati ma deve essere fatto in maniera lecita, corretta e trasparente. Il GDPR garantisce così che la raccolta dei dati personali degli utenti avvenga in maniera conforme alla legge e trasparente nei confronti degli interessati, evitando qualsiasi forma di omissione. I dati personali di un individuo possono essere trattati esclusivamente se il trattamento è legittimo, ovvero fondato sul consenso dell'interessato, necessario per l'esecuzione di un contratto, o supportato da un'altra delle basi giuridiche previste *dall'articolo 6 del GDPR. Il consenso* costituisce una delle possibili basi legittime per il trattamento dei dati. Esso non può essere un consenso generale ma bensì deve essere specifico, ossia riferito a una finalità ben definita. Proprio perché deve essere un consenso specifico il titolare del trattamento è tenuto a fornire un'adeguata informativa e garantire il diritto alla portabilità dei dati. Oltre al consenso troviamo altre basi giuridiche stabilite dall'articolo 6 tra cui *l'adempimento di un contratto o esecuzione di misure precontrattuali* che rendono lecito il trattamento dei dati. Questa base giuridica può essere utilizzata solo per trattamenti strettamente necessari all'esecuzione del contratto. Infatti, la necessità del trattamento è giustificata solo se il contratto non può essere completamente adempiuto senza l'utilizzo dei dati personali. Un'altra base giuridica definita dall'articolo 6 è *l'obbligo legale*. Esso presenta però delle condizioni come, ad esempio, che l'obbligo legale per il trattamento dei dati personali deve essere stabilito da una norma giuridica, che può essere di origine europea o nazionale, applicabile allo Stato membro in cui opera il titolare del trattamento; non solo, un'altra condizione è che le disposizioni legali devono prevedere un obbligo vincolante per il trattamento dei dati personali, chiaramente definito e preciso. Inoltre,

[52] **ALTALEX**, *Art. 5 GDPR - Principi applicabili al trattamento di dati personali*, 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-5-gdpr-principi-trattamento-di-dati-personali

devono almeno essere specificate le finalità per le quali i dati devono essere trattati, ed infine, come ultima condizione che rendono applicabile come base giuridica l'obbligo legale è quello che l'obbligo deve essere imposto al titolare del trattamento, e non agli interessati i cui dati vengono trattati. Il trattamento dei dati personali è consentito se come base giuridica si ha *l'interesse vitale* della persona interessata o di altre persone. Nasce così come una delle basi giuridiche il bisogno di proteggere gli interessi vitali dei singoli. Un esempio potrebbe essere il caso di un bambino che si perde in un centro commerciale: in questa situazione, i dati del minore possono essere trattati (ad esempio, attraverso l'annuncio del suo nome tramite il sistema di altoparlanti) per garantire la sua sicurezza e il suo ricongiungimento con i genitori. In questo caso, il trattamento dei dati personali si basa su una giustificazione legale che impone che l'elaborazione dei dati sia necessaria per proteggere la vita o la sicurezza dell'interessato, qualora non siano disponibili altre basi giuridiche applicabili. Inoltre, questa base giuridica non prevede il consenso dell'interessato se non è richiesto, soprattutto quando questi non è in grado di fornirlo come nel caso del minore. La quinta base giuridica prevista dall'articolo 6 del GDPR è il *legittimo interesse* del titolare o di soggetti terzi destinatari dei dati. L'interesse nel contesto del trattamento dei dati personali rappresenta il privilegio o l'obiettivo che il titolare del trattamento intende ottenere attraverso l'elaborazione delle informazioni relative agli interessati. Questo interesse, per essere considerato valido, deve rispettare una serie di criteri che ne garantiscono la conformità alle normative e il bilanciamento rispetto ai diritti fondamentali degli interessati. L'interesse affrontato dal GDPR deve essere un interesse *lecito* e questo comporta che il trattamento dei dati personali non può andare contro alle norme stabilite dalla legge, come ad esempio attività illecite o violazioni delle persone coinvolte. Dopodiché l'interesse deve essere un interesse *chiaro* e *specifico* e quindi deve essere un interesse che deve essere descritto in modo dettagliato e non in maniera generale. Proprio per valutare se l'interesse legittimo perseguito sia prevalente rispetto agli interessi o ai diritti fondamentali della persona interessata, viene eseguito il cosiddetto *balancing test.* Questo test di bilanciamento degli interessi è un passaggio imprescindibile per poter utilizzare il legittimo interesse per il trattamento dei dati personali. Infatti, l'obiettivo di questo test è verificare che quel determinato interesse legittimo può essere considerato idoneo ad essere utilizzato come condizione di liceità in base alle finalità specifiche di ogni trattamento. Il legittimo interesse previsto dal GDPR può essere utilizzato come base giuridica autonoma solo se il test di bilanciamento produce un esito favorevole. Nel caso in cui produce un esito negativo vuol dire che l'interesse del titolare risulta predominante e quindi il trattamento non è consentito; mentre se l'esito risulta favorevole vuol dire che invece risulta predominante l'interesse del titolare del trattamento e può essere legittimamente effettuato anche senza il consenso dell'interessato senza fare riferimento ad altre basi di liceità previste dall'articolo 6 del Regolamento. L'ultima base giuridica prevista dall'articolo 6 del

GDPR riguarda lo *svolgimento di un'attività di interesse pubblico o legata all'esercizio di autorità pubblica.* La norma riguarda l'interesse pubblico dell'Unione Europea o di uno Stato membro. Il termine "pubblici poteri" si riferisce a un mandato assegnato dall'Unione Europea o da uno Stato membro, escludendo quindi i compiti conferiti da legislazioni estere che non rientrano nell'ambito di applicazione di questa disposizione. I pubblici poteri o i compiti di interesse pubblico devono essere attribuiti da normative ordinarie o da altre fonti giuridiche ufficiali. Inoltre, la norma deve specificare con chiarezza il tipo di trattamento consentito. Per avvalersi di questa base giuridica, è necessario che il trattamento sia strettamente legato all'esecuzione del compito attribuito. Il secondo principio che troviamo alla lettera b. dell'articolo 5 riguarda la *limitazione delle finalità*. Il GDPR punta a sottolineare un elemento importante alla lettera b., e cioè quello che non è concesso utilizzare finalità diverse da quelle prestabilite. Infatti, esso dichiara che i dati personali sono "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali[53]". Le finalità prescritte devono essere rispettate fino all'ultimo e non è possibile trattare dati di cui si è in possesso per fini diversi da quelli stabiliti inizialmente. Nel caso ci fossero dei cambiamenti delle finalità, in quel caso bisogna che ci sia un ulteriore consenso da parte dell'interessato. Inoltre, l'articolo dichiara che è permesso effettuare un trattamento ulteriore dei dati raccolti, senza richiedere un nuovo consenso, purché le finalità siano compatibili con quelle originarie. Queste finalità che non hanno bisogno di un ulteriore consenso sono: *l'archiviazione per interesse pubblico* ed è la prima finalità citata che riguarda il preservare di quei dati che servono per tutelare la memoria collettiva, il salvaguardare documenti di interesse sociale o mantenere informazioni rilevanti per la comunità; *ricerca scientifica e storica* che riguarda l'utilizzo di dati per studi che contribuiscono al progresso della conoscenza o alla comprensione del passato; e infine, *fini statistici* e cioè l'analisi dei dati in forma aggregata per ottenere informazioni generali o trend utili per decisioni politiche, economiche o sociali. Il secondo principio fondamentale stabilito dal GDPR sulla protezione dei dati all'articolo 5 paragrafo 1, lettera c. è *la minimizzazione dei dati.* Esso stabilisce che i dati personali devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati[54]". L'importanza della limitazione dei dati e

[53] **GDPR TEXT**, *Articolo 5 RGPD. Principi applicabili al trattamento di dati personali*, https://gdpr-text.com/it/read/article-5/#:~:text=or%20statistical%20purposes-,1.,in%20conformit%C3%A0%20del%20presente%20regolamento

[54] **MAMMOLI A**, *Cosa significa il principio di minimizzazione nel GDPR?*, 2023, https://accademiaitalianaprivacy.it/dettaglioNews.asp?id=764#:~:text=Cosa%20significa%20il%20principio%20di%20minimizzazione%20nel%20GDPR%3F&text=Ci%C3%B2%20comporta%20che%20i%20titolari,necessario%20per%20raggiungere%20tale%20scopo.

la loro conservazione a quanto è necessario per le finalità stabilite dal trattamento sono ciò che definisce il principio di minimizzazione. Il GDPR, a tal proposito, stabilisce all'articolo 5, lettera c, che coloro che trattano i dati non possono raccogliere informazioni personali che risultino eccessive o non pertinenti rispetto alle finalità per le quali sono stati raccolti. Inoltre, il principio di minimizzazione permette che quei dati raccolti siano corretti aggiornati e sicuri attraverso l'utilizzo di misure di sicurezza che permettano che non ci siano intrusioni non autorizzate, perdite di dati e usi indebiti. Questo principio comporta che c'è un voler avere un pieno controllo del GDPR sulla gestione dei dati e che prevalga sempre il rispetto per quelli che sono i diritti alla privacy delle persone coinvolte. L'obiettivo diventa quello di avere un trattamento dei dati condotto in maniera proporzionata, trasparente e sicura evitando qualsiasi violazione dei diritti fondamentali dei soggetti coinvolti. Un esempio pratico del principio di minimizzazione dei dati può essere il caso di una registrazione a un servizio online, come un sito e-commerce. L'utente che decide di creare un account per acquistare un prodotto dovrà fornire al sito, nel rispetto sempre del principio di minimizzazione dei dati, solo le informazioni strettamente necessarie per completare l'operazione, né più né meno. Le informazioni che verrebbero richieste sono ad esempio il nome e il cognome per l'identificazione e la spedizione del prodotto; dopodiché verrebbe richiesto l'indirizzo di consegna per recapitare il prodotto e l'indirizzo e-mail per ulteriori comunicazioni relative all'ordine; infine, un'ultima informazione che verrebbe richiesta è il metodo di pagamento e quindi ad esempio i dati della carta o un collegamento a un portafoglio digitale. Le informazioni che non hanno bisogno di essere necessariamente richieste sono ad esempio il numero di telefono, se non strettamente necessario per la consegna; oppure la data di nascita, sempre se non è rilevante per l'acquisto o per verificare un requisito di età, come accade per l'acquisto di alcolici dove è necessario fornire l'età e dichiarare di essere maggiorenni; un'altra categoria di informazioni che non devono essere richieste sono tutte quelle informazioni che riguardano la sfera personale come il titolo di studio, la professione, l'orientamento sessuale che sarebbero informazioni superflue per le finalità dichiarate. In conformità con il principio di minimizzazione dei dati previsto dall'articolo 5, lettera c, del GDPR, il sito non conserverà i dati di pagamento oltre il tempo necessario per completare l'acquisto, salvo che l'utente non autorizzi esplicitamente la conservazione dei dati della propria carta di credito per acquisti futuri. Inoltre, una volta raggiunte le finalità per cui i dati sono stati raccolti, essi saranno eliminati e non utilizzati per altri scopi, oppure resi anonimi. Ad esempio, nel caso di un acquisto su un e-commerce, ciò avviene dopo la consegna del prodotto e la gestione di eventuali resi. Quest'esempio dimostra come nel principio di minimizzazione tutto gira intorno alle finalità stabilite dal trattamento e tutto

quello che non è necessario non ha bisogno di essere fornito dall'interessato. Ovviamente non tutti i casi sono uguali, ogni caso necessita di determinate informazioni rispetto ad altre, come ad esempio dell'acquisto di alcolici che l'età è un'informazione obbligatoria rispetto all'acquisto di un indumento che non lo necessita. L'approccio principale deve essere sempre quello di rispettare la minimizzazione dei dati, limitando la raccolta e il trattamento dei dati personali a ciò che è strettamente necessario. Un ulteriore principio considerato fondamentale per il trattamento dei dati personali che è rappresentato dalla lettera d., dell'articolo 5 del GDPR è *l'esattezza.* Infatti, l'articolo cita che i dati personali devono essere "esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati[55]". Questo significa che chi tratta i dati personali di un soggetto deve fare di tutto perchè questi possano essere considerati precisi e aggiornati. Infatti, ciò implica che questi dati trattati debbano riflettere fedelmente la realtà e contemporaneamente devono essere mantenuti aggiornati, qualora fosse necessario farlo, per garantire che rimangano rilevanti e corretti rispetto agli scopi per cui vengono utilizzati. Le informazioni devono essere raccolte e gestite in maniera non obsoleta, errata o incompleta e questo può avvenire attraverso un'accurata analisi da parte del titolare del trattamento. Questa responsabilità porta il titolare del trattamento a intraprendere tutte le misure ragionevoli per individuare e correggere eventuali imprecisioni, o per eliminare i dati che non risultano più conformi agli obiettivi prefissati. Questo principio non si limita a una mera questione tecnica o formale, ma ha implicazioni dirette sulla tutela dei diritti degli interessati. Dati imprecisi o non aggiornati possono infatti comportare rischi significativi, come decisioni errate basate su informazioni errate, con conseguenti danni economici, morali o reputazionali per le persone coinvolte. A questo proposito il GDPR pone attenzione al principio di esattezza attraverso anche altri due articoli e cioè l'articolo 16 e l'articolo 18. L'articolo 16 tratta quello che è il *diritto di rettifica:* "l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa[56]". Questo articolo permette agli interessati di avere il diritto alla rettifica così come anche il *diritto all'oblio*, richiamato dall'articolo 17 del GDPR e cioè la cancellazione dei dati e la cessazione del trattamento quando questi non risultano più pertinenti alle finalità per le quali erano

[55] **PRIVAZY PLAN**, *art 5 "principi applicabili al trattamento dei dati personali*, https://www.privacy-regulation.eu/it/5.htm

[56] **PRIVAZY PLAN**, *art 16 "diritto di rettifica"*, https://www.privacy-regulation.eu/it/16.htm#:~:text=EU%20RGPD,%22Diritto%20di%20rettifica%22&text=L'interessato%20ha%20il%20diritto,lo%20riguardano%20senza%20ingiustificato%20ritardo.

stati inizialmente raccolti o utilizzati. Infatti, l'articolo 17 cita testualmente che "l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali[57]". L'articolo 16 e l'articolo 17 dimostrano come il diritto alla rettifica e il diritto all'oblio sono strumenti chiave per tutelare la dignità e la privacy degli interessati, pur bilanciandosi con altri diritti e obblighi di rilevanza pubblica o giuridica. Tutto ciò per dire che il principio di esattezza non tocca soltanto questioni tecnica o formale, ma bensì va a toccare direttamente la tutela dei diritti degli interessati. I rischi che possono comportare il trattamento di dati imprecisi o non aggiornati sono molteplici, come ad esempio decisioni errate basate su informazioni errate che comportano così danni economici, morali o reputazionali per le persone coinvolte. Un esempio pratico del principio di esattezza lo troviamo nel caso di un cliente che cambia indirizzo di residenza e comunica la modifica all'azienda. In questo caso, è responsabilità del titolare del trattamento aggiornare tempestivamente il database per evitare l'invio di fatture o comunicazioni all'indirizzo errato. Se l'azienda non aggiornasse le informazioni in questione, potrebbe inviare documenti riservati a terzi, violando la privacy del cliente e compromettendo la conformità al GDPR. L'importanza del principio di esattezza dei dati non sta solo nel rispetto delle normative, ma anche nel prevenire errori che potrebbero causare danni agli interessati o all'organizzazione stessa. Alla lettera e., dell'articolo 5 del GDPR troviamo il quinto principio fondamentale per trattare i dati personali ed è *la limitazione della conservazione*. La limitazione della conservazione viene citata dall'articolo dichiarando che i dati devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato[58]". La conservazione dei dati, quindi, non è soggetta a parametri fissi in termini di durata, ma dipende dalle finalità specifiche per le quali è necessario conservare determinati dati, rispetto ad altri. Ogni trattamento ha delle specifiche finalità che a sua volta hanno delle tempistiche di conservazione che varia dal trattamento stesso. Ad esempio, nel caso in cui un'azienda raccolga dati dai curriculum dei candidati durante un processo di selezione, una volta concluso il processo l'azienda procederà ad assumere alcuni candidati, escludendone altri. I dati di coloro che vengono

[57] **PRIVAZY PLAN**, *art 17 "diritto alla cancellazione",* https://www.privacy-regulation.eu/it/17.htm

[58] **PRIVAZY PLAN**, *art 5 "Principi applicabili al trattamento di dati personali", https://www.privacy-regulation.eu/it/5.htm*

scartati, non avendo più una finalità immediata per il trattamento dei loro dati, non verranno conservati. Nel rispetto del principio della limitazione della conservazione l'azienda in questo contesto conserverà i dati del candidato assunto solo per la gestione del rapporto di lavoro, come ad esempio contratti, buste paghe o comunicazioni in generale. I dati dei candidati che sono stati scartati devono essere cancellati entro un tempo prestabilito, eccetto che l'azienda non abbia ottenuto dal candidato il consenso esplicito a conservare i propri dati per un periodo più lungo, ad esempio per eventuali future opportunità lavorative. Ovviamente questo è uno dei tanti esempi per cui possano essere conservati i dati personali più a lungo; infatti, vengono richiamati nell'articolo motivi di interesse storico, pubblico o scientifico. In questi casi bisognerà che i dati siano adeguatamente protetti attraverso misure come l'anonimizzazione. Se prendiamo l'esempio dei dati sanitari che vengono raccolti e conservati durante il trattamento di cura vediamo che una volta concluso il processo di cura l'ospedale non ha bisogno di conservare quei dati per altro tempo, eccetto per finalità di ricerca come, ad esempio, per lo studio dell'evoluzione di una determinata malattia. In questo caso il GDPR stabilisce che queste informazioni trattenute per finalità scientifica vengano anonimizzate, eliminando qualsiasi informazione che possa ricondurre ai pazienti come, ad esempio, il nome o il numero di telefono. Nel caso in cui non possano essere anonimizzati e bene far sì che essi vengano in qualche modo crittografati per impedire accessi non autorizzati. Tutto questo deve essere effettuato con tutte le garanzie necessarie per tutelare i diritti e la privacy degli interessati. L'ultimo principio stabilito dalla lettera f., dell'articolo 5 riguarda *il principio di integrità e riservatezza.* Esso stabilisce che i dati devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali[59]". Questo principio intende garantire un livello di sicurezza in base al rischio, facendo sì che vengano implementate misure adeguate che possano proteggere i dati da accessi non autorizzati, dalla perdita dalla distruzione o danni accidentali. Più alto è il rischio più devono essere efficaci le misure che servono per minimizzare i rischi. Non si tratta di una semplice salvaguardia di determinati dati, ma bensì un'integrazione di sistemi di protezione adeguati ad avere un ulteriore tutela nei confronti degli interessati. I principi appena descritti richiamano la predominanza del GDPR nel far sì che alla base di tutto deve esserci il rispetto dei dati personali dei soggetti coinvolti. I dati personali che sono proprietà degli interessati nel momento in cui permettono ai terzi di utilizzarli per determinate finalità non vuol dire che non siano più i titolari di quei dati, ma bensì continuano ad avere i pieni diritti sugli

[59] **ALTALEX**, *Art. 5 GDPR - Principi applicabili al trattamento di dati personali*, 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-5-gdpr-principi-trattamento-di-dati-personali

stessi. È compito di chi tratta i dati gestirli in maniera conforme al GDPR e sempre in maniera rispettosa dei diritti dell'interessato, ed è quello che è alla base del concetto del *principio di accountability.* Il principio di accountability o responsabilizzazione viene richiamato al paragrafo 2 dell'articolo 5 del GDPR che stabilisce che "il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo[60]". Infatti, non basta rispettare le norme stabilite dal GDPR, ma bisognerà provare di averle rispettate. Si tratta di un approccio proattivo alla protezione dei dati, in cui il titolare non solo rispetta le regole, ma è anche in grado di fornire evidenze concrete delle misure adottate per garantire la sicurezza, la riservatezza e il rispetto dei diritti degli interessati. Provare di aver rispettato la normativa del GDPR significa che chi tratta i dati deve essere in grado di predisporre e conservare una registrazione accurata delle proprie attività di trattamento dei dati. Inoltre, è indispensabile includere nella documentazione necessaria anche le misure di sicurezza adottate, in modo da poter dimostrare l'effettiva protezione dei dati personali. In relazione al principio di accountability, che implica l'adozione di misure per garantire il rispetto del Regolamento, l'articolo 24 sottolinea l'importanza di adottare azioni adeguate che dimostrino che il trattamento dei dati sia stato effettuato in conformità con il Regolamento UE. In conclusione, possiamo considerare questi principi fondamentali una piena garanzia per far sì che ci sia il rispetto dei diritti fondamentali degli interessati che assicuri un trattamento dei dati conforme alle normative, un trattamento equilibrato rispetto agli scopi perseguiti e, soprattutto, improntato soprattutto a criteri di trasparenza e correttezza. Il GDPR pone particolare attenzione alle finalità e alla conservazione dei dati, sottolineando l'importanza di proteggerli adeguatamente una volta trattati. Inoltre, garantisce agli interessati un pieno controllo sui propri dati, anche quando questi vengono messi a disposizione dei titolari del trattamento per il loro utilizzo. Per questo è indispensabile che questi principi vengano attuati proprio perché c'è il bisogno di garantire la correttezza e la privacy dei dati personali, assicurandone una protezione costante e un aggiornamento regolare, in modo da preservarne l'accuratezza e l'affidabilità in qualsiasi momento. I principi del GDPR (Regolamento Generale sulla Protezione dei Dati) assumono un ruolo cruciale in un'epoca in cui la digitalizzazione pervade ogni aspetto della nostra vita quotidiana. Il monitoraggio continuo delle attività individuali, attraverso l'uso massiccio di tecnologie avanzate, ha reso centrale la questione della consapevolezza rispetto ai dati personali e alle modalità con cui vengono trattati. Il GDPR quindi, non si limita a stabilire regole per i titolari del trattamento dei dati, ma ridefinisce il rapporto tra cittadini e tecnologie, ponendo l'accento su diritti fondamentali come il consenso informato, il diritto di accesso e trasparenza, e il diritto alla

[60] **PRIVAZY PLAN**, *art 5 "Principi applicabili al trattamento di dati personali"*, https://www.privacy-regulation.eu/it/5.htm

cancellazione (o "diritto all'oblio"). Tali diritti non sono solo strumenti giuridici, ma incarnano una nuova forma di responsabilità condivisa: quella degli individui, chiamati a essere consapevoli e proattivi nella gestione dei propri dati, e quella delle organizzazioni, che devono adottare pratiche trasparenti e rispettose. In un contesto dominato dalla raccolta e dall'elaborazione automatizzata di informazioni, valorizzare e proteggere queste garanzie è essenziale per preservare la libertà e la dignità delle persone. Spesso considerate scontate, le tutele previste dal GDPR rappresentano invece la linea di confine tra una società digitale equa e una dominata da pratiche invasive e discriminatorie. La loro difesa non è solo una questione tecnica o giuridica, ma una battaglia per i diritti umani nell'era dell'informazione.

2. IMPATTO DELLA NORMATIVA SULLA PROTEZIONE DEI DATI SULLE STRATEGIE DI CYBERSECURITY

La nascita del GDPR ha significato dei grossi cambiamenti in ambito di sicurezza informatica, dando a questo tema un ulteriore importanza a quelle che sono le strategie da attuare per difendere i dati da quelli che possono essere ipotetici attacchi cyber. Oggi milioni di utenti cedono i propri dati a varie piattaforme di archiviazione e servizi digitali basati sul cloud, e proprio per questo sempre di più le violazioni diventano più frequenti e soprattutto più aggressive. La tutela garantita da parte del GDPR al trattamento di questi dati così importanti rappresenta il fulcro all'interno della disciplina della cybersecurity rivestendo un ruolo cruciale. Questo perché implementare misure tecniche di sicurezza specifiche per la protezione dei dati personali, in conformità al regolamento, risulta essere un approccio integrato all'interno delle strategie di cybersecurity da attuare. Cosa accadrebbe se non esistessero le normative che oggi salvaguardano la privacy di ogni utente? E quale sarebbe il destino dei milioni di dati gestiti dalle organizzazioni senza un quadro normativo che ne garantisca la protezione? L'assenza di regole porterebbe a una completa libertà nel trattamento dei dati, consentendo a chiunque di appropriarsi di informazioni sensibili e utilizzarle senza limiti. Proprio per questo motivo, il GDPR riveste un ruolo fondamentale nella protezione dei dati, offrendo un insieme integrato di misure organizzative, procedurali e tecniche. Queste misure, agendo in sinergia, mirano a ridurre il rischio di compromissione delle informazioni aziendali più critiche. Il quadro normativo imposto dal GDPR prevede delle sanzioni estremamente severe per le violazioni. Innanzitutto, l'articolo 33 al paragrafo 1 del Regolamento stabilisce una cosa importante e cioè le violazioni devono essere segnalate immediatamente per dare modo a chi ha subito una violazione di essere a conoscenza di ciò. Per questo l'articolo 33 dice chiaramente che "in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a

norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.[61]" Le violazioni oltre ad essere comunicate devono essere contrastate attraverso delle vere e proprio sanzioni amministrative. Le sanzioni che stabilisce il GDPR all'articolo 83 non sono uguali per tutti, ma dipendono dai diversi casi e dalla loro gravità. Infatti, esistono infrazioni che hanno una minore gravità e per questo l'articolo 83 paragrafo 4 "prevede sanzioni che possono arrivare fino a 10 milioni di euro e per quanto riguarda le imprese prevede il 2% del fatturato mondiale annuo[62]". Per le sanzioni più gravi l'articolo 83 paragrafo 5 stabilisce "sanzioni amministrative pecuniare che possono arrivare fino a 20 milioni di euro, o per le imprese fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente[63]". La solidità del Regolamento del GDPR non sta soltanto nello stabilire delle norme che facciano da "paracadute" nel caso di violazione dei dati personali, ma bensì anche nello stabilire dei principi che siano orientati alla cybersecurity fondati su quelli che sono le analisi del rischio. Questo significa che non si tratta solo di regole da seguire in maniera preventiva al danno, ma si tratta di disposizioni che sono appropriate, adattabili e su misura al contesto. Per questo la tutela della privacy e della sicurezza dei dati porta il GDPR ad avere come obiettivo principale quello di evitare che questi dati cadono nelle mani di cybercriminali, essendo una fonte molto importante per i loro disonesti piani. Il legame che avviene tra le strategie di cybersecurity e il Regolamento del GDPR sta proprio nell'adottare delle vere e proprie misure che diano la possibilità alle organizzazioni di poter gestire il rischio di essere colpiti da minacce informatiche. Questo non significa che le misure da attuare siano capaci di evitare ogni possibile minaccia, ma possono essere un incentivo in più per avere una visione interna ed esterna di tutti i rischi possibili e soprattutto le conseguenze che queste minacce possono portare alle organizzazioni e ai singoli individui. Infatti, il GDPR considera fondamentale da una parte analizzare i rischi e dall'altra ritiene che ci debba essere un lavoro di valutazione per capire se le misure adottate siano conformi e adeguate al contesto. Il GDPR, infatti, richiama l'importanza di attuare queste misure tecniche e organizzative proprio nell'articolo 25 con un particolare riferimento a quella che è la *privacy by design* e la *privacy by default.* Il primo paragrafo dell'articolo 25 del GDPR inizia affrontando la cosiddetta *privacy by design* nel quale queste misure vengono affrontate sia nella fase

[61] **PRIVAZY PLAN**, *articolo 33 "Notifica di una violazione dei dati personali all'autorità di controllo"*, https://www.privacy-regulation.eu/it/33.htm

[62] **ALTALEX**, *Art. 83 GDPR - Condizioni generali per infliggere sanzioni amministrative pecuniarie*, 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-83-gdpr-condizioni-generali-per-infliggere-sanzioni-amministrative-pecuniarie

[63] **PRIVAZY PLAN**, *articolo 83 "Condizioni generali per infliggere sanzioni amministrative pecuniarie"*, https://www.privacy-regulation.eu/it/83.htm

di progettazione sia durante la sua esecuzione. Queste misure mirano a tutelare i diritti degli interessati, garantendo che la protezione dei dati non venga applicata solo in una fase successiva, ma sia integrata fin dalla progettazione dei trattamenti. Ciò può essere realizzato attraverso l'implementazione di soluzioni organizzative e tecniche volte ad assicurare una protezione completa dei dati personali, come la minimizzazione dei dati raccolti o l'adozione di misure di sicurezza adeguate a salvaguardare le informazioni sensibili degli interessati. Il secondo paragrafo, invece, affronta il principio della *privacy by default*, che prevede l'adozione di processi di sicurezza configurati per impostazione predefinita in modo da trattare esclusivamente i dati strettamente necessari alle finalità previste. L'obiettivo principale della privacy by default è evitare il trattamento di dati superflui e non pertinenti, consentendo così la raccolta esclusiva dei dati essenziali. Ciò comporta una limitazione degli accessi ai dati, garantendo un utilizzo responsabile da parte di coloro che ne hanno realmente bisogno. Il GDPR con questo articolo intende proteggere i dati di milioni di utenti riducendo i possibili rischi di violazione da parte di cybercriminali; ma non solo, esso con l'articolo 25 mira a mettere al primo posto i diritti dei soggetti attraverso misure efficaci e proporzionate. Con il passare del tempo e l'evoluzione continua delle tecnologie, sono emersi rischi sempre più gravi legati alla possibilità che criminali informatici o soggetti opportunisti possano accedere a dati sensibili o appropriarsene. Tali rischi riguardano sia la vulnerabilità degli utenti individuali, sia il furto di informazioni riservate appartenenti a organizzazioni, sfruttando eventuali vulnerabilità nei sistemi di sicurezza. Proprio l'utilizzo di queste tecnologie può comportare dei grossi danni alla privacy del soggetto di cui i dati si tratta, ed è per questo che entra in ballo l'articolo 35 del GDPR che riguarda quella valutazione che serve per prevenire potenziali violazioni della privacy e quindi garantire che il trattamento dei dati sia conforme alla normativa. Tutto ciò può essere messo in atto da quella che viene chiamata la *DPIA (Data Protection Impact Assessment)*. La DPIA è un processo dedicato proprio all'analisi dell'impatto sulla protezione dei dati, con l'obiettivo di valutare tutti gli aspetti di un trattamento dati, dall'esaminare le esigenze fino ad arrivare a quelli che sono i rischi che possono derivare da quel determinato trattamento. Questo comporta che la DPIA ha come obiettivo quello di fare in modo che i trattamenti siano sicuri e che l'acquisizione di determinati dati siano giustificati da degli obiettivi consoni, in modo che non vengano trattati dati inutili. La Data Protection Impact Assessment non è una procedura obbligatoria, ma bensì è una procedura che deve essere utilizzata solo in determinate circostanze che non sempre si presentano. Bisogna però tenere a mente che, quando un trattamento può comportare un rischio per le persone fisiche, allora lì bisogna attuare una valutazione d'impatto. Un esempio che richiederebbe l'obbligo di effettuare una valutazione d'impatto e quindi una DPIA è l'uso di tecnologie innovative, come l'implementazione di sistemi di intelligenza artificiale o il monitoraggio biometrico. Infatti, una delle più grandi società

aeroportuali come Roma Fiumicino ha richiesto nel 2016 l'autorizzazione per implementare un sistema di videosorveglianza con riconoscimento facciale proprio per tenere sotto controllo il flusso dei passeggeri. In questo caso la DPIA è necessaria proprio perché il trattamento comporta un rischio elevato per i diritti e le libertà delle persone fisiche, a causa del monitoraggio sistematico attraverso l'implementazione di sistemi che possono ledere i diritti delle persone fisiche, e in questo caso dei passeggeri. Implementare queste tecnologie possono creare dei grossi vantaggi, ma il suo utilizzo deve essere bilanciato con la necessità di proteggere i diritti fondamentali di ognuno, e per questo le organizzazioni devono in primis assicurarsi di rispettare quelle che sono le normative vigenti e in materia di protezione dati. Nel caso in cui un trattamento che presenta un rischio elevato non è preceduto da una DPIA, e questo porta a una violazione della sicurezza o dei diritti dei soggetti, l'organizzazione potrebbe incorrere in sanzioni significative previste dal GDPR. Un caso emblematico avvenuta nel 2022 di una mancata esecuzione di una DPIA riguarda proprio l'Azienda Sanitaria Unica Regionale (ASUR) della regione Marche. L'azienda sanitaria in questione ha implementato dei sistemi di geolocalizzazione dei propri dipendenti tramite dispositivi mobili aziendali senza effettuare una DPIA preventiva. La sanzione inflitta dal GDPR nei confronti dell'azienda sanitaria era dovuta ad una errata progettazione dell'applicazione "Smart4You". Questa app intendeva creare un sistema che potesse gestire i dati relativi allo screening Covid-19, ma un'errata gestione ha fatto sì che si potesse accedere in maniera non autorizzati ai profili sanitari di altri utenti. Il GDPR ha stabilito che l'azienda sanitaria aveva gravemente violato, oltre agli obblighi relativi alla sicurezza, anche l'articolo 35 del Regolamento, non avendo effettuato una valutazione d'impatto necessaria per garantire la protezione dei dati sensibili degli utenti. Questa omissione ha esposto milioni di dati al rischio di finire nelle mani sbagliate violando profondamente la privacy dei pazienti. L'assenza dell'obbligo di effettuare la DPIA non esonera il titolare del trattamento dal dover giustificare le proprie scelte. È fondamentale documentare in modo chiaro e conforme le motivazioni che hanno portato a decidere di non svolgere la valutazione d'impatto, altrimenti si rischia di incorrere in delle pesanti sanzioni da parte del GDPR. Le sanzioni che vengono attribuite a chi non rispetta le disposizioni del Regolamento consistono "in una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore[64]". Inoltre, nella gestione delle sfide affrontate dalle diverse organizzazioni, il ruolo del *Data Protection Officer (DPO)* assume un'importanza fondamentale. Questa figura professionale garantisce che il titolare del trattamento, e

[64] **CAMATA A**, *la valutazione di impatto sulla protezione dei dati (DIPIA)*, https://www.studiocamata.it/valutazione-di-impatto-sulla-protezione-dei-dati/

non solo, rispetti i requisiti stabiliti dal GDPR. Il DPO riveste un ruolo cruciale in caso di violazioni dei dati, poiché si occupa di prevenire possibili fughe di informazioni sensibili. Infatti, tra i suoi obiettivi principali vi sono il contenimento degli effetti di eventuali fuoriuscite di dati e l'adozione di misure per evitare che simili episodi si ripetano in futuro. Nel caso in cui questa figura debba affrontare un furto di dati da parte di cybercriminali, deve essere pronta ad agire in conformità con il GDPR, valutando le aree in cui è possibile migliorare la sicurezza dei sistemi informatici e delle reti. L'obiettivo è gestire tempestivamente ed efficacemente le possibili violazioni future, minimizzando i rischi e ottimizzando le misure di protezione. In particolare, il Considerando 75 del GDPR affronta quei rischi di cui il DPO tiene conto nella propria attività di consulenza. Questi rischi riguardano le discriminazioni, furti e danni economici/sociali che portano a dei danni non solo reputazionali, ma anche una vera violazione della riservatezza dei dati; rischi riguardanti la limitazione del controllo dei dati personali e la loro gestione; rischi legati a quelli che sono i dati sensibili, e quindi tutti quei dati che riguardano informazioni sull'ambito delle opinioni politiche, convinzioni religiose, o tutte quelle informazioni legate ai reati commessi; rischi riguardanti la profilazione e quindi l'utilizzo di aspetti che possano creare dei profili individuali; rischi riguardanti i dati persone fragili come ad esempio i minori; infine, il trattamento esteso di dati personali che coinvolgono numerosi individui. Un altro Considerando che oltre ad affrontare l'obbligo di notificare una violazione all'autorità competente entro dei termini ben prestabiliti e cioè 72 ore dal momento in cui si è appreso la violazione, è il Considerando 85. Esso oltre ad affrontare l'urgenza nel comunicare, affronta i rischi che potrebbero causare danni agli individui, come ad esempio la perdita di gestione dei dati o lo stesso furto di dati. Un altro organo che si intreccia in maniera significativa al DPO, specialmente quando si tratta di prevenire reati informatici è l'*OdV (organismo di vigilanza).* Questo organismo "è previsto dal D.Lgs. 231/01 ed è un ente interno all'azienda dotato di autonomi poteri di iniziativa e di controllo che hai il compito di vigilare affinché non si verifichino condotte fraudolente da parte delle figure apicali dell'organizzazione[65]". A differenza del DPO, che si concentra sull'analisi delle possibili cause che potrebbero condurre a una violazione da parte di cybercriminali, l'Organismo di Vigilanza è incaricato di contrastare e monitorare costantemente i potenziali reati derivanti da cyberattacchi all'interno dell'organizzazione. Per affrontare determinati rischi si ha bisogno di precise competenze tecniche e continui aggiornamenti nelle misure di attuazione. Queste competenze non sono sempre parte integrante del DPO e dell'OdV; infatti, per quanto siano organi di controllo necessitano ulteriormente di supporto da parte di professionisti esperti. In conclusione, il GDPR rappresenta un

[65] **VEGA FORMAZIONE**, *organismo di vigilanza (ODV): cosa prevede il D.LGS. 231/01*, https://www.vegaformazione.it/PB/organismo-di-vigilanza-231-p242.html#:~:text=L'Organismo%20di%20Vigilanza%20(ODV,delle%20figure%20apicali%20dell'organizzazione.

pilastro fondamentale nella protezione dei dati personali e nella promozione della sicurezza informatica. Questo regolamento non si limita a fornire un quadro normativo rigoroso, ma funge anche da guida strategica per le organizzazioni nell'affrontare le sfide legate alla gestione dei dati in un panorama digitale in continua evoluzione. Le severe sanzioni per le violazioni e il ruolo cruciale delle figure di controllo, come il DPO e l'OdV, sottolineano l'importanza di un approccio responsabile e proattivo nella gestione dei dati. In un'epoca in cui i rischi legati ai cyberattacchi sono in costante aumento, il GDPR si conferma come uno strumento indispensabile per proteggere le informazioni sensibili, prevenire abusi e assicurare che la sicurezza e la privacy rimangano priorità assolute per individui e organizzazioni.

3. PROSPETTIVE FUTURE: L'EVOLVERE DELL'UEBA E DEL MACHINE LEARNING NELLA DIFESA CIBERNETICA

Con il continuo avanzare delle tecnologie e l'introduzione di strumenti di difesa sempre più innovativi, emerge con chiarezza quanto sia fondamentale la sicurezza informatica nella società moderna. Diventa cruciale esaminare non solo le potenziali cause degli attacchi, ma in particolare i comportamenti degli utenti che potrebbero compromettere la sicurezza all'interno delle organizzazioni. Questo aspetto è al centro del *processo UBA* (User Behavior Analytics) che analizza tali dinamiche per identificare e mitigare i rischi in modo proattivo. Questo processo analizza i comportamenti degli utenti fisici proprio perché è importante acquisire una prospettiva completa dei comportamenti degli utenti in modo da valutare che le attività svolte siano innanzitutto conformi alla normativa, ma soprattutto che potrebbero comportare degli attacchi informatici. L'analisi svolta dal processo UBA impedisce che possibili hacker possano entrare in possesso di dati sensibili e utilizzarli per compromettere l'intera organizzazione e non solo. Infatti, il processo UBA ha come obiettivo principale quello di contrastare e far sì che le organizzazioni siano pronte ad affrontare le possibili sottrazioni illegali di dati da parte di cybercriminali. Uno strumento di analisi come questo permette di avere sotto controllo tutte le attività interne ed esterne all'organizzazione, in modo che, se viene individuato un comportamento che può compromettere l'organizzazione o gli stessi utenti, può avvertire gli utenti in maniera tempestiva attraverso delle notifiche che avvisino i diretti interessati dell'avvenuta violazione. I sistemi di analisi, come l'UBA, rappresentano un'evoluzione rispetto ai tradizionali metodi di monitoraggio, mirando a identificare in modo più efficace le potenziali minacce. Sebbene l'analisi dei comportamenti degli utenti non garantisca la rilevazione di tutte le azioni potenzialmente dannose per un'organizzazione, questo strumento può comunque rappresentare un mezzo utile per individuare possibili minacce alla sicurezza informatica. L'obiettivo di strumenti come quello UBA è di individuare tutto ciò che può intaccare l'intera organizzazione, come ad

esempio software dannosi, sottrazioni di dati sensibili o semplicemente rischi che possono essere causati da soggetti interni all'organizzazione che possono compromettere interi sistemi. Inoltre, questi strumenti consentono di raccogliere informazioni sugli utenti e sulle loro attività, ad esempio tramite elenchi che dettagliano le azioni compiute. Gli strumenti UBA acquisiscono anche dati sui movimenti degli utenti, monitorando l'accesso alle risorse e verificando l'identità degli stessi. L'analisi dei comportamenti degli utenti consente un controllo costante sulle loro azioni. Grazie alla quantità di dati raccolti, gli strumenti UBA permettono di ottenere un quadro completo dei comportamenti, identificando modelli che potrebbero essere utili come riferimento all'interno delle organizzazioni. Questo sistema adottato dai processi UBA porta ad avere sotto controllo i comportamenti degli utenti e identificare le anomalie all'interno di determinate attività svolte dagli stessi. Facendo così c'è una migliore padronanza di quella che è la gestione della sicurezza informatica dell'organizzazione, ma anche la sua efficienza operativa. Per avere un'analisi più precisa ed efficiente gli strumenti UBA sfruttano dei metodi di analisi più innovativi che permettono di esaminare grandi quantità di dati in maniera più dettagliata. Un esempio di queste tecnologie che vengono utilizzati dagli strumenti UBA è il *Machine Learning*. Il Machine Learning "è un sottoinsieme dell'intelligenza artificiale (AI) che si occupa di creare sistemi che apprendono o migliorano le performance in base ai dati che utilizzano[66]". Queste tecnologie innovative permettono agli strumenti UBA di essere più precisi e, soprattutto, di adattarsi continuamente alle evoluzioni che avvengono all'interno delle organizzazioni e alle funzioni che gli utenti svolgono al loro interno. L'utilizzo del Machine Learning permette oltre ad avere una maggiore analisi dei comportamenti degli utenti in maniera dettagliata, permette anche di eseguire le operazioni con estrema velocità integrando dati provenienti da diverse fonti e analizzando un numero maggiore di dettagli. Infatti, ciò permette di avere una maggiore tempestività nell'individuare comportamenti che possono essere non conformi e che potrebbero portare l'organizzazione a dei rischi consistenti. Attraverso queste linee guida e soprattutto attraverso l'utilizzo del Machine Learning è possibile individuare maggiormente le anomalie e rilevare quelle che sono le discrepanze rispetto ai modelli comportamentali degli utenti, facendo sì che strumenti come l'AI e il Machine Learning siano un incentivo in più per aiutare strumenti UBA a riconoscere situazioni di attività malevole all'interno dell'organizzazione. Non tutti i comportamenti degli utenti possono essere considerati anomali e ingiustificati e quindi possono sembrare che essi possano creare delle situazioni di minaccia per l'organizzazione quando poi possono risultare semplicemente delle azioni di minore importanza. Proprio per questo gli strumenti UBA prima di segnalare eventuali

[66] **ORACLE CLOUD INFRASTRUCTURE (OCI)**, *Cos'è il Machine Learning?*, https://www.oracle.com/it/artificial-intelligence/machine-learning/what-is-machine-learning/

azioni non conformi analizza bene le situazioni proprio per capire se è necessario segnalare al team addetto alla sicurezza tale situazione. Per questo vengono utilizzati degli indicatori di rischi, proprio perché in base al punteggio di questi indicatori si valuta la gravità del comportamento rilevato, e solo se il punteggio è elevato necessita di essere segnalato. Questo metodo riduce il rischio di sommergere il team con notifiche di scarsa rilevanza, ma permette comunque di individuare un quadro generale delle attività irregolari, che potrebbero segnalare una potenziale minaccia informatica. Nel caso in cui viene rilevata un'anomalia che può creare una particolare gravità, allora in quel caso pur essendo un'unica anomalia può essere notificata. Tutto questo per far sì che il Security Operation Center sia informato soltanto nel caso di vere e proprie situazioni di minaccia e quindi quando il livello di rischio risulta elevato. Ciò evidenzia l'importanza degli strumenti UBA nel supportare il SOC nel rilevare azioni sospette da parte di utenti malintenzionati che sono riusciti ad accedere ai sistemi dell'organizzazione. Oggi la maggior parte delle organizzazioni subiscono azioni dannose proprio dall'interno, da coloro che operano internamente all'organizzazione e che approfittano della loro conoscenza per accedere in maniera impropria ai sistemi dell'organizzazione. Questo tipo di minacce sono molto difficili da individuare essendo svolte da coloro che hanno l'autorizzazione, ad esempio, ad accedere determinati dati ma poi ne fanno un uso illecito. Proprio per questo l'intervento degli strumenti UBA sono un ottimo mezzo per intervenire e notificare questi comportamenti che possono essere una potenziale minaccia per l'organizzazione. Inoltre, gli strumenti UBA agiscono anche nel caso in cui venga individuata una violazione degli account da parte di cybercriminali che agiscono approfittando di possibili vulnerabilità interne e solo grazie all'uso di questi strumenti, è possibile aumentare l'efficienza nel contrastare minacce di questo tipo. Questo evidenzia come gli strumenti UBA siano particolarmente efficaci nel rilevare schemi di comportamento anomalo a lungo termine, riuscendo a individuare attività sospette anche quando sono abilmente mascherate. Nel 2015, gli strumenti UBA si evolsero, ampliando la loro capacità di analisi non solo ai comportamenti umani, ma anche a tutto ciò che non è umano, come server, router e altre infrastrutture digitali. Questa evoluzione riguarda gli strumenti *UEBA (User and Entity Behavior Analytics)*, sviluppati per analizzare grandi quantità di dati, inclusi quelli generati anche da entità non umane oltre che umane. Essi creano modelli di riferimento utili per identificare i comportamenti appropriati all'interno di un'organizzazione, consentendo di monitorare le attività e individuare potenziali minacce che potrebbero trasformarsi in attacchi informatici. Questo meccanismo viene incentivato maggiormente attraverso l'uso di tecniche di Machine Learning che permettono di avere un maggiore rilevamento delle minacce, monitorando tutti i comportamenti su ampie aspettative che consentono di individuare più facilmente minacce che sono difficili da individuare. Inoltre, l'utilizzo di meccanismi di Machine Learning permette ai sistemi UEBA di segnalare soltanto situazioni di comportamenti che possono

causare dei rischi elevati all'interno dell'organizzazione, evitando di segnalare situazioni di minore importanza. Questo permette di evitare di segnalare qualsiasi minaccia che possa presentarsi e allo stesso tempo permette di riuscire a reagire di fronte alle minacce in maniera preventiva, e quindi contrastandole prima che esse causino ulteriori danni. Con il passare del tempo e con il continuo evolversi di quelle che sono le nuove tecniche di Machine Learning ci sarà sempre di più un miglioramento nell'analisi dei comportamenti che permetterà di conseguenza, di rilevare in maniera più tempestiva le diverse irregolarità presenti all'interno dell'organizzazione. Il miglioramento di questi algoritmi permetterà di conseguenza di migliorare ulteriormente quelli che sono i processi UEBA, riuscendo a gestire situazioni di maggiore complessità in maniera più efficiente e soprattutto permette così di salvaguardare quella che è la sicurezza all'interno dell'organizzazione. Se consideriamo gli strumenti di sicurezza tradizionali, notiamo una risposta meno tempestiva e reattiva rispetto alle soluzioni moderne. Quest'ultime, grazie all'uso del Machine Learning, offrono un controllo più avanzato e una capacità di rilevamento superiore, permettendo di identificare in modo più efficace le minacce che potrebbero compromettere la sicurezza di un'organizzazione. Un ulteriore punto di forza degli strumenti UEBA viene implementata da un altro modello di comportamento che risulta essere un'ulteriore evoluzione delle tecnologie di sicurezza: il *Network Detection and Response (NDR)*. Infatti, "le soluzioni di rilevamento e risposta della rete (NDR) sono progettate per rilevare le minacce informatiche sulle reti aziendali utilizzando l'intelligenza artificiale (IA), l'apprendimento automatico (ML) e l'analisi dei dati[67]". Il NDR analizza i traffici che avvengono all'interno dell'organizzazione creando dei veri e propri modelli da seguire per individuare quelli che poi sono probabili traffici insoliti e scorretti, offrendo una gamma più ampia di funzionalità per il rilevamento e la risposta alle minacce su tutta la rete. Integrare i sistemi UEBA con le soluzioni NDR attraverso anche l'uso di algoritmi come il Machine Learning può essere un'ottima combinazione per avere un pieno controllo di quelle che ad oggi sono diventate le minacce, e cioè sempre più insidiose e devastanti per le organizzazioni. Questo approccio, oltre a migliorare la capacità di identificare potenziali minacce, offre una sicurezza più completa, permettendo all'organizzazione di contrastare efficacemente la diffusione delle minacce informatiche. Questo dimostra come l'evoluzione delle tecnologie di analisi comportamentale rappresenta un elemento cruciale per la sicurezza informatica delle organizzazioni moderne. L'integrazione di algoritmi avanzati di Machine Learning consente non solo di monitorare e rilevare anomalie in modo tempestivo, ma anche di distinguere tra attività realmente pericolose e comportamenti di minore rilevanza, ottimizzando così la gestione dei rischi.

[67] **CHECK POINT**, *What is Network Detection and Response (NDR)?*, https://www.checkpoint.com/it/cyber-hub/cloud-security/what-is-network-detection-and-response-ndr/#:~:text=What%20is%20Network%20Detection%20and,e%20l'analisi%20dei%20dati.

Questi strumenti non si limitano a reagire alle minacce esistenti, ma agiscono in modo preventivo, contribuendo a creare un ambiente digitale più sicuro e resiliente. L'adozione di tali tecnologie, sempre più integrate e sofisticate, sarà determinante per affrontare le sfide future, garantendo alle organizzazioni un controllo più efficace sulle proprie operazioni e proteggendo la loro integrità contro le minacce informatiche in costante evoluzione.

4. LA TUTELA DELLA PROPRIETÁ INTELLETTUALE: GARANZIA PER L'INNOVAZIONE E LA COMPETITIVITÁ GLOBALE

La tutela della proprietà intellettuale sta assumendo un ruolo sempre più centrale a livello globale, specialmente in un contesto caratterizzato dall'accelerazione dell'innovazione tecnologica e dalla crescente competizione tra organizzazioni. Per proprietà intellettuale "si riferisce a un sistema di tutela giuridica del frutto dell'attività creativa e inventiva umana nel campo artistico, scientifico e industriale[68]". Essa non protegge la creazione fisica in sé, ma si concentra sulla tutela dell'idea e dell'invenzione del creatore, evitando che possano essere sfruttate indebitamente dai concorrenti. La protezione delle idee e la loro concretizzazione diventano oggetto di tutela nel momento in cui si trasformano in qualcosa di reale e tangibile. Tutto ciò riguarda quello che la creatività umana può ideare e quindi innovazioni anche a livello tecnologico, creazioni artistiche, marchi e altri simboli che nascono dal frutto dell'ingegno del creatore. Il concetto di proprietà intellettuale inizia a emergere negli anni '60 con lo Statuto dei Monopoli in Gran Bretagna, quando si iniziò a discutere dei brevetti per valorizzare l'economia dell'epoca. Dopodiché, nei primi anni '70 con la nascita dello Statuto di Anna si comincia a dare l'esclusiva sull'opera all'autore anziché allo stampatore, sancendo la nascita del diritto d'autore. Inoltre, si inizia a dare voce al termine "proprietà intellettuale" proprio con l'Organizzazione Mondiale della Proprietà Intellettuale (OMPI) che venne "istituita dalla Convenzione di Stoccolma del 14 luglio 1967, entrata in vigore nel 1970, e conta oggi 188 Paesi membri. Nel 1974 è divenuta Agenzia specializzata delle Nazioni Unite[69]". Infatti, l'obiettivo primario dell'OMPI è di tutelare la proprietà intellettuale dando valore a quella che è il loro contributo nel favorire il progresso creativo e l'inventiva. In Italia, la legge sul diritto d'autore avviene con la

[68] **MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE**, *Cos'è la proprietà intellettuale*, https://www.esteri.it/it/diplomazia-economica-e-politica-commerciale/diplomaziaeconomica/tutela-e-promozione-della-proprieta/cos-e-la-proprieta-intellettuale/

[69] **RAPPRESENTANZA PERMANENTE D'ITALIA PRESSO LE NAZIONI UNITE E LE ALTRE ORGANIZZAZIONI INTERNAZIONALI A GINEVRA**, *L'Organizzazione Mondiale della Proprietà Intellettuale (OMPI),* https://italiarappginevra.esteri.it/it/litalia-e-ooii/proprieta-intellettuale/#:~:text=L'Organizzazione%20Mondiale%20per%20la,conta%20oggi%20188%20Paesi%20membri.

Legge 22 aprile del 1941, n. 633, nel quale all'articolo 1 dichiara che "sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione[70]". L'importanza nel tutelare i diritti della proprietà intellettuale ha un valore anche a livello concorrenziale, dove ci si ritrova ad essere tutti contro tutti, dove delle volte per puntare all'eccellenza si cerca delle scorciatoie non consentite, come ad esempio il copiare e lo sfruttare idee di un altro concorrente. Per questo entra in gioco la tutela della proprietà intellettuale, proprio per potersi difendere da azioni di questo tipo e soprattutto per dare valore al sapere in tutte le sue forme. Per questo la proprietà intellettuale riguarda più in dettaglio quello che è il monopolio su beni intangibili che tocca l'ambito dell'arte e quindi il *diritto d'autore.* Esso riguarda il diritto su opere letterarie come i romanzi, su opere visive come un dipinto, su opere coreografiche e infine, su opere cinematografiche. Il diritto d'autore rappresenta un principio fondamentale nella società dell'informazione, dove ogni individuo, in quanto creatore e produttore di contenuti, contribuisce a un patrimonio intellettuale che necessita di protezione. La tutela garantita dal diritto d'autore non si limita alla salvaguardia degli interessi economici legati alla creazione dei contenuti, ma si basa anche su un principio di giustizia naturale. Questo principio assicura che l'espressione della personalità degli autori rimanga loro esclusiva, riconoscendo il legame unico tra l'autore e la sua opera. Di conseguenza, ogni utilizzo dei contenuti senza l'autorizzazione dell'autore è vietato, a tutela di tale connessione personale ed esclusiva. Il secondo gruppo che riguarda il monopolio su beni intangibili è la *proprietà industriale* e in particolare i *brevetti* e cioè quei diritti che riguardano le scoperte tecnologiche. Il brevetto conferisce un monopolio che garantisce un diritto di esclusiva su una specifica invenzione, costituendo un'eccezione al principio secondo cui la conoscenza è, per sua natura, un bene pubblico. In pratica, brevettare significa trasformare una conoscenza in proprietà privata, limitando ai concorrenti la possibilità di sfruttarla a fini commerciali. Sebbene alcuni sostengano che l'essere umano continuerebbe a inventare anche in assenza di brevetti, la realtà mostra che chi realizza un'invenzione tende a brevettarla. Questo aumenta il valore dell'invenzione stessa, poiché il brevetto consente al titolare di proteggersi dalla copia da parte di altri. Dopodiché, fanno parte di questo gruppo i *marchi*, che rappresentano tutti gli elementi distintivi dei prodotti e dei servizi. Il marchio è un elemento fondamentale nel mercato, presente da sempre proprio perché risponde all'esigenza di differenziazione. Inoltre, i marchi favoriscono anche il miglioramento dei prodotti, incentivando la qualità e l'innovazione attraverso la riconoscibilità e la competizione. Il terzo

[70] **NORMATTIVA IL PORTALE DELLA LEGGE VIGENTE**, *art. 1 disposizioni sul diritto d'autore*, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1941-04-22;633!vig#:~:text=Sono%20protette%20ai%20sensi%20di,o%20la%20forma%20di%20espressione.

elemento di questo gruppo è il *design* che riguarda la progettazione dei prodotti, includendo tutti gli aspetti che ne caratterizzano l'aspetto esteriore, come le forme, i contorni e simili. Nell'attuale organizzazione produttiva della maggior parte delle imprese, detenere i diritti su un design significa avere il controllo sulla filiera produttiva. Questo consente di garantire che tutti i soggetti coinvolti nella realizzazione di un determinato manufatto riconoscano che esso deriva dall'idea inventiva e dalla capacità creativa del titolare del design. Infine, le *indicazioni geografiche* rappresentano diritti legati a beni che interessano l'intero territorio, come nel caso dei prodotti alimentari. In questo ambito si osserva una combinazione di interessi pubblici e privati: il settore pubblico gioca un ruolo fondamentale nel coordinare l'utilizzo di alcuni toponimi, ossia nomi di luoghi, strettamente associati a produzioni radicate nel territorio. Queste produzioni, grazie al legame con il territorio, riescono a esprimere e valorizzare la storia e la cultura locale. In questo contesto, le nuove tecnologie, come la blockchain, offrono soluzioni innovative per proteggere la proprietà intellettuale. In Italia la Blockchain è stata per la prima volta disciplinata "nel Decreto Semplificazioni di Dicembre 2018, convertito in legge l'11 Febbraio 2019, nel quale dichiara che la memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica [71]". La blockchain affonda le sue radici nel 2008, quando un inventore noto con lo pseudonimo di Satoshi Nakamoto ideò un sistema di pagamento virtuale chiamato bitcoin. Tra le criptovalute più celebri nate in quell'anno, i bitcoin rappresentano una valuta digitale utilizzabile esclusivamente mediante un codice informatico specifico. Il sistema basato sulla blockchain ha rivoluzionato le transazioni finanziarie, eliminando la necessità di intermediari e consentendo scambi diretti tra debitore e creditore. La blockchain, che letteralmente significa "catena di blocchi,", funge da registro digitale trasparente e distribuito, capace di registrare dati in modo sicuro e resistente ad alterazioni non autorizzate o distorsioni, sia da parte di terzi che degli operatori della rete. Sebbene originariamente progettata per supportare le criptovalute, la tecnologia blockchain ha trovato applicazioni che vanno ben oltre questo ambito. Grazie alla sua struttura decentralizzata, la blockchain consente la creazione di archivi di informazioni condivisi e inalterabili, offrendo trasparenza e garantendo la possibilità di consultare e verificare i dati caricati sulla piattaforma. Un campo di applicazione particolarmente significativo è quello della proprietà intellettuale, in particolare per la gestione e la tutela dei beni intangibili. Molte organizzazioni, infatti, mostrano una scarsa propensione a proteggere le proprie innovazioni attraverso il deposito di brevetti o la registrazione di modelli, spesso per i costi elevati o le difficoltà nel dimostrare la titolarità e la

[71] **SALARIS S**, *Blockchain e proprietà intellettuale: a cosa serve e ultimi sviluppi*, 2023, https://blog.4bmc.ch/blockchain-e-proprieta-intellettuale-a-cosa-serve-2020/

datazione delle proprie invenzioni. È in questo contesto che la blockchain si rivela uno strumento prezioso, permettendo di fornire prove certe e inconfutabili riguardo alla data, al contenuto e alla titolarità delle innovazioni. Questo è particolarmente utile per le organizzazioni che non desiderano o non possono ricorrere al deposito di un brevetto. Ad esempio, un'azienda che sviluppa un design innovativo per un prodotto, ma che non voglia affrontare i costi di registrazione o preferisca mantenere la riservatezza, potrebbe caricare il design sulla blockchain per garantirne la protezione e la tracciabilità. Da quel momento, il design sarebbe inequivocabilmente riconducibile a tale azienda, con una data certa conferita dalla blockchain stessa. Questo approccio consente all'organizzazione di ottenere, a costi contenuti, una prova giuridicamente valida da utilizzare in caso di necessità di tutela. Un aspetto distintivo e innovativo della blockchain è che elimina la figura dell'intermediario. La garanzia della titolarità, della datazione e della validità del contenuto non è affidata a un'autorità centrale, ma è intrinsecamente assicurata dalla natura della blockchain stessa. Grazie alla sua struttura basata su una catena di blocchi interconnessi, la blockchain garantisce l'immutabilità e l'incorruttibilità delle informazioni registrate. Questa eliminazione degli intermediari non solo semplifica il processo, ma riduce anche i costi, poiché non è necessario remunerare soggetti incaricati di certificare l'autenticità dei dati. È importante, tuttavia, sottolineare che la blockchain non sostituisce il brevetto o la registrazione di un design, ma rappresenta un'alternativa vantaggiosa in termini di durata della tutela e di flessibilità. Inoltre, la tecnologia blockchain rappresenta non solo un vantaggio per le organizzazioni come strumento di tutela delle proprie creazioni, ma anche un efficace mezzo per prevenire attacchi informatici e rafforzare la protezione dei dati. Questo avviene grazie a un incremento della riservatezza, che assicura un maggiore anonimato degli utenti; all'integrità dei dati, che rende le informazioni registrate sulla blockchain immutabili e non eliminabili; e, infine, alla capacità della blockchain di ridurre i punti vulnerabili di un'organizzazione, rendendo più difficile per gli hacker accedere a dati sensibili. La tutela della proprietà intellettuale rappresenta quindi non solo una garanzia per gli autori e i creatori di poter esercitare un diritto esclusivo sulle proprie opere, invenzioni e creazioni, ma anche un elemento chiave per favorire il progresso tecnologico e la competitività economica. Attraverso strumenti giuridici consolidati, come il diritto d'autore, i brevetti e i marchi, e l'adozione di nuove tecnologie come la blockchain, si rafforza la protezione delle idee, valorizzando il legame unico tra il creatore e la sua opera. Questo approccio non solo difende le innovazioni e il patrimonio culturale, ma contribuisce anche a prevenire abusi e pratiche sleali, creando un ecosistema in cui il sapere e la creatività possano prosperare. In questo contesto, la proprietà intellettuale emerge come un pilastro fondamentale per la creazione di una società che valorizzi e rispetti l'ingegno umano, favorendo al contempo uno sviluppo sostenibile e giusto.

IV. SONY E L'ATTACCO PSN DEL 2011: UN CASO EMBLEMATICO NELLA CYBERSECURITY

1. ANALISI DELL'ATTACCO ALLA SONY E DEL SUO IMPATTO

Nel panorama della sicurezza informatica molte delle più grandi organizzazioni hanno dovuto affrontare, grazie al continuo progresso delle tecnologie, l'evolvere delle violazioni da parte di hacker sempre più preparati e sempre più spietati. Molte organizzazioni si ritrovano spesso nel mirino di quelli che sono i cyberattacchi che con il passare del tempo si dimostrano sempre più capaci di infiltrarsi all'interno delle organizzazioni e violare quelli che sono i dati sensibili al proprio interno. Le motivazioni dietro questi attacchi possono essere molteplici: motivazioni che vanno da ragioni personali a motivazioni criminali e politiche. Prendiamo gli innumerevoli casi di dipendenti che per vendicarsi di situazioni interne all'organizzazioni che, avendo ancora accesso ai sistemi aziendali, decidono di utilizzare le sue credenziali per sabotare i server, cancellare dati importanti o divulgare informazioni sensibili dell'azienda a concorrenti o al pubblico. come ad esempio dopo un licenziamento. Come il caso anche di un furto di proprietà intellettuale da parte di un dipendente che si sente sottovalutato potrebbe sottrarre progetti riservati o brevetti per venderli o divulgarli, causando danni economici e reputazionali all'azienda. Nel caso di intenti di criminali e politici un esempio potrebbe essere quello di un gruppo di hacker che lancia una campagna mirata a rubare denaro e dati personali. potrebbe essere rappresentato da un attacco informatico a un'infrastruttura governativa. Immagina che un gruppo di hacker, motivato da scopi politici, lanci un attacco a una serie di sistemi di una nazione straniera. L'obiettivo potrebbe essere quello di compromettere la sicurezza dei dati sensibili, come informazioni relative alla politica interna o alla sicurezza nazionale, al fine di destabilizzare il governo o favorire un particolare gruppo o ideologia politica. Ad esempio, durante le elezioni presidenziali in un paese, gli hacker potrebbero interferire con i sistemi di voto elettronico, manipolando i risultati per favorire un candidato o un partito, oppure diffondere disinformazione attraverso attacchi a piattaforme social media per influenzare l'opinione pubblica. Questi attacchi avrebbero una chiara finalità politica, ma anche criminale, poiché mirano a ottenere vantaggi illeciti tramite il sabotaggio dei processi democratici o l'accesso a informazioni riservate. Uno degli attacchi informatici che più ha sconvolto l'opinione pubblica fu quello avvenuto nel 2014 ai danni della Sony. La storia di questa azienda, oggi tra le più celebri al mondo, ha origini umili e straordinarie. Akio

Morita, uno dei fondatori, nacque in una famiglia benestante in Giappone. Fin da giovane dimostrò un grande interesse per la matematica e la fisica, tanto da iscriversi all'Università Imperiale di Osaka, dove sviluppò una crescente passione per le tecniche di registrazione del suono. Dopo la laurea, Morita si arruolò nella Marina Imperiale giapponese, dove incontrò l'ingegnere Masaru Ibuka. Da questa amicizia nacque l'idea che avrebbe portato alla fondazione della Sony. Nel 1946, i due amici aprirono il loro primo negozio di elettronica. Nonostante un inizio difficile con un prodotto fallimentare, un cuociriso, continuarono a sperimentare, fino a ottenere un grande successo nel 1950 con il primo registratore a nastro. Nel 1955 lanciarono la loro prima radio, la "Sony TR-55", seguita dalla rivoluzionaria radio a transistor tascabile, la "Sony TR-63". Quest'ultima ebbe un tale successo che la crescita della domanda costrinse l'azienda a trasferirsi in una sede più grande. Nel 1958, il nome dell'azienda divenne ufficialmente "Sony Corporation". Il nome "Sony" deriva dal latino *sonus*, che significa "suono". L'espansione internazionale portò anche alla creazione di una sede a New York. Negli anni '60, Sony continuò a innovare: nel 1964 introdusse l'"MD-5", il primo computer desktop a transistor, e nel 1968 lanciò la sua prima TV a colori. Un momento cruciale arrivò nel 1975 con il videoregistratore "Betamax". Nonostante la sua qualità superiore, il Betamax non riuscì a imporsi sul mercato a causa del costo elevato e della forte concorrenza del formato VHS. Tuttavia, nel 1979, Sony rivoluzionò il mercato con il lancio del "Walkman", il primo lettore di cassette portatile abbinato a cuffie leggere, che permetteva di ascoltare musica ovunque. Nel 1982 Sony lanciò un lettore CD portatile, e tre anni dopo introdusse una videocamera leggera e compatta che utilizzava videocassette da 8 millimetri, diventando un best-seller. Negli anni '90, l'azienda si affermò ulteriormente entrando nel mercato dei videogiochi con la divisione "Sony Computer Entertainment". Nel 1994, il lancio della PlayStation a 32 bit fu un successo mondiale. Nel 1997, in collaborazione con Intel, Sony introdusse la linea di computer "VAIO". Parallelamente, continuava a innovare nel settore televisivo, presentando nel 1996 il suo primo televisore a schermo piatto e, nel 1998, il primo modello digitale ad alta definizione. Con il passare del tempo e la scomparsa dei due fondatori, Sony si concentrò sempre più sullo sviluppo di prodotti digitali, come la PlayStation, e sull'integrazione di software e hardware, mantenendo la sua posizione di leader nel settore tecnologico. Durante gli anni in cui Sony sembrava rimanere indietro rispetto alla crescente connettività online, l'azienda aveva comunque compreso l'importanza della transizione verso l'era digitale. Già prima che la Xbox di Microsoft sbarcasse in Nord America, Sony aveva intuito la necessità di connettere la PlayStation 2 alla rete e immaginava un futuro in cui la console non fosse solo un dispositivo per giocare, ma un vero e proprio portale di intrattenimento integrato, con film, musica e videogiochi. Tuttavia, questo ambizioso progetto non si concretizzò mai del tutto. Nonostante ciò, la PS2 si affermò come la console più venduta di tutti i tempi, anche se il suo supporto

al gioco online rimase limitato. Tuttavia, la PS2 ospitò numerosi giochi online di successo, mantenendo viva la visione di Sony di un'esperienza di gioco connessa. Nel 2005, con il lancio della PlayStation 3, Sony presentò le specifiche tecniche della nuova console durante l'Electronic Entertainment Expo (E3), una delle fiere di videogiochi più importanti al mondo. Tuttavia, rispetto ai suoi concorrenti, Sony sembrò ancora una volta in ritardo sul fronte della connettività. Nello stesso anno, Microsoft lanciò la Xbox 360, che ridefinì il gioco online con una piattaforma completa e intuitiva, includendo funzionalità come chat di gruppo e messaggistica integrata. Questa offerta attirò milioni di giocatori, consolidando la Xbox 360 come la piattaforma ideale per il multiplayer online. Il successo di Microsoft spinse Sony a migliorare la propria offerta, ma il progetto della PS3 incontrò numerose difficoltà. I costi elevati dei componenti hardware e la complessità del sistema resero la console costosa e difficile da produrre. Inoltre, Sony sottovalutò l'importanza di un'infrastruttura online competitiva e si affidò all'idea che i propri utenti fossero disposti a pagare un prezzo elevato per una console tecnologicamente avanzata. Questo approccio si rivelò parzialmente fallace. Al momento del lancio, la PS3 integrava finalmente il PlayStation Store, un portale basato sul web per l'acquisto e il download di contenuti. Tuttavia, il sistema presentava gravi limitazioni, come l'impossibilità di scaricare file in background o di accedere alla lista amici e ai messaggi durante il gioco. Questi problemi, insieme al prezzo elevato e alla mancanza di alcune funzionalità essenziali già offerte dai concorrenti, portarono a una diminuzione delle vendite e a numerose critiche da parte degli utenti. Sony, consapevole delle lacune, lavorò per migliorare il prodotto nel tempo, introducendo funzionalità richieste dagli utenti, come l'XMB in-game, che consentiva di accedere alle impostazioni e alle sezioni del sistema senza dover uscire dal gioco. Questi aggiornamenti, insieme a un impegno costante nel contenere i costi e offrire giochi innovativi, permisero a Sony di riconquistare gradualmente terreno. Nonostante questi progressi, il sistema di sicurezza della PS3 si rivelò vulnerabile. Già nel 2009, attacchi hacker misero a rischio il controllo della console. Tra i casi più noti spicca l'azione di George Francis Hotz, conosciuto come GeoHot, famoso per aver violato anche i sistemi Apple. GeoHot, insieme al gruppo di hacker fail0verflow, scoprì falle nella sicurezza della PS3, pubblicando nel 2011 le chiavi di accesso della console, che potevano essere utilizzate per installare software non autorizzato, inclusi giochi pirata. Sony rispose rapidamente, rimuovendo le chiavi dai siti web e presentando un'ordinanza restrittiva contro GeoHot e fail0verflow. La disputa si concluse con un accordo legale in cui GeoHot si impegnava a non hackerare più prodotti Sony. Tuttavia, mentre questa vicenda era ancora in corso, Sony subì un ulteriore attacco devastante da parte di un altro gruppo hacker. Questa volta, le conseguenze furono ancora più gravi, con i dati personali di milioni di utenti compromessi, causando un danno significativo alla reputazione dell'azienda e mettendo a dura prova la fiducia degli utenti.

L’attacco hacker avvenne proprio il 21 aprile 2011 e riguardava uno dei servizi più forti della Sony che contraddistingueva il marchio: il servizio PlayStation Network (PSN). Questo servizio era stato offerto dalla Sony proprio nel 2006 ed era una piattaforma che in continua evoluzione. Esso permetteva agli utenti di giocare online, interagire con amici e familiari in qualsiasi parte del mondo e navigare su internet. Il PSN permetteva che tutte le azioni svolte dagli utenti venissero controllate e supervisionate dalla Sony stessa. Come tutti i servizi offerti da queste piattaforme hanno bisogno di una connessione Internet ed è obbligatorio registrare un account personale e quindi l’utente dovrà fornire determinati dati per poter usufruire del servizio online. Proprio quei dati furono oggetto dell’attacco hacker, nel quale milioni di dati furono compromessi da violazioni esterne. Queste violazioni hanno compromesso i dati personali di circa 77 milioni di account, direttamente collegati agli utenti. L’attacco prese il nome “PSN Hack” e sconvolse l’intera opinione pubblica e gli stessi utenti che si ritrovano i loro account compromessi e i loro dati. Un altro servizio che fu compromesso oltre al PSN fu il Qriocity. Questa piattaforma fu creata nel 2009 ed era una “piattaforma di servizi online in grado di connettere numerosi dispositivi Sony dotati di accesso alla rete, consentendo così agli utenti di vivere un'esperienza di intrattenimento di elevata qualità[72]”. La piattaforma, infatti, era pensata per offrire contenuti multimediali come brani musicali, contenuti audiovisivi, videogiochi e libri digitali. L’attacco, verificatosi tra il 17 e il 19 aprile, costrinse l’azienda a bloccare l'accesso al sistema per prevenire la perdita di ulteriori dati. Di conseguenza, i servizi del PlayStation Network rimasero fuori uso fino a quando non fu chiarito cosa stesse accadendo. Gli utenti si ritrovarono da un giorno all’altro a non poter più accedere ai propri account delle proprie consoles Playstation 3 pensando infatti, che fosse un problema di manutenzione o semplicemente dei problemi connessione al sistema. Infatti, numerosi erano i messaggi di errore che accoglievano chi provava ad accedere ai propri account e Sony prima di comunicare ai propri utenti cosa stesse succedendo preferì accertarsi del danno in corso e soprattutto cercò di rasserenare gli utenti che la situazione si sarebbe risolta nel breve periodo. Infatti, il danno però era molto più grande di quello che si immaginava e l’azienda Sony commentò ufficialmente la situazione pubblicando sulla pagina ufficiale di PlayStation che c’era un’interruzione e che la causa era in fase di accertamento. Non viene detto molto altro a parte che ci sarebbe stato un comportamento mirato da parte del team che stava lavorando per far funzionare

[72]**BORDINI A**, *Sony estende il servizio "Video On Demand powered by Qriocity" all'Europa*, 2010, https://www.hwupgrade.it/news/multimedia/sony-estende-il-servizio-video-on-demand-powered-by-qriocity-all-europa_33601.html

i servizi al più presto. Nei giorni successivi Sony comunica che era avvenuta un'intrusione esterna nella rete Playstation Network e che tale servizio sarebbe rimasto offline, nel frattempo, che l'azienda conduca le opportune indagini per approfondire il problema, ma soprattutto per cercare di proteggere il funzionamento sei servizi in futuro. Non si trattava soltanto di ripristinare il servizio, si trattava di comprendere quanto fosse compromesso. Il PSN rimase inattivo per impedire ulteriori tentativi di accesso a ciò a cui si era avuto accesso, cosa di cui al momento Sony non era ancora pienamente a conoscenza. Gli utenti furono compromessi e i responsabili di questo attacco hacker riuscirono ad ottenere dati sensibili come il nome, l'indirizzo, e-mail, data di nascita, la cronologia degli acquisti, password e dati della carta di credito. La notizia fa scalpore su tutti i mezzi di comunicazione mondiali ed ora che Sony era diventata vittima di una delle più grandi violazioni di dati online. L'azienda si ritrovò a dover rispondere agli utenti sul perché l'azienda ha comunicato il tutto dopo e perché i consumatori non sono stati informati subito e soprattutto perché non c'è stata quella trasparenza che la Sony ha sempre vantato di avere. La Sony volle chiarire che c'era stata una differenza di tempistica tra quando la società ha identificato l'intrusione e quando ha scoperto che i dati dei consumatori erano stati compromessi. La rete venne chiusa dopo che è stata scoperta la violazione e con l'aiuto di esperti esterni, si cercò di capire la portata di questa violazione e per questo ci vollero dei giorni anche se la Sony stessa capì subito a cosa questo attacco hacker era riuscita ad accedere. Infatti, la preoccupazione maggiore da parte degli utenti e della stessa Sony era che da quando era stato bloccato il sistema da parte dell'azienda era passato del tempo e quindi gli utenti continuavano ad accedere non immaginando che i propri dati erano nelle mani degli hacker da alcuni giorni. Inizialmente questo attacco venne attribuito ad un gruppo di hacker denominato Anonymous che "è un movimento decentralizzato di hacktivismo che agisce in modo coordinato per perseguire un obiettivo concordato[73]". Questo gruppo hacker utilizzava tutti gli strumenti digitali a disposizione per far valere quello che è la libertà di manifestazione del pensiero, e quindi attraverso attacchi hacker questo gruppo intende difendere quella che è la chiarezza e l'equità sociale da parte anche di istituzioni e governi oltre che organizzazioni ritenuti colpevoli di non rispettare questi principi e di voler solo il bene dei propri interessi. Il nome del gruppo richiama la loro esigenza di rimanere anonimi, anche con l'utilizzo di maschere del celebre personaggio di "V per vendetta" che si ribella alle ingiustizie e gli abusi del potere. Tre anni prima del caso Sony ci fu un atto di protesta che fece scalpore e cioè quello del progetto Chanology. Questo progetto" è stato lanciato pubblicamente in forma di un video pubblicato su YouTube, 'Messaggio a Scientology', il 21 gennaio 2008. Il video affermava che il

[73] **WIKIPEDIA**, *Anonymous*, https://it.wikipedia.org/wiki/Anonymous

gruppo Anonymous vedeva le azioni di Scientology come una forma di censura, ed affermava l'intenzione del gruppo di espellere la chiesa da Internet[74]".

Si iniziò a ipotizzare che la violazione dei dati potesse essere attribuita al gruppo Anonymous, ritenendo che, a seguito della disputa legale con GeoHot, il collettivo avesse deciso di intraprendere un'azione punitiva contro Sony. Questa ipotesi trovò terreno fertile anche a causa di un messaggio diffuso da Anonymous, nel quale il gruppo dichiarava apertamente che la Sony avrebbe subito delle conseguenze per le sue azioni nei confronti di Geohot e Graf Chokolo. Quest'ultimo era un noto hacker che aveva rilasciato un firmware personalizzato che avrebbe ripristinato un altro sistema operativo sulla PlayStation 3 che era stato rimosso in seguito ad un aggiornamento della Sony. Questa funzione era l'OtherOS che:

"era una funzione presente sulle prime versioni della PlayStation 3 che permette di installare un sistema operativo secondario, come Linux o FreeBSD. Utilizzando questa funzione, è possibile utilizzare la PS3 come se fosse un PC, sfruttando mouse e tastiera ed utilizzando qualsiasi applicazione sviluppata per il sistema installato[75]".

Il sistema operativo Linux, quello su cui puntava a ripristinare Chokolo, considerato: " il primo rappresentante del software cosiddetto "libero" ("freesoftware", in inglese), ovvero quel software che viene distribuito con una licenza che ne permette non solo l'utilizzo da parte di chiunque ed in qualsiasi circostanza ma anche la modifica, la copia e l'analisi[76]". Al contempo, il sistema operativo FreeBSD che:

"è un sistema operativo utilizzato soprattutto in ambito server e questo è dovuto alla stabilità e scalabilità della sua parte di networking; grande attenzione è posta inoltre anche alle problematiche di sicurezza, ed attualmente sono disponibili tre sistemi di firewall (IPFW, IPFilter e PF), integrato nel sistema a partire dalla versione 6.0[77]".

La differenza tra i due sistemi operativi risiede innanzitutto nella licenza dove il sistema FreeBSD utilizza una licenza BSD (Berkeley Software Distribution) che risulta essere più flessibile consentendo l'integrazione del codice in software proprietari senza l'obbligo presentare anche le modifiche annesse; mentre il sistema operativo Linux presenta una licenza meno flessibile che è il

[74] **WIKIPEDIA**, *Progetto Chanology*, https://it.wikipedia.org/wiki/Progetto_Chanology

[75] **WIKIPEDIA**, *OtherOS,* https://it.wikipedia.org/wiki/OtherOS

[76] **LINUX.IT**, *Cos'è Linux*, https://www.linux.it/linux/

[77] **WIKIPEDIA**, *FreeBSD*, https://it.wikipedia.org/wiki/FreeBSD

GPL (Gnu General Public License) che a differenza della licenza BSD richiede la condivisione del codice sorgente delle modifiche; per quanto riguarda invece l'architettura il sistema operativo FreeBSD presenta un sistema operativo completo che presenta sia un kernel che "è un programma situato al centro del sistema operativo che ha generalmente un controllo completo dell'intero sistema e fornisce un accesso sicuro e controllato dell'hardware ai processi in esecuzione sul computer[78]", sia altri strumenti, mentre il sistema operativo Linux si riferisce solo al kernel; anche per quanto riguarda il sistema di gestione dei pacchetti dove il sistema operativo FreeBSD utilizza solo il sistema Ports e i pacchetti binari per la gestione dei pacchetti; mentre il sistema operativo Linux usano diversi gestori di pacchetti a seconda della distribuzione, come APT (Advance Packaging Tool) che è un gestore di pacchetti " è rinomato per la sua solida gestione delle dipendenze e le funzionalità di aggiornamento automatico, che lo rendono uno strumento indispensabile per questi sistemi[79]". I due sistemi operativi differenziavano anche nella prestazione essendo che il sistema operativo FreeBSD è noto per la sua stabilità, affidabilità e performance, specialmente in ambiti come i server e i sistemi di rete; mentre il sistema operativo Linux ha ha un supporto più ampio per hardware e driver moderni, risultando più adatto a un'ampia varietà di dispositivi. Anche nel supporta hardware troviamo delle differenze tra i due sistemi operativi, essendo che nel FreeBSD ha un supporto hardware meno ampio rispetto al Linux, mentre il Linux ha un supporto hardware molto vasto. Inoltre, principalmente si differenzia anche per il suo utilizzo: il FreeBSD è utilizzato maggiormente per applicazioni server, reti, e sistemi che richiedono alta stabilità e controllo; mentre il sistema operativo Linux ha un'adozione molto più ampia, sia in server che in desktop e dispositivi mobili (es. Android). Infine, Linux rispetto al FreeBSD vanta di avere diverse risorse di apprendimento disponili rispetto al FreeBSD che si concentra su determinati settori. La popolarità del sistema Linux per gli hacker sta proprio in questo, al suo essere accessibile al pubblico e far sì che sia oggetto di minacce di qualsiasi tipo. Infatti, questo sistema operativo è oggetto di numerosi attacchi ma "in molti casi, Linux offre protezione solo per le minacce basate su script, come virus e worm. Ma ve ne sono varie altre, tra cui pacchetti di trojan specifici per Linux che installano backdoor, malware e ransomware. Altre minacce includono malware basato su

[78] **WIKIPEDIA**, *Kernel*, https://it.wikipedia.org/wiki/Kernel#Kernel_monolitici

[79]**PHOENIX NA**, *Che cos'è un gestore di pacchetti?* 2024, https://www.phoenixnap.it/glossario/cos%27%C3%A8-un-gestore-di-pacchetti#:~:text=Le%20Gestore%20pacchetti%20APT%2C%20utilizzato,strumento%20indispensabile%20per%20questi%20sistemi.

applicazioni adware, spyware e keylogger[80]". Infatti, in quel periodo avere un sistema operativo come Linux su PlayStation 3 avrebbe comportato un maggiore controllo della console da parte degli attaccanti in questione. Il messaggio in cui Anonymous attaccava la Sony in seguito all'ordinanza contro i due hacker per aver violato la legge sul copyright e cioè la Digital Millenium Copyright Act che "e la legge rende illegali tutti quei processi produzione e divulgativi di tecnologie, strumenti o servizi che possano essere usati per aggirare le misure di accesso soggetto al DRM (Digital Rights Management) compresa l'elusione di un dispositivo di controllo d'accesso[81]" e accusati di frode informatica. La frode informatica è disciplinata dall'art. 640 ter del Codice penale che "punisce chi altera, in qualsiasi modo, il funzionamento di un sistema informatico o interviene senza alcun diritto e con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinente, procurando a sé o ad altri un ingiusto profitto[82]". Quest'azione da parte di Anonymous voleva essere un modo per minare il potenziale della Sony con un messaggio ben chiaro:

"Congratulazioni Sony, ti sei guadagnata l'attenzione del gruppo Anonymous. La tua azione legale nei confronti dei nostri amici Geohot e Graf_Chokolo, non solo ci ha indignati, ma la riteniamo assolutamente imperdonabile. Sei colpevole di aver censurato le tue malefatte e di aver perseguito coloro che cercavano di scoprire la verità. Hai anche violato la privacy di migliaia di persone per i tuoi interessi personali e per questo subirai la vendetta degli Anonymous...l'informazione è libera e lo sarà per sempre, noi siamo Anonymous, siamo una legione, non dimentichiamo, ma soprattutto non perdoniamo[83]".

Tuttavia, nonostante le speculazioni, non ci furono prove definitive che collegassero Anonymous alla violazione dei dati. Sony stessa non confermò mai ufficialmente tale coinvolgimento, lasciando il dubbio irrisolto e impedendo di rassicurare pienamente gli utenti. Nei giorni successivi Anonymous dichiarò che attraverso un altro comunicato che non c'entrava niente con la violazione dei dati e che il loro obiettivo punitivo era nei confronti della Sony e non degli utenti della Sony. Infatti, il gruppo sottolineò il fatto che rubare determinate informazioni personali dei giocatori andava contro i loro principi, poiché non avrebbero voluto mai colpire gli utenti. Un aspetto che destava maggiormente

[80] **ACRONIS**, *È necessario un software antivirus per Linux?* 2023, https://www.acronis.com/it-it/blog/posts/linux-antivirus/#:~:text=Per%20gli%20hacker%20che%20desiderano,rispetto%20ad%20altri%20sistemi%20operativi.

[81] **FATTURA 24**, *DMCA Digital Millennium Copyright Act*, https://www.fattura24.com/glossario/d/dmca/

[82] **BANFI F,** *La differenza tra frode informatica e truffa*, 2023, https://www.dirittoconsenso.it/2023/05/11/la-differenza-tra-frode-informatica-e-truffa/

[83] **HD BLOG**, *Il Team Anonymous dichiara guerra a Sony*, 2011,https://www.hdblog.it/2011/04/05/il-team-anonymous-dichiara-guerra-a-sony/

la preoccupazione degli utenti era che c'era la possibilità che questo gruppo hacker fosse entrato in possesso dei dati delle carte di credito e quindi del proprio codice di sicurezza. Non si poteva riuscire a confermare se ci fosse stato delle violazioni delle carte di credito degli utenti ma non si poteva nemmeno confermare che questo non fosse successo nel mentre gli utenti ancora accedevano alla propria console ignari di quello che stava succedendo. La Sony non riusciva a dare una spiegazione a tutto quello che stava succedendo e soprattutto non poteva dichiarare che nessun dato era stato compromesso e che nessuna conseguenza sarebbe potuta accadere. Il rischio che gli hacker avessero in mano i dati delle carte credito permetteva a loro di accedere ad altri dati attraverso l'uso di comunicazioni che portano ad ingannare l'utente, come per esempio finte segnalazioni da parte della propria banca o da parte di e-mail che segnalano l'urgenza di verificare il proprio account attraverso un link. Inoltre, questo avrebbe portato l'utente (ignaro di quello che stava succedendo al PSN) a ritenere queste segnalazioni legittime avendo un tono urgente che porta l'utente poi a cliccare su quel link. Una volta cliccato, l'utente verrebbe reindirizzato a un sito fraudolento che avrebbe replicato quello ufficiale, dove gli verrebbe chiesto di inserire informazioni personali come nome utente, password o persino dati della carta di credito. Questo era solo uno dei tanti rischi che la violazione dei dati nei confronti degli utenti della Sony poteva comportare. L'attacco alla PlayStation Network può essere paragonato proprio ad una bomba inesplosa abbandonata in un luogo affollato. Inizialmente, sembra innocua, magari addirittura dimenticata, ma il potenziale pericolo rimane. Nessuno sa esattamente quando o se esploderà, né quale sarà l'entità del danno. Tuttavia, se dovesse attivarsi, le conseguenze potrebbero essere devastanti: un'esplosione che colpisce chiunque si trovi nel raggio d'azione, causando danni ben oltre il punto di origine. Allo stesso modo, i dati rubati durante una violazione possono sembrare innocui nell'immediato, ma rimangono un rischio costante. Possono essere venduti, utilizzati per furti di identità o attacchi mirati, con ripercussioni che si estendono nel tempo e colpiscono molti individui. Proprio come una bomba, il danno di una violazione non si limita al momento in cui avviene, ma si diffonde, colpendo in modi imprevedibili e su scala potenzialmente vasta. Infatti, gli utenti non solo rischiavano violazioni ma rischiavano che i loro dati venissero venduti dagli hacker sul dark web. Il dark web "è un gruppo di siti Internet nascosti e accessibili solo attraverso un browser apposito. Il suo scopo è mantenere l'attività online anonima e privata, spesso a sostegno di attività e applicazioni illegali, ma non solo. Ad esempio, alcuni lo usano per aggirare la censura imposta dal loro governo[84]". Questo mercato illegale comporta quindi anche la vendita di dati di carte di credito e la possibilità di falsificare i dati originari sottratti alle vittime da

[84] **KARPERSKY**, *Cos'è e come entrare nel Dark web*, https://www.kaspersky.it/resource-center/threats/deep-web

parte degli hacker e generando così milioni di documenti come carta d'identità, patenti, passaporti etc. In merito alla vendita dei dati delle carte di pagamento un'analisi recente ha individuato che "è stata una società di sicurezza informatica a scoprire di recente un archivio di 6 milioni di carte di pagamento rubate e messe in vendita sul dark web. All'interno di questo database, 80 mila carte sarebbero di cittadini italiani. Il prezzo medio richiesto per ognuna sarebbe di 8,10 euro[85]". Per tanto i 77 milioni di utenti a cui sono stati violati i dati personali si sono ritrovati davanti a questa possibile realtà: e cioè la possibilità che i loro dati sensibili siano oggetto di commercio illegale all'interno del dark web. Ma non solo, questa situazione assume contorni ancora più preoccupanti, poiché i danni potenziali si estendono oltre all' accesso non autorizzato a dati personali, anche l'esposizione dei sistemi digitali degli utenti a potenziali minacce. Gli utenti ormai avevano bisogno di risposte e soprattutto avevano bisogno di capire se c'era il rischio che le conseguenze sarebbero state ancora più devastanti di quanto già erano. In merito a ciò è stata organizzata dalla Sottocommissione per il Commercio, la Manifattura e il Commercio della Camera dei Rappresentanti degli Stati Uniti una riunione proprio per dare le giuste risposte in merito a quest'attacco. Le risposte fornite da sono state poi rese pubbliche, sottolineando l'impegno di Sony nel chiarire le modalità e le implicazioni di questa violazione criminale. Questo evento non ha fatto altro che minare ulteriormente la fiducia degli utenti nei confronti dell'azienda, generando un profondo senso di insicurezza. L'attacco al PSN ha avuto un impatto psicologico significativo, trasformando un momento di svago e spensieratezza, come quello del gioco online, in una fonte di ansia e preoccupazione. Gli utenti, che vedevano il gaming come un'attività leggera e rilassante, si sono ritrovati a vivere con il timore che la loro privacy potesse essere nuovamente violata in qualsiasi momento. Questo ha creato un senso persistente di insicurezza, alimentando il dubbio che, mentre si giocava, qualcuno potesse raccogliere altre informazioni personali, rendendo impossibile tornare a vivere l'esperienza di gioco con la stessa tranquillità di prima. Giocare online comporta inevitabilmente l'esposizione a possibili minacce che potrebbero portare gli utenti, anche involontariamente, a fornire informazioni personali. Questi dati possono essere sfruttati da hacker per infiltrarsi nei sistemi o, più semplicemente, ottenere accesso alle nostre informazioni. Sebbene i sistemi di difesa moderni rendano sempre più difficile eludere le protezioni, come dimostrato dall'attacco alla Sony, nulla può essere dato per scontato. La stessa Sony, infatti, si è trovata impreparata di fronte a un attacco che ha sconvolto l'opinione pubblica, violando i dati di milioni di utenti e instillando in loro una crescente diffidenza nei confronti dei sistemi di gioco online.

[85] **CALZOLARI M**, *Carte di pagamento: nel dark web si vendono "kit" di informazioni personali*, 2023, https://medium.com/@marcocamisanicalzolari/carte-di-pagamento-nel-dark-web-si-vendono-kit-di-informazioni-personali-450af160f89

Inoltre, la leggerezza con cui molti utenti trattano la sicurezza contribuisce a perpetuare questo stato di vulnerabilità. La mancanza di attenzione a circostanze fondamentali, come la creazione di password semplici o ripetute, o l'assenza di un monitoraggio attento degli accessi agli account, facilita enormemente il lavoro dei criminali informatici, che approfittano delle debolezze umane. Queste pratiche superficiali di gestione della sicurezza rendono ancora più vulnerabili gli utenti, soprattutto quando non si considera l'importanza di proteggere i propri dati personali durante la navigazione online o il gioco. Inoltre, c'è una convinzione errata che piattaforme sicure, gestite da colossi tecnologici come Sony, siano immuni da attacchi hacker. Questa percezione di sicurezza fa sì che gli utenti non siano abbastanza vigili, dando per scontato che i loro dati siano sempre protetti e che un'esperienza di gioco online non comporti rischi. Tuttavia, come il caso del 2011 ha mostrato, anche le organizzazioni più potenti possono essere vulnerabili. Pertanto, sebbene le aziende debbano adottare misure di sicurezza efficaci, è altrettanto fondamentale che gli utenti siano consapevoli dei potenziali pericoli e si preparino a riconoscere le minacce durante l'interazione con le piattaforme di gioco online, proteggendo attivamente i propri dati. Un elemento cruciale che ha avuto un impatto significativo nell'attacco al PSN è stato il fattore tempo. Basti pensare alla rapidità con cui un hacker può accedere ai nostri dati, spesso in pochi millesimi di secondo e senza destare sospetti. Questo aspetto rende il crimine digitale particolarmente insidioso, in netto contrasto con le truffe tradizionali, come quelle telefoniche, in cui un truffatore deve guadagnarsi la fiducia della vittima prima di manipolarla per ottenere informazioni personali o il numero di una carta di credito. In tali casi, la vittima dispone di un margine temporale maggiore per analizzare la situazione, riflettere e potenzialmente riconoscere il raggiro, interrompendo la conversazione. Gli inganni tradizionali si basano sul dialogo diretto e sulla persuasione, offrendo alla vittima un'opportunità concreta di valutare ciò che sta accadendo. Al contrario, un attacco informatico avviene in modo rapido e silenzioso, cogliendo spesso le vittime di sorpresa. Questo è particolarmente evidente nel caso dell'attacco alla Sony: gli utenti, spesso giovani o addirittura minorenni, si trovano a giocare in un ambiente che percepiscono come sicuro e familiare. La sensazione di comfort e la percezione di trovarsi in una sorta di "mondo parallelo" possono abbassare le difese psicologiche, rendendo gli utenti più vulnerabili. Un altro fattore determinante è l'impulsività degli utenti, spesso disposti ad accettare rapidamente determinate richieste pur di non interrompere il gioco. Ad esempio, notifiche apparentemente innocue su sconti imperdibili o contenuti gratuiti sul PlayStation Store possono reindirizzare a siti fraudolenti. Chi naviga abitualmente su queste piattaforme non sempre immagina che dietro tali notifiche si nascondano tentativi di phishing. Un utente che, ad esempio, ha appena acquistato un gioco potrebbe ricevere una notifica che segnala il mancato pagamento e, spinto dalla fretta, potrebbe non sospettare un attacco. Allo stesso modo, notifiche che avvertono di attività

sospette sull'account PSN possono indurre l'utente a cliccare frettolosamente, desideroso di risolvere il problema per tornare a giocare. La realtà del PlayStation Network è particolarmente popolare tra i giovani, inclusi molti minorenni. Sony stessa, attraverso il suo sito, fornisce indicazioni per tutelare gli utenti tra i 7 e i 17 anni, come quella di non rivelare mai la propria password, nemmeno in cambio di giochi o denaro. Tra le disposizioni fornite, ce n'è una specifica che riguarda le possibili truffe in cui impone di 'non rivelare a nessuno la tua password, nemmeno se ti dicono che ti daranno giochi o soldi in cambio. Potrebbero utilizzare la tua password per rubare il tuo account[86]". Tuttavia, l'ingenuità e la scarsa consapevolezza dei rischi online rendono i minori particolarmente esposti. Il GDPR, all'art. 12 "impone al titolare del trattamento di fornire l'informativa su come vengono trattati i dati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori[87]". È importante sottolineare come i minori prestino spesso poca attenzione ai pericoli online, sottovalutando i rischi a cui sono esposti, soprattutto mentre giocano. La Sony non ha la certezza che tra i 77 milioni di utenti i cui dati sono stati compromessi non ci fossero minori, ma nemmeno può escluderlo. È evidente che il rischio che i dati violati appartengano a minori non è trascurabile, e quindi la possibilità che questi dati siano stati utilizzati per scopi dannosi, compromettendo la privacy dei giovani, non può essere sottovalutata. Un fenomeno diffuso online è il *digital kidnapping* che riguarda "un vero e proprio "rapimento digitale" attraverso il quale i cybercriminali "duplicano" l'identità per le finalità più disparate utilizzando i dati e informazioni dei minori[88]", e questo può avvenire anche in una piattaforma gaming come quella della Sony. Ad esempio, un malintenzionato potrebbe usare i dati rubati per creare un profilo falso, spacciandosi per un coetaneo e contattando il minore tramite la chat della piattaforma, instaurando così un rapporto di fiducia e raccogliendo ulteriori informazioni personali. La vulnerabilità psicologica dei minori li rende un target privilegiato per gli hacker, che sfruttano la loro fragilità emotiva e la scarsa consapevolezza dei pericoli online. Inoltre, un altro fattore che contribuisce all'impulsività degli utenti è la frenesia di continuare a giocare senza essere disturbati da notifiche. La paura, infatti, rende le persone psicologicamente più fragili e impulsive,

[86] **PSN**, *Regolamento PlayStation Network*, https://www.playstation.com/it-it/legal/psn-rules/

[87]**GDPR**, *Pagina informativa su minori, nuove tecnologie e protezione dei dati,* https://www.garanteprivacy.it/temi/minori#:~:text=L'articolo%2012%20del%20GDPR,informazioni%20destinate%20specificamente%20ai%20minori.

[88] **MARTORANA M, PINELLI L,** *Digital kidnapping, minacciata la sicurezza dei bambini (e non solo),* 2020, https://www.agendadigitale.eu/sicurezza/digital-kidnapping-cosi-mettiamo-in-pericolo-la-sicurezza-nostra-e-dei-bambini/

portandole a cliccare su link senza valutare correttamente le conseguenze. Nel caso dell'attacco alla Sony, gli utenti inizialmente si sono trovati confusi e nervosi, non sapendo cosa stesse succedendo, e vivendo un lungo periodo di down del sistema senza ricevere risposte adeguate dalla compagnia. Successivamente, è subentrata la paura, alimentata dalla comunicazione di Sony riguardo alla possibile violazione dei dati degli utenti. Nonostante Sony avesse investito in tecnologie di sicurezza per proteggere i propri sistemi, l'attacco ha evidenziato quanto anche aziende con solide basi di sicurezza possano trovarsi vulnerabili. Tuttavia, la responsabilità dell'attacco non può ricadere esclusivamente sugli utenti, sebbene la loro scarsa attenzione online, sia sulle piattaforme di gioco che su qualsiasi altro sito, li renda più esposti al rischio di compromettere i propri dati personali. Questo caso dovrebbe servire da lezione per tutti, evidenziando i pericoli del mondo digitale e l'importanza di essere consapevoli della potenza e delle conseguenze devastanti che possono derivare dal fatto che i propri dati finiscono nelle mani sbagliate. Sebbene il fattore umano possa influire sugli attacchi informatici, la Sony ha dovuto affrontare una situazione in cui la responsabilità degli utenti è stata marginale, ma non del tutto assente, sottolineando che anche una minima distrazione online può esporre i dati personali a seri rischi. In conclusione, l'attacco subito dal PlayStation Network di Sony rappresenta non solo un evento significativo per l'industria tecnologica e videoludica, ma anche un punto di riflessione profonda sulla vulnerabilità del mondo digitale e sui rischi che si celano dietro le nostre interazioni quotidiane online. Questo incidente ha sollevato numerosi interrogativi riguardo alla sicurezza dei dati degli utenti, al ruolo delle aziende nella protezione delle informazioni sensibili e alla responsabilità degli utenti nell’adottare comportamenti sicuri nel cyberspazio. In primo luogo, l’attacco al PSN ha evidenziato come, nonostante gli sforzi costanti delle aziende per sviluppare e implementare sistemi di sicurezza avanzati, nessuna piattaforma digitale è immune da minacce. La sicurezza informatica è un settore in continua evoluzione, e mentre nuove difese vengono progettate, al contempo emergono nuove tecniche da parte degli hacker, che sfruttano vulnerabilità sconosciute o debolezze impreviste nei sistemi. In questo contesto, è fondamentale riconoscere che nessun sistema, per quanto sofisticato, può garantire una protezione totale. Anche le aziende più attente e preparate, come Sony, possono trovarsi vulnerabili di fronte ad attacchi estremamente sofisticati e ben pianificati. Sebbene Sony abbia investito ingenti risorse nella protezione dei suoi sistemi, la violazione subita dimostra che gli hacker sono in grado di aggirare anche le misure di sicurezza più robuste. Questo pone una questione rilevante: quanto è davvero sicuro il nostro mondo digitale? Inoltre, l’attacco al PSN ha sottolineato la crescente importanza della privacy dei dati. La protezione delle informazioni personali non è più solo una questione di convenienza, ma una necessità fondamentale. In un’epoca in cui le piattaforme online raccolgono e archiviano enormi quantità di dati su ogni aspetto della nostra vita, dalle preferenze di gioco ai dettagli bancari, la violazione della

privacy non è solo un danno economico, ma anche un danno psicologico e sociale. L'accesso non autorizzato a dati sensibili può avere conseguenze devastanti per gli utenti, che possono subire frodi, furti d'identità e persino danni irreparabili alla loro reputazione online. In questo scenario, diventa essenziale che le aziende non solo adottino misure di sicurezza avanzate, ma che siano anche trasparenti nella gestione dei dati e nella comunicazione con gli utenti riguardo alle vulnerabilità e alle possibili minacce. Il ruolo degli utenti in questo contesto non può essere ignorato. L'attacco al PSN ha messo in luce come anche la distrazione o la scarsa consapevolezza degli utenti possano contribuire, volontariamente o involontariamente, a compromettere la sicurezza delle proprie informazioni personali. In molti casi, gli utenti sono spinti dalla fretta, dalla frenesia di continuare a giocare o dalla paura di perdere il progresso nel gioco, a ignorare i rischi e a compiere azioni imprudenti, come cliccare su link sospetti o accettare richieste senza riflettere. Questa impulsività, spesso alimentata da emozioni come la confusione, la frustrazione o il desiderio di risolvere rapidamente un problema, può rivelarsi fatale. In particolare, i minori sono tra i soggetti più vulnerabili in questo contesto. La loro naturale curiosità e la scarsa consapevolezza dei pericoli online li rendono bersagli ideali per gli hacker. La presenza di piattaforme di gioco, come il PSN, che coinvolgono milioni di giovani utenti, richiede una particolare attenzione alla protezione dei dati e alla sensibilizzazione sui rischi digitali. Non solo le aziende, ma anche i genitori e gli educatori devono essere attivamente coinvolti nella formazione dei più giovani riguardo ai pericoli della rete e ai comportamenti sicuri da adottare. L'attacco al PSN ha inoltre portato alla luce un altro aspetto fondamentale: la necessità di una maggiore trasparenza da parte delle aziende in caso di violazioni della sicurezza. Sony, pur avendo una politica di protezione avanzata, non ha evitato il disastro, e la risposta iniziale al problema è stata insufficiente. Gli utenti hanno sperimentato un lungo periodo di incertezza e frustrazione, senza sapere con certezza cosa fosse accaduto e come i loro dati fossero stati compromessi. La comunicazione tempestiva e chiara è essenziale per consentire agli utenti di comprendere i rischi a cui sono stati esposti e di prendere le misure necessarie per proteggersi, come il cambiamento delle password o la verifica delle transazioni bancarie. Un altro elemento che emerge dall'analisi di questo attacco è la necessità di una responsabilità condivisa nella protezione dei dati. Le aziende devono fare la loro parte implementando tecnologie di sicurezza all'avanguardia, ma anche gli utenti devono essere consapevoli dei rischi e adottare comportamenti prudenti online. È essenziale che gli utenti comprendano che la sicurezza informatica non è solo una questione di protezione da parte delle aziende, ma anche una responsabilità personale. Le misure preventive, come l'utilizzo di password sicure, l'aggiornamento regolare dei software e l'adozione di strumenti di protezione come l'autenticazione a due fattori, sono scelte che ogni utente dovrebbe fare per ridurre i rischi. Infine, l'attacco al PSN ha avuto un impatto significativo sull'immagine di Sony e ha influenzato

profondamente la fiducia degli utenti verso le piattaforme online. La lezione più importante che emerge da questo incidente è che la sicurezza non deve mai essere un aspetto secondario. Le aziende devono continuare a investire in ricerca e innovazione per proteggere i propri sistemi e i dati degli utenti, ma allo stesso tempo devono collaborare con enti pubblici e privati per creare un ambiente digitale più sicuro e consapevole. Solo attraverso un approccio integrato, che coinvolga tutti gli attori in gioco, sarà possibile ridurre i rischi e garantire che la rete rimanga un luogo sicuro, protetto e affidabile. L'attacco al PSN è stato un campanello d'allarme per l'intero ecosistema digitale. Ha messo in evidenza le vulnerabilità del nostro mondo online e l'importanza della collaborazione tra aziende, governi e utenti per affrontare le minacce informatiche. La sicurezza digitale è una responsabilità collettiva, e solo con una maggiore consapevolezza, educazione e attenzione alle best practices potremo sperare di proteggere le informazioni personali e prevenire tragedie come quella che ha colpito milioni di utenti di Sony.

2. STRATEGIE DI CONTENIMENTO E RIPRISTINO DELLA SONY POST-ATTACCO

Il 26 aprile 2011, dopo giorni di inattività del PlayStation Network e una comunicazione inizialmente poco trasparente, Sony decise di affrontare la situazione con sincerità, rivelando l'entità dell'accaduto e il rischio per i dati personali di 77 milioni di utenti. L'azienda ammise che gli account PSN erano stati compromessi, e che l'entità responsabile dell'attacco aveva ottenuto informazioni sensibili come nomi, indirizzi, e-mail e altri dati personali. Sony avvertì gli utenti del rischio di phishing tramite e-mail, telefonate o truffe postali, specialmente per coloro che utilizzavano le stesse credenziali su altri servizi. Proprio per questo, consigliò di cambiare immediatamente le password e di monitorare attentamente i propri estratti conto per individuare eventuali attività sospette, soprattutto legate alle carte di credito. Il CEO di Sony si trovò a fronteggiare non solo le critiche degli utenti, che si chiedevano perché l'attacco non fosse stato comunicato immediatamente, ma anche le numerose segnalazioni di vulnerabilità del PSN, ormai note alla comunità di hacker della PlayStation 3. Queste falle di sicurezza, pur sconosciute a molti utenti, erano state ampiamente discusse negli ambienti tecnici, portando a un crescente scetticismo sulla capacità di Sony di proteggere i dati. Per affrontare la crisi, Sony tenne una conferenza stampa il 1° maggio a Tokyo, durante la quale si scusò pubblicamente per le proprie mancanze, assumendosi la responsabilità dell'accaduto. L'azienda riconobbe che l'attacco aveva messo in luce debolezze significative, ma ribadì il proprio impegno a rafforzare la sicurezza grazie a un team di esperti. Per riconquistare la fiducia degli utenti, Sony annunciò una serie di misure: un pacchetto di "benvenuto" per tutti gli utenti

PSN, comprensivo di 30 giorni gratuiti di PlayStation Plus (un servizio in abbonamento con vantaggi come accesso al multiplayer online, giochi gratuiti e sconti esclusivi), oltre a una selezione di giochi gratuiti a scelta degli utenti. Durante la conferenza, Sony dettagliò anche le nuove misure per prevenire attacchi futuri. L'azienda spiegò che, nonostante le informazioni delle carte di credito fossero crittografate e non ci fossero prove di utilizzi fraudolenti, avrebbe comunque implementato miglioramenti significativi alla sicurezza.

Tra questi:

- L'aggiunta di un team dedicato alla sicurezza informatica.
- Software di monitoraggio automatizzato.
- Livelli avanzati di crittografia dei dati.
- Sistemi di rilevamento avanzati e firewall aggiuntivi.

Queste misure, testate e monitorate da una terza parte indipendente, sarebbero state accompagnate dall'obbligo per tutti gli utenti di creare una nuova password al momento del ripristino dei servizi, per garantire un accesso sicuro. Nonostante questi sforzi, Sony subì poco dopo un secondo attacco, che compromise altri 25 milioni di account. L'incidente sottolineò ulteriormente l'importanza di un rafforzamento continuo della sicurezza, evidenziando le sfide legate alla protezione dei dati personali in un'epoca di crescente minaccia informatica. Il comunicato stampa rilasciato dall'azienda, sebbene non totalmente correlato a PSN, la Sony Online Entertainment viene compromessa

"col furto di 10.700 file di pagamento di clienti in Austria, Germania, Paesi Bassi e Spagna e 12.700 numeri relativi a carte di credito o bancomat. Sony ha reso noto che dai suoi server sono stati rubati nomi, indirizzi, e-mail, date di nascita, numeri di telefono e altre informazioni di 24,6 milioni di clienti di giochi per pc, nonché un «vecchio database» del 2007[89]".

Questo evento costrinse Sony a prolungare ulteriormente la sospensione del servizio, mentre la società avviava un'indagine approfondita per valutare l'entità della violazione e comprenderne appieno le implicazioni. In quel momento, non era chiaro se questa nuova scoperta avrebbe ritardato ulteriormente il ripristino del PlayStation Network. Gli utenti, già frustrati, cercavano risposte che

[89] **CORRIERE DELLA SERA**, *Secondo attacco hacker alla Sony:*

rubati i dati di altri 25 milioni di utenti, 2011, https://www.corriere.it/cronache/11_maggio_03/sony-hacker-internet_03b16ed0-7564-11e0-88f0-a00eb5833fe6.shtml

Sony fornì attraverso un comunicato dettagliato. L'azienda spiegò come fosse venuta a conoscenza della violazione, delineando le azioni intraprese per affrontare la situazione e rassicurare i consumatori, promettendo trasparenza e soluzioni concrete. Sony ribadì il proprio impegno ad agire con cautela e a condividere informazioni solo dopo un'attenta verifica dei fatti. Inoltre, l'azienda sottolineò che stava lavorando anche sul fronte legale e investigativo, collaborando con le autorità competenti per fare chiarezza sull'accaduto. La scoperta dell'intrusione risale al 19 aprile, quando i membri del team Sony Entertainment America notarono attività anomale, come il riavvio improvviso di alcuni sistemi non programmato, un segnale che destò seria preoccupazione all'interno dell'organizzazione. Il 20 aprile, venne rilevato che dati non autorizzati erano stati trasferiti dal PlayStation Network. Due giorni dopo, il 22 aprile, Sony inviò tutte le informazioni e le prove raccolte all'FBI, avviando così un'indagine ufficiale. Oltre a collaborare con le autorità, Sony assunse una seconda società di sicurezza per esaminare i server coinvolti. Questa analisi rivelò che gli intrusi avevano utilizzato tecniche estremamente sofisticate e aggressive per accedere ai sistemi, complicando ulteriormente la situazione. La decisione di ingaggiare un ulteriore team di esperti aveva l'obiettivo di analizzare in profondità l'entità della violazione e identificare eventuali ulteriori compromissioni, inclusi i dati relativi alle carte di credito. Durante l'indagine, furono individuati file sospetti che portarono a ipotizzare un possibile coinvolgimento del gruppo Anonymous, aggiungendo un ulteriore livello di complessità al caso. Con questi sforzi, Sony si impegnò a garantire la massima trasparenza e a fornire tutte le informazioni necessarie agli utenti, cercando di ripristinare non solo il servizio, ma anche la fiducia del pubblico. Tuttavia, il gruppo ha ribadito con fermezza che, pur avendo condotto attacchi di negazione del servizio (DDoS), il loro intento non era quello di compromettere la rete né di agire con intenzioni malevole. La Sony iniziò a ritrovarsi ad affrontare molteplici cause legali già intentate e una multa "di 250.000 sterline (pari a 295.096 euro) dall'Information Commissioners Office inglese. Nello specifico, Sony avrebbe violato il Data Protection Act deludendo tutti gli utenti che avevano fornito all'azienda i propri dati sensibili e, soprattutto, mettendoli in pericolo di trovarsi vittime di furti di identità[90]". Successivamente, Sony cercò di riconquistare la fiducia degli utenti offrendo a tutti gli interessati una polizza assicurativa contro il furto di identità del valore di 1 milione di dollari. Questo gesto, inteso come segno di buona volontà, mirava a rimediare agli errori commessi e a recuperare parte della fiducia perduta. Nel frattempo, le fasi finali dei test interni per il ripristino del PlayStation Network cominciarono a

[90] **NEOSQUALL**, *Sony multata di 250.000 Sterline a seguito del data breach del 2011*, 2013, https://www.spaziogames.it/notizie/sony-multata-di-250000-sterline-a-seguito-del-data-breach-del-2011-279080

prendere forma, sebbene richiedessero ancora tempo a causa dell'ulteriore intrusione che aveva colpito Sony Online Entertainment. Il 14 maggio, Kazuo Hirai, allora dirigente di Sony, annunciò ulteriori aggiornamenti e novità sui servizi PlayStation che l'azienda avrebbe implementato per garantire maggiore sicurezza e funzionalità agli utenti. Da quando le reti Sony erano state vittime degli attacchi hacker, l'azienda aveva lavorato incessantemente per riportare online i servizi di gioco e multimediali. Alla fine, i servizi furono completamente ripristinati, iniziando dal Nord America e proseguendo con altri territori. Funzionalità come l'elenco amici e la chat per lo streaming di giochi online tornarono pienamente operative. Per accedere nuovamente al PlayStation Network, fu necessario installare un aggiornamento del firmware di sistema e modificare le password. Tuttavia, molti utenti inizialmente incontrarono problemi con il sistema di reimpostazione delle credenziali, il quale subì rallentamenti e blocchi, prolungando ulteriormente il processo di sospensione del sistema. Una volta risolti i problemi, gli utenti poterono scegliere tra una selezione di giochi gratuiti disponibili in base alla loro regione, insieme a un'estensione di un giorno per gli abbonamenti attivi. Mentre milioni di giocatori in tutto il mondo erano semplicemente felici di essere tornati online, Sony si trovò ad affrontare un costo elevato per la crisi. L'azienda stimò che l'interruzione fosse costata quasi 200 milioni di dollari, senza contare la multa per la violazione del Data Protection Act e le numerose cause legali che avrebbe affrontato fino al 2015. Inoltre, la prolungata inattività del PlayStation Network rappresentò una significativa perdita di entrate per molti sviluppatori di videogiochi, specialmente in vista dell'Electronic Entertainment Expo del 2011, un evento cruciale per l'industria del settore. Jack Tretton amministratore delegato della Sony, era anche "un imprenditore e dirigente d'azienda statunitense, membro del comitato consultivo di Genotaur, una startup che si occupa di intelligenza artificiale, e di LifeApps Digital Media, un editore digitale di prodotti e servizi incentrati su salute, fitness e sport[91]". Proprio perché amministratore delegato della Sony rilasciò delle scuse pubbliche ai creatori di videogiochi che hanno per anni collaborato con la Sony in merito a quello che era successo. Questo perché l'interruzione delle reti fu molto costosa per la Sony ma soprattutto per gli editori di videogiochi che si sono ritrovati da un momento all'altro ad avere un down delle reti. Proprio perché essi sono i partner più fidati della Sony che hanno permesso alla Playstation di esserci, questo caso ha fatto perdere un po' di fiducia anche da parte loro nei confronti della Sony. Ed è proprio nei loro confronti e nei confronti dei consumatori che la Sony si sentì più sconfitta, perché risultava essere una sconfitta personale nei confronti di chi di più ha riposto fiducia nel progetto della PlayStation. Il portare gli utenti a non fare ciò che più piace e cioè quello di connettersi e giocare con amici in tutto

[91] **WIKIPEDIA**, *Jack Tretton*, https://it.wikipedia.org/wiki/Jack_Tretton

il mondo e goderti le numerose opzioni di intrattenimento su PlayStation Network. C'era ancora molta polvere depositata su molte domande riguardanti l'interruzione, vale a dire ancora non si sapeva con certezza chi fosse il vero responsabile dell'attacco, ma c'erano soltanto ipotesi che non potevano soddisfare le domande degli utenti. Infatti, in merito non sono mai stati effettuati arresti in relazione diretta all'hacking del PSN. Mentre molti puntano il dito contro Anonymous, ma si tratta semplicemente di indizi senza alcuna prova concreta, soprattutto data la natura del gruppo che non perseguivano mai i dati personali degli utenti. Le tracce che portavano a pensare ad Anonymous, anche nel caso di sospetti per il caso anche della violazione sui server SOE, poteva essere uno stratagemma per tenere lontane dai veri intrusi. In qualità di amministratore delegato di Sony, rilasciò pubbliche scuse ai creatori di videogiochi che per anni avevano collaborato con l'azienda, esprimendo rammarico per l'accaduto. L'interruzione delle reti non si rivelò soltanto estremamente costosa per Sony, ma anche per gli editori di videogiochi, che si ritrovarono improvvisamente privati di una piattaforma fondamentale per il loro business. Questi partner, considerati tra i più fidati e strategici per il successo di PlayStation, persero in parte la fiducia nella capacità di Sony di garantire sicurezza e stabilità, un colpo che l'azienda avvertì come una sconfitta personale. Il sentimento di fallimento si estese anche nei confronti dei consumatori, ai quali Sony non era riuscita a garantire ciò che più amavano: connettersi, giocare con amici in tutto il mondo e sfruttare le molteplici opzioni di intrattenimento offerte dal PlayStation Network. Questa incapacità di preservare un'esperienza di gioco fluida e sicura pesava profondamente sull'immagine dell'azienda. Al tempo, molte domande sull'interruzione restavano senza risposta. Non era ancora chiaro chi fosse il reale responsabile dell'attacco, e le ipotesi circolanti non bastavano a soddisfare le preoccupazioni degli utenti. Nonostante numerosi sospetti, non furono mai effettuati arresti legati direttamente all'hacking del PSN. Molti puntarono il dito contro Anonymous, ma le accuse si basavano su indizi deboli, senza prove concrete. La natura del gruppo, notoriamente contraria all'uso dei dati personali degli utenti, rendeva queste supposizioni poco credibili. Inoltre, le tracce che sembravano condurre ad Anonymous, inclusi i sospetti relativi alla violazione dei server di Sony Online Entertainment (SOE), potevano essere state create ad arte per sviare le indagini e distogliere l'attenzione dai veri responsabili. C'era chi sosteneva che il gruppo *Lulzsec,* un gruppo hacker che

"divenne famoso per questi suoi attacchi di rilievo e per i suoi messaggi sarcastici pubblicati dopo gli attacchi. Il gruppo non compieva attacchi a scopo di lucro, infatti i membri di Lulz dichiarano che la principale motivazione è divertirsi nel causare caos; lo scopo bensì è quello di far risaltare il più possibile l'aspetto comico dei propri attacchi[92]".

[92] **WIKIPEDIA**, *LulzSec*, https://it.wikipedia.org/wiki/LulzSec

Alcuni ritenevano che Anonymous fosse responsabile dell'attacco al PSN, ma non esisteva alcuna conferma che il gruppo fosse effettivamente coinvolto. Questa confusione potrebbe essere nata dall'associazione con un attacco informatico avvenuto anni dopo ai danni di Sony Pictures. In quell'occasione il settore cinematografico fu vittima da parte di questo gruppo hacker

"della violazione di dati come password, indirizzi e-mail, date di nascita e altre informazioni degli utenti iscritti a SonyPictures.com. Sarebbero stati violati anche gli account degli amministratori del sistema, cosa che avrebbe consentito agli hacker di ottenere codici promozionali per scaricare gratuitamente tre milioni e mezzo di file musicali dal negozio online delle canzoni del catalogo Sony[93]".

Per quanto riguarda l'attacco al PSN, la sua vera portata e le effettive vulnerabilità sfruttate non furono mai del tutto chiarite, complice anche la diffusione di numerose fake news sull'evento. Nonostante Sony avesse potenziato notevolmente i sistemi di sicurezza per prevenire futuri attacchi, la rete rimase vulnerabile ad attacchi di negazione del servizio (DDoS). Tutto ciò dimostra che la grandezza e la solidità dei sistemi di sicurezza informatici non garantiscono necessariamente l'impenetrabilità. Un esempio emblematico di questa vulnerabilità, avvenuto nello stesso anno, è l'attacco subito da RSA Security, una delle aziende più autorevoli nel campo della sicurezza informatica negli Stati Uniti. Anche un'organizzazione di tale calibro è stata messa a dura prova dai cybercriminali, sottolineando come nessun sistema, per quanto avanzato, possa dirsi completamente al sicuro.

Essa "è un pioniere della cybersecurity, che integra l'intelligenza artificiale per migliorare la gestione del rischio digitale e la sicurezza delle identità. Le sue soluzioni utilizzano l'apprendimento automatico per rilevare le anomalie, gestire le identità e fornire informazioni sulle minacce in tempo reale, aiutando le organizzazioni ad affrontare preventivamente i rischi informatici[94]".

Nonostante fosse un colosso della sicurezza informatica, RSA Security subì uno dei più significativi attacchi della storia proprio nel 2011, lo stesso anno in cui venne colpito il PlayStation Network. Gli hacker riuscirono a compromettere la tecnologia SecurID, un sistema progettato per permettere agli sviluppatori di integrare l'autenticazione a due fattori RSA SecurID direttamente nelle applicazioni Android. Questo sistema offriva un ulteriore livello di protezione, migliorando la sicurezza complessiva. Tuttavia, la compromissione di questa tecnologia non metteva a rischio solo RSA, ma anche milioni di aziende che si affidavano a questo strumento per la protezione dei propri dati e

[93] **IL POST**, *Il nuovo attacco informatico contro Sony*, 2011, https://www.ilpost.it/2011/06/03/sony-pictures-attacco-hacker/

[94] **AI CORPORATE**, *RSA Security*, https://aicorporate.it/companies-a-z/Details/10197

sistemi. La potenza di questo strumento stava proprio sul fatto che "le applicazioni mobile che integrano direttamente la tecnologia Rsa SecurID offrono alle organizzazioni la garanzia che le proprie risorse siano disegnate per essere protette da accessi non autorizzati, senza che questo abbia alcun impatto sul loro utilizzo da parte degli utenti[95]". Milioni di organizzazioni e aziende di grande rilievo si affidavano a questa tecnologia con assoluta fiducia nella sua affidabilità, grazie alla reputazione e al prestigio di RSA Security, un autentico colosso nel settore della sicurezza informatica. Questa tecnologia era annessa a dei dispositivi elettronici, i token, "che andava ad aggiungersi alla classica password di accesso, per rendere più difficoltoso l'eventuale tentativo di furto dei dati da parte degli hacker[96]". Questa soluzione offriva alle organizzazioni la possibilità di implementare una sicurezza più avanzata e intuitiva, indipendentemente dal dispositivo utilizzato. Tuttavia, si rivelò un punto debole del sistema, consentendo agli hacker di compromettere l'intera infrastruttura. La vulnerabilità, inizialmente non rilevata, colse tutti di sorpresa, poiché era impensabile che un'organizzazione così potente potesse subire una violazione di tale portata. Si trattava di una vulnerabilità, ma nello specifico di una *vulnerabilità zero-day*, ovvero una falla sconosciuta fino al momento dell'attacco, che lasciava il sistema esposto senza possibilità di intervento immediato Essa che riguarda "una qualunque vulnerabilità di un software non nota ai suoi sviluppatori o da essi conosciuta ma non gestita. La loro criticità è evidente: chiunque sia a conoscenza della debolezza di un software, ignota ai suoi stessi creatori, potrà utilizzarla a proprio favore sicuro di portare a buon fine i propri attacchi[97]". Come accaduto per Sony, anche la violazione subita da RSA Security ha comportato costi significativi e danni reputazionali, ma con importanti differenze tra i due casi. L'attacco al PlayStation Network è stato silenzioso, avvenuto senza che gli utenti si rendessero conto di quanto stava accadendo e senza alcun avvertimento diretto. Al contrario, l'attacco a RSA Security è stato condotto tramite e-mail fraudolente inviate agli utenti dell'azienda. Queste e-mail, apparentemente innocue, non destavano sospetti, ma in realtà costituivano l'ingresso per un sofisticato attacco hacker mirato non a singoli utenti, come nel caso di Sony, ma a enti governativi e aziende che utilizzavano la tecnologia SecurID, mettendo a rischio informazioni

[95] **NETWORK DIGITAL 360**, *Nuovi strumenti Rsa rendono più sicuro Android*, 2011, https://www.zerounoweb.it/mobility/nuovi-strumenti-rsa-rendono-piu-sicuro-android/

[96] **BITMAT**, *Cosa sono gli RSA Token e come proteggono le nostre operazioni on line*, 2018, https://www.toptrade.it/categorie-funzionali/home-page/primo-piano/cosa-sono-gli-rsa-token-e-come-proteggono-le-nostre-operazioni-on-line/

[97] **FERAZZA F**, Vulnerabilità zero-day: cosa sono e come funziona il mercato nero degli exploit, 2021, https://www.cybersecurity360.it/nuove-minacce/vulnerabilita-zero-day-cosa-sono-e-come-funziona-il-mercato-nero-degli-exploit/

estremamente sensibili. Anche le risposte delle due aziende hanno evidenziato approcci differenti. La Sony, criticata per la mancanza di trasparenza nella gestione dell'incidente, ha cercato di riconquistare la fiducia degli utenti offrendo compensazioni come giochi gratuiti e innovativi strumenti di protezione. RSA Security, invece, ha affrontato un pesante danno reputazionale e ha tentato di risolvere la crisi distribuendo nuove chiavi di autenticazione, operazione che ha comportato ulteriori costi. Inoltre, i due eventi hanno messo in luce diverse vulnerabilità. Il caso del PlayStation Network ha evidenziato le debolezze della piattaforma Sony nella protezione dei dati degli utenti, spingendo l'azienda a rafforzare significativamente la sicurezza. RSA Security, dal canto suo, ha reagito sviluppando nuove tecnologie di autenticazione per evitare future violazioni. Questi due episodi rappresentano un chiaro richiamo alle sfide della sicurezza informatica, che colpiscono in contesti diversi ma evidenziano vulnerabilità comuni nei sistemi, indipendentemente dalla loro complessità o dalla loro portata. Entrambi dimostrano che nessun sistema è completamente immune agli attacchi e sottolineano l'importanza di adottare misure proattive, come l'implementazione di crittografia avanzata, l'autenticazione multifattoriale e una costante attività di monitoraggio e aggiornamento. Questi eventi servono da monito per rafforzare la resilienza delle infrastrutture digitali e richiamano la necessità di una collaborazione globale per affrontare minacce sempre più sofisticate. La sicurezza informatica non può essere considerata un elemento accessorio, ma deve diventare una priorità assoluta, sia per proteggere gli utenti comuni sia per garantire la stabilità di istituzioni e aziende. Come dimostrano i due casi, un attacco può avere conseguenze devastanti, sia a livello individuale, come nel caso di Sony, sia a livello istituzionale e aziendale, come accaduto con RSA Security. Riflettendo sull'interruzione che ha generato panico tra gli utenti di PSN, sorge spontanea la domanda sul motivo per cui Sony non fosse sufficientemente preparata ad affrontare una situazione di tale portata. Sebbene sia chiaro che non esista un sistema di sicurezza infallibile e che persino le agenzie governative possano essere compromesse da un attacco ben coordinato, come quello che Sony ha subito, è evidente che PlayStation Network (PSN) sembrava essere strutturato con misure di sicurezza minime. Un esempio lampante è la difficoltà di compiere operazioni basilari come cambiare il proprio ID PlayStation, che è il nome univoco utilizzato per identificarsi sulla piattaforma. Questo compito è diventato praticamente impossibile a causa di come la rete è stata progettata fin dall'inizio. La risposta di Sony a queste problematiche riguardanti PSN avrebbe potuto causare gravi interruzioni, ad esempio compromettendo classifiche e dati di gioco se si fosse cercato di giocare a titoli meno recenti. Inoltre, l'introduzione della verifica in due passaggi su PSN è arrivata solo dopo che Xbox One aveva già implementato questa funzionalità, evidenziando una reattività lenta e poco proattiva nel rispondere alle esigenze di sicurezza. Infatti, Microsoft aveva implementato questa funzione nel 2013, mentre la Sony nel 2016. Questa verifica in due passaggi era un modo per assicurare un ulteriore

sicurezza che "permetteva quando gli utenti immettevano l'ID di accesso e password da computer, dispositivo mobile o tablet o dalla tua console PlayStation, veniva inviato al cellulare un codice di verifica univoco per fare in modo che soltanto l'utente autorizzato possa accedere[98]". La verifica a due passaggi permetteva di accedere alla PlayStation Network e usufruire i servizi direttamente dalla propria console. Inoltre, veniva richiesto di creare delle password più solide per evitare intrusioni e attivando la verifica in due passaggi avrebbe un ulteriore sicurezza agli utenti. La crisi che stava affrontando Sony non si limitava a preoccupazioni di breve periodo, ma si proiettava soprattutto sul lungo termine: quando i consumatori avrebbero ripreso a fidarsi dell'azienda? E, sul piano competitivo, quanto questa situazione avrebbe favorito i concorrenti? La vulnerabilità di Sony offriva infatti ai concorrenti un'opportunità per guadagnare terreno, proponendo servizi che rispondevano meglio alle esigenze degli utenti, soprattutto nel settore del gaming, in grande espansione tra i giovani. Gli utenti si trovavano inevitabilmente a confrontare l'offerta di Sony con quella di competitor come Microsoft e altri, spinti dalla necessità di maggiore sicurezza. Mentre alcuni rimanevano fedeli all'azienda anche dopo il caos, molti altri sceglievano di rivolgersi a servizi alternativi, ritenuti più affidabili, soprattutto in termini di protezione dei dati. La violazione alla PlayStation Network (PSN) non solo ha evidenziato la necessità di migliorare il servizio offerto, ma ha posto al centro del dibattito la sicurezza dei dati degli utenti. Per questi ultimi, l'incidente ha instillato una paura concreta: giocare online non poteva più essere considerato sicuro. La sicurezza è diventata un requisito imprescindibile, paragonabile a quella degli airbag nelle automobili: quando un guidatore si mette al volante, si aspetta che in caso di incidente il sistema di sicurezza funzioni e lo protegga. Allo stesso modo, un utente che gioca online desidera avere la certezza che i propri dati siano al sicuro. L'attacco alla PSN ha segnato un punto di svolta, imponendo una trasformazione immediata nel settore tecnologico: Sony non poteva più permettersi di trattare la protezione dei dati come un aspetto marginale o essere poco trasparente nei confronti dei consumatori, la cui fiducia è fondamentale. Da quel momento, la sicurezza informatica è diventata una priorità assoluta. Oggi, gli utenti affrontano le loro partite digitali con la sicurezza come primo pensiero, proprio come salgono in auto con la certezza che gli airbag li proteggeranno in caso di necessità. Questa consapevolezza non è più un'opzione, ma un requisito imprescindibile per continuare a conquistare e mantenere la fiducia dei consumatori. L'attacco al PlayStation Network del 2011 rappresenta un momento spartiacque per Sony, evidenziando le fragilità di un colosso tecnologico nell'era delle minacce informatiche avanzate.

[98] **PSN**, *La sicurezza prima di tutto, proteggi al massimo il tuo account*, https://www.playstation.com/it-it/playstation-network/two-step-verification/#:~:text=Come%20funziona,che%20soltanto%20tu%20possa%20accedere.

Nonostante il danno iniziale alla reputazione e i costi economici significativi, la risposta dell'azienda ha mostrato un lento ma deciso percorso verso il recupero. Sony ha trasformato una crisi devastante in un'opportunità per migliorare la sicurezza, rivedere i propri processi interni e ripristinare la fiducia degli utenti, pur riconoscendo i limiti delle proprie misure iniziali. La comunicazione trasparente, seppur tardiva, l'implementazione di strumenti di protezione innovativi e il rafforzamento delle infrastrutture informatiche hanno segnato i passi successivi dell'azienda. Tuttavia, la vicenda ha lasciato cicatrici profonde non solo sulla reputazione di Sony, ma anche nella relazione con i consumatori e i partner strategici. Gli eventi del 2011 hanno sottolineato quanto sia vitale per le organizzazioni moderne adottare un approccio proattivo alla sicurezza informatica. La sofisticazione degli attacchi, come dimostrato dal caso Sony e da altri incidenti paralleli (es. RSA Security), richiede un'evoluzione costante delle strategie di protezione. Nessun sistema è completamente immune, ma un'attenta pianificazione, un monitoraggio continuo e un investimento nei talenti e nelle tecnologie giuste possono mitigare significativamente i rischi. Sony, pur essendo inizialmente impreparata, ha dimostrato che un'azienda può rialzarsi da una crisi di tale portata attraverso scelte coraggiose, come collaborare apertamente con le autorità, assumere esperti indipendenti e fornire compensazioni ai propri utenti. Le conseguenze di questo incidente sono state molteplici. Da un lato, Sony ha dovuto affrontare un esame approfondito del proprio approccio alla protezione dei dati, accettando critiche e intraprendendo riforme radicali. Dall'altro, il settore tecnologico ha tratto una lezione preziosa sull'importanza della trasparenza, della comunicazione tempestiva e della costruzione di infrastrutture resilienti. La decisione di offrire assicurazioni contro il furto di identità e pacchetti gratuiti per gli utenti, sebbene percepita come una mossa tardiva da molti, ha dimostrato l'intenzione dell'azienda di riconciliarsi con la propria comunità. Un aspetto cruciale emerso da questa vicenda è l'importanza della fiducia in un ecosistema digitale sempre più interconnesso. Per Sony, la perdita temporanea di credibilità non si è limitata ai consumatori, ma ha coinvolto anche sviluppatori e partner, evidenziando il ruolo centrale della sicurezza nel mantenere un solido rapporto commerciale. La percezione di vulnerabilità ha reso evidente che la forza di un marchio non si basa solo sulla qualità del prodotto, ma anche sulla capacità di garantire la protezione degli utenti. Il confronto con altri casi, come l'attacco a RSA Security, ha ulteriormente evidenziato la complessità delle minacce informatiche. Entrambi gli eventi hanno dimostrato che la vulnerabilità può colpire persino le organizzazioni più avanzate, ma anche che la rapidità e l'efficacia della risposta sono elementi fondamentali per limitare i danni. L'episodio di RSA, seppur meno visibile al grande pubblico rispetto al caso Sony, ha avuto implicazioni più ampie, mettendo in pericolo dati sensibili a livello aziendale e governativo. Questo confronto ha posto in evidenza due approcci diversi alla gestione delle crisi: Sony ha adottato misure tangibili per il consumatore finale, mentre RSA ha dovuto affrontare una crisi di fiducia tra le

organizzazioni che si affidavano alla sua tecnologia. Il caso Sony ha anche aperto un dibattito su come le aziende debbano bilanciare sicurezza, usabilità e tempestività. L'introduzione di sistemi di crittografia più avanzati, firewall multipli e team dedicati alla sicurezza informatica rappresenta uno standard minimo per le organizzazioni odierne. Tuttavia, l'incidente ha anche messo in luce la necessità di un cambio di paradigma: passare da un approccio reattivo a uno preventivo. Investire in tecnologie emergenti, come l'intelligenza artificiale per il monitoraggio delle minacce, può diventare un punto di svolta per evitare futuri episodi di simile portata. Nonostante gli sforzi di ripresa, l'eredità del 2011 resta un monito per Sony e per l'intero settore tecnologico. La vicenda ha ridefinito le aspettative degli utenti in termini di sicurezza e trasparenza, ponendo l'accento sulla responsabilità delle aziende nel proteggere le informazioni personali. Inoltre, ha contribuito ad aumentare la consapevolezza globale sulla sicurezza informatica, influenzando regolamenti e normative a livello internazionale, come il successivo GDPR. In definitiva, la lezione principale che emerge da questo caso è che le crisi non devono essere viste come un punto di arrivo, ma come un'opportunità per ricostruire e innovare. Sony, pur attraversando una delle sfide più difficili della sua storia, è riuscita a riposizionarsi come un'azienda resiliente, pronta a investire nella sicurezza e nell'integrità dei suoi servizi. La strada per riconquistare la fiducia degli utenti e dei partner è stata lunga, ma ha dimostrato che, con la giusta combinazione di trasparenza, impegno e innovazione, è possibile superare anche le crisi più complesse e preservare il valore di un marchio.

3. IMPLICAZIONI DELL'ATTACCO INFORMATICO ALLA SONY PER CYBERSECURITY GLOBALE E PER LE AZIENDE MULTINAZIONALI

L'attacco alla PSN di Sony nel 2011 ha rappresentato un punto di svolta nella consapevolezza globale sulla sicurezza informatica. Questo evento ha spinto milioni di organizzazioni a riflettere sulla solidità delle proprie difese digitali, portandole a valutare se attribuissero la giusta importanza alla protezione dei dati sensibili dei loro clienti e alla mitigazione dei rischi aziendali. Investire nella sicurezza informatica non significa solo adottare nuove tecnologie, ma anche interrogarsi sull'efficacia delle misure esistenti nel contrastare possibili attacchi hacker. Proprio per questo, molte aziende si sono chieste se, come Sony, avessero vulnerabilità nei propri sistemi di sicurezza. Immaginiamo le conseguenze per le numerose organizzazioni che gestiscono dati aziendali sensibili o operazioni bancarie: senza adeguate misure di protezione, informazioni cruciali potrebbero essere compromesse o finire nelle mani sbagliate. La violazione di database interi potrebbe destabilizzare interi settori, causando danni irreparabili non solo alle singole imprese, ma anche alla sicurezza nazionale. Un esempio concreto di quanto gravi possano essere le ripercussioni di un attacco

informatico su scala nazionale è quanto accaduto alle infrastrutture energetiche ucraine nel 2016. In quell'occasione, un attacco hacker paralizzò la rete elettrica, lasciando milioni di persone senza luce e riscaldamento. Questo evento evidenziò una grave falla nei sistemi di sicurezza, dimostrando come la protezione delle infrastrutture critiche sia una priorità assoluta per evitare scenari catastrofici. Questo malware prendeva il nome di *CrashOverride* "che sarebbe il primo del genere di malware progettato e utilizzato per attaccare reti elettriche[99]". Questo caso dimostra come una violazione da parte di un gruppo hacker possa causare danni di portata ben più ampia rispetto a quelli derivanti da un attacco a un singolo sistema, per quanto esso sia fondamentale. L'attacco alla PSN ha spinto molte organizzazioni e infrastrutture a rafforzare le proprie misure di sicurezza, lavorando per prevenire scenari simili e proteggere i propri dati sensibili. Tra le iniziative adottate nel tempo a seguito dell'attacco a Sony, e con il progresso delle conoscenze in ambito di sicurezza informatica, molte aziende hanno implementato programmi di sensibilizzazione interni. Questi percorsi formativi sono stati progettati per insegnare ai dipendenti a riconoscere e gestire le minacce informatiche, aumentando la consapevolezza sui rischi e preparando sia il personale interno che gli stakeholder esterni ad affrontare possibili attacchi. Un esempio concreto di un'azienda che ha investito in tali programmi è Microsoft, che ha collaborato con la Fondazione Mondo Digitale per promuovere la formazione sulla sicurezza informatica e la prevenzione delle minacce digitali, ed era un "organizzazione non profit impegnati nella diffusione della cultura dell'innovazione per una nuova economia della conoscenza come motore di sviluppo del paese[100]". Insieme, hanno sviluppato un programma di formazione sulla sicurezza informatica con l'obiettivo di offrire una visione più ampia delle minacce digitali attuali e della loro continua evoluzione. L'iniziativa non si limita a fornire conoscenze di base, ma evidenzia come l'avanzamento delle minacce richieda competenze sempre più avanzate, andando oltre le nozioni tradizionali della cybersicurezza. Per questo, il programma formativo di Microsoft mira non solo a sensibilizzare sulle nuove minacce informatiche e sul loro funzionamento, ma anche a incentivare la crescita del settore della sicurezza digitale, fornendo strumenti concreti per affrontare le sfide future. Questo progetto prende il nome di *Ambizione Italia per la cybersicurezza* che "è focalizzato sulle competenze digitali per l'occupazione di nuovi posti di

[99] **FREDIANI C**, *Individuata la prima "arma digitale" per attacchi contro reti elettriche*, 2017, https://www.lastampa.it/esteri/2017/06/13/news/individuata-la-prima-arma-digitale-per-attacchi-contro-reti-elettriche-1.34582808/

[100]**FONDAZIONE MONDO DIGITALE**, *Chi Siamo*, https://www.mondodigitale.org/chi-siamo

lavoro nel campo della sicurezza informatica[101]". Un'altra strategia adottata dalle organizzazioni per rafforzare la sicurezza informatica è stata l'implementazione di simulazioni di attacchi tramite e-mail di phishing. Questi test consentono di valutare la reazione dei dipendenti di fronte a messaggi ingannevoli, verificando la loro capacità di riconoscere tentativi di sottrazione di dati sensibili. Oltre a testare l'attenzione e la preparazione del personale, queste simulazioni permettono anche di analizzare l'efficacia dei sistemi di sicurezza aziendali. L'obiettivo è capire se le misure adottate siano in grado di identificare e bloccare e-mail fraudolente, riducendo così il rischio di violazioni e migliorando la protezione complessiva dei dati. A riguardo una compagnia statunitense, la *Fortinet*, "specializzata nello sviluppo di software, dispositivi e servizi di sicurezza informatica quali firewall, antivirus, sistemi di prevenzione delle intrusioni e di sicurezza degli endpoint[102]", ha sviluppato un servizio di prevenzione di quelle che sono dell'e-mail truffa: *FortiPhish.* FortiPhish utilizza simulazioni di e-mail ingannevoli con l'obiettivo di testare la capacità dei dipendenti di riconoscere tentativi di sottrazione di dati sensibili. Queste simulazioni coprono una vasta gamma di possibili minacce, esponendo i lavoratori a scenari realistici che spaziano dagli attacchi più sofisticati ai malware più comuni. Il sistema analizza le reazioni dei dipendenti, valutando il loro livello di consapevolezza e individuando eventuali lacune nella formazione sulla sicurezza informatica. Questo strumento si rivela particolarmente efficace per rafforzare la protezione aziendale contro le tecniche di social engineering, riducendo il rischio che i dipendenti diventino l'anello debole della catena di sicurezza. Oltre a queste simulazioni, anche la comunicazione visiva gioca un ruolo fondamentale nella sensibilizzazione. Molte organizzazioni adottano locandine ben visibili negli uffici o post informativi sui social media, con l'obiettivo di mettere in guardia sia i dipendenti che i consumatori sui pericoli del phishing e sulle tecniche utilizzate dagli hacker per ingannare gli utenti e infiltrarsi nei sistemi. Un esempio di locandina creata per sensibilizzare la sicurezza informatica è quella promossa da *Ludoteca del Registro.it,* con un poster chiamato "a scuola di cybersecurity", che "individua le 10 regole che ogni ragazza e ragazzo si devono conoscere per navigare in sicurezza il web e i social, evitando quei comportamenti che possono mettere a rischio i propri dati o coinvolgerli in relazioni e contesti nocivi[103]". Questo progetto dimostra come anche iniziative mirate possano contribuire alla diffusione di una maggiore consapevolezza digitale, in questo caso tra i più giovani, favorendo una cultura informatica più responsabile e sicura fin dall'infanzia. Un altro strumento

[101]**FONDAZIONE MONDO DIGITALE**, *Ambizione Italia per la cybersecurity*, https://www.mondodigitale.org/progetti/ambizione-italia-la-cybersecurity

[102]**WIKIPEDIA**, *Fortinet*, https://it.wikipedia.org/wiki/Fortinet

[103]**LUDOTECA REGISTRO.IT**, *Manifesto "A scuola di cybersecurity",* https://www.ludotecaregistro.it/manifesto-a-scuola-di-cybersecurity/

fondamentale per rafforzare la sicurezza informatica e coinvolgere attivamente le organizzazioni sono gli eventi. Questi rappresentano un'opportunità preziosa per aziende e professionisti del settore di confrontarsi sulle strategie adottate, condividere esperienze e migliorare le proprie misure di protezione. Un esempio di eventi più importanti che si svolge annualmente è il *Digital Italy Summit.* Quest'evento "è il punto più alto in cui Protagonisti dell'Economia, Autorità di Governo e del Mondo Accademico e della Ricerca, Esperti Italiani e Internazionali si confrontano sui più recenti trend tecnologici e sul loro impatto sui processi di innovazione digitale del nostro paese[104]". Proprio in occasione del Digital Italy Summit fu organizzato un evento che affrontava proprio la questione della sicurezza informatica e cioè il *Cybersecurity Summit* dove "in un'era caratterizzata da rapide innovazioni tecnologiche e da una crescente sofisticazione delle minacce cyber, il Summit mira a fornire una piattaforma di dialogo, apprendimento e condivisione delle migliori pratiche e delle più recenti soluzioni nel campo della cybersecurity[105]". Un altro evento di grande rilevanza per la sicurezza informatica è il Forum ICT Security, che riunisce esperti del settore per discutere le sfide più attuali e le strategie di protezione più efficaci. Il forum affronta un'ampia gamma di tematiche, dalle minacce più comuni nelle organizzazioni agli attacchi più sofisticati, analizzando soluzioni avanzate per rendere i sistemi informatici più sicuri e resilienti. Vengono inoltre presentate tecniche di difesa e casi di studio concreti, offrendo lezioni preziose per professionisti e aziende. Se l'attacco alla PSN di Sony fosse stato trattato in un evento del genere, avrebbe rappresentato un caso di studio esemplare sugli attacchi informatici dell'epoca. Gli esperti avrebbero potuto analizzare nel dettaglio le vulnerabilità sfruttate, le risposte adottate e le strategie preventive che avrebbero potuto mitigare il danno. Un forum di questo tipo, infatti, permette di approfondire l'importanza di implementare soluzioni avanzate per la protezione dei dati, evidenziando come una maggiore preparazione avrebbe potuto evitare una violazione di tale portata. Eventi come il Forum ICT Security offrono un'opportunità unica per aziende e professionisti di collaborare nella ricerca di metodi innovativi per affrontare le sfide della cybersecurity. L'attacco alla PSN di Sony, che ha compromesso i dati personali di 77 milioni di utenti, ha spinto molte organizzazioni a riesaminare le proprie strategie di protezione dei dati e a valutare l'adozione di misure più robuste per prevenire simili incidenti in futuro. Nel dettaglio una strategia di protezione dei dati "è un approccio sistematico per salvaguardare i dati sensibili da perdita, danno o accesso non autorizzato. Involge l'implementazione di un insieme

[104] **THE INNOVATION GROUP**, *digital summit 2024*, 2024, https://www.theinnovationgroup.it/events/digital-italy-summit-2024/?lang=it

[105] **THE INNOVATION GROUP**, *cybersecurity summit 2024*, 2024, https://www.theinnovationgroup.it/events/digital-italy-summit-2024/cybersecurity-summit-2024-roma/?lang=it

di politiche, procedure e tecnologie per garantire che i dati rimangano sicuri durante tutto il loro ciclo di vita[106]". Tale strategia si estende ben oltre la semplice difesa da attacchi hacker: il suo obiettivo è preservare integrità, riservatezza e disponibilità dei dati, assicurandosi che possano essere monitorati dall'organizzazione per individuare tempestivamente eventuali violazioni o anomalie. Tuttavia, il controllo sui dati deve essere rigidamente regolato: non tutti i dipendenti dovrebbero avere libero accesso alle informazioni sensibili, poiché un accesso indiscriminato potrebbe facilitare abusi o utilizzi impropri. Dopo episodi come l'attacco alla PSN di Sony, diventa sempre più cruciale per le aziende evitare gli stessi errori e garantire la protezione della privacy dei propri consumatori. La fiducia dei clienti nei confronti di un'azienda è paragonabile a quella riposta in un ristorante: quando si ordina un pasto, ci si aspetta ingredienti freschi, una cucina pulita e il rispetto delle norme igieniche. Se queste aspettative vengono tradite – ad esempio, trovando qualcosa di indesiderato nel piatto – è altamente probabile che il cliente non torni mai più. Allo stesso modo, i consumatori si aspettano che le aziende trattino i loro dati con cura e rispetto. Una violazione della privacy equivale a servire un piatto contaminato: non solo delude le aspettative, ma mina irrimediabilmente la fiducia, rendendo difficile riconquistarla. Per questo motivo, le organizzazioni – dopo il caso Sony e molte altre violazioni informatiche – non devono solo investire in maggiori misure di protezione, ma anche garantire trasparenza sulle modalità e sugli strumenti adottati per la sicurezza dei dati. Solo così possono dimostrare ai clienti che la loro privacy è una priorità assoluta. Prendiamo ad esempio Ikea, che nella sua campagna di protezione e trasparenza ha dichiarato apertamente che, per molti anni, le aziende hanno raccolto informazioni sui clienti senza mai mettere in discussione se fosse davvero giusto farlo. Spesso, infatti, le aziende trattano i dati dei clienti come se fossero di loro proprietà. Ikea, invece, si è impegnata a restituire il controllo dei dati ai consumatori. Oggi, i clienti si trovano ad affrontare esperienze difficili, come quella vissuta da Sony, che li ha portati a sentirsi incompresi e vulnerabili. Molti non sanno cosa accade ai loro dati e questo genera sfiducia. Se un'azienda non è trasparente su come gestisce le informazioni personali, perde il rapporto di fiducia che dovrebbe instaurare con i propri consumatori. È fondamentale adottare un approccio centrato sulle persone, che non solo tenga conto della digitalizzazione e delle nuove tecnologie, ma che anche affermi i valori e la lealtà dell'organizzazione. I dati sono una componente fondamentale in tutte le operazioni interne di un'azienda. Per evitare che un approccio orientato al cliente venga compromesso, ogni organizzazione deve ripensare i suoi processi attraverso la lente dei consumatori e riconoscere l'importanza dei dati come potenziale risorsa. I consumatori devono essere messi al primo posto, e

[106] **DATA SUNRISE**, *strategia protezione dei dati*, https://www.datasunrise.com/it/centro-di-conoscenza/strategia-di-protezione-dei-dati/

soprattutto i loro dati devono essere adeguatamente tutelati attraverso nuovi sistemi di controllo che proteggano la privacy e assicurino trasparenza. Molte organizzazioni, per rafforzare il legame con i consumatori, hanno iniziato a testare le loro tecniche di sicurezza direttamente con il pubblico, così da consolidare la fiducia. Non è più accettabile che le aziende lascino i consumatori all'oscuro di situazioni critiche, come nel caso di Sony. Le aziende devono comprendere cosa succede ai dati degli utenti, come vengono utilizzati e, soprattutto, se sono al sicuro. Questo ha portato molte organizzazioni a concentrare la propria mission sulla trasparenza, rendendo chiaro come vengono trattati i dati e come si protegge la privacy degli utenti. In questo contesto, Ikea ha mostrato come trasparenza e consapevolezza siano fondamentali per instaurare un rapporto di fiducia. La sua app, ad esempio, illustra chiaramente agli utenti le opzioni relative ai dati: durante l'iscrizione, gli utenti sono informati sulle funzionalità personalizzabili dell'app, come la possibilità di salvare i propri prodotti preferiti. Ma ciò che distingue Ikea è la possibilità di controllo che l'utente ha sui propri dati. L'app spiega in modo trasparente i vantaggi della condivisione dei dati, ma informa anche che il consumatore ha sempre il diritto di decidere come questi vengano utilizzati, garantendo la possibilità di non condividerli affatto. Questa filosofia mira a creare un'esperienza sicura, dove il consumatore si sente protetto sia nell'uso dell'app che nell'interazione con il sito. Ikea vuole stabilire un dialogo continuo con i suoi utenti, promuovendo un'esperienza che sia vantaggiosa sia per il consumatore che per l'azienda, senza compromettere la privacy. Questo approccio, secondo Ikea, non è solo un buon affare, ma è anche la cosa giusta da fare. Oggi, l'intelligenza artificiale gioca un ruolo fondamentale nell'evoluzione delle tecniche di protezione. Data la crescente complessità delle minacce informatiche, le aziende devono essere pronte a rispondere efficacemente, e l'intelligenza artificiale rappresenta un alleato indispensabile nel migliorare le difese informatiche. Senza soluzioni all'avanguardia, le organizzazioni non possono sentirsi sicure nel fronteggiare minacce sempre più sofisticate. L'intelligenza artificiale "permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico[107]". n ambito di sicurezza, l'IA si rivela uno strumento prezioso per monitorare e analizzare i comportamenti interni all'organizzazione, individuando con maggiore precisione attività sospette, siano esse causate da minacce esterne o da comportamenti anomali all'interno dell'azienda, come nel caso di dipendenti che possano abusare dei propri accessi. Grazie all'IA, queste attività possono essere rilevate in tempo reale, con segnalazioni automatizzate e misure più efficaci per contrastare possibili attacchi prima

[107] **TEMATICHE PARLAMENTO EUROPEO**, *Che cos'è l'intelligenza artificiale?*, 2023, https://www.europarl.europa.eu/topics/it/article/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata

che causino danni maggiori. Inoltre, l'IA ha la capacità di elaborare una quantità enorme di dati, permettendo alle organizzazioni di effettuare correzioni rapide e precise, in modo che i processi non vengano rallentati dall'elaborazione manuale. Questo approccio non solo velocizza l'analisi, ma garantisce anche che vengano adottate soluzioni che, manualmente, sarebbero impossibili da realizzare. L'implementazione dell'intelligenza artificiale rende possibile, ad esempio, il riconoscimento tempestivo di e-mail sospette, come nel caso di tentativi di phishing, o il rilevamento di movimenti irregolari negli account aziendali, sia esterni che interni. L'intelligenza artificiale interviene su compiti complessi che richiedono un'attenzione continua da parte degli esseri umani, specialmente nell'ambito della cybersecurity. Non si tratta più solo di riconoscere un virus noto, ma di sviluppare algoritmi in grado di prevedere e identificare minacce sconosciute in tempo reale, rendendo il sistema proattivo. È come se l'IA fornisse al sistema immunitario umano strumenti potenti, che vanno ben oltre le capacità umane, permettendo di affrontare situazioni molto più complesse. Il tempo è un fattore cruciale nelle organizzazioni: ogni istante in cui la sicurezza non è sufficientemente robusta rappresenta una finestra di opportunità per gli hacker. Attacchi come quello alla PSN hanno dimostrato quanto sia costosa una vulnerabilità, con enormi perdite sia economiche che di reputazione. Più il sistema è lento o vulnerabile, maggiore è il rischio di compromissione. L'intelligenza artificiale è anche più accurata dell'uomo nel rilevare minacce, evitando che piccoli malfunzionamenti vengano confusi con intrusioni. Un sistema basato sull'IA è in grado di distinguere rapidamente un attacco hacker da un normale guasto tecnico, riducendo significativamente i margini di errore. Questo è particolarmente importante quando si affrontano attacchi da parte di criminali informatici, che sempre più spesso sfruttano algoritmi avanzati per creare minacce più sofisticate e difficili da individuare. Tuttavia, l'uso dell'IA non è limitato alla protezione. Purtroppo, gli stessi hacker possono utilizzarla per potenziare i loro attacchi, creando minacce ancora più gravi. Un esempio concreto è l'uso dell'IA per generare e-mail di phishing altamente personalizzate e difficili da riconoscere. Se un'e-mail truffaldina già di per sé presenta molteplici insidie, l'uso dell'IA consente di rendere ancora più verosimili questi messaggi, aumentando notevolmente il rischio che i dipendenti cadano nel tranello. Per questo, l'intelligenza artificiale sta trasformando il panorama della cybersecurity, migliorando le difese contro le minacce tradizionali e, al contempo, amplificando la portata delle minacce stesse, se utilizzata per scopi malevoli. La sfida per le organizzazioni è quindi duplice: adottare l'IA per proteggersi dai rischi informatici, ma anche prepararsi a fronteggiare i nuovi pericoli che questa tecnologia può portare. Un esempio pratico potrebbe essere un dipendente di un'azienda che utilizza regolarmente un software di gestione dei progetti come Asana che "impostare obiettivi a livello aziendale, gestire piani strategici e portare a termine il lavoro su un'unica

piattaforma[108]", o Trello che "è uno strumento che consente ai gruppi di gestire visivamente qualsiasi tipo di progetto, flusso di lavoro o monitoraggio dei task[109]". Gli hacker, sfruttando l'intelligenza artificiale e l'elaborazione del linguaggio naturale, possono analizzare informazioni pubbliche (come il profilo LinkedIn del dipendente o altre informazioni condivise online) per ricostruire dettagli sulla sua posizione lavorativa, i colleghi con cui collabora e i progetti a cui è associato. A questo punto, l'hacker può inviare una e-mail apparentemente innocua, che sembra provenire da un collega, chiedendo di apportare modifiche a un documento attraverso un link. Inizialmente, l'e-mail potrebbe non destare sospetti, soprattutto perché include dettagli concreti e pertinenti, come il nome di un progetto specifico e quelli di altri colleghi coinvolti. Questi dettagli possono essere resi plausibili grazie all'accesso a informazioni pubbliche o, peggio, a una violazione precedente dei dati. In questo scenario, l'intelligenza artificiale viene utilizzata per creare una grafica e una firma aziendale che sembrano autentiche, aggiungendo un ulteriore livello di credibilità al messaggio. Inoltre, l'e-mail contiene elementi come il nome del progetto e dei colleghi, che contribuiscono a rendere l'inganno ancora più convincente. La menzione di scadenze imminenti potrebbe spingere il dipendente a cliccare sul link in modo frettoloso, senza sospetti. Il link, però, porta a una pagina di accesso falsa, che replica fedelmente l'interfaccia di Asana, Trello o di un altro software aziendale. Quando il dipendente inserisce le proprie credenziali, queste vengono catturate dagli hacker, che ora hanno accesso al sistema aziendale, mettendo a rischio i dati aziendali e potenzialmente causando gravi danni. Un caso molto diffuso è quello dell'uso della tecnologia di *deepfake* che "è una tecnica per la sintesi dell'immagine umana basata sull'intelligenza artificiale, usata per combinare e sovrapporre immagini e video esistenti con video o immagini originali, tramite una tecnica di apprendimento automatico, conosciuta come rete antagonista generativa[110]". Purtroppo, tale tecnologia può causare gravi danni alla reputazione di un'azienda, poiché i contenuti creati tramite deepfake possono non solo danneggiare l'immagine del brand, ma anche allontanare i consumatori. Un esempio di attacco alla reputazione tramite deepfake potrebbe essere un video falso in cui il CEO di una multinazionale, ad esempio un'azienda farmaceutica o tecnologica, appare mentre fa dichiarazioni controverse o

[108] **ASANA**, *L'unica piattaforma di gestione del lavoro sviluppata per essere scalabile*, https://asana.com/it/product

[109] **ATLASSIAN TRELLO**, *Trello consente ai gruppi di gestire task e progetti più facilmente*, https://trello.com/it/tour

[110] **WIKIPEDIA**, *Deepfake,* https://it.wikipedia.org/wiki/Deepfake#:~:text=Il%20deepfake%20(parola%20coniata%20nel,conosciuta%20come%20rete%20antagonista%20generativa.

inappropriate. In questo video, il CEO potrebbe sembrare affermare che l'azienda abbia intenzionalmente ridotto la qualità dei suoi prodotti per aumentare i margini di profitto, o addirittura fare commenti discriminatori, sessisti o razzisti, completamente falsi ma estremamente realistici. Il video deepfake verrebbe poi diffuso rapidamente sui social media, dove gli utenti, spesso poco inclini a verificare la veridicità dei contenuti, lo condividono senza pensarci due volte. In poche ore, il video può diventare virale, scatenando un'ondata di indignazione pubblica. Questo porta i consumatori a mettere in discussione non solo la serietà dell'azienda, ma anche la sua sincerità. Una smentita da parte dell'azienda potrebbe non essere sufficiente a convincere i consumatori a ricredersi. Inoltre, tale attacco potrebbe allontanare anche i partner commerciali, che non si riconoscono più nei valori fondamentali dell'azienda dopo un episodio del genere. Oltre a ciò, l'azienda si troverebbe ad affrontare ingenti costi comunicativi per cercare di dimostrare che si trattava di un deepfake, con l'obiettivo di riparare al danno e far capire ai consumatori che la sua lealtà non è stata compromessa. Questo esempio dimostra come l'intelligenza artificiale possa essere uno strumento potente per migliorare la sicurezza informatica, ma allo stesso tempo come gli algoritmi possano essere utilizzati anche per individuare i punti deboli di un'organizzazione e sfruttarli contro di essa. Un caso emblematico di attacco informatico, come quello alla PSN della Sony nel 2011, avvenne in un periodo in cui l'intelligenza artificiale per la cybersecurity non era ancora sviluppata come lo è oggi. All'epoca, l'azienda non disponeva di algoritmi avanzati di intelligenza artificiale per proteggere i suoi sistemi, ma oggi le organizzazioni hanno la possibilità di utilizzare tecnologie molto più sofisticate per prevenire e contrastare minacce di questo tipo. Negli anni in cui si è verificato l'attacco alla Sony, esistevano già sistemi di rilevamento delle intrusioni (IDS) che "poteva aiutare ad accelerare e automatizzare il rilevamento delle minacce di rete avvisando gli amministratori della sicurezza di minacce note o potenziali o inviando avvisi a uno strumento di sicurezza centralizzato[111]". Vi erano anche altri strumenti di analisi, ma l'intelligenza artificiale come metodo per rilevare minacce in tempo reale non era ancora diffusa come lo è oggi. Tuttavia, ciò non significa che, se la Sony avesse avuto algoritmi di intelligenza artificiale, l'attacco sarebbe stato evitato. L'intelligenza artificiale avrebbe potuto rappresentare un fattore aggiuntivo nel rilevamento tempestivo della minaccia, ma il problema principale risiedeva nel fatto che, all'epoca, Sony non disponeva di misure di sicurezza adeguate, nemmeno quelle più basilari. Di conseguenza, era impensabile che potesse implementare strumenti avanzati come l'intelligenza artificiale per difendersi in modo efficace. Nel 2011, l'intelligenza artificiale non aveva ancora il ruolo cruciale che ha oggi nella sicurezza informatica. A

[111] **IBM**, *Che cos'è un sistema di rilevamento delle intrusioni (IDS)?,* https://www.ibm.com/it-it/topics/intrusion-detection-system

quel tempo, per esempio, l'adozione degli assistenti vocali era in rapida espansione, con Apple che lanciava Siri come uno dei primi assistenti vocali di massa. Pertanto, è difficile stabilire se, anche con l'intelligenza artificiale in uso, la Sony avrebbe potuto evitare o contrastare l'attacco. Sebbene gli algoritmi avanzati possano certamente migliorare la sicurezza e facilitare il rilevamento delle minacce, non è realistico pensare che sole le tecnologie di intelligenza artificiale sarebbero state sufficienti. La Sony, durante quel periodo, presentava numerose vulnerabilità nella sua sicurezza, e l'intelligenza artificiale, sebbene utile, non sarebbe stata una "salvaguardia" definitiva senza altre misure di protezione solide. Infatti, è impensabile fare affidamento esclusivamente sugli algoritmi, trascurando altre azioni fondamentali come l'addestramento dei dipendenti a riconoscere situazioni di rischio (i quali, infatti, sono i primi bersagli di attacchi di phishing) e una difesa mirata contro attacchi specifici. Questi erano precisamente gli aspetti che mancavano nella strategia di sicurezza della Sony al momento dell'attacco. Infatti, l'intelligenza artificiale oggi gioca un ruolo essenziale nella protezione delle organizzazioni, nel 2011 la sua applicazione nel contesto della cybersecurity era ancora embrionale, e il vero problema per Sony era la carenza di un approccio olistico alla sicurezza informatica. Quest'ultima è quella che oggi chiameremmo *incident response* che "è quell'attività necessaria nel momento in cui un'azienda si trova a dover fronteggiare un attacco o un incidente di sicurezza e comprende tutte le fasi di gestione, contenimento, mitigazione e ripristino dei sistemi[112]". Rispetto al contesto in cui operava Sony nel 2011, oggi è fondamentale avere personale specializzato in queste attività. Ad esempio, nel caso di un attacco ransomware, la risoluzione potrebbe avvenire ripristinando i backup, o, purtroppo, pagando il riscatto. Tuttavia, se il ripristino avviene senza seguire un approccio strutturato di incident response, è possibile che, anche dopo giorni o settimane di lavoro, l'attaccante abbia mantenuto una persistenza nei backup o che le vulnerabilità che hanno permesso l'intrusione non siano state effettivamente corrette. In questo caso, l'azienda potrebbe ritrovarsi da capo, senza aver realmente neutralizzato la minaccia. Per questo motivo, è essenziale adottare un piano di incident response per garantire che ogni fase del ripristino avvenga con un approccio sicuro e sistematico. Oggi molte aziende sono strutturate attorno a un incident plan, un piano che definisce chiaramente come agire e chi contattare in caso di incidente. Questo approccio consente di rispondere in modo rapido ed efficiente, aumentando significativamente l'efficacia e la tempestività dell'intervento. Va anche sottolineato che nel 2011, quando Sony subì l'attacco, non tutti i settori erano pronti a rispondere alle nuove sfide legate all'intelligenza artificiale. Sebbene ci fosse

[112]**MEGGIATO R**, *Incident response: i consigli per costruire una efficace strategia di risposta ai cyber attacchi, 2022*, https://www.cybersecurity360.it/soluzioni-aziendali/incident-response-i-consigli-per-costruire-una-efficace-strategia-di-risposta-ai-cyber-attacchi/

interesse e ricerca in questo ambito, l'intelligenza artificiale non era ancora una tecnologia completamente adottata nel mondo aziendale. Molte aziende stavano iniziando a investire in questo campo emergente, ma la visione di intelligenza artificiale che abbiamo oggi era ben lontana dalla realtà di tredici anni fa. Un momento simbolico di quell'anno fu la vittoria di IBM Watson contro due campioni umani nel quiz televisivo Jeopardy. Watson, utilizzando tecniche avanzate di intelligenza artificiale, esaminava rapidamente le opzioni di risposta, assegnando loro un grado di affidabilità e completando il processo in meno di tre secondi. Questo evento segnò una pietra miliare nell'evoluzione dell'IA, ma la sua applicazione nel campo della cybersecurity era ancora lontana dall'essere una realtà consolidata nelle aziende. Essa ha "ha acceso la curiosità per le "macchine in grado di pensare" e ha esteso le possibilità di applicazione dell'AI in ambito aziendale[113]". L'evento rappresentato dalla vittoria di IBM Watson nel quiz televisivo Jeopardy ha messo in evidenza la potenza dell'elaborazione del linguaggio naturale e dell'intelligenza artificiale, suscitando un crescente interesse tra le aziende riguardo alle potenzialità di queste tecnologie nei diversi settori. All'epoca l'utilizzo del machine learning e il deep learning che "è un sottoinsieme di machine learning che utilizza reti neurali multilivello, chiamate reti neurali profonde, per simulare il complesso potere decisionale del cervello umano[114]", stavano ancora emergendo in quell'anno ma non erano ancora così diffusi nelle soluzioni aziendali. Oggi, invece, le organizzazioni che implementano l'intelligenza artificiale sono più numerose di quelle che non lo fanno, soprattutto a causa dell'incremento delle violazioni della sicurezza informatica in vari settori, tra cui quello sanitario. In effetti, "circa la metà (47%) di tutte le organizzazioni sanitarie ha dichiarato di aver subito una violazione dei dati pari o superiore a 1 milione di dollari[115]". Questo perché:

"dal 2018 a oggi, gli attacchi sono aumentati del 61,5%, in Italia la crescita complessiva raggiunge ben il 300%. Secondo il rapporto Clusit, nei primi sei mesi del 2023 gli attacchi cyber sono aumentati del 40% nel nostro Paese e oltre il 35% è andato a buon fine grazie al malware, la principale tecnica di incursione utilizzata dai criminali[116]".

---

[113] **IBM**, *Da IBM Watson a watsonx*, https://www.ibm.com/it-it/watson

[114]**HOLDSWORTH J, SCAPICCHIO M**, *Cos'è il deep learning?*, https://www.ibm.com/it-it/topics/deep-learning

[115]**L.O**, *Cybersecurity, inizia l'era della DefenseGpt: il 69% delle aziende userà la* GenAI, 2023, https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-inizia-lera-della-defencegpt-il-69-delle-aziende-usera-la-genai/

[116] **CARUCCI M**, *Sicurezza informatica. Più attacchi con l'intelligenza artificiale*, 2024, https://www.avvenire.it/economia/pagine/sicurezza-informatica-piu-attacchi-con-l-avvento-dell-intelligenza-artificiale

Sebbene l'intelligenza artificiale rappresenti uno strumento potente nella protezione dei sistemi, non è una garanzia di inattaccabilità. È fondamentale che venga integrata con altri strumenti e misure di sicurezza, altrimenti si rischia di sottovalutare l'importanza di approcci umani e altri strumenti nel lungo processo di adattamento alla tecnologia e ai cambiamenti. Immaginiamo un'azienda che utilizza un sistema basato sull'intelligenza artificiale per filtrare le e-mail sospette e bloccare i tentativi di phishing. Tuttavia, un attaccante esperto riesce a creare un'e-mail che imita perfettamente la comunicazione di un fornitore affidabile, aggirando i filtri dell'IA. Se i dipendenti si affidano completamente al sistema e non sono adeguatamente formati per riconoscere segnali di phishing (come un dominio leggermente alterato o una richiesta insolita di trasferimento di fondi), potrebbero cadere nella trappola, compromettendo la sicurezza aziendale. Questo dimostra che, sebbene l'intelligenza artificiale sia un alleato potente, non è mai sufficiente da sola: è necessario un controllo umano e il buon senso. Nel settore dell'industria videoludica, l'intelligenza artificiale svolge principalmente un ruolo creativo, come evidenziato dal Gaming Report di Unity Technologies 2024. In questo ambito, l'IA viene utilizzata per sviluppare nuovi personaggi, velocizzare la creazione di modelli 3D, superfici dettagliate, sequenze video e movimenti animati, offrendo un'esperienza utente unica piuttosto che migliorare la sicurezza informatica. Sony, nel corso degli anni, ha abbracciato questi algoritmi per fornire un'esperienza innovativa ai suoi utenti, con grafiche in 3D e l'uso di algoritmi per ottimizzare la creazione dei giochi e ridurre i costi, raggiungendo pubblici sempre più ampi. Un esempio significativo di innovazione grazie all'IA è il sistema di comando vocale, che è diventato uno degli aggiornamenti più apprezzati per la comodità di navigare e giocare senza l'uso del controller. Esso "è una periferica per sistemi di intrattenimento, usato per fornire l'input in un videogioco. Un controller è tipicamente connesso a una console o a un computer da un cavo o da una connessione senza fili[117]". Bisogna sottolineare come, anche a livello normativo, la situazione si sia evoluta già prima del caso dell'attacco alla PSN di Sony del 2011. Oggi la questione della violazione della privacy risulta ancora più complessa e articolata, con conseguenze sanzionatorie più severe. Non tutti i comportamenti hanno lo stesso peso in termini di conseguenze, e negli anni sono stati introdotti nuovi reati che prevedono sanzioni più rigide per le violazioni del Regolamento, garantendo una protezione più efficace della privacy e prevenendo ulteriori infrazioni. Ad esempio, nel contesto lavorativo, il controllo illecito delle e-mail aziendali dei dipendenti costituisce una violazione. Se

[117] **WIKIPEDIA**, *Controller (videogiochi)*, https://it.wikipedia.org/wiki/Controller_(videogiochi)#:~:text=Un%20controller%2C%20detto%20anche%20game,l'input%20in%20un%20videogioco.&text=Un%20controller%20%C3%A8%20tipicamente%20connesso,da%20una%20connessione%20senza%20fili.

un'azienda monitora sistematicamente le comunicazioni senza informare i lavoratori, accedendo illegittimamente ai contenuti personali senza una motivazione legittima, si verifica una violazione dell'articolo 13 e 14 del GDPR. Il datore di lavoro può accedere alle informazioni dei dipendenti solo se strettamente necessario per ragioni lavorative, evitando trattamenti eccessivi o non autorizzati. Inoltre, è vietato l'accesso a informazioni condivise online, ad esempio sui social network, senza il consenso del dipendente, in quanto ciò comporterebbe una grave mancanza di trasparenza e una lesione del diritto alla privacy. Questa situazione implica anche una violazione una dello statuto del lavoratore regolato dall'art. 4 L. 300/1970 che stabilisce che:

È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalita' di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna[118]".

Il dipendente si trova nella situazione di non sapere se il datore di lavoro ha accesso anche ad altre informazioni senza che lui lo sappia. Per questo l'articolo 615 ter del Codice Penale dichiara che "chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni[119]". Infine, c'è una supervisione eccessiva da parte del datore di lavoro nei confronti del dipendente, che si configura come una vera violazione della privacy e della libertà del personale del dipendente. A riguardo l'articolo 32 del GDPR tratta proprio la sicurezza del trattamento dove "tra le predette misure vi è certamente la formale, e precisa individuazione e ripartizione dei ruoli e relative responsabilità interne all'azienda in materia di trattamento dati nonché l'adozione di un regolamento aziendale (da condividere necessariamente con i soggetti destinatari) per il corretto utilizzo degli strumenti informatici, dei dispositivi aziendali (smartphone, PC, tablet

[118] **GAZZETTA UFFICIALE**, *Art. 4. (Impianti audiovisivi)*, https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=4&art.versione=1&art.codiceRedazionale=070U0300&art.dataPubblicazioneGazzetta=1970-05-27&art.idGruppo=1&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=0#:~:text=Art.,dell'attivita'%20dei%20lavoratori.

[119] **BROCARDI.IT**, *Dispositivo dell'art. 615 ter Codice Penale*, https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-iv/art615ter.html#:~:text=Dispositivo%20dell'art.,615%20ter%20Codice%20Penale&text=Chiunque%20abusivamente%20si%20introduce%20in,reclusione%20fino%20a%20tre%20anni.

ecc.), della posta elettronica e della rete internet onde codificare cogenti regole comportamentali[120]". Un altro aspetto rilevante riguarda il trattamento illecito dei dati dopo la cessazione del rapporto di lavoro. Se l'azienda continua ad accedere alla posta elettronica dell'ex dipendente si configura una violazione dei principi di liceità, minimizzazione e limitazione della conservazione. A riguardo il dipendente potrebbe fare causa per la violazione della privacy e ottenere un risarcimento danni e l'azienda potrebbe subire una sanzione che "ammonta fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente fino al 4%[121]". Ovviamente qualsiasi caso ha bisogno che sia valutato e provato e che ci sia una davvero una violazione della privacy che porteranno a delle conseguenze dipenderanno in base al fatto concreto. Per questo, nel caso di determinate violazioni del Regolamento il Codice della privacy stabilisce delle conseguenze ben precise: ad esempio l'art 167 D.lgs. 196/2003 al comma 1 del Codice della privacy stabilisce che:

"salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi[122]".

L'articolo in questione vuole salvaguardare i dati personali del soggetto in modo che determinate azioni non rimangano impunibili e soprattutto che non riaccadano di nuovo nel lungo periodo. In particolare, esso intende a fermare eventuali azioni fraudolenti che possano compromettere la privacy degli individui. Un altro reato che comporta una violazione della privacy di un soggetto è quello stabilito dall'art. 167 bis D.lgs. 196/2003 comma 1 del Codice della privacy che stabilisce che:

"salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2 ter, 2 sexies e 2 octies, è punito con la reclusione da uno a sei anni[123]".

---

[120] **BIONDI A**, *Violazione della privacy: la responsabilità disciplinare e risarcitoria del dipendente*, 2023, https://www.cybersecurity360.it/legal/privacy-dati-personali/violazione-della-privacy-la-responsabilita-disciplinare-e-risarcitoria-del-dipendente/#post-69016-footnote-5

[121] **PANETTA R**, *Gdpr, sanzioni e responsabilità: tutto ciò che c'è da sapere*, 2018, https://www.agendadigitale.eu/sicurezza/privacy/gdpr-sanzioni-e-responsabilita-tutto-cio-che-ce-da-sapere/

[122] **BROCARDI.IT**, *Articolo 167 Codice della privacy*, https://www.brocardi.it/codice-della-privacy/parte-iii/titolo-iii/capo-ii/art167.html

[123] **BROCARDI.IT**, *Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*, https://www.brocardi.it/codice-della-privacy/parte-iii/titolo-iii/capo-ii/art167bis.html

La norma mira a sanzionare le condotte illecite legate alla violazione dei dati personali, prevenendo pratiche non autorizzate come l'acquisizione illegale o la vendita non consentita di informazioni sensibili. L'obiettivo è garantire che la sicurezza e la protezione dei dati rimangano una priorità assoluta, imponendo severe conseguenze a chiunque ne faccia un uso improprio. Per quanto riguarda l'acquisizione illecita di dati personali, l'art art. 167 ter D.lgs. 196/2003 comma 1 del Codice della privacy disciplina questo concetto su larga scala dichiarando che:

"salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni[124]".

Esso vuole essere un mezzo per evitare furti o acquisizioni non consentite che possano causare danno ad esempio ai cittadini, sia in termini di privacy sia in termini di incolumità, e per questo che tale norma intende salvaguardare la privacy delle persone impedendo che informazioni delicate cadano nelle mani sbagliate per scopi illeciti e dannosi. Dopodiché la violazione della privacy si ha nel caso di violazione dell'art. 168 D.lgs. 196/2003 che al comma 1 dichiara che "salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni[125]". L'obiettivo della norma in questione è quella di garantire l'integrità dei procedimenti e delle indagini svolte dal Garante, evitando che ci siano informazioni non veritiere che possono modificare l'esito riguardante i procedimenti legati alla protezione dei dati personali. Fornire informazioni false o ingannevoli potrebbe compromettere la verifica della conformità al GDPR e alle normative nazionali sulla protezione dei dati, danneggiando sia gli individui che i processi di regolamentazione. Le indagini da parte del Garante devono mantenere una propria integrità e al contempo qualsiasi decisione che viene presa deve essere rispettata. Tutto ciò ci fa capire come la normativa in relazione alla tutela della privacy ha reso più solido il quadro normativo sulla protezione dei dati personali, introducendo nuove fattispecie di reato e adeguando le normative esistenti alle disposizioni del Regolamento (UE) 2016/679 (GDPR). Inoltre, con il passare del tempo l'integrazione tra il Codice Privacy e il GDPR ha rafforzato le garanzie per gli interessati, evitando sovrapposizioni sanzionatorie e potenziando le misure punitive per contrastare in modo più efficace le violazioni della

[124] **BROCARDI.IT**, *Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*, https://www.brocardi.it/codice-della-privacy/parte-iii/titolo-iii/capo-ii/art167ter.html

[125] **TOGA**, *Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*, 2018, https://app.toga.cloud/codici/codice-della-privacy/14/13947/art-168-falsita-nelle-dichiarazioni-al-garante-e-interruzione-dell-esecuzione-dei-compiti-o-dell-esercizio-dei-poteri-del-garante

privacy. Oggi maggiormente l'inasprimento delle pene per il trattamento illecito, la diffusione su larga scala e l'acquisizione fraudolenta di dati personali evidenzia la crescente attenzione del legislatore alla tutela delle informazioni sensibili, in un contesto sempre più esposto ai rischi della digitalizzazione. Inoltre, la violazione della PSN ha coinvolto ben 77 milioni di utenti, rappresentando un grave attacco alla privacy. Un episodio di tale portata avrebbe potuto dar luogo a quello che oggi è noto come *doxing*, con la diffusione non autorizzata di dati sensibili online e conseguenze potenzialmente dannose per le vittime. Esso infatti, "è la pratica di cercare e diffondere pubblicamente online informazioni personali e private (come ad es. nome e cognome, indirizzo, numero di telefono etc.) o altri dati riguardanti una persona, di solito con intento malevolo[126]". Questo fenomeno può avere conseguenze gravi per l'utente, il cui nome, cognome e altri dati personali possono finire esposti sul web. I social network, spesso utilizzati per raccogliere informazioni con estrema facilità, rappresentano oggi uno dei principali punti di vulnerabilità per la privacy. Inoltre, questo fenomeno può danneggiare gravemente la reputazione dell'utente o dell'organizzazione coinvolta, poiché le informazioni diffuse online, spesso difficili da controllare o smentire, possono avere un impatto duraturo sull'immagine pubblica. Il doxing non solo porta a una violazione della privacy e dell'immagine ma riguarda ancora di più la sicurezza dell'individuo soprattutto in un'era sempre più digitale. La divulgazione di determinate informazioni può avere conseguenze devastanti per la vittima, tra cui atti di molestia, uso fraudolento di dati personali che possono portare il criminale a creare un'identità falsa con i dati rubati e, in alcuni casi, rischi per l'incolumità fisica delle vittime. Il collegamento con il caso dell'attacco alla PSN sta nel fatto che non sappiamo se i dati di 77 milioni di utenti sia stato fenomeno di doxing, perché non c'è mai stata una certezza all'epoca dell'attacco di quanto e cosa è stato precisamente violato e soprattutto se ce stata una diffusione online di dati sottratti agli utenti della Sony. All'epoca dell'attacco alla PSN nel 2011, Sony non avrebbe potuto immaginare che un fenomeno oggi così diffuso, come il doxing, potesse esserne una possibile conseguenza. Se un episodio simile si verificasse oggi, le ripercussioni sarebbero ancora più gravi: i dati di 77 milioni di utenti potrebbero essere diffusi nel darknet che "è una rete virtuale privata, situata nel dark web, nella quale gli utenti si connettono solamente con persone di cui si fidano[127]", su forum dedicati, facilitando la compravendita di informazioni sensibili da parte di cybercriminali per scopi illeciti. Le possibili conseguenze di un attacco come quello subito da Sony nel 2011 sarebbero state estremamente gravi, soprattutto se si fosse verificato in un contesto attuale. Innanzitutto, il furto di dati avrebbe potuto

[126] **WIKIPEDIA**, *Doxing*, https://it.wikipedia.org/wiki/Doxing

[127] **WIKIPEDIA**, *Darknet*, https://it.wikipedia.org/wiki/Darknet

consentire agli hacker di aprire conti bancari, sottoscrivere contratti o effettuare transazioni illegali a nome delle vittime. Un altro rischio concreto legato a un possibile caso di doxing sarebbe stato quello delle molestie e delle minacce personali: gli utenti della PlayStation Network avrebbero potuto ritrovarsi bersaglio di ricatti e intimidazioni, con la costante paura che le proprie informazioni sensibili venissero utilizzate contro di loro. Un'ulteriore conseguenza critica avrebbe riguardato la sicurezza finanziaria: se i dettagli delle carte di credito o dei metodi di pagamento fossero stati esposti, avrebbero potuto essere utilizzati per transazioni fraudolente. Inoltre, i cybercriminali, una volta entrati in possesso dei dati personali degli utenti, avrebbero potuto assumere la loro identità per aprire conti finanziari, sottoscrivere servizi o addirittura ottenere crediti e prestiti senza il consenso dei legittimi proprietari. Non si può escludere, poi, che gli hacker avrebbero avuto accesso a messaggi privati o altre informazioni riservate degli utenti, minacciandoli di rivelarle a familiari, amici o colleghi. Un'altra possibile tecnica di attacco sarebbe stata l'invio di e-mail fraudolente, apparentemente provenienti da Sony o da servizi affiliati, con l'obiettivo di ingannare gli utenti e spingerli a fornire ulteriori credenziali di accesso o informazioni bancarie. All'epoca dell'attacco, le infrastrutture di sicurezza informatica di Sony non erano particolarmente robuste, rendendola un bersaglio vulnerabile. Solo dopo la violazione, l'azienda ha adottato misure più avanzate, come sistemi di crittografia più sofisticati e un monitoraggio della rete più efficace. Tuttavia, sebbene Sony avesse dichiarato che i dati delle carte di credito fossero criptati, non si poteva escludere il rischio che gli hacker fossero comunque riusciti a decifrarli o a ottenere informazioni sufficienti per compiere frodi online. Questo caso dimostra chiaramente come l'assenza di adeguati strumenti di protezione possa portare a fenomeni di doxing su larga scala, con conseguenze devastanti per gli utenti. Oggi, con l'entrata in vigore del Regolamento UE 2016/679 (GDPR), un attacco simile avrebbe avuto un impatto diverso, sia in termini di gestione della crisi che di responsabilità legale. Sony sarebbe stata obbligata ad adottare misure di sicurezza più stringenti e a notificare tempestivamente la violazione dei dati personali agli utenti e alle autorità competenti, garantendo maggiore trasparenza e tutele più efficaci per i consumatori. Infatti, riguardo al ritardo con cui Sony comunicò la violazione, il GDPR prevede misure specifiche per tutelare gli utenti in situazioni simili a quelle affrontate dai clienti della PSN. In particolare, l'articolo 33 impone l'obbligo di notifica tempestiva in caso di violazione dei dati personali. Il comma 1 dello stesso articolo stabilisce che:

"In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un

rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo[128]".

Inoltre, il GDPR all'articolo 34 stabilisce anche che "quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo[129]". Il GDPR avrebbe imposto a Sony l'obbligo di comunicare la violazione agli utenti entro 72 ore, garantendo una maggiore tutela dei consumatori e limitando il danno reputazionale per l'azienda. Una risposta tempestiva e trasparente avrebbe infatti contribuito a preservare la fiducia degli utenti nel marchio. Inoltre, il GDPR stabilisce specifici obblighi di sicurezza, disciplinati dall'articolo 32, che avrebbero richiesto a Sony di implementare misure di protezione più efficaci per tutelare i dati personali, colmando le evidenti lacune emerse nell'attacco del 2011. Un aspetto fondamentale introdotto dal GDPR è la supervisione rigorosa delle autorità di protezione dei dati, che avrebbero potuto imporre a Sony l'adozione di strategie di sicurezza più avanzate e maggiore trasparenza nella gestione dell'incidente, con il rischio di sanzioni severe in caso di non conformità. L'entrata in vigore del GDPR ha rappresentato un passo significativo nella protezione dei dati personali, imponendo obblighi più stringenti alle aziende che gestiscono informazioni sensibili. Rispetto al contesto in cui avvenne l'attacco alla PSN, oggi vi è una maggiore attenzione alla sicurezza informatica, considerata un elemento essenziale per le organizzazioni che operano nel digitale. Le aziende hanno una responsabilità più elevata nell'adozione di misure adeguate alla protezione dei dati personali, con il rischio di pesanti sanzioni in caso di negligenza. Il GDPR ha inoltre rafforzato i diritti degli utenti, consolidando il diritto di accesso, il diritto alla cancellazione (diritto all'oblio) e il diritto alla portabilità dei dati, promuovendo maggiore trasparenza nella gestione delle informazioni personali. L'introduzione di sanzioni più severe ha reso il mancato rispetto della normativa estremamente oneroso per le aziende: una violazione come quella subita da Sony nel 2011 oggi comporterebbe multe di entità significativamente maggiore. Inoltre, il GDPR ha ampliato la responsabilità delle imprese nel trattamento dei dati, imponendo in alcuni casi la nomina di un Responsabile della Protezione dei Dati (DPO) e l'implementazione di rigorose politiche interne per garantire la sicurezza e la conformità. Le aziende che trattano dati sensibili o operano su larga scala sono obbligate a condurre una valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment -

[128] **GDPR TEXT**, *Articolo 33 RGPD. Notifica di una violazione dei dati personali all'autorità di controllo*, https://gdpr-text.com/it/read/article-33/

[129] **BROCARDI.IT**, *Comunicazione di una violazione dei dati personali all'interessato*, https://www.brocardi.it/regolamento-privacy-ue/capo-iv/sezione-2/art34.html

DPIA) prima di avviare nuovi trattamenti, per identificare e mitigare potenziali rischi. Inoltre, l'attuale quadro normativo prevede un controllo più stringente da parte delle autorità di protezione dei dati, come il Garante italiano, che hanno il potere di effettuare indagini, emettere ordini vincolanti e imporre sanzioni alle aziende non conformi. In definitiva, il GDPR ha reso il sistema di protezione dei dati molto più rigoroso rispetto al periodo in cui avvenne l'attacco alla PSN di Sony. Oggi, le aziende devono non solo adottare misure preventive per evitare violazioni, ma anche rispondere rapidamente ed efficacemente nel caso in cui si verifichino, affrontando conseguenze legali ed economiche più severe. In un mondo sempre più digitale e interconnesso, la protezione della privacy e la sicurezza dei dati rappresentano una priorità imprescindibile per tutte le organizzazioni. In conclusione, possiamo dire che l'attacco alla PSN di Sony nel 2011 ha segnato un punto di svolta nella consapevolezza globale sulla cybersecurity, evidenziando l'importanza di strategie di protezione sempre più avanzate per la salvaguardia dei dati sensibili. Da allora, il panorama della sicurezza informatica ha subito un'evoluzione significativa, con l'adozione di misure più stringenti sia a livello aziendale che normativo. Il rafforzamento delle strategie di prevenzione, la diffusione di programmi di sensibilizzazione e l'introduzione di tecnologie avanzate, come l'intelligenza artificiale e il machine learning, hanno reso le organizzazioni più resilienti di fronte alle minacce informatiche. Tuttavia, la crescente sofisticazione degli attacchi dimostra che la sicurezza informatica è un processo in continua evoluzione, che richiede un approccio olistico e dinamico. Le aziende non possono limitarsi a implementare strumenti tecnologici avanzati, ma devono promuovere una cultura della sicurezza che coinvolga attivamente dipendenti, stakeholder e utenti finali. Inoltre, il rafforzamento del quadro normativo con il GDPR ha imposto obblighi più stringenti in materia di protezione dei dati, contribuendo a garantire una maggiore trasparenza e accountability da parte delle imprese. L'attacco alla Sony è stato un monito per l'intero settore digitale, dimostrando che la sicurezza informatica non può più essere considerata un costo secondario, ma un investimento strategico fondamentale per la protezione della privacy, la tutela della fiducia dei consumatori e la stabilità economica delle imprese. In un'epoca caratterizzata dall'interconnessione globale e dall'uso crescente di tecnologie avanzate, la sfida della cybersecurity è più attuale che mai: solo attraverso un impegno costante nell'innovazione e nella prevenzione sarà possibile affrontare con successo le minacce del futuro.

CONCLUSIONE

La cybersecurity si conferma oggi come un pilastro essenziale per la protezione dei dati, delle infrastrutture critiche e della privacy individuale. L'evoluzione delle minacce informatiche ha dimostrato che nessuna organizzazione, pubblica o privata, può considerarsi immune dagli attacchi informatici, rendendo necessaria una strategia globale di prevenzione, mitigazione e risposta agli incidenti. Analizzando l'evoluzione storica delle minacce digitali, si comprende come gli attacchi informatici siano passati da semplici atti di vandalismo digitale a strumenti sofisticati di spionaggio, sabotaggio e crimine organizzato. Eventi come l'attacco alla Sony nel 2011 hanno evidenziato le vulnerabilità dei sistemi aziendali e l'importanza di strategie di sicurezza avanzate. La violazione del PlayStation Network ha compromesso milioni di dati sensibili degli utenti, causando danni economici e di reputazione considerevoli per l'azienda. Questo episodio ha spinto molte multinazionali a riconsiderare le proprie politiche di sicurezza, rafforzando gli investimenti nella protezione dei dati e nella resilienza informatica. L'adozione di modelli di sicurezza come la triade CIA (Confidentiality, Integrity, Availability) e il framework DREAD ha fornito una base solida per l'analisi e la gestione del rischio informatico. Tuttavia, con l'avvento delle tecnologie emergenti, come l'intelligenza artificiale e il machine learning, si sta assistendo a un'evoluzione delle strategie di difesa. L'uso dell'UEBA (User and Entity Behavior Analytics) permette oggi di identificare comportamenti anomali all'interno delle reti, contribuendo a un approccio proattivo nella cybersecurity. Le normative, come il GDPR, hanno imposto standard rigorosi per la protezione dei dati personali, costringendo le aziende a implementare misure di sicurezza adeguate. L'impatto della regolamentazione ha favorito una maggiore consapevolezza sui temi della privacy e della protezione delle informazioni, delineando un quadro normativo sempre più stringente e necessario per contrastare le minacce informatiche. Le sfide future nella cybersecurity saranno sempre più complesse e richiederanno un impegno congiunto da parte di governi, aziende e singoli utenti. La protezione della proprietà intellettuale, la salvaguardia delle infrastrutture critiche e la resilienza alle minacce informatiche diventeranno elementi imprescindibili per garantire la sicurezza globale. La collaborazione internazionale e lo sviluppo di tecnologie avanzate saranno fondamentali per contrastare la crescente sofisticazione degli attacchi. In definitiva, investire nella cybersecurity non rappresenta solo una necessità tecnica, ma un imperativo strategico per la protezione dell'economia digitale e della società moderna. L'approccio alla sicurezza informatica deve essere dinamico, adattabile e basato su una cultura della prevenzione e della formazione continua. Solo attraverso un impegno costante e condiviso sarà possibile costruire un ecosistema digitale sicuro, resiliente e capace di affrontare le sfide future con determinazione ed efficacia.

SITOGRAFIA

ACCADEMIA ITALIANA PRIVACY, *Sicurezza dei dati: pseudonimizzazione o anonimizzazione?,* 2022, https://www.accademiaitalianaprivacy.it/dettaglioNews.asp?id=646#:~:text=Il%20dato%20anonimo%20non%20%C3%A8%20definito%20nel%20GDPR&text=%E2%80%9Cdecifratura%20non%20autorizzata%20della%20pseudonimizzazione,possibile%20%E2%80%9Criaccoppiare%E2%80%9D%20le%20informazioni.

ACRONIS, *È necessario un software antivirus per Linux?*, https://www.acronis.com/it-it/blog/posts/linux-antivirus/#:~:text=Per%20gli%20hacker%20che%20desiderano,rispetto%20ad%20altri%20sistemi%20operativi.

ADONOPOULOS G, **NAPOLETANO E,** *Proof of Work: cos'è e come funziona,* https://www.forbes.com/advisor/it/investire/criptovalute/proof-of-work-significato/

AGENZIA PER L'ITALIA DIGITALE, *linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/ privacy by design*, https://www.agid.gov.it/sites/default/files/repository_files/documentazione/linee_guida_modellazione_minacce_e_individuazione_azioni_di_mitigazionev1.0.pdf

AGICAP, *Cosa si intende per asset di un'azienda*, https://agicap.com/it/articolo/asset-aziendale/

AI CORPORATE, *RSA Security*, https://aicorporate.it/companies-a-z/Details/10197

AKAMAI, *Che cos'è un attacco DDoS?,* https://www.akamai.com/it/glossary/what-is-ddos

AKAMAI, *Che cos'è una rete per la distribuzione dei contenuti (CDN)?*, https://www.akamai.com/it/glossary/what-is-a-cdn

ALABISO A, IANNILLI L, *Cyber e human espionage: un approccio olistico alla cyberwarfare,* 2022, https://www.cybersecurity360.it/nuove-minacce/cyber-e-human-espionage-un-approccio-olistico-alla-cyberwarfare/

ALTALEX, *Art. 32 GDPR - Sicurezza del trattamento*, 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-32-gdpr-sicurezza-del-trattamento

ALTALEX, *Art. 5 GDPR - Principi applicabili al trattamento di dati personali*, 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-5-gdpr-principi-trattamento-di-dati-personali

ALTALEX, *Art. 6 GDPR - Liceità del trattamento*, 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-6-gdpr-liceita-del-trattamento

ALTALEX, *Art. 83 GDPR - Condizioni generali per infliggere sanzioni amministrative pecuniarie,* 2019, https://www.altalex.com/documents/news/2018/04/12/articolo-83-gdpr-condizioni-generali-per-infliggere-sanzioni-amministrative-pecuniarie

ALWAREBYTES, *Che cos'è il malware?*, https://www.malwarebytes.com/it/malware?srsltid=AfmBOoo0aaUwVWS44pjZUL3ERrLSrdmZ9ILsK4l35ZJk7_8HV3POB4F7

ALWAREBYTES, *Che cos'è un virus polimorfico?,* https://www.malwarebytes.com/it/polymorphic-virus

ALWAREBYTES, *cos'è il BSOD - Blue Screen Of Death*, https://www.malwarebytes.com/it/cybersecurity/computer/blue-screen-of-death

ALWAREBYTES, *Cryptojacking: di cosa si tratta?,* https://www.malwarebytes.com/it/cryptojacking

AMALFITANO R, *La storia di PlayStation 3*, https://gameplay.cafe/retrogaming/la-storia-di-playstation-3/#:~:text=All'inizio%20del%202005%2C%20l,di%20boomerang%20del%20controller%20Sixaxis

APP MASTER, *La guida completa all'alta disponibilità e al failover su DigitalOcean*, 2023, https://appmaster.io/it/blog/alta-disponibilita-e-failover-su-digitalocean

ASANA, *L'unica piattaforma di gestione del lavoro sviluppata per essere scalabile*, https://asana.com/it/product

ATLASSIAN TRELLO, *Trello consente ai gruppi di gestire task e progetti più facilmente*, https://trello.com/it/tour

ATLASSIAN, *Gestione degli imprevisti per i team high velocity,* https://www.atlassian.com/it/incident-management/kpis/reliability-vs-availability

AXITEA SECURITY EVOLUTION, *Cos'è lo Shadow IT: esempi di "IT ombra", rischi e soluzioni,* https://www.axitea.com/it/blog/cos-e-lo-shadow-it-esempi-di-it-ombra-rischi-e-soluzioni/

AZIONA, *API cosa sono e come funzionano*, 2021, https://www.azionadigitale.com/api-cosa-sono-e-come-funzionano/

AZZELLINI G, *Informazioni cyber e iniziativa di condivisione dell'intelligence (CIISI-UE),* 2023, https://www.antiriciclaggiocompliance.it/informazioni-cyber-e-iniziativa-di-condivisione-dellintelligence-ciisi-ue/

BALABIO B, ORLANDO B, *Record per il mercato italiano della cybersecurity: 2,15 miliardi di euro, +16%*, https://www.osservatori.net/cybersecurity-data-protection/comunicato-cybersecurity-italia-mercato-crescita/

BANFI F, *La differenza tra frode informatica e truffa*, 2023, https://www.dirittoconsenso.it/2023/05/11/la-differenza-tra-frode-informatica-e-truffa/

BASSANINI M, *Phishing: cos'è e come prevenirlo*, 2023, https://www.it-impresa.it/blog/phishing-attack/

BELLOJOS L, *Che cos'è un checksum e come usarlo*, 2024, https://www.ninjaone.com/it/blog/cos-e-un-checksum/

BIBLUS, *Disponibilità di un sistema: cos'è, come si calcola e in cosa differisce dalle metriche di affidabilità*, 2023, https://biblus.acca.it/disponibilita-di-un-sistema-cose-come-si-calcola-e-in-cosa-differisce-dalle-metriche-di-affidabilita/

BOCCHI C, *Conservazione dei dati, principio di limitazione e obbligo di cancellare quelli non (più) necessari*, 2022, https://www.cybersecurity360.it/legal/privacy-dati-personali/conservazione-dei-dati-principio-di-limitazione-e-obbligo-di-cancellare-quelli-non-piu-necessari/#:~:text=5%2C%20paragrafo%201%2C%20lettera%20e,sono%20trattati%20%5B%E2%80%A6%5D%C2%BB.

BONOMI E, *Il principio di finalità del trattamento nel GDPR*, 2023, https://www.studioessepi.it/magazine/privacy/principio-finalita-trattamento-gdpr

BOOLEBOX, *Cybersecurity e sanità: minacce, rischi e possibili soluzioni per un settore sempre più nel mirino degli hacker*, 2023, https://www.boolebox.com/it/cybersecurity-in-sanita-minacce-e-difese-possibili/#:~:text=Il%20settore%20sanitario%20%C3%A8%20stato,contro%20il%2012%25%20del%202022.

BORDIN A, *Sony estende il servizio "Video On Demand powered by Qriocity" all'Europa*, 2010, https://www.hwupgrade.it/news/multimedia/sony-estende-il-servizio-video-on-demand-powered-by-qriocity-all-europa_33601.html

BOZZO A, *Impariamo la privacy con il sorriso :-) l'art. 5 parte terza, il principio di esattezza*, 2023, https://www.consultingpb.com/blog/diritto-rovescio/impariamo-la-privacy-con-il-sorriso-lart-5-parte-terza-il-principio-di-esattezza/

BRESSANI C, *Storia ed evoluzione delle minacce Informatiche*, 2024, https://www.gesca.it/storia-ed-evoluzione-delle-minacce-informatiche/

BROCARDI.IT, *Accesso abusivo ad un sistema informatico o telematico*, https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-iv/art615ter.html#:~:text=Dispositivo%20dell'art.,615%20ter%20Codice%20Penale&text=Chiunque%20abusivamente%20si%20introduce%20in,reclusione%20fino%20a%20tre%20anni.

BROCARDI.IT, *Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*, https://www.brocardi.it/codice-della-privacy/parte-iii/titolo-iii/capo-ii/art167ter.html

BROCARDI.IT, *Comunicazione di una violazione dei dati personali all'interessato*, https://www.brocardi.it/regolamento-privacy-ue/capo-iv/sezione-2/art34.html

BROCARDI.IT, *Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala,* https://www.brocardi.it/codice-della-privacy/parte-iii/titolo-iii/capo-ii/art167bis.html

BROCARDI.IT, *Trattamento illecito di dati*, https://www.brocardi.it/codice-della-privacy/parte-iii/titolo-iii/capo-ii/art167.html

BRUNO G, *Diritto alla privacy: la storia e l'evoluzione*, 2023, https://www.diritto.it/diritto-alla-privacy-la-storia-e-l-evoluzione/#_ftn2

BUCHICCHIO E, CAPO D, *Breve storia dei malware: l'evoluzione delle specie dalle origini ai giorni nostri*, 2020, https://www.ictsecuritymagazine.com/articoli/breve-storia-dei-malware-levoluzione-delle-specie-dalle-origini-ai-giorni-nostri/

BUTTI G, *Le misure di sicurezza nel GDPR: quali sono, come applicarle, costi di attuazione*, 2021, https://www.cybersecurity360.it/legal/privacy-dati-personali/le-misure-di-sicurezza-nel-gdpr-quali-sono-come-applicarle-costi-di-attuazione/

BUTTI G, *Resilienza, contro gli attacchi informatici: linee guida per le aziende*, 2018, https://www.cybersecurity360.it/soluzioni-aziendali/resilienza-contro-gli-attacchi-informatici-linee-guida-per-le-aziende/#:~:text=propriet%C3%A0%20dei%20materiali%20di%20resistere,negativi%20ecc.%3A%20resilienza%20sociale.

CALZOLARI M, *Carte di pagamento: nel dark web si vendono "kit" di informazioni personali,* 2023, https://medium.com/@marcocamisanicalzolari/carte-di-pagamento-nel-dark-web-si-vendono-kit-di-informazioni-personali-450af160f89

CARUCCI M, *Sicurezza informatica. Più attacchi con l'intelligenza artificiale* , 2024, https://www.avvenire.it/economia/pagine/sicurezza-informatica-piu-attacchi-con-l-avvento-dell-intelligenza-artificiale

CHECK POINT, *Che cos'è il Trojan di accesso remoto (RAT)?,* https://www.checkpoint.com/it/cyber-hub/threat-prevention/what-is-remote-access-trojan/

CHECK POINT, *Che cos'è lo spyware?,* https://www.checkpoint.com/it/cyber-hub/threat-prevention/what-is-spyware/

CHECK POINT, *NOC e SOC a confronto*, https://www.checkpoint.com/it/cyber-hub/threat-prevention/what-is-soc/noc-vs-soc-whats-the-difference/#:~:text=Il%20NOC%20%C3%A8%20responsabile%20di,potrebbero%20interrompere%20tali%20operazioni%20commerciali

CHECK POINT, *SOC-as-a-Service*, https://www.checkpoint.com/it/cyber-hub/threat-prevention/what-is-soc/soc-as-a-service/

CHECK POINT, *Tipi di minacce alla sicurezza informatica*, https://www.checkpoint.com/it/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/

CHECK POINT, *What is Network Detection and Response (NDR)?,* https://www.checkpoint.com/it/cyber-hub/cloud-security/what-is-network-detection-and-response-ndr/#:~:text=What%20is%20Network%20Detection%20and,e%20l'analisi%20dei%20dati.

CNS TECH, *Cyber-spionaggio: cos'è, e come prevenirlo?*,2021, https://www.cnsspa.it/cyber-spionaggio-cose-e-come-prevenirlo/

COLACICCO C, *Privacy e cyber security, ecco le norme e le misure per proteggere i dati*, 2020, https://www.cybersecurity360.it/legal/privacy-dati-personali/privacy-e-cyber-security-ecco-le-norme-e-le-misure-per-proteggere-i-dati/

COLLINI M, *Anonimizzazione dei dati personali: un percorso per orientarsi,* 2021, https://privacygdpr.it/news-privacy-sanita/anonimizzazione-dei-dati-personali-un-percorso-per-orientarsi/#:~:text=Per%20essere%20pi%C3%B9%20precisi%2C%20il,riferiscono%20a%20una%20persona%20fisica

CONFERSERCENTI, *Sicurezza informatica: Confesercenti-SWG, un'impresa su quattro colpita, il 52% potenzierà sistemi di difesa nel 2023*, 2023, https://www.confesercenti.it/blog/sicurezza-informatica-confesercenti-swg-unimpresa-su-quattro-colpita-il-52-potenziera-sistemi-di-difesa-nel-2023/

CORRIERE DELLA SERA, *Secondo attacco hacker alla Sony: rubati i dati di altri 25 milioni di utenti,* 2011, https://www.corriere.it/cronache/11_maggio_03/sony-hacker-internet_03b16ed0-7564-11e0-88f0-a00eb5833fe6.shtml

COZZI P, *Videosorveglianza con riconoscimento facciale: cosa prevede il GDPR*, https://lumi4security.it/videosorveglianza-riconoscimento-facciale-cosa-prevede-gdpr/?utm_source=chatgpt.com

CYBEROO, *Nessun piano B: perché un Incident Response Plan è l'unico di cui hai bisogno*, 2024, https://blog.cyberoo.com/nessun-piano-b-perche-un-incident-response-plan-e-lunico-di-cui-hai-bisogno

CYBEROO, *NOC e SOC: differenze e opportunità per una cybersecurity efficace*, 2024, https://blog.cyberoo.com/noc-e-soc-differenze-e-opportunita-per-una-cyber-security-efficace#:~:text=I%20NOC%20si%20concentrano%20sulla,in%20atto%20dai%20criminali%20informatici

DAMATO A, *Soluzioni GRC: analisi dei rischi cyber tra limiti e opportunità*, 2024, https://www.ictsecuritymagazine.com/articoli/soluzioni-grc-analisi-dei-rischi-cyber-tra-limiti-e-opportunita/

DATA SUNRISE, *strategia di protezione dei dati*, https://www.datasunrise.com/it/centro-di-conoscenza/strategia-di-protezione-dei-dati/

DE ROGATIS D, *Flame: malware o cyber weapon?,* 2012, https://www.html.it/articoli/flame-malware-o-cyber-weapon/

DE STEFANO S, *Melissa: il virus informatico che il 26 marzo 1999 paralizzò il mondo*, 2020, https://leganerd.com/2020/03/26/melissa-il-virus-informatico-che-il-26-marzo-1999-paralizzo-il-mondo/

DEFENCE TECH, *1° attacco hacker della storia*, https://www.defencetech.it/2022/01/14/1-attacco-hacker-della-storia/#:~:text=Accadde%20il%202%20Novembre%201988,nei%20computer%20connessi%20ad%20Internet.

DELLA QUEVA I*, Reveton ransomware, 5 motivi per cui rimanere alla larga dall'infezione,* https://cyberment.it/ransomware-attacchi/reveton-ransomware-5-motivi-per-cui-rimanere-alla-larga-dallinfezione/

DI SANTO A, *La storia dell'hacking*, https://www.adora-ict.com/la-storia-dellhacking/

DORON P, *Dalla sicurezza delle applicazioni alla sicurezza della catena di fornitura del software: è necessario un nuovo approccio*, https://scribesecurity.com/it/blog/application-security-to-software-supply-chain-security/

DRAGONI G, *CISO: chi è e cosa fa un responsabile della sicurezza*, 2024, https://blog.osservatori.net/it_it/ciso-cosa-fa-responsabile-security?_gl=1*1n8r4y2*_ga*MTA0NTE1Mjk4LjE3Mjg3MjA0NzE.*_ga_8JFFBZLKC3*MTcyODgyOTQyOC40LjEuMTcyODgzMTQ2My4wLjAuMA.

EITCA, *Quali sono i controlli di accesso discrezionale (DAC) e i relativi limiti in termini di rischi per la sicurezza?,* 2023, https://it.eitca.org/cybersecurity/eitc-is-cssf-computer-systems-security-fundamentals/security-vulnerabilities-damage-mitigation-in-computer-systems/linux-containers/examination-review-linux-containers/what-are-discretionary-access-control-dac-and-its-limitations-in-terms-of-security-risks/

ENCYCLOPEDIA KASPERSKY, *1987*, https://encyclopedia.kaspersky.it/knowledge/year-1987/

ENCYCLOPEDIA KASPERSKY, *Anni '80*, https://encyclopedia.kaspersky.it/knowledge/years-1980s/#:~:text=Lehigh%20infettava%2C%20in%20primo%20luogo,%2C%20eventualmente%2C%20anche%20se%20stesso

FADDA D, *Sanità, attacco informatico al Fatebenefratelli Sacco di Milano: i dati sono online,* 2022, https://www.cybersecurity360.it/nuove-minacce/ransomware/attacco-informatico-allasst-fatebenefratelli-sacco-di-milano-potrebbe-essere-un-ransomware/#:~:text=Il%20gruppo%20criminale%20Vice%20Society%20ha%20rivendicato%20l'attacco%20informatico,e%20Macedonio%20Melloni%20di%20Milano.

FASTWEB PLUS, *Cos'è Cryptolocker e come evitarlo*, https://www.fastweb.it/fastweb-plus/digital-magazine/cos-e-cryptolocker-e-come-evitarlo/

FASTWEB PLUS, *La storia di Sony*, 2016, https://www.fastweb.it/fastweb-plus/digital-magazine/la-storia-di-sony/

FASTWEB PLUS, *Malware: cosa sono, come funzionano e come difendersi*, https://www.fastweb.it/fastweb-plus/digital-dev-security/i-malware-cosa-sono-cosa-fanno-e-perche-sono-pericolosi/

FATTURA 24, *DMCA Digital Millennium Copyright Act*, https://www.fattura24.com/glossario/d/dmca/

FELICI M, *firewall e controllo perimetrale*, 2020, https://www.computersec.it/2020/07/14/firewall-e-controllo-perimetrale/

FERAZZA F, *Vulnerabilità zero-day: cosa sono e come funziona il mercato nero degli exploit*, 2021, https://www.cybersecurity360.it/nuove-minacce/vulnerabilita-zero-day-cosa-sono-e-come-funziona-il-mercato-nero-degli-exploit/

FILADELFIO E, *Least privilege: dati al sicuro da accessi non autorizzati col principio del privilegio minimo*, 2021, https://www.cybersecurity360.it/soluzioni-aziendali/least-privilege-dati-al-sicuro-da-accessi-non-autorizzati-col-principio-del-privilegio-minimo/

FONDAZIONE MONDO DIGITALE, *Mission*, https://www.mondodigitale.org/chi-siamo

FRA: EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Carta dei diritti fondamentali dell'Unione europea*, https://fra.europa.eu/it/eu-charter/article/8-protezione-dei-dati-di-carattere-personale#:~:text=1.,fondamento%20legittimo%20previsto%20dalla%20legge.

FRANCHINA L, *Infrastrutture Critiche, cosa sono e come proteggerle*, 2016, https://www.ictsecuritymagazine.com/articoli/infrastrutture-critiche/

FREDIANI C, *Individuata la prima "arma digitale" per attacchi contro reti elettriche*, 2017, https://www.lastampa.it/esteri/2017/06/13/news/individuata-la-prima-arma-digitale-per-attacchi-contro-reti-elettriche-1.34582808/

GAZZETTA UFFICIALE, *Art. 4. (Impianti audiovisivi),* https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=4&art.versione=1&art.codiceRedazionale=070U0300&art.dataPubblicazioneGazzetta=1970-05-27&art.idGruppo=1&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=0#:~:text=Art.,dell'attivita'%20dei%20lavoratori.

GDPR TEXT, *Articolo 33 GDPR. Notifica di una violazione dei dati personali all'autorità di controllo*, https://gdpr-text.com/it/read/article-33/

GDPR TEXT, *Considerando 75*, https://gdpr-text.com/it/read/recital-75/

GDPR TEXT, *Considerando 85,* https://gdpr-text.com/it/read/recital-85/

GDPR, *Articolo 5 GDPR. Principi applicabili al trattamento di dati personali*, https://gdpr-text.com/it/read/article-5/#:~:text=or%20statistical%20purposes-,1.,in%20conformit%C3%A0%20del%20presente%20regolamento

GDPR: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Pagina informativa su minori, nuove tecnologie e protezione dei dati,* https://www.garanteprivacy.it/temi/minori#:~:text=L'articolo%2012%20del%20GDPR,informazioni%20destinate%20specificamente%20ai%20minori.

GDPR: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Titolare, responsabile e incaricato - Individuazione del 'titolare del trattamento' - 9 dicembre 1997 [30915],* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30915#:~:text=675%2F1996%2C%20il%20%22titolare,ci%C3%B2%20che%20riguarda%20la%20sicurezza.

GDPR: GARANTE PER LA PROTEZIONE DEI DATI, *Convenzione 108: pubblicata in Gazzetta Ufficiale la legge che ratifica in Italia il Protocollo di modifica,* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9585156#:~:text=La%20convenzione%20aggiornata%20prevede%20la,e%20di%20imporre%20sanzioni%20amministrative.

GDPR: GARNTE PER LA PROTEZIONE DEI DATI PERSONALI, *Cosa intendiamo per dati personali?,* https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/2002896#:~:text=Sono%20dati%20personali%20le%20informazioni,sua%20situazione%20economica%2C%20ecc..

GENERATION ITALY, *Come iniziare a lavorare nel settore della cybersecurity*, https://italy.generation.org/blog/come-iniziare-a-lavorare-nel-settore-della-cybersecurity/?utm_source=GoogleAds&utm_campaign=GoogleAds_CPC_B2C_Recurring_IT_2023_Q4_NPM___AWR_Text_BrandAboutGen__AdGrant_AllGroups_AllGroups__&urlRecruitmentChannel=GoogleAds_CPC_B2C_Recurring_IT_2023_Q4_NPM___AWR_Text_BrandAboutGen__AdGrant_AllGroups_AllGroups__&gad_source=1&gclid=Cj0KCQjwmOm3BhC8ARIsAOSbapXu7LMn-K7Ozj-vkuYhTTbzscZw0bOljQoEid16Gxrt3Su9cgc0MNsaApCMEALw_wcB

GIULIANO GROUP, *SOC as a Service, perché investire su Security Operations*, https://www.giulianogroup.it/2023/12/12/soc-as-a-service-security-operations/#:~:text=%E2%80%8BSOC%20as%20a%20Service,e%20sotto%20forma%20di%20servizio

gli attacchi continuano a crescere nel primo trimestre dell'anno, 2023, https://clusit.it/wp-content/uploads/area_stampa/2023/Rapporto_Clusit_2023_Healthcare-Security-Summit.pdf

GORETTA R, *Le tecniche di balancing test a sostegno del legittimo interesse: regole applicative*, 2020, https://www.cybersecurity360.it/legal/privacy-dati-personali/le-tecniche-di-balancing-test-a-sostegno-del-legittimo-interesse-regole-applicative/

GOVERNO ITALIANO PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Principi fondamentali,* https://www.governo.it/it/costituzione-italiana/principi-fondamentali/2839#:~:text=limiti%20della%20Costituzione.-,Art.,solidariet%C3%A0%20politica%2C%20economica%20e%20sociale.

GOVERNO ITALIANO PRESIDENZA DEL CONSIGLIO, *Comunicato stampa del Consiglio dei Ministri n. 71*, 2024, https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-71/25086

GUZZO A, *Il concetto di privacy*, 2009, https://www.diritto.it/il-concetto-di-privacy/#:~:text=Warren%20e%20Brandeis%20(successivamente%20quest,le%20coordinate%20legali%20della%20privacy.

HD BLOG, *Il Team Anonymous dichiara guerra a Sony*, 2011, https://www.hdblog.it/2011/04/05/il-team-anonymous-dichiara-guerra-a-sony/

HOLDSWORTH J, SCAPICCHIO M, *Cos'è il deep learning?* , 2024, https://www.ibm.com/it-it/topics/deep-learning

HSC SYSTEM, *Sicurezza digitale: l'importanza della cyber security oggi*, 2021, https://www.hscsystem.it/blog/sicurezza-digitale-l-importanza-della-cyber-security-oggi

IBM, *Alta disponibilità attraverso la ridondanza*, 2025, https://www.ibm.com/docs/it/db2/11.5?topic=strategies-redundancy

IBM, *Che cos'è un sistema di rilevamento delle intrusioni (IDS)?,* https://www.ibm.com/it-it/topics/intrusion-detection-system

IBM, *Che cos'è una superficie di attacco?,* https://www.ibm.com/it-it/topics/attack-surface

IBM, *Cos'è la gestione delle patch?,* https://www.ibm.com/it-it/topics/patch-management

IBM, *Cos'è la sicurezza IT?,* https://www.ibm.com/it-it/topics/it-security

IBM, *Da IBM Watson a watsonx*, https://www.ibm.com/it-it/watson

ICOS, *AkamaiTechnologies*, https://www.icos.it/brand/akamai/

IL POST, *Il nuovo attacco informatico contro Sony*, 2011, https://www.ilpost.it/2011/06/03/sony-pictures-attacco-hacker/

ILGER.COM, *Qual è il primo virus informatico della storia?,* 2024, https://www.ilger.com/blog-ilger/qual-e-il-primo-virus-informatico-della-storia/

INFORMATICA E INGEGNERIA ONLINE, *Il Segreto della Sicurezza Digitale: L'Algoritmo di Crittografia RSA*, https://vitolavecchia.altervista.org/il-segreto-della-sicurezza-digitale-lalgoritmo-di-crittografia-rsa/

INRECRUTING ZUCCHETTI, *Onboarding: cos'è, come farlo e perchè è importante*, 2024, https://www.in-recruiting.com/it/onboarding-definizione-significato/

IONOS, *File system: cosa sono e quali sono quelli più importanti*, 2020, https://www.ionos.it/digitalguide/server/know-how/file-system/

IONOS, *Memcached in breve: funzione e utilizzo*, 2021, https://www.ionos.it/digitalguide/hosting/tecniche-hosting/che-cose-memcached/

IT GOVERNANCE, *Cos'è la cyber security?,* https://www.itgovernance.eu/it-it/what-is-cyber-security-it

KASPERSKY, *Cos'è e come entrare nel Dark web*, https://www.kaspersky.it/resource-center/threats/deep-web

KEEPER, *Che cos'è un attacco alla supply chain?,* https://www.keepersecurity.com/it_IT/threats/supply-chain-attack.html#:~:text=Un%20attacco%20alla%20supply%20chain%2C%20noto%20anche%20come%20attacco%20a,la%20supply%20chain%2C%20appunto).

KEEPER, *Cos'è il controllo degli accessi in base al ruolo?,* https://www.keepersecurity.com/it_IT/resources/glossary/what-is-role-based-access-control/

KOSINSKY M, *Che cos'è l'hacking?* 2024, https://www.ibm.com/it-it/topics/cyber-hacking

KOSTICO N, *Che cos'è un gestore di pacchetti?*, 2024, https://www.phoenixnap.it/glossario/cos%27%C3%A8-un-gestore-di-pacchetti#:~:text=Le%20Gestore%20pacchetti%20APT%2C%20utilizzato,strumento%20indispensabile%20per%20questi%20sistemi.

L.O, *Cybersecurity, inizia l'era della DefenseGpt: il 69% delle aziende userà la GenAI* , 2023, https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-inizia-lera-della-defencegpt-il-69-delle-aziende-usera-la-genai/

LABOR PROJECT, *La valutazione di impatto sulla protezione dei dati (DPIA): il fai da te è possibile?*, https://laborproject.it/2022/07/27/la-valutazione-di-impatto-sulla-protezione-dei-dati-dpia-il-fai-da-te-possibile/?utm_source=chatgpt.com

LAHORE A, *Trent'anni fa nasceva Brain, il primo virus dei computer*, 2016, https://www.rainews.it/archivio-rainews/articoli/Trent-anni-fa-il-primo-virus-informatico-di-massa-a7d97dac-f3c4-4f1d-9005-ff94befa788e.html?refresh_ce

LAMBERTI C, *Gli strumenti di contrasto al terrorismo e al cyber-terrorismo*

LANA A, *I love You, venti anni fa il primo virus informatico che ha messo il mondo in ginocchio*, 2020, https://www.corriere.it/tecnologia/20_maggio_04/i-love-you-venti-anni-fa-primo-virus-informatico-che-ha-messo-mondo-ginocchio-71e8565a-8dda-11ea-b08e-d2743999949b.shtml

LANZILLOTTA F, *George Francis Hotz in arte GeoHot, la storia di un giovane hacker che ha sconvolto la apple e la sony, 2013*, https://www.biteyourconsole.net/2013/06/30/george-francis-hotz-in-arte-geohot-la-storia-di-un-piccolo-hacker-che-ha-sconvolto-la-apple-e-la-sony/

LEONARDI D, *Ken Kutaragi: l'inventore di PlayStation*, https://www.playstationgeneration.it/2010/08/ken-kutaragi.html

LOGUERCIO L, *Darpa, che cos'è e che cosa sta facendo l'agenzia statunitense a cui si ispira EneaTech*, 2021, https://www.economyup.it/innovazione/darpa-che-cose-e-che-cosa-sta-facendo-lagenzia-statunitense-a-cui-si-ispira-eneatech/

LUDOTECA REGISTRO.IT, *Manifesto "A scuola di cybersecurity"*, https://www.ludotecaregistro.it/manifesto-a-scuola-di-cybersecurity/

MAMMOLI A, *Il principio di minimizzazione nel GDPR*, 2023, https://accademiaitalianaprivacy.it/dettaglioNews.asp?id=764#:~:text=Cosa%20significa%20il%20principio%20di%20minimizzazione%20nel%20GDPR%3F&text=Ci%C3%B2%20comporta%20che%20i%20titolari,necessario%20per%20raggiungere%20tale%20scopo.

MARCHI E DISEGNI COMUNITARI, *Che cos'è e come funziona la proprietà intellettuale?,* 2022, https://www.marchiedisegni.eu/che-cose-proprieta-intellettuale/

MARTORANA M, PINELLI L, *Digital kidnapping, minacciata la sicurezza dei bambini (e non solo)*, 2020, https://www.agendadigitale.eu/sicurezza/digital-kidnapping-cosi-mettiamo-in-pericolo-la-sicurezza-nostra-e-dei-bambini/

MEGGIATO R, *Incident response: i consigli per costruire una efficace strategia di risposta ai cyber attacchi*, 2022, https://www.cybersecurity360.it/soluzioni-aziendali/incident-response-i-consigli-per-costruire-una-efficace-strategia-di-risposta-ai-cyber-attacchi/

MICHEAL PAGE, *Consigli di management*, https://www.michaelpage.it/advice/consigli-di-management/business-insights/l%E2%80%99importanza-di-non-sottovalutare-la-cybersecurity

MICROSOFT, *Che cos'è un endpoint?,* https://www.microsoft.com/it-it/security/business/security-101/what-is-an-endpoint#:~:text=Gli%20endpoint%20sono%20dispositivi%20fisici%20che%20si%20connettono%20e%20scambiano,virtuali%2C%20dispositivi%20incorporati%20e%20server.

MICROSOFT, *Cos'è il controllo degli accessi?,* https://www.microsoft.com/it-it/security/business/security-101/what-is-access-control

MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNALE, *La libera circolazione e il sistema Schengen,* https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/dossier/la-libera-circolazione-e-il-sistema-schengen/#:~:text=L'area%20Schengen%20%C3%A8%20una,Germania%2C%20Lussemburgo%20e%20Paesi%20Bassi.

MINISTERO DEGLI AFFARI ESTERI E DELLA COOPERAZIONE INTERNAZIONALE, *Cos'è la proprietà intellettuale*, https://www.esteri.it/it/diplomazia-economica-e-politica-commerciale/diplomaziaeconomica/tutela-e-promozione-della-proprieta/cos-e-la-proprieta-intellettuale/

MIRABELLA M, *La DPIA (Data Protection Impact Assessment) in cinque step*, 2023, https://www.cyberacademy.online/blog/230110-la-dpia-in-5-step

MONDO 27001, *Cybersecurity: report enisa 2022,* https://www.mondo27001.it/cybersecurity-report-enisa-2022/

MONDO PRIVACY, *GDPR: I CONCETTI DI RISERVATEZZA, INTEGRITA' E DISPONIBILITA'*, 2023, https://mondoprivacy.it/blog/gdpr/gdpr-riservatezza-integrita-e-disponibilita/

MONTELLA P, *Valutazione d'impatto sulla protezione dei dati: quando e come realizzare una DPIA*, 2020, https://www.cybersecurity360.it/legal/privacy-dati-personali/valutazione-dimpatto-sulla-protezione-dei-dati-quando-e-come-realizzare-una-dpia/

NARDI V, *Hacker, storia di un malinteso*, 2023, https://microdesign.it/blog/hacker-storia-di-un-malinteso

NARDINI R, *Crittografia avanzata delle e-mail, i protocolli SSL e TLS: cosa sono, come funzionano e come usarli*, 2023, https://www.cybersecurity360.it/soluzioni-aziendali/crittografia-avanzata-delle-e-mail-i-protocolli-ssl-e-tls-cosa-sono-come-funzionano-e-come-usarli/

nel contesto europeo, https://www.vittimologia.it/rivista/articolo_lamberti_2014-02.pdf

NEOSQUALL, *Sony multata di 250.000 Sterline a seguito del data breach del 2011*, 2013, https://www.spaziogames.it/notizie/sony-multata-di-250000-sterline-a-seguito-del-data-breach-del-2011-279080

NETWORK DIGITAL 360, *Nuovi strumenti Rsa rendono più sicuro Android*, 2011, https://www.zerounoweb.it/mobility/nuovi-strumenti-rsa-rendono-piu-sicuro-android/

NEW INNOVATE PER CRESCERE, *Gruppi di continuità: cosa sono, a cosa servono e come funzionano*, https://www.newcomm.it/informatica-e-networking/gruppi-di-continuita-ups/

NOONAN L, *I 10 più grandi attacchi DDoS e come la tua organizzazione può trarne insegnamento,* https://www.metacompliance.com/it/blog/cyber-security-awareness/10-biggest-ddos-attacks-and-how-your-organisation-can-learn-from-them

NORMATIVA IL PORTALE DELLA LEGGE VIGENTE, *LEGGE 22 aprile 1941, n. 633*, https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1941-04-22;633!vig#:~:text=Sono%20protette%20ai%20sensi%20di,o%20la%20forma%20di%20espressione.

OFFICE ADVICE, *Art. 8 – Convenzione Europea dei Diritti dell'uomo (CEDU),* https://officeadvice.it/cedu/articolo-8/

ORACLE ITALIA, *Cos'è il Machine Learning?*, https://www.oracle.com/it/artificial-intelligence/machine-learning/what-is-machine-learning/

PAGLIA S, *PlayStation Plus: cos'è, come funziona, prezzi e come abbonarsi*, 2024, https://multiplayer.it/articoli/playstation-plus-cose-come-funziona-prezzi-come-abbonarsi.html

PATHS: A PHILOSOPHICAL APPROACH TO THINKING SKILSS, *SAMUEL WARREN & LOUIS BRANDEIS - The right to privacy*, https://formazione.indire.it/paths/samuel-warren-and-louis-brandeis-the-right-to-privacy

PETRICCA R, *Strategie di Gestione della Sicurezza: Strumenti e Tecnologie di Difesa*, 2024, https://arenadigitale.it/2024/09/24/strategie-di-gestione-della-sicurezza-strumenti-e-tecnologie-di-difesa/

PIVA A, *Sicurezza dei Dati e i tre requisiti della Cyber Security*, 2019, https://blog.osservatori.net/it_it/sicurezza-informatica-disponibilita-e-integrita-dei-dati

PLAYSTATION, *Come modificare l'ID online per PSN*, https://www.playstation.com/it-it/support/account/change-psn-online-id/#:~:text=Un%20ID%20online%20%C3%A8%20un%20nome%20univoco%20utilizzato%20per%20identificarti%20su%20PSN.

PLAYSTATION, *Regolamento PlayStation Network*, https://www.playstation.com/it-it/legal/psn-rules/

PLAYSTATION, *Verifica in 2 passaggi*, https://www.playstation.com/it-it/playstation-network/two-step-verification/#:~:text=Come%20funziona,che%20soltanto%20tu%20possa%20accedere.

PONTI C, *Responsabile del trattamento, chi è e cosa fa: tutto quello che c'è da sapere* , 2022, https://www.agendadigitale.eu/sicurezza/privacy/responsabile-del-trattamento-chi-e-e-cosa-fa-tutto-quello-che-ce-da-sapere/

PRIVACY, *Italia: Ordinanza ingiunzione nei confronti di Azienda sanitaria unica regionale Marche*, 2022, https://privacygdpr.it/sanzioni-garanti-europei/italia-ordinanza-ingiunzione-nei-confronti-di-azienda-sanitaria-unica-regionale-marche/

PRIVACYLAB, *Come si è arrivati al GDPR: dalla privacy al Regolamento*, 2020, https://www.privacylab.it/IT/989/come-si-e-arrivati-al-gdpr-dalla-privacy-al-regolamento/

PRIVAZY PLAN, *Articolo 16 EU GDPR "Diritto di rettifica",* https://www.privacy-regulation.eu/it/16.htm#:~:text=EU%20RGPD,%22Diritto%20di%20rettifica%22&text=L'interessato%20ha%20il%20diritto,lo%20riguardano%20senza%20ingiustificato%20ritardo.

PRIVAZY PLAN, *Articolo 17 EU RGPD "Diritto alla cancellazione («diritto all'oblio»)",* https://www.privacy-regulation.eu/it/17.htm

PRIVAZY PLAN, *Articolo 5 EU GDPR "Principi applicabili al trattamento di dati personali",* https://www.privacy-regulation.eu/it/5.htm

PRIVAZY PLAN, *Articolo 83 EU GDPR "Condizioni generali per infliggere sanzioni amministrative pecuniarie"*, https://www.privacy-regulation.eu/it/83.htm

PRO G, *Threat modeling, cos'è e quali metodologie usare per l'identificazione delle minacce*, 2020, https://www.cybersecurity360.it/soluzioni-aziendali/threat-modeling-cose-e-quali-metodologie-usare-per-lidentificazione-delle-minacce/

PROOFPOINT, *Cos'è un ransomware?,* https://www.proofpoint.com/it/threat-reference/ransomware

PURESTORAGE, *Che cos'è UEBA? Definizione, vantaggi e modalità di funzionamento*, https://www.purestorage.com/it/knowledge/what-is-ueba.html

RACKONE, *Failover*, https://www.rackone.it/glossario/failover/

RAPPRESENTANZA PERMANENTE D'ITALIA PRESSO LE NAZIONI UNITE E LE ALTRE ORGANIZZAZIONE INTERNANZIONALI GINEVRA, *L'Organizzazione Mondiale della Proprietà Intellettuale (OMPI)*, https://italiarappginevra.esteri.it/it/litalia-e-ooii/proprieta-intellettuale/#:~:text=L'Organizzazione%20Mondiale%20per%20la,conta%20oggi%20188%20Paesi%20membri.

RED HOT CYBER, *Elk Cloner. Il primo virus informatico della storia*, 2021, https://www.redhotcyber.com/post/dagli-scherzi-agli-apt/

RED HOT CYBER, *Pronto Soccorso bloccato in USA. 6 ospedali rimangono senza sistemi a causa di un ransomware. E se succedesse in Italia?,* 2023, https://www.redhotcyber.com/post/pronto-soccorso-bloccato-in-usa-6-ospedali-rimangono-senza-sistemi-a-causa-di-un-ransomware-e-se-succedesse-in-italia/

RED HOT CYBER, *Slammer, il primo worm ad usare una bug non fixato da 6 mesi*, 2022, https://www.redhotcyber.com/post/slammer-il-primo-worm-ad-usare-una-bug-non-fixato-da-6-mesi/

REDAZIONE BITMAT, *Cosa sono gli RSA Token e come proteggono le nostre operazioni on line*, 2018, https://www.toptrade.it/categorie-funzionali/home-page/primo-piano/cosa-sono-gli-rsa-token-e-come-proteggono-le-nostre-operazioni-on-line/

rubati i dati di altri 25 milioni di utenti, 2011, https://www.corriere.it/cronache/11_maggio_03/sony-hacker-internet_03b16ed0-7564-11e0-88f0-a00eb5833fe6.shtml

SAETTA B, *Convenzione 108 del Consiglio d'Europa*, 2023, https://protezionedatipersonali.it/convenzione-108-consiglio-europa

SALARIS S, *Blockchain e proprietà intellettuale: a cosa serve e ultimi sviluppi [2023],* 2023, https://blog.4bmc.ch/blockchain-e-proprieta-intellettuale-a-cosa-serve-2020/

SALESFORCE, *Che cos'è il cloud computing?,* https://www.salesforce.com/it/learning-centre/tech/cloudcomputing/

SAUNTEUSANIO L, *Cos'è il sistema GRC e perché sta diventando sempre più importante*, 2022, https://www.eqs.com/it/polo-di-conoscenza-compliance/blog/gestione-dei-processi-grc/

SBARAGLIA G, *Cyberwarfare: la guerra cibernetica tra stati. Casi famosi*, https://flashstart.com/it/cyberwarfare-la-guerra-cibernetica-tra-stati-casi-famosi/

SBARAGLIA G, *Gestione delle password: cosa sono gli hash e a cosa servono*, 2022, https://www.cybersecurity360.it/outlook/gestione-delle-password-cosa-sono-gli-hash-e-a-cosa-servono/

SCAPICCHIO M, DOWNIE A, FINIO M, *Cos'è un SOC?,* 2024, https://www.ibm.com/it-it/topics/security-operations-center

SEALPATH, *I 3 tipi di Crittografia in Dettaglio*, https://www.sealpath.com/it/blog/tipi-di-crittografia-guida/

SECURITY SUMMIT VERTICAL, *Cyber Security nella Sanità,*

SEPE L, *Incident response, cos'è e come funziona passo per passo: ecco cosa fare,* 2020, https://www.cybersecurity360.it/soluzioni-aziendali/incident-response-cose-e-come-funziona-passo-per-passo-ecco-cosa-fare/

SERVICEMATICA, *Endpoint: cosa sono e perché sono fondamentali per la sicurezza informatica*, 2020, https://servicematica.com/endpoint-cosa-sono-e-perche-sono-fondamentali-per-la-sicurezza-informatica/

SERVIDIO G, *Creeper è il primo malware della storia: chi l'ha sviluppato e perché*, 2024, https://www.geopop.it/creeper-e-il-primo-malware-della-storia-chi-lha-sviluppato-e-perche/

SOPHOS, *Garantiamo i migliori risultati di sicurezza per le organizzazioni che hanno bisogno di soluzioni concrete*, https://www.sophos.com/it-it/company#:~:text=Sophos%20sfrutta%20i%20dati%20di,un'enorme%20variet%C3%A0%20di%20attacchi

SPARLING C, GEBHARDT M, *Il più vasto attacco DDoS mai lanciato in Europa*, 2022, https://www.akamai.com/it/blog/security/largest-european-ddos-attack-ever

SPASOJEVIC A, *Definizione del controllo di accesso obbligatorio (MAC)*, 2023, https://phoenixnap.it/glossario/controllo-accessi-obbligatorio-mac

STEFANI A, *Monitoraggio continuo in cyber security: un approccio metodologico*, 2022, https://www.cybersecurity360.it/soluzioni-aziendali/monitoraggio-continuo-in-cyber-security-un-approccio-metodologico/

STOLAS INFORMATICA, *Insider Threat e sicurezza informatica: la guida completa*, https://stolasinformatica.eu/sicurezza/insider-threat-sicurezza-informatica-guida/

STOLAS INFORMATICA, *Threat Modeling: Cosa è e quali sono le migliori metodologie*, https://stolasinformatica.eu/sicurezza/threat-modeling-cosa-migliori-metodologie-guida-completa/

STUDIO CAMATA, *La Valutazione di Impatto sulla Protezione dei Dati (DIPIA)*, https://www.studiocamata.it/valutazione-di-impatto-sulla-protezione-dei-dati/

SWG, *storia e innovazione*, https://www.swg.it/chisiamo

TELSY, *Risk Analysis e VAPT: come gestire il rischio cyber*, https://www.telsy.com/risk-analysis-e-vapt-come-gestire-il-rischio-cyber/#:~:text=VAPT%3A%20Penetration%20Test,le%20vulnerabilit%C3%A0%20dei%20sistemi%20stessi.

TEMATICHE PARLAMENTO EUROPEO, *Che cos'è l'intelligenza artificiale?* , 2023, https://www.europarl.europa.eu/topics/it/article/20200827STO85804/che-cos-e-l-intelligenza-artificiale-e-come-viene-usata

THE INNOVATION GROUP, *ENISA Threat Landscape 2022: minacce, impatti, industria del cyber crime,* 2022, https://channels.theinnovationgroup.it/cybersecurity/enisa-threat-landscape-2022/#:~:text=ENISA%20Threat%20Landscape%202022%3A%20minacce%2C%20impatti%2C%20industria%20del%20cyber%20crime,-7%20novembre%202022&text=L'Agenzia%20dell'Unione%20europea,globale%20delle%20minacce%20di%20cybersecurity.

TIG: THE INNOVATION GROUP, *CYBERSECURITY SUMMIT 2024 – Roma*, 2024, https://www.theinnovationgroup.it/events/digital-italy-summit-2024/cybersecurity-summit-2024-roma/?lang=it

TIG: THE INNOVATION GROUP, *DIGITAL ITALY SUMMIT 2024*, 2024, https://www.theinnovationgroup.it/events/digital-italy-summit-2024/?lang=it

TOGA, *168 - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*, https://app.toga.cloud/codici/codice-della-

privacy/14/13947/art-168-falsita-nelle-dichiarazioni-al-garante-e-interruzione-dell-esecuzione-dei-compiti-o-dell-esercizio-dei-poteri-del-garante

TOM'S HARDWARE, *Storm Worm, ovvero come trasformare un PC in uno zombie*, 2015, https://www.tomshw.it/altro/i-virus-piu-devastanti-della-storia/storm-worm-ovvero-come-trasformare-un-pc-in-uno-zombie

UNIONE EUROPEA, *Agenzia dell'Unione europea per la cibersicurezza (ENISA),* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_it#:~:text=L'ENISA%20contribuisce%20alla%20politica,prepararsi%20alle%20future%20sfide%20informatiche.

USERCENTRICS COOKIEBOT*, Cos'è il GDPR*, https://www.cookiebot.com/it/gdpr/

VALENTINI A, *Il SOC: cos'è, i suoi compiti e il ruolo nella risposta agli incidenti di sicurezza*, 2022, https://www.cybersecurity360.it/soluzioni-aziendali/focus-on-soc-capability/

VEGA FORMAZIONE, *Organismo di Vigilanza (ODV): cosa prevede il D.Lgs.231/01,* https://www.vegaformazione.it/PB/organismo-di-vigilanza-231-p242.html#:~:text=L'Organismo%20di%20Vigilanza%20(ODV,delle%20figure%20apicali%20dell'organizzazione.

VOIPTEL ITALIA, *La Ridondanza: Il Segreto per una Resilienza Infallibile nel Mondo Digitale*, https://voiptelitalia.it/la-ridondanza-il-segreto-una-resilienza-infallibile-nel-mondo-digitale#:~:text=Cos'%C3%A8%20la%20Ridondanza%3F,il%20suo%20posto%2C%20senza%20interruzioni.

WIKIPEDIA, *(c)Brain*, https://it.wikipedia.org/wiki/(c)Brain

WIKIPEDIA, *Akamai Technologies,* https://it.wikipedia.org/wiki/Akamai_Technologies#:~:text=Akamai%20Technologies%2C%20Inc., contenuti%20via%20Internet%20(CDN).

WIKIPEDIA, *Anonymous*, https://it.wikipedia.org/wiki/Anonymous

WIKIPEDIA, *Application programming interface,* https://it.wikipedia.org/wiki/Application_programming_interface

WIKIPEDIA, *CIH (virus),* https://it.wikipedia.org/wiki/CIH_(virus)

WIKIPEDIA, *Controller (videogiochi),* https://it.wikipedia.org/wiki/Controller_(videogiochi)#:~:text=Un%20controller%2C%20detto%20anche%20game,l'input%20in%20un%20videogioco.&text=Un%20controller%20%C3%A8%20tipicamente%20connesso,da%20una%20connessione%20senza%20fili.

WIKIPEDIA, *Darknet*, https://it.wikipedia.org/wiki/Darknet

WIKIPEDIA, *Doxing*, https://it.wikipedia.org/wiki/Doxing

WIKIPEDIA, *Electronic Entertainment Expo,* https://it.wikipedia.org/wiki/Electronic_Entertainment_Expo

WIKIPEDIA, *Elk Cloner*, https://it.wikipedia.org/wiki/Elk_Cloner

WIKIPEDIA, *Fortinet*, https://it.wikipedia.org/wiki/Fortinet

WIKIPEDIA*, GitHub*, https://it.wikipedia.org/wiki/GitHub

WIKIPEDIA, *Hacking*, https://it.wikipedia.org/wiki/Hacking

WIKIPEDIA, *Happy99*, https://it.wikipedia.org/wiki/Happy99

WIKIPEDIA, *Infrastrutture critiche*, https://it.wikipedia.org/wiki/Infrastrutture_critiche

WIKIPEDIA, *Jack Tretton*, https://it.wikipedia.org/wiki/Jack_Tretton

WIKIPEDIA, *Kernel*, https://it.wikipedia.org/wiki/Kernel#Kernel_monolitici

WIKIPEDIA, *LulzSec*, https://it.wikipedia.org/wiki/LulzSec

WIKIPEDIA, *Malware*, https://it.wikipedia.org/wiki/Malware

WIKIPEDIA, *Morris worm*, https://it.wikipedia.org/wiki/Morris_worm

WIKIPEDIA, *OtherOS*, https://it.wikipedia.org/wiki/OtherOS

WIKIPEDIA, *Progetto Chanology*, https://it.wikipedia.org/wiki/Progetto_Chanology

ZAMPETTI M, *GDPR e minimizzazione dei dati, casi pratici d'applicazione*, 2020, https://www.cybersecurity360.it/legal/privacy-dati-personali/gdpr-e-minimizzazione-dei-dati-casi-pratici-dapplicazione/

ZANOTTI L, *Backup: cos'è, a cosa serve, come e quando farlo*, 2024, https://www.zerounoweb.it/software/backup-cose-a-cosa-serve-come-e-perche-farlo/

ZANOTTI L, *SIEM: cos'è e come garantisce la sicurezza delle informazioni*, 2019, https://www.cybersecurity360.it/soluzioni-aziendali/siem-cos-e-come-garantisce-la-sicurezza-delle-informazioni/

ZANOTTI L, *User Behavior Analysis: UBA o UEBA? Ecco come scegliere*, 2023, https://www.zerounoweb.it/techtarget/searchsecurity/user-behavior-analysis-uba-o-ueba-ecco-come-scegliere/

ZINATO M, *Il DES*, 2006, https://www.html.it/pag/16475/il-des/