UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

AFFRONTARE LE MINACCE DIGITALI: UN'ANALISI APPROFONDITA DELLA CYBERSECURYTY NEL CONTESTO ATTUALE

Francesco Albertini

0350752

Anno accademico 2023/2024

Sommario

ABSTRACT

Nell'epoca digitale, la *cybersecurity* gioca un ruolo cruciale nel proteggere sistemi, reti e dati da minacce informatiche sempre più sofisticate. Con l'avanzare delle tecnologie digitali e l'aumento delle minacce, la sicurezza informatica diventa prioritaria per individui, aziende e istituzioni.

Il mercato della *cybersecurity* ha raggiunto valori miliardari grazie all'impiego diffuso di intelligenza artificiale e apprendimento automatico per prevenire attacchi informatici.

Tra le principali minacce ci sono *malware* come virus, *worm*, *trojan*, *ransomware*, *spyware* e *adware*, concepiti per danneggiare o infiltrarsi nei sistemi; *phishing,* una truffa online per ottenere informazioni sensibili; *social engineering,* manipolazioni psicologiche per scopi dannose; attacchi DDoS, che sovraccaricano servizi online; *exploit,* che sfruttano vulnerabilità nei sistemi; e vulnerabilità *zero-day,* pericolose per l'assenza di soluzioni immediate.

Le strategie di difesa includono software *antivirus*, *firewall*, sistemi di rilevamento e prevenzione delle intrusioni, crittografia, autenticazione a più fattori e buone pratiche di sicurezza come aggiornamenti regolari e backup.

Politiche e procedure definiscono linee guida per ridurre i rischi e garantire una gestione efficace delle risorse informatiche. È fondamentale un piano di risposta agli incidenti per reagire tempestivamente agli attacchi.

Il GDPR, introdotto nel 2018 dall'Unione Europea, conferisce diritti sui dati personali e impone misure di protezione. L'interconnessione tra *cybersecurity* e protezione dei dati personali mira a salvaguardare le informazioni dagli accessi non autorizzati.

L'intelligenza artificiale e l'apprendimento automatico saranno cruciali nel futuro della *cybersecurity*, consentendo l'automatizzazione dell'analisi dei dati e l'individuazione tempestiva di anomalie e attacchi. Tuttavia, l'impiego di intelligenza artificiale presenta sfide in termini di privacy, e la normativa continuerà a evolversi verso maggiore conformità e sicurezza informatica.

1. INTRODUZIONE

La *cybersecurity*, o sicurezza informatica, rappresenta uno dei pilastri fondamentali nell'era digitale in cui viviamo, in quanto dedicato alla protezione di sistemi informatici, reti, programmi e dati da attacchi dannosi, accessi non autorizzati o qualsiasi altra forma di minaccia informatica.

In un mondo sempre più interconnesso, dove la tecnologia permea ogni aspetto della vita quotidiana e delle attività aziendali, la *cybersecurity* diventa fondamentale per garantire la *privacy*, la riservatezza e l'integrità delle informazioni.

Con l'aumento della complessità delle minacce informatiche e delle tecnologie digitali, la *cybersecurity* diventa sempre più critica per individui, aziende, istituzioni governative e organizzazioni di ogni settore.

La *cybersecurity* si occupa di sviluppare strategie, protocolli e tecnologie per identificare, prevenire e rispondere a una vasta gamma di minacce informatiche, che includono *malware*, *phishing*, attacchi DDoS (*Distributed Denial of Service*), violazioni della sicurezza dei dati e molti altri.

Questa non è solo una questione tecnologica, ma anche strategica e organizzativa. Richiede un approccio olistico che coinvolga politiche di sicurezza, procedure di gestione del rischio, formazione del personale e l'implementazione di soluzioni tecnologiche avanzate.

Solo attraverso un impegno costante e una consapevolezza diffusa è possibile contrastare efficacemente le minacce informatiche e garantire un ambiente digitale sicuro e affidabile.

La *cybersecurity*, quindi, rappresenta un campo in continua evoluzione, dove la collaborazione tra esperti, l'innovazione tecnologica e la consapevolezza degli utenti sono fondamentali per garantire la protezione dei dati e la sicurezza delle reti informatiche.

2. STORIA DELLA CYBERSECURITY

La storia della *cybersecurity* ha inizio negli anni '70, quando i computer e Internet erano ancora in fase di sviluppo. In quel periodo, le minacce alla sicurezza informatica erano facilmente identificabili e provenivano principalmente da *insider* malintenzionati che accedevano a documenti riservati.

Nel 1971, Bob Thomas, ricercatore presso BBN *Technologies*, creò il primo *worm* informatico, cioè un tipo di *malware* progettato per diffondersi attraverso le reti informatiche, chiamato "*Creeper*" ed in grado lasciare un messaggio: "*I'M THE CREEPER: CATCH ME IF YOU CAN*". Questo evento segnò l'inizio dell'utilizzo di *virus* e *worm* per scopi diversi dal semplice interesse accademico.

Negli anni '80, con la diffusione dei *Bulletin Board System* (BBS), i virus informatici iniziarono a diffondersi rapidamente. Nel 1987 nacque il primo antivirus commerciale, sviluppato da Andreas Lüning e Kai Figge per l'Atari ST. Nello stesso anno, tre cecoslovacchi crearono la prima versione di NOD antivirus e John McAfee fondò la McAfee rilasciando VirusScan.

Il decennio successivo vide una crescita esponenziale delle minacce informatiche, con l'avvento di Internet e la diffusione di informazioni personali *online*. Le organizzazioni criminali iniziarono a rubare dati da privati e governi, spingendo lo sviluppo di *firewall* e antivirus su larga scala.

Nel 2000, con l'avvento della tecnologia mobile e dei *social media*, la *cybersecurity* diventa ancora più complessa. Emergono nuove minacce come il *phishing,* lo *spam* e i *ransomware*. Le normative sulla privacy, come l'HIPAA (*Health Insurance Portability and Accountability Act*) negli Stati Uniti e il GDPR (*General Data Protection Regulation*) in Europa, pongono ulteriori requisiti per la protezione dei dati personali.

La cybersecurity è diventata un tema centrale nei dibattiti globali, con attacchi sempre più sofisticati e devastanti. Si registra un aumento significativo degli attacchi mirati a grandi aziende, istituzioni governative e infrastrutture critiche. Allo stesso tempo, si assiste a una maggiore collaborazione tra governi, aziende e organizzazioni internazionali per contrastare le minacce informatiche.

Oggi, il mercato della *cybersecurity* vale miliardi di dollari e continua a crescere a ritmo sostenuto. L'intelligenza artificiale e l'apprendimento automatico vengono sempre più utilizzati per rilevare e prevenire le minacce informatiche in tempo reale. Tuttavia, le sfide rimangono complesse, con nuove minacce che continuano a emergere e evolversi costantemente.

Alcuni degli incidenti storici più significativi includono:

- Il Morris Worm del 1988, che causò il blocco di gran parte di internet
- Stuxnet nel 2010, il primo *malware* utilizzato come arma, che interferì con il programma nucleare iraniano
- La violazione di Yahoo nel 2013-2014, il furto di dati personali di 3 miliardi di utenti

3. PRINCIPALI MINACCE INFORMATICHE

Le minacce informatiche sono sempre in evoluzione e comprendono una vasta gamma di attacchi che possono compromettere la sicurezza dei sistemi informatici. Tra le minacce più rilevanti si includono *malware* come *virus*, *worm* e *trojan*, il *phishing* e il *social engineering*, gli attacchi DDoS (*Distributed Denial of Service*), le violazioni di dati e le vulnerabilità *zero-day*.

3.1 MALWARE

Il *malware* è un termine generico che include un software dannoso progettato per danneggiare o infiltrarsi nei sistemi informatici. Alcune tipologie di *malware* sono:

- *VIRUS*: sono programmi progettati per infettare altri file o programmi nel sistema, propagandosi quando tali file vengono eseguiti
- *WORM*: sono simili al virus, ma differiscono per il fatto che possono propagarsi autonomamente senza bisogno di un file ospite
- *TROJAN*: sono programmi che si fingono di essere affidabili o utili, ma in realtà contengono funzionalità dannose. Possono aprire una "porta posteriore" nel sistema per consentire l'accesso da remoto agli hacker, rubare dati sensibili o danneggiare il sistema
- *RANSOMWARE*: è un tipo di *malware* che crittografa i file della vittima e richiede un pagamento di riscatto per fornire la chiave di decrittazione
- *SPYWARE*: è un tipo di *malware* che monitora le attività dell'utente senza il loro consenso, raccogliendo informazioni sensibili come password, informazioni bancarie o dati di navigazione
- *ADWARE*: questo *malware* mostra annunci pubblicitari indesiderati sul computer dell'utente, spesso generando entrate per gli autori del *malware* attraverso clic fraudolenti o installazioni di software non desiderato

3.2 PHISHING

Il *phishing* è una forma di truffa online in cui i truffatori cercano di ottenere informazioni sensibili come password, dati finanziari o altre informazioni personali tramite l'inganno. Questo genere di attacco avviene di solito tramite e-mail contraffatte, messaggi di testo, chiamate telefoniche o siti web falsi che sembrano provenire da fonti affidabili come istituti finanziari, aziende o enti governativi.

I truffatori di solito cercano di ingannare le persone inducendole a fornire le proprie informazioni sensibili o ad eseguire azioni dannose, come il *download* di *malware*, cliccando su link malevoli o aprendo allegati dannosi.

3.3 SOCIAL ENGINEERING

Il *social engineering* è un metodo utilizzato dai criminali informatici per ottenere informazioni sensibili o persuadere le persone a compiere determinate azioni attraverso l'inganno psicologico e la manipolazione. Questo approccio sfrutta la fiducia, l'ingenuità o la vulnerabilità umana anziché sfruttare direttamente vulnerabilità tecniche nei sistemi informatici.

Gli attaccanti possono costruire rapporti di fiducia con le loro vittime nel tempo, fingendo di essere amici, colleghi o addirittura autorità legittime. Una volta guadagnata la fiducia della vittima, gli aggressori possono chiedere informazioni sensibili o convincere la vittima a compiere azioni dannose.

L'inganno può coinvolgere la creazione di siti web o account sui social media falsi per impersonare persone o organizzazioni legittime al fine di ingannare le persone e ottenere informazioni sensibili.

3.4 ATTACCHI DDOS

Un attacco DDoS, acronimo di *Distributed Denial of Service* (Servizio Distribuito di Negazione), è un tipo di attacco informatico progettato per rendere inaccessibili i servizi online saturandoli con un elevato volume di traffico proveniente da molteplici fonti distribuite su Internet. L'obiettivo principale di un attacco DDoS è quello di sovraccaricare i server di destinazione, impedendo loro di rispondere alle richieste legittime degli utenti.

3.5 EXPLOITS E VULNERABILITÀ ZERO-DAY

Un *exploit* è un software, un codice o una sequenza di comandi progettati per sfruttare una vulnerabilità specifica in un sistema informatico o un'applicazione. Gli *exploits* possono essere utilizzati per ottenere accesso non autorizzato a sistemi, eseguire codice malevolo, ottenere informazioni sensibili o causare danni ai dati o ai dispositivi.

Una vulnerabilità *zero-day* è una falla di sicurezza particolarmente pericolosa perché gli sviluppatori non hanno avuto modo di creare e distribuire una correzione prima che i criminali informatici inizino a sfruttarle. Questo rende difficile proteggere i sistemi contro gli attacchi basati su queste vulnerabilità fino a quando non viene rilasciata una patch o una contromisura efficace.

4. TECNICHE DI DIFESA

La *cybersecurity* è un campo cruciale per proteggere le informazioni sensibili e prevenire attacchi informatici dannosi. Le tecniche di difesa sono varie e includono l'uso di software *antivirus* e *antimalware*, *firewall*, sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), crittografia, autenticazione a più fattori e l'implementazione di buone pratiche di sicurezza come gli aggiornamenti regolari e i backup.

4.1 SOFTWARE ANTIVIRUS E ANTIMALWARE

I software *antivirus* e *antimalware* sono strumenti essenziali per proteggere i sistemi informatici da *virus*, *malware*, *spyware* e altre minacce informatiche. Questi programmi scansionano i file e il traffico di rete alla ricerca di potenziali minacce e li eliminano o li isolano per prevenire danni ai dispositivi e alle reti.

Molti prodotti *antivirus* e *antimalware* combinano funzionalità di entrambe le categorie per offrire una protezione più completa contro le minacce informatiche. È importante mantenere aggiornati i software *antivirus e anti-malware* per garantire che siano in grado di rilevare e rimuovere le minacce più recenti.

4.2 FIREWALL

I *firewall* sono dispositivi o software progettati per monitorare e controllare il traffico di rete in entrata e in uscita. Questi strumenti creano una barriera tra la rete interna e Internet, consentendo di bloccare il traffico dannoso e non autorizzato. I *firewall* possono essere configurati per consentire o bloccare specifici tipi di traffico in base alle regole definite dall'amministratore di rete.

Esistono tre tipi di *firewall*:

1. *FIREWALL DI RETE*: questi operano a livello di rete e possono essere hardware o software. Proteggono una rete di computer controllando il traffico in entrata e in uscita in base a regole predefinite. Ad esempio, un *firewall* di rete può bloccare il traffico proveniente da indirizzi IP sospetti o da determinate porte di rete. Un esempio comune di firewall di rete è il *firewall* fornito dai router domestici o aziendali;
2. *FIREWALL HOST*: operano a livello di sistema operativo su un singolo computer. Questi *firewall* monitorano il traffico in ingresso e in uscita da e verso quel computer specifico. Possono essere configurati per bloccare determinati tipi di traffico o connessioni. Un esempio è il *firewall* integrato nei sistemi operativi come Windows Firewall o iptables in Linux.
3. *FIREWALL A LIVELLO DI APPLICAZIONE (O PROXY)*: operano a livello di applicazione, controllando e filtrando il traffico in base al tipo di applicazione o protocollo. Questi *firewall* offrono un controllo più granulare sul traffico, ma possono essere più complessi da configurare e gestire. Un esempio di *firewall* a livello di applicazione è un *proxy web* come Squid.

4.3 SISTEMI DI RILEVAMENTO E PREVENZIONE DELLE INTRUSIONI (IDS/IPS)

I sistemi di rilevamento e prevenzione delle intrusioni monitorano costantemente il traffico di rete alla ricerca di attività sospette o potenziali violazioni della sicurezza.

Un IDS analizza il traffico di rete in tempo reale per individuare pattern di comportamento anomalo che potrebbero indicare una possibile violazione della sicurezza.

Un IPS va oltre il semplice rilevamento delle intrusioni e può intraprendere azioni immediate per bloccare o mitigare gli attacchi in corso.

4.4 CRITTOGRAFIA E AUTENTICAZIONE A PIÙ FATTORI

La crittografia è il processo di trasformazione dei dati in un formato indecifrabile, noto come testo cifrato, utilizzando algoritmi matematici complessi. Solo coloro che possiedono

una chiave crittografica appropriata possono decifrare e leggere i dati cifrati. La crittografia è utilizzata per proteggere la riservatezza e l'integrità dei dati durante la trasmissione e l'archiviazione.

Un esempio di utilizzo della crittografia avviene nelle transazioni online. Quando si inseriscono i dettagli della carta di credito durante il checkout, questi dati sensibili devono essere protetti durante la trasmissione e anche quando vengono memorizzati dal negozio online. La crittografia viene utilizzata per rendere illeggibili queste informazioni sensibili a chiunque tenti di intercettarle o accedervi senza autorizzazione.

L'autenticazione a più fattori è un processo di verifica dell'identità degli utenti utilizzando più metodi di autenticazione. Richiede che gli utenti forniscano almeno due fattori di autenticazione diversi, tra cui qualcosa che conoscono (come una password), qualcosa che possiedono (come un token di sicurezza) e/o qualcosa che sono (come un'impronta digitale).

4.5 BUONE PRATICHE DI SICUREZZA

Oltre alle tecnologie di difesa, è essenziale adottare buone pratiche di sicurezza informatica. Queste includono l'applicazione di aggiornamenti regolari per mantenere i sistemi al sicuro da vulnerabilità note, l'implementazione di procedure di backup per proteggere i dati da perdite accidentali o attacchi *ransomware* e l'educazione degli utenti sulle minacce informatiche e sulle *best practices* per una navigazione sicura in rete.

Inoltre, sensibilizzare e formare continuamente gli utenti sulle minacce informatiche e sulle *best practices* di sicurezza è fondamentale per mantenere un ambiente digitale e sicuro. Gli utenti possono essere il punto debole nella catena di sicurezza informatica, quindi educarli sull'identificazione e la gestione delle minacce è cruciale. Questo non solo riduce il rischio di violazioni della sicurezza, ma anche promuove una cultura di consapevolezza che può proteggere sia gli individui che le organizzazioni da gravi danni finanziari e reputazionali. La

formazione continua garantisce che gli utenti siano al passo con le nuove minacce e le contromisure più efficaci, contribuendo così a mantenere al sicuro i dati e i sistemi.

5. CYBERSECURITY NELLE ORGANIZZAZIONI

La *cybersecurity* è fondamentale per proteggere le organizzazioni da minacce informatiche sempre più sofisticate e dannose. Un attacco informatico può causare gravi danni, come la perdita di dati sensibili, interruzioni delle attività, danni di reputazione e pesanti sanzioni legali e finanziarie. Inoltre, la maggior parte degli incidenti di sicurezza è causata da errori umani, come cadere vittima di *phishing* o usare password deboli. Pertanto, investire nella *cybersecurity* è essenziale per garantire la continuità aziendale e la fiducia dei clienti.

Le politiche e le procedure di sicurezza sono fondamentali per garantire la protezione dei dati e dei sistemi informatici all'interno di un'organizzazione. Questi documenti forniscono linee guide e regole che devono essere seguite da tutti i dipendenti per ridurre al minimo i rischi di violazioni della sicurezza e garantire una gestione efficace delle risorse informatiche. Ciò include sviluppare una *policy* di sicurezza aziendale che definisca ruoli, responsabilità e linee guida per l'uso sicuro di dispositivi e dati; implementare controlli di accesso, crittografia e backup dei dati per proteggere le informazioni critiche; mantenere aggiornati sistemi operativi, software e firewall per chiudere le vulnerabilità e definire procedure per la gestione degli incidenti e il ripristino in caso di attacchi.

Molte violazioni della sicurezza informatica sono causate da errori umani, come cliccare su link dannosi o condividere informazioni sensibili con persone non autorizzate. Pertanto, la formazione sensibilizza i dipendenti sui rischi associati alle pratiche insicure e li aiuta a identificare e mitigare potenziali minacce; inoltre, fornisce ai dipendenti le conoscenze e le competenze necessarie per adottare le migliori pratiche di sicurezza informatica ed include la comunicazione delle politiche e delle procedure di sicurezza dell'azienda, aiutando i dipendenti a comprendere le regole e le normative da seguire per proteggere i dati e i sistemi aziendali.

Nonostante le misure di prevenzione, gli incidenti di sicurezza possono comunque verificarsi. È quindi essenziale avere un piano di *incident response* per rispondere in modo

rapido ed efficace.

La prima fase della gestione degli incidenti è il rilevamento. Gli incidenti di sicurezza possono essere identificati attraverso monitoraggio continuo dei sistemi, segnalazioni a parte degli utenti o attraverso sistemi di rilevamento delle intrusioni.

Una volta che un incidente è stato rilevato, viene avviata un'indagine per valutare la sua portata, le cause e l'impatto sull'organizzazione.

Dopo aver valutato l'incidente, vengono adottate misure per contenere e mitigare i danni. Una volta contenuto, viene avviato il processo di recupero e ripristino dei sistemi e dei dati compromessi.

Risolto l'incidente, viene condotta un'analisi post-incidente per comprendere appieno le cause sottostanti, le lezioni apprese e le azioni correttive da intraprendere per prevenire futuri incidenti simili. Questo processo di revisione post-mortem è essenziale per migliorare continuamente le pratiche di sicurezza informatica dell'organizzazione.

6. NORMATIVE E REGOLAMENTAZIONI – IL GDPR

Le normative sulla *cybersecurity* variano da paese a paese e possono includere standard settoriali, leggi sulla privacy e regolamenti specifici per settori sensibili come quello finanziario o sanitario. Il GDPR, acronimo di *General Data Protection Regulation*, è una delle normative più rilevanti nel campo della protezione dei dati personali. Introdotto dall'Unione Europea (UE) ed è diventato pienamente operativo il 25 maggio 2018, sostituendo la precedente Direttiva sulla protezione dei dati del 1995, il GDPR conferisce agli individui una serie di diritti in merito ai propri dati.

Il rapporto tra la *cybersecurity* e la protezione dei dati personali, incluso il GDPR, è profondamente intrecciato, poiché entrambi si concentrano sulla salvaguardia delle informazioni sensibili dagli accessi non autorizzati e dalle minacce informatiche. La *cybersecurity* si occupa della difesa dei sistemi informatici e delle reti da pericoli come *malware* e intrusioni, mentre la protezione dei dati personali si concentra sulla sicurezza e la privacy delle informazioni degli individui.

Il GDPR ha introdotto requisiti specifici per garantire la sicurezza dei dati personali, impegnando le organizzazioni ad adottare misure tecniche e organizzative adeguate. Queste misure comprendono controlli di accesso, crittografia dei dati e monitoraggio delle attività di rete, tra gli altri, al fine di proteggere i dati da violazioni e accessi non autorizzati.

Inoltre, il GDPR richiede alle organizzazioni di notificare le violazioni dei dati personali alle autorità competenti e agli individui interessati entro tempi definiti. Una solida infrastruttura di *cybersecurity* è cruciale per rilevare e rispondere prontamente a tali violazioni, consentendo alle organizzazioni di conformarsi ai requisiti normativi e di limitare i danni potenziali.

Le organizzazioni sono tenute a rispettare principi fondamentali come la trasparenza e la limitazione della finalità, dimostrando la conformità con il GDPR e notificando le violazioni

dei dati personali alle autorità competenti entro tempi definiti. Le sanzioni per violazioni del GDPR possono essere severe, con multe fino a 20 milioni di euro o il 4% del fatturato annuo globale, a seconda di quale sia maggiore.

Il GDPR ha avuto un impatto significativo sul modo in cui le organizzazioni raccolgono, elaborano e gestiscono i dati personali, incoraggiando una maggiore trasparenza, responsabilità e rispetto della privacy dei dati. Ha anche influenzato normative e regolamentazioni in altri paesi al di fuori dell'UE, poiché molte organizzazioni globali hanno dovuto adeguarsi ai suoi requisiti per continuare a fare affari con i residenti dell'UE.

7. FUTURO DELLA CYBERSECURITY

Il futuro della *cybersecurity* sarà caratterizzato da una serie di trend emergenti che plasmeranno il modo in cui proteggiamo i nostri sistemi e dati. Tra questi, l'intelligenza artificiale (*AI*) e l'apprendimento automatico (*machine learning*) giocheranno un ruolo fondamentale.

L'*AI* consentirà di automatizzare l'analisi dei dati e individuare più rapidamente pattern e anomalie, permettendo di identificare e rispondere agli attacchi cibernetici in modo più tempestivo. Algoritmi di *AI* e *machine learning* potranno essere utilizzati per automatizzare numerose attività, riducendo i carichi di lavoro e i costi organizzativi. Tuttavia, l'*AI* presenta anche sfide in termini di privacy, poiché rende più difficile distinguere gli umani dalle macchine online, portando molte persone a spostare le loro attività offline.

Un altro trend chiave sarà la crescente adozione dell'*Internet of Things (IoT)*. Entro il 2050, città e case intelligenti saranno la norma, con dispositivi *smart* come assistenti vocali, aspirapolvere e servizi igienici che rappresenteranno punti deboli per i cybercriminali. In questo mondo iperconnesso, le minacce introdotte dai criminali informatici si moltiplicheranno. Entro il 2030, alternative sicure rimuoveranno e sostituiranno dispositivi *IoT* con codice obsoleto e vulnerabile.

La *cybersecurity* avrà un ruolo cruciale nel proteggere le infrastrutture critiche, che saranno sempre più dipendenti da sistemi computerizzati. Attacchi mirati a infrastrutture come reti elettriche, sistemi idrici o ospedali potrebbero avere conseguenze catastrofiche. La *cybersecurity* dovrà evolversi per affrontare queste minacce, adottando un approccio proattivo basato sulla resilienza e la capacità di ripresa.

Inoltre, ci sarà una maggiore attenzione alla prevenzione e alla preparazione. Entro i prossimi 5-10 anni, pianificare proattivamente per incidenti di sicurezza o violazioni dei dati sarà fondamentale. Ci si aspetta di vedere un maggiore enfasi su *playbook* di preparazione

e risposta agli incidenti, oltre a un maggiore investimento nell'istruzione e nella formazione dei dipendenti.

Lo sviluppo di normative continuerà. Oltre al GDPR, PIPEDA e CCPA, si prevedono ulteriori regolamenti a livello statale o regionale. Le aziende che lavorano con informazioni di identificazione personale dovranno dare priorità alla conformità. Inoltre, l'assicurazione informatica guiderà la domanda di valutazioni della sicurezza informatica, con i fornitori che richiederanno o incentiveranno i clienti a sottoporsi a tali valutazioni come parte del processo di sottoscrizione o delle condizioni di polizza.

In conclusione, il futuro della *cybersecurity* è un territorio in costante evoluzione, plasmato dalle sfide emergenti, dall'avanzamento della tecnologia e dalle tattiche in continua evoluzione degli attaccanti. L'*AI* e l'*IoT* avranno un impatto significativo, richiedendo un approccio proattivo e adattivo per proteggere sistemi e infrastrutture critiche. La *cybersecurity* dovrà continuare a evolversi per rimanere un passo avanti rispetto alle minacce in rapida evoluzione.

8. CONCLUSIONI

La *cybersecurity* ha radici profonde che si intrecciano con lo sviluppo delle tecnologie digitali nel corso degli anni. Questa disciplina si è evoluta costantemente per fronteggiare un panorama sempre mutevole di minacce informatiche. *Malware, attacchi DDoS, phishing* e altre forme di intrusione rappresentano alcune delle molteplici minacce che le organizzazioni devono affrontare quotidianamente. Per difendersi da tali attacchi, vengono impiegate una serie di tecniche e strumenti, tra cui *firewall, antivirus, crittografia e autenticazione*. Tuttavia, la difesa contro le minacce digitali non può prescindere da solide strategie di *cybersecurity*, che includono ruoli dedicati e piani di risposta agli incidenti. Inoltre, normative come il GDPR hanno introdotto regole stringenti per la protezione dei dati personali e la sicurezza informatica, imponendo alle organizzazioni di adottare misure specifiche per garantire la conformità. Guardando al futuro, il campo della *cybersecurity* si trova di fronte a nuove sfide e opportunità. Tecnologie emergenti come l'*IoT*, il cloud e l'*AI* offrono nuove frontiere di rischio, ma anche possibilità di miglioramento continuo attraverso l'innovazione e l'adattamento delle nuove minacce.

La *cybersecurity* è un aspetto cruciale in un mondo sempre più digitalizzato e interconnesso. I rischi di attacchi informatici e violazioni dei dati sono in continua crescita, con potenziali conseguenze disastrose per individui, aziende e istituzioni. È fondamentale mantenere alta l'attenzione sulla sicurezza informatica, investendo in formazione, tecnologie all'avanguardia e *best practice*.

Il panorama della *cybersecurity* è destinato a cambiare rapidamente, con l'emergere di nuove minacce e tecnologie. Per stare al passo, è necessario un cambiamento culturale che veda la sicurezza informatica come una priorità strategica, non un mero adempimento. Servono investimenti costanti, collaborazione tra pubblico e privato, e una forza lavoro qualificata e aggiornata. Solo così potremo affrontare le sfide future e sfruttare appieno i benefici del digitale, proteggendo ciò che conta di più: dati, sistemi e reputazione.

BIBLIOGRAFIA E SITOGRAFIA

20 Emerging Cybersecurity Trends to Watch Out in 2024, https://www.simplilearn.com/top-cybersecurity-trends-article, consultato il 01/06/2024.

AI e Cybersecurity: come l'AI sta cambiando la sicurezza informatica, https://magazine.relatech.com/ai-e-cybersecurity-come-lai-sta-cambiando-la-sicurezza-informatica, consultato il 26/05/2024.

Cos'è un attacco informatico?, https://www.cisco.com/c/it_it/products/security/common-cyberattacks.html, consultato il 26/05/2024.

Cybersecurity, che cos'è e perché è una priorità per le aziende, https://www.agendadigitale.eu/sicurezza/cybersecurity-che-cose-e-perche-e-una-priorita-per-le-aziende/, consultato il 26/05/2024.

Cyber security, le minacce informatiche al giorno d'oggi: quali sono e come riconoscerle, https://www.cybersecurity360.it/nuove-minacce/cyber-security-le-minacce-informatiche-al-giorno-doggi-quali-sono-e-come-riconoscerle/, consultato il 26/05/2024.

Cybersecurity History: Hacking & Data Breaches, https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches, consultato il 25/05/2024.

Cybersecurity Predictions 2023-2027: Trends and Challenges, https://www.ermes.company/blog/cybersecurity-predictions-2023-2027-trends-and-challenges/, consultato il 01/06/2024.

Cyber Security Testing, https://www.checkpoint.com/it/cyber-hub/cyber-security/cyber-security-testing-types-of-cybersecurity-testing/, consultato il 27/05/2024.

Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9543401/, consultato il 24/05/2024.

GDPR e Cybersecurity: tutto quello che dovreste sapere, https://cyberment.it/sicurezza-informatica/gdpr-e-cybersecurity-tutto-quello-che-dovreste-sapere/, consultato il 30/05/2024.

How to Create a Cybersecurity Incident Response Plan, https://hyperproof.io/resource/cybersecurity-incident-response-plan/, consultato il 28/05/2024.

Il GDPR come legge sulla sicurezza informatica? Sinergie e nodi da sciogliere, https://www.agendadigitale.eu/sicurezza/il-gdpr-come-legge-sulla-sicurezza-informatica-sinergie-e-nodi-da-sciogliere/, consultato il 30/05/2024.

Incident Response Plan: Frameworks and Steps, https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/, consultato il 28/05/2024.

Normative Cyber Security: Codice Privacy e GDPR, https://lecs.io/normative-cyber-security-codice-privacy-e-gdpr/, consultato il 30/05/2024.

Seven trends that could shape the "official future" of cybersecurity in 2030, https://cltc.berkeley.edu/publication/seven-trends-cybersecurity-2030/, consultato il 01/06/2024.

Sicurezza informatica e protezione dati aziendali: tutto quello che devi sapere, https://www.scao.it/sicurezza-informatica-e-protezione-dati-aziendali-tutto-quello-che-devi-sapere/, consultato il 26/05/2024.

Significant Cyber Incidents, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents, consultato il 25/05/2024.

Some of The Biggest Cyber Security Breaches in History, https://intaso.co/news/some-of-the-biggest-cyber-security-breaches-in-history/, consultato il 25/05/2024.

Test Cyber Security: Protezione Avanzata per Dispositivi, https://www.test-ing.it/test-cyber-security/, consultato il 27/05/2024.

Top 7 Cyber Security Trends in 2024, https://www.checkpoint.com/cyber-hub/cyber-security/top-7-cyber-security-trends-in-2024/, consultato il 01/06/2024.

What is Cyber Security? Definition, Meaning, and Purpose, https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-cybersecurity/, consultato il 24/05/2024.

What is Incident Response? Process, Frameworks, ands Tools, https://www.bluevoyant.com/knowledge-center/what-is-incident-response-process-frameworks-and-tools, consultato il 28/05/2024.

What is the future of cybersecurity?, https://fieldeffect.com/blog/what-is-the-future-of-cyber-security, consultato il 01/06/2024.