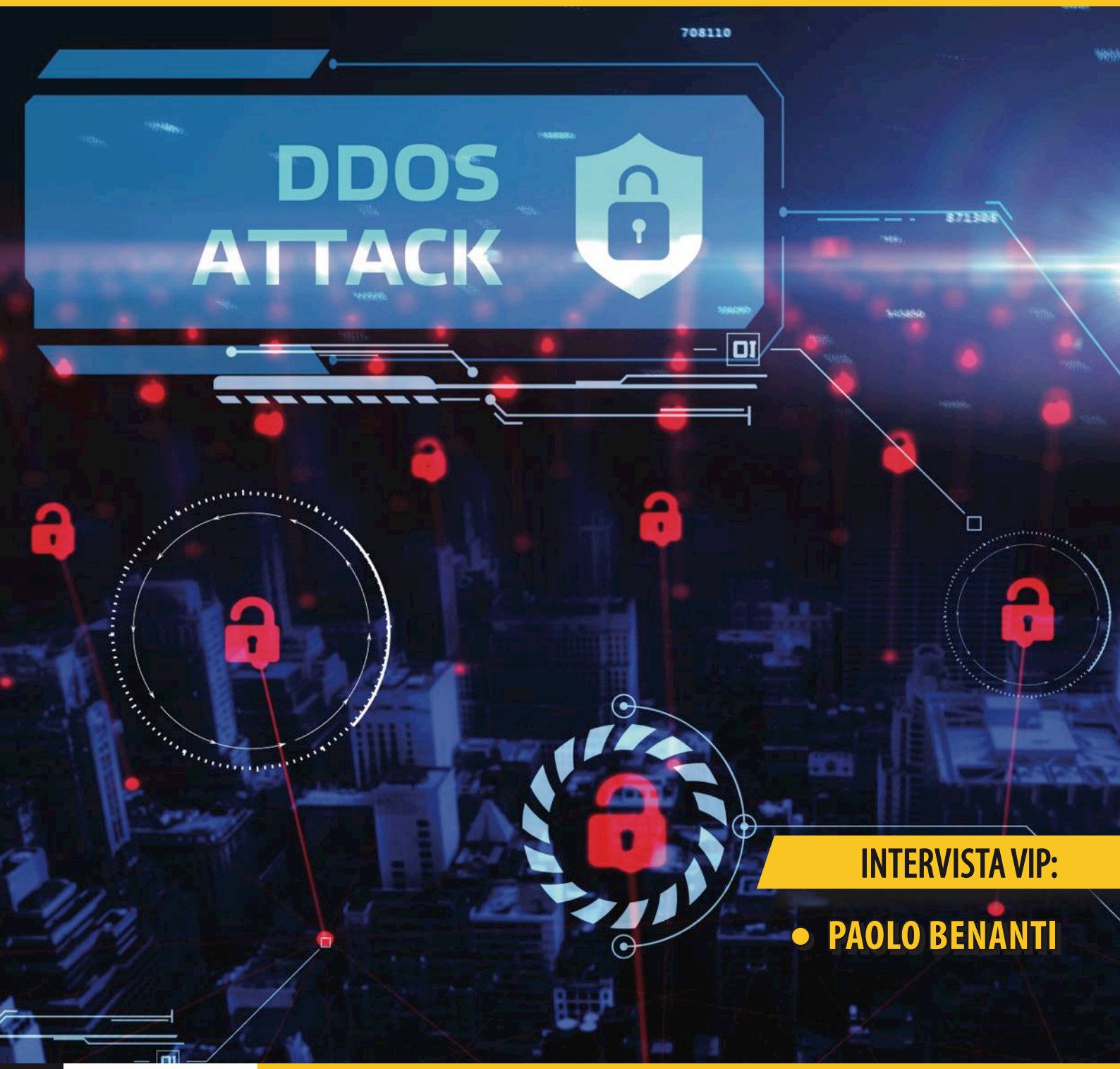
Cybersecurity Trends

Edizione italiana, N. 1 / 2025



INTERVISTA VIP:

- PAOLO BENANTI

Folder centrale: Attacchi DDoS

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Cybersecurity Trends

Leggi la rivista **online** quando
e dove vuoi!
Puoi scegliere tra news, articoli,
interviste, nuove sezioni,
approfondimenti,
rubriche e contenuti multimediali.

Scopri anche la nuova sezione
dedicata agli esperti della cyber security!
Al suo interno
Hacking Around e Technical Video.

Nella sezione Rubriche:
Bibliografia
Dalla Redazione
Dalle Aziende
Dalle Università
Eventi
Offerte di Lavoro

www.cybertrends.it

Indice

L'arma digitale dei moderni conflitti.

Autore: Nicola Sotira

Nel mondo sempre più connesso di oggi, la guerra, da tempo, non si combatte più solo con armi convenzionali e si parla sempre più spesso di contesto ibrido. Una nuova frontiera del conflitto si gioca nel cyberspazio. Tra le armi digitali più diffuse e meno costose ci sono gli **attacchi DDoS** – Distributed Denial of Service – capaci di mettere fuori servizio siti web, server e infrastrutture critiche. In molti casi, questi attacchi non sono solo frutto di cybercriminalità comune, ma rappresentano strumenti geopolitici veri e propri, usati da Stati e gruppi affiliati per indebolire, spiare o intimidire rivali internazionali. Un attacco DDoS mira a **rendere inaccessibile un servizio online** sovraccaricandolo di richieste. In pratica, migliaia o milioni di dispositivi (spesso infettati da malware e controllati da remoto, formando una "botnet") inviano traffico simultaneo a un bersaglio finché non collassa o smette di rispondere. A differenza di un normale attacco hacker, il DDoS **non viola i sistemi** per rubare dati, ma punta a bloccare la funzionalità del servizio. È una forma di "saturazione" digitale che mira a disturbare, danneggiare economicamente o inviare un messaggio politico. Ovviamente in questo caso non siamo del dominio dell'accesso abusivo ai sistemi, ma comunque abbiamo un tema di indisponibilità del dato.

Il DDoS è diventato uno strumento geopolitico per le seguenti motivazioni:

- **Costo basso, impatto alto:** Non servono risorse enormi per lanciare un attacco efficace. È possibile affittare botnet per poche centinaia di euro e causare danni da milioni.
- **Negabilità plausibile:** È difficile risalire con certezza all'origine dell'attacco, il che permette agli Stati di agire indirettamente, usando gruppi proxy.
- **Obiettivi flessibili:** I DDoS possono colpire governi, banche, media, infrastrutture critiche, aziende. Il loro effetto può essere destabilizzante, anche senza causare danni permanenti.

Gli attacchi DDoS non causano solo disagi tecnici. Il loro impatto si estende su più livelli:

- **Psicologico:** un attacco DDoS contro un sito governativo può alimentare il senso di vulnerabilità.
- **Economico:** la paralisi di servizi bancari o e-commerce può tradursi in perdite concrete.
- **Propagandistico:** sono atti visibili, facili da rivendicare, e spesso vengono usati per fare notizia.

Negli ultimi anni, i governi occidentali hanno cominciato a rafforzare la propria capacità di difesa e risposta ai DDoS. La NATO, inoltre, ha incluso la **cyberdifesa tra i suoi compiti fondamentali**, e l'Unione Europea ha varato la **EU Cybersecurity Strategy**, con investimenti su CERT (Computer Emergency Response Teams) nazionali e sovranazionali. Il rischio maggiore è che **gli attacchi DDoS diventino solo la punta dell'iceberg** in un conflitto digitale più ampio. Se finora sono stati usati per destabilizzare o mandare segnali, potrebbero in futuro essere combinati con attacchi distruttivi contro infrastrutture critiche: centrali, ospedali, reti elettriche, trasporti.

Gli attacchi DDoS sono oggi armi **geopolitiche a tutti gli effetti** e la loro semplicità tecnica nasconde un potenziale destabilizzante enorme, soprattutto se usati in coordinamento con altre forme di aggressione; fisica, informativa o economica.

Nel contesto geopolitico attuale, dominato da tensioni tra grandi potenze, conflitti regionali e instabilità globale, **la guerra cibernetica è già realtà**, e i DDoS sono uno degli strumenti principali di questo nuovo arsenale. Prepararsi a difendersi da questi attacchi non è solo una questione tecnica: è una questione di **sicurezza nazionale**. ■

BIO

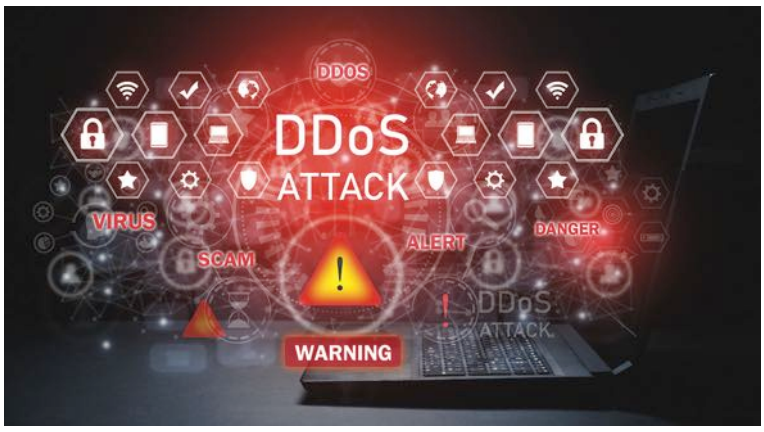
Nicola Sotira è Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Attacchi Distributed Denial-of-Service (DDoS): una minaccia crescente per i settori italiani.

Autore: Ilaria Buonagurio

Gli attacchi DDoS (Distributed Denial-of-Service) sono una preoccupazione importante nel campo della cybersecurity. Questi attacchi hanno come obiettivo l'interruzione del normale traffico di un server, di un servizio o di una rete presi di mira, sovraccaricandoli con una quantità enorme di traffico internet. Negli ultimi anni, i settori italiani sono diventati sempre più spesso bersaglio di queste minacce informatiche, rendendo necessaria una comprensione più approfondita e meccanismi di difesa robusti.

Un attacco DDoS coinvolge più sistemi informatici compromessi, spesso definiti botnet, che vengono utilizzati per inondare il bersaglio con un traffico eccesivo. Ciò può causare la lentezza o la totale assenza di risposta del server o della rete bersaglio, negando agli utenti legittimi l'accesso al servizio. L'obiettivo principale è quello di interrompere le operazioni aziendali, con conseguenti danni finanziari e di reputazione.



Gli attacchi DDoS possono essere classificati a grandi linee in tre categorie principali. Il primo tipo è quello degli attacchi volumetrici, che mirano a sovraccaricare l'obiettivo generando un'enorme quantità di traffico. Questo flusso di dati può presentarsi in varie forme, come flood UDP e flood ICMP, entrambi studiati per esaurire la larghezza di banda del sistema bersaglio.

La seconda categoria è quella degli attacchi di protocollo. Questi attacchi sfruttano le vulnerabilità dei protocolli di rete per interrompere il normale funzionamento dell'obiettivo. Esempi di attacchi di protocollo sono i SYN flood, in cui l'attaccante invia una serie di richieste SYN al sistema

BIO

Ilaria Buonagurio è un ingegnere con la passione per la cybersecurity, con uno spiccato interesse per la sicurezza industriale e l'automazione. È spinta dall'amore per la soluzione di problemi logici e dalla curiosità di capire come funzionano le cose, come possono essere migliorate e perché funzionano nel modo in cui funzionano. Professionalmente, ricopre il ruolo di coordinatore globale per Offensive Security, in una delle principali aziende italiane di moda e retail. Si occupa di selezionare e implementare nuove soluzioni tecniche e processi per proteggere i perimetri IT e OT. Fornisce inoltre servizi di consulenza ad altre funzioni interne sulla Security By Design per progetti aziendali critici. Il suo mix unico di competenze tecniche, capacità di risolvere i problemi e curiosità culturale la rendono una risorsa preziosa nel campo in continua evoluzione della cybersecurity.

dell'obiettivo per consumare le risorse del server e gli attacchi a pacchetti frammentati, che prevedono l'invio di pacchetti malformati all'obiettivo per causare congestione e interruzione della rete.

Infine, gli attacchi di livello applicativo si concentrano su applicazioni o servizi specifici, con l'obiettivo di esaurire le risorse dell'applicazione presa di mira. Esempi comuni di questo tipo di attacco sono gli HTTP flood, in cui l'attaccante invia numerose richieste HTTP a un server Web per sopraffarlo, e i DNS query flood, che comportano il bombardamento di un server DNS con un elevato volume di richieste per interromperne il servizio.

Diversi settori, in particolare le piattaforme di e-commerce, le istituzioni finanziarie e i servizi online, hanno registrato un aumento significativo degli attacchi DDoS. L'impatto di questi attacchi può essere devastante in più modi.

In primo luogo, c'è la questione della perdita finanziaria. I tempi di inattività causati dagli attacchi DDoS possono comportare significative perdite finanziarie. Ad esempio, un sito di e-commerce che non funziona durante le ore di punta dello shopping può perdere migliaia di euro. Questo colpo finanziario improvviso può essere particolarmente dannoso per le aziende che si basano sopattutto sulle transazioni online.

In secondo luogo, gli attacchi DDoS possono causare danni alla reputazione. Interruzioni frequenti o prolungate possono danneggiare la reputazione di un'azienda, facendo perdere la fiducia e la fedeltà dei clienti. I clienti si aspettano un servizio affidabile e quando un'azienda non riesce a mantenerlo a causa di attacchi ripetuti, può causare un danno a lungo termine all'immagine del brand.

Infine, l'interruzione dell'operatività è un'altra delle principali conseguenze degli attacchi DDoS. Questi attacchi possono interrompere le attività aziendali, con ripercussioni su tutto, dal servizio clienti alla gestione della catena di approvvigionamento. Quando i sistemi non funzionano, i dipendenti potrebbero non essere

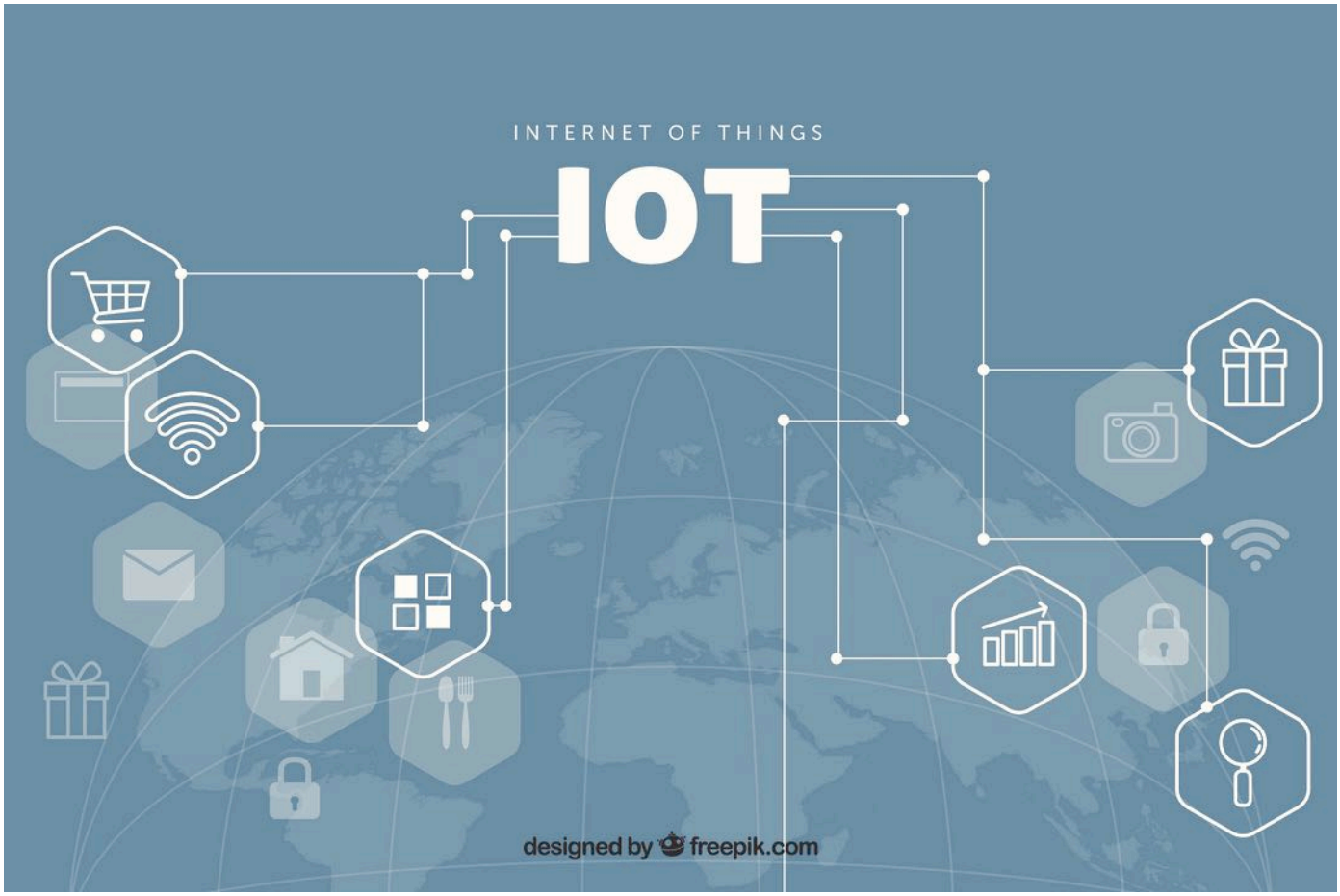
in grado di svolgere efficacemente le proprie mansioni, causando ritardi e inefficienze che possono ripercuotersi su tutta l'organizzazione.

Il panorama degli attacchi DDoS si sta evolvendo e sta modellando il panorama delle minacce cyber. Comprendere queste tendenze è fondamentale per le organizzazioni che vogliono sviluppare strategie efficaci per difendersi da questi attacchi sempre più sofisticati.

Una tendenza degna di nota è l'aumento degli attacchi ipervolumetrici. Questi attacchi sono caratterizzati da una quantità enorme di traffico; l'enorme volume di traffico generato in questi attacchi è spesso ottenuto attraverso l'uso di botnet di grandi dimensioni, che possono sovraccaricare anche le difese di rete più robuste. Un esempio è l'attacco da record che ha colpito un'azienda di telecomunicazioni dell'Asia orientale nel gennaio 2025, con un picco di ben 5,6 Tbps e una durata di 80 secondi.

Un'altra tendenza significativa è il passaggio agli attacchi di livello applicativo. A differenza degli attacchi volumetrici che inondano la rete di traffico, gli attacchi di livello applicativo mirano ad applicazioni e servizi specifici. Ciò li rende più difficili da rilevare e mitigare, poiché spesso imitano il comportamento legittimo degli utenti. Gli aggressori possono sfruttare le vulnerabilità delle applicazioni web, dei database o di altri servizi critici, causando interruzioni che possono essere difficili da rintracciare e risolvere. Un episodio significativo è stato l'attacco HTTP/s Rapid Reset del 2023, che ha mandato in tilt numerosi servizi online sfruttando le vulnerabilità del protocollo HTTP e ha raggiunto un picco di poco superiore a 201 milioni di richieste al secondo.

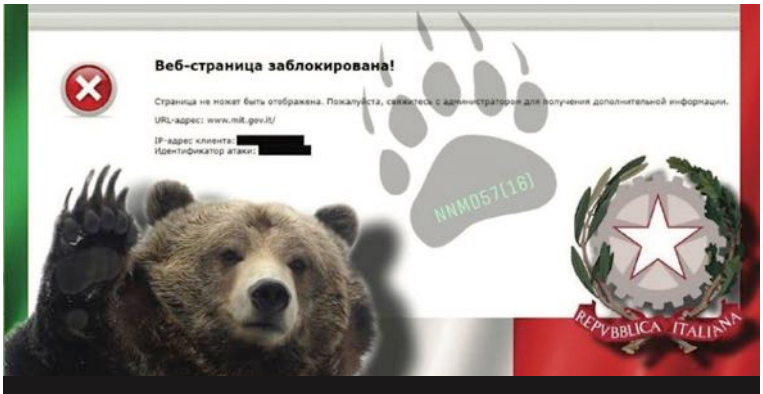
La comparsa di piattaforme DDoS-as-a-Service ha anche reso più facile per gli aggressori lanciare attacchi sofisticati senza richiedere la conoscenza di tecniche approfondite. Queste piattaforme offrono strumenti e servizi già pronti che possono essere noleggiati o acquistati, consentendo anche agli attaccanti meno esperti di eseguire campagne DDoS complesse. Questa democratizzazione delle capacità di attacco ha portato ad un aumento della frequenza e della gravità degli incidenti DDoS.



Inoltre, la proliferazione dei dispositivi Internet of Things (IoT) ha contribuito alla creazione di grandi botnet utilizzate per lanciare attacchi DDoS su vasta scala. I dispositivi IoT, spesso privi di solide misure di sicurezza, possono essere facilmente compromessi e integrati nelle botnet. Una volta entrati a far parte di una botnet, questi dispositivi possono essere utilizzati per generare quantità significative di traffico, amplificando l'impatto degli attacchi DDoS.

Negli ultimi anni, diversi attacchi DDoS di alto profilo hanno preso di mira le aziende italiane, causando interruzioni significative ed evidenziando l'importanza di solide misure di cybersecurity.

Nell'agosto 2023, una serie di attacchi ha interrotto i servizi online di diverse istituzioni finanziarie. Questi incidenti hanno sottolineato la vulnerabilità del settore bancario alle minacce informatiche ed evidenziato la necessità di rafforzare i protocolli di sicurezza per proteggere i dati finanziari sensibili e garantire la continuità dei servizi online.



© Rainews

Un recente incidente degno di nota ha coinvolto nove siti web del Governo italiano, tra cui quelli del Ministero degli Esteri e dei principali aeroporti di Milano. L'attacco del gennaio 2025 è stato condotto da un gruppo filorusso noto come "Noname57". Sebbene l'attacco abbia causato interruzioni temporanee, è stato mitigato in 109 minuti dimostrando la resilienza delle difese di cybersecurity dell'Italia.

Lo stesso gruppo di hacker, a febbraio 2025, ha lanciato una serie di attacchi DDoS contro diverse aziende e istituzioni italiane. Gli attacchi avevano l'obiettivo di interrompere le operazioni di enti strategici, tra cui aeroporti, autorità, banche e aziende private. Nonostante la portata significativa degli attacchi, l'Agenzia nazionale italiana per la sicurezza informatica (ACN) ha risposto prontamente, mitigando l'impatto e garantendo che le interruzioni fossero ridotte al minimo. Questo incidente sottolinea la continua minaccia rappresentata dagli attacchi informatici a sfondo politico ed evidenzia l'importanza di solide misure di sicurezza informatica per proteggere le infrastrutture critiche.

Per proteggersi dagli attacchi DDoS, si possono adottare diverse strategie efficaci. Un approccio fondamentale è l'analisi del traffico, che prevede il monitoraggio regolare del traffico di rete per identificare comportamenti insoliti che potrebbero indicare un attacco DDoS. Tenendo sotto controllo il traffico, le aziende possono individuare tempestivamente le potenziali minacce e adottare le misure appropriate per mitigarle.

Un'altra strategia importante è il rate limiting. Questa tecnica aiuta a controllare la quantità di traffico che può raggiungere il server, evitando che venga sopraffatto da richieste eccessive. Impostando dei limiti al numero di richieste che un server può gestire in un determinato lasso di tempo, le aziende possono ridurre il rischio che i loro sistemi vengano messi fuori uso da un'ondata di traffico dannoso.

Anche l'implementazione di firewall per applicazioni Web (WAF) è una misura di protezione fondamentale contro gli attacchi DDoS. I WAF filtrano e monitorano il traffico HTTP tra un'applicazione web e Internet, bloccando il traffico dannoso prima che possa raggiungere il server. Questo ulteriore livello di sicurezza aiuta a salvaguardare le applicazioni web da vari tipi di attacchi, compresi quelli che mirano a vulnerabilità specifiche.

Inoltre, molte aziende offrono servizi specializzati di protezione DDoS in grado di rilevare e mitigare gli attacchi in tempo reale. Questi servizi forniscono funzionalità avanzate di rilevamento e risposta alle minacce, assicurando che le aziende possano rispondere rapidamente e neutralizzare gli attacchi DDoS nel momento in cui si verificano. Sfruttando questi servizi, le aziende possono migliorare la loro posizione di sicurezza complessiva e ridurre al minimo l'impatto di potenziali attacchi.

In sintesi, l'aumento degli attacchi DDoS rappresenta una seria minaccia per diversi settori, con perdite finanziarie, danni alla reputazione e interruzioni operative tra gli impatti più significativi. Le organizzazioni devono essere particolarmente attente e proattive nell'implementazione di solide misure di sicurezza per mitigare questi rischi.

Gli attacchi DDoS rappresentano una minaccia significativa per i settori italiani, con il rischio di causare ingenti danni finanziari e di reputazione. Comprendendo la natura di questi attacchi e implementando solide strategie di mitigazione, le aziende possono proteggersi meglio e garantire la continuità delle loro operazioni. Poiché le minacce informatiche continuano ad evolversi, rimanere informati e preparati è fondamentale per proteggere il sistema digitale italiano.

Bibliographical References

- Cloudflare. "What is a DDoS Attack?"
- Fortinet. "What is a DDoS Attack? DDoS Meaning, Definition & Types."
- Microsoft Security. "What Is a DDoS Attack?"
- Example of an Italian e-commerce platform attack.
- CrowdStrike. "What Is a DDoS Attack? Mitigation & Protection."
- Cybersecurity Insiders. "Italy faces DDOS attacks from Russia."
- DDoS Internet Security. "IOTW Italian Banks Hit with DDoS Attacks." ■

La gestione degli attacchi DDoS.

Autore: Simone Coltellese

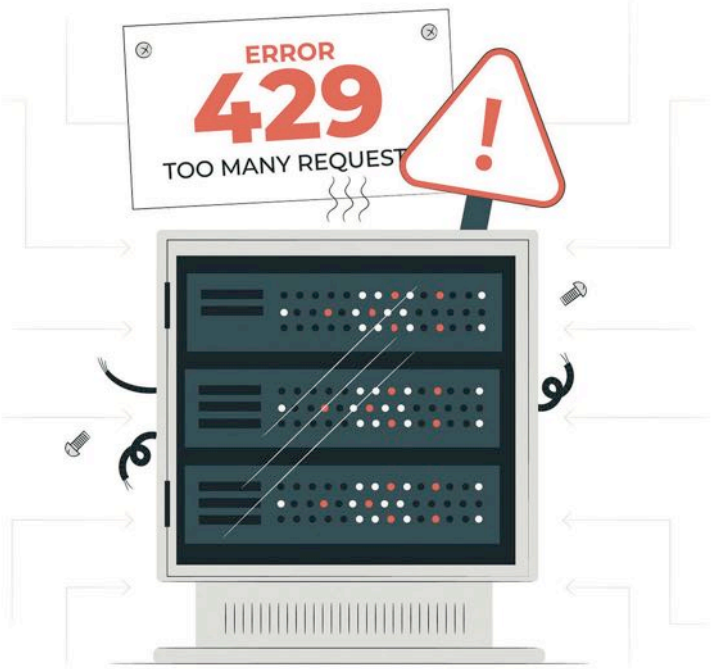
Gli **attacchi DDoS** *(Distributed Denial of Service)* continuano a occupare una posizione di primo piano nel panorama delle minacce *cyber*. L'acutizzarsi delle tensioni geopolitiche, con particolare riferimento ai conflitti tra Russia e Ucraina e Israele-Hamas, ha comportato anche una progressiva ascesa di collettivi che, motivati da interessi politici e/o sociali (cc.dd. *Hacktivist*), conducono con maggiore frequenza operazioni *cyber* prevalentemente mediante attacchi di tipo DDoS e prendendo di mira organizzazioni senza distinzione di settore.

BIO

Simone Coltellese è un analista di sicurezza e frodi informatiche presso il CERTFin – CERT Finanziario Italiano. Ha conseguito la laurea triennale e magistrale in Ingegneria Informatica presso l'Università di Roma "La Sapienza" rispettivamente nel 2016 e nel 2020. Con il suo lavoro di tesi ha contribuito alla pubblicazione di un articolo scientifico, *"Triage of IoT Attacks Through Process Mining"*, presentato alle Conferenza Internazionale "On the Move to Meaningful Internet Systems". Al CERTFin, svolge principalmente le attività *Information Sharing e Cyber Threat Intelligence*. Inoltre, partecipa stabilmente ai gruppi di lavoro del PSSG *(Payment Security Support Group)* e del PSFPWG *(Payment Scheme Fraud Prevention Working Group)* istituiti dallo European Payment Council (EPC). I suoi interessi includono la *cybersecurity engineering, Infosharing models* e l'*intelligence* sulle minacce cyber.

Gli attacchi DDoS sono tra quelli più **difficili da mitigare**, anche per le organizzazioni più preparate. I motivi di tale difficoltà sono molteplici:

- **Risorse illimitate:** a volte gli attaccanti hanno a disposizione un arsenale talmente vasto da poter lanciare attacchi DDoS iper-volumetrici;
- **DDoS-as-a-Service:** con la nascita di questo nuovo mercato anche gli attaccanti con basse capacità sono in grado di poter lanciare un attacco DDoS semplicemente pagando una *fee*;
- **Evoluzione delle tecniche e tattiche:** attaccanti con elevate capacità sfruttano debolezze nei protocolli di rete, impiegano tecniche di amplificazione (ad esempio negli attacchi *DNS amplification*) per incrementare la portata dei loro attacchi e combinano insieme più tecniche (i cosiddetti attacchi multi-vettore) complicandone la gestione da parte dei difensori.



Alla luce di quanto sopra, è necessario comprendere che non sono più sufficienti i soli investimenti in servizi di sicurezza che spesso vengono etichettati come soluzioni di prevenzione. Tali soluzioni, in realtà, sono strumenti reattivi e di mitigazione piuttosto che vere e proprie misure

preventive. Difatti, mentre possiamo mitigare una buona parte di attacchi DDoS, non è possibile pensare di poterli mitigare tutti.

Nonostante, quindi, strumenti come *Web Application Firewall* (WAF) e *Intrusion Detection Systems* (IDS) rimangano una componente fondamentale, è ancor di più importante investire su una **strategia di difesa completa** che non si basi esclusivamente sul concetto della prevenzione ma che combini insieme diversi approcci al fine di gestire al meglio un attacco DDoS.

Una delle fasi fondamentali di tale strategia è quella della **preparazione**. La preparazione ad un attacco DDoS non può essere ridotta alla sola creazione di un *Incident Response Team* (IRT). Essere preparati a un attacco DDoS significa anche:

- progettare un'**architettura solida e anti-DDoS** adottando buone pratiche di sicurezza di rete e delle applicazioni web;
- **esercitarsi periodicamente** per migliorare processi e piani di risposta nonché testare la propria infrastruttura simulando attacchi DDoS al fine di migliorare le misure di sicurezza.

La strategia deve anche garantire che la **risposta** ad un attacco DDoS sia **rapida**, **efficace** e **coordinata**. Per garantire la tempestività, un'organizzazione non può prescindere dal **monitorare costantemente** il traffico di rete e la propria infrastruttura al fine di rilevare e identificare anomalie e attività sospette nel minor tempo possibile. Tuttavia, distinguere tra traffico legittimo e traffico malevolo rimane senza dubbio una delle sfide principali nel mitigare un attacco DDoS. La sfida deriva soprattutto dalla diversità di tali attacchi, che possono assumere varie forme ed essere anche molto sofisticati. A tal fine, è quindi indispensabile impiegare strumenti che monitorino la rete in tempo reale, stabilendo prima una **baseline** dei normali modelli di traffico per registrare rapidamente le deviazioni. Inoltre, è bene tenere a mente che tali baseline delle prestazioni dell'infrastruttura e dei servizi erogati devono essere monitorate e aggiornate costantemente. Difatti, delle semplici soglie statiche potrebbero non cogliere una regolare crescita del normale traffico di rete, innescando quindi falsi positivi.

	Attacco Volumetrico	Attacco al Protocollo	Attacco al livello applicativo
Target	La rete	Apparecchiature di rete intermedie come router, firewall, EDS/IPS e bilanciatori di carico (L3 e L4)	Web applications e web server (L7)
Metrica	Bit al secondo (bps), Gigabit al secondo (Gbps)	Pacchetti al secondo (PPS)	Richieste al secondo (RPS)
Categoria	Connectionless	Connection-based	Connection-based
Caratteristiche	- High volume - Inonda la rete con richieste apparentemente legittime	- Vengono sfruttati scenari in cui il target riceve una richiesta/pacchetto da un computer per poi rimanere in attesa di ulteriori comunicazioni mantenendo allocate le relative risorse - Gli attacchi più noti sono quelli che prendono di mira le tabelle di stato del protocollo TCP	- Low-rate - Imita il comportamento dell'utente
Esempi	Smurf Attacks, UDP flood, ICMP Floods, IP/ICMP Fragmentation, Amplification/ Reflection DDoS etc..	SYN flood, TCP flood, Ping of Death (PoD), etc..	HTTP flood, Slowloris, attacchi sui DNS (e.g. DNS laundering), etc..

- **identificare** gli *asset* e i servizi suscettibili di tali attacchi e **proteggere** interamente il perimetro esposto;
- **ridurre la superfice di attacco** per limitare quanto più possibile l'esposizione e avvalersi di servizi anti-DDoS aggiuntivi.

Ogni attacco DDoS è unico e una risposta adeguata può differire in base alla sua natura e severità. Pertanto, sin dalle prime sue prime fasi, risulta importante svolgere delle **analisi** esaminando i log, gli *alert* e qualsiasi informazione utile a trovare indizi circa la fonte e la tipologia di attacco. Le analisi di dati e informazioni dovrebbero essere svolte tenendo conto almeno dei seguenti obiettivi:

- Comprendere il flusso logico dell'attacco e identificare i componenti degli asset dell'infrastruttura interessati;
- Identificare l'origine dell'attacco;
- Identificare la tipologia di attacco;
- Determinare la magnitudo dell'attacco;
- Identificare gli aspetti che caratterizzano il traffico malevolo e le differenze rispetto al traffico genuino;
- Determinare l'impatto sulla clientela e/o sugli utenti interni.

Tuttavia, in parallelo alle attività di analisi volte a determinare tipologia e

impatti, è di fondamentale importanza attuare le **misure di contenimento** al fine di limitare quanto più possibile i danni e il consumo di risorse. Nella maggior parte dei casi, tali misure non saranno sufficienti da sole a neutralizzare completamente l'attacco. Tra le misure di contenimento sono da valutare sicuramente il filtraggio indirizzi IP, l'abilitazione e prioritizzazione degli IP in whitelist, il rafforzamento delle componenti IT e il *Geo-Blocking*. Ovviamente, tali misure devono essere applicate con criterio in quanto potrebbero provocare effetti controproducenti.

Una volta compresa la tipologia e i tratti distintivi dell'attacco DDoS si potranno adottare le misure di contenimento e mitigazione più adeguate al fine di bloccare l'attacco.

Ad esempio, diversamente da quelli a livello di rete, gli attacchi DDoS a livello applicativo (L7) non possono essere mitigati facendo leva sulla sola capacità di rete. Difatti, la maggior parte delle organizzazioni contrasta tale tipologia di attacchi mediante l'utilizzo di WAF, applicando delle *signature* specifiche, o ricorrendo a servizi anti-DDoS forniti da aziende specializzate.

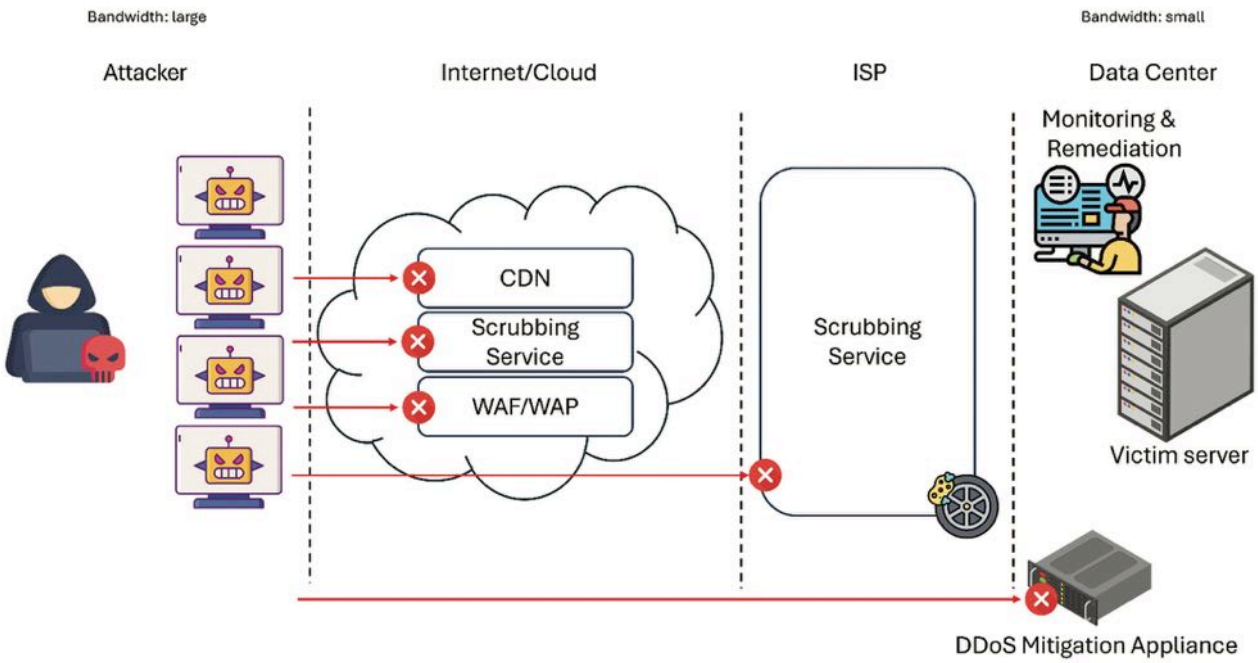
Durante le attività di risposta e mitigazione è necessario mantenere un **coordinamento** tra le varie funzioni aziendali e gli *stakeholder* coinvolti che spesso includono anche figure esterne alla propria organizzazione, come ad esempio ISP, CSP e fornitori di servizi anti-DDoS. A tal proposito, l'attivazione di una ***war room*** semplifica l'esecuzione di vari processi, considerando che tutte le parti coinvolte avranno la possibilità di avere una visione completa e non frammentata della gestione e degli sviluppi dell'incidente.

Dopo aver risolto l'incidente, il team dovrebbe concentrarsi sull'individuarne le cause eseguendo una ***Root Cause Analysis*** (RCA) e revisionando complessivamente tutta la sua gestione. Dovrà quindi essere realizzato un report *post mortem* dell'incidente che dovrà trattare almeno i seguenti punti:

- **Riepilogo dell'incidente:** dettagli su cosa è successo, i servizi e i clienti interessati, la gravità dell'incidente e il personale coinvolto nella risoluzione;
- **Root Cause Analysis:** descrive i punti di errore, le principali cause dell'incidente e che cosa l'ha provocato. Il *team* può utilizzare l'approccio delle *5-Whys* per scoprire le circostanze che hanno portato a un incidente;
- **Azioni intraprese:** delinea le azioni o i passaggi intrapresi per rilevare, valutare e risolvere l'incidente;
- **Timeline dell'incidente:** specifica il momento degli eventi significativi, il momento del rilevamento, della correzione, dell'escalation, della risoluzione e così via;
- **Conclusioni e next step:** spiega che cosa è andato bene, che cosa non è andato bene e i passaggi da intraprendere per scongiurare il ripetersi dell'incidente.

Inoltre, è necessario avviare un processo di ***lesson learned*** coinvolgendo sia i membri dell'IRT che le altre parti dell'organizzazione coinvolte nella gestione dell'incidente stesso. L'obiettivo di tale processo sarà quello di **migliorare le procedure di risposta** da applicare in eventuali attacchi futuri **colmando gap e debolezze** emerse in precedenza. In particolare, devono essere identificate le specifiche aree che richiedono miglioramenti, come l'aggiornamento delle *policy*, l'implementazione di meccanismi di difesa aggiuntivi, la formazione di nuovi membri del team, l'ammodernamento dell'infrastruttura IT, l'adeguatezza dei servizi anti-DDoS adottati e così via.

In conclusione, il sempre più crescente numero di attacchi DDoS deve essere considerato come un campanello di allarme per chi deve garantire la sicurezza e la continuità aziendale della propria organizzazione. Implementare un'adeguata strategia di difesa può certamente identificare e contrastare i vettori di attacco e al contempo contenere gli attacchi DDoS prima che causino danni significativi ai servizi e gli *asset* presi di mira. ■



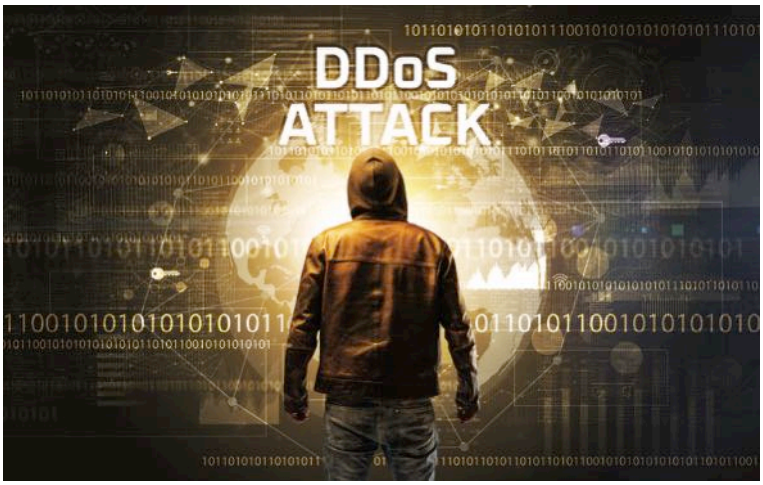
Il futuro della protezione DDoS: andare oltre le difese reattive.

Autore: Orly Mager

Introduzione

Il panorama della sicurezza informatica è in rapida evoluzione e gli attacchi DDoS (Distributed Denial of Service) stanno diventando una delle principali preoccupazioni per le organizzazioni di tutto il mondo. Ciò che è accaduto nel febbraio 2025 ci ha ricordato questa crescente minaccia: l'Italia ha dovuto affrontare una serie di devastanti attacchi DDoS che hanno colpito banche, aeroporti, sistemi di trasporto e servizi governativi, tra cui la Banca d'Italia, gli aeroporti di Linate e Malpensa, il Ministero degli Affari Esteri e l'Aeronautica Militare. Questi attacchi, attribuiti al gruppo di hacker filorussi NoName057, evidenziano come le tensioni geopolitiche e l'hacktivismo stiano alimentando l'aumento delle disruption informatiche.

Nonostante gli ingenti investimenti in tecnologie di mitigazione DDoS, le aziende continuano a soffrire di costosi tempi di inattività e interruzioni del servizio. Ciò mette in luce una falla critica: non nei meccanismi di protezione in sé, ma nel modo in cui vengono configurati e mantenuti. La causa principale della maggior parte delle vulnerabilità DDoS risiede nelle configurazioni errate, che creano migliaia di punti di ingresso sfruttabili dagli aggressori.



Il problema principale: perché la mitigazione DDoS tradizionale è insufficiente

Le organizzazioni in genere si affidano a soluzioni DDoS ibride sempre attive per proteggere la propria infrastruttura. Tuttavia, queste soluzioni richiedono una continua revisione per adattarsi alle architetture di rete in continua evoluzione e ai metodi di attacco in evoluzione. L'incapacità di tenere il passo con questi continui cambiamenti porta a configurazioni errate, lasciando le organizzazioni esposte.

Per mettere questo dato in prospettiva, si consideri un'organizzazione con 100 indirizzi IP (ognuno dei quali rappresenta un servizio pubblico) e 150 potenziali vettori di attacco DDoS attraverso i livelli 3, 4 e 7. Ciò equivale a una superficie di attacco di 15.000 possibili vulnerabilità, una sfida enorme per i team di sicurezza che si affidano a test manuali e difese reattive.

Invece di affrontare in modo proattivo queste debolezze, le aziende spesso si trovano a correggere le configurazioni errate solo dopo che un attacco ha già causato danni, con conseguenti tempi di inattività prolungati e interruzioni operative.

BIO

Orly Mager è un'esperta di cybersecurity con una vasta esperienza nella sicurezza di rete e nella mitigazione degli attacchi. Ha collaborato con aziende tecnologiche leader, aiutando le organizzazioni a rafforzare la loro posizione di sicurezza informatica contro le minacce in evoluzione. La sua esperienza nelle soluzioni di sicurezza proattive l'ha resa un leader nella lotta contro gli attacchi DDoS.

La pressione normativa: il costo della non-compliance

Gli enti regolatori hanno preso atto del crescente panorama delle minacce informatiche e stanno attuando politiche rigorose per imporre la resilienza operativa.

- **DORA (Digital Operational Resilience Act):** Questa normativa impone test regolari di cybersecurity per garantire la business continuity. La mancata conformità può comportare multe significative, costringendo le organizzazioni ad adottare misure di sicurezza proattive.
- **Direttiva NIS2:** Richiede alle aziende di condurre valutazioni periodiche delle vulnerabilità e ritiene i dirigenti personalmente responsabili se non affrontano i rischi informatici. Questo aggiunge un ulteriore livello di pressione sulle aziende per migliorare le loro strategie di difesa DDoS.

Con l'inasprirsi dei requisiti normativi, le organizzazioni devono passare da una gestione reattiva degli incidenti a valutazioni proattive e continue della sicurezza per evitare sanzioni e danni alla reputazione.

MAZEBOLT

La soluzione: Gestione continua della vulnerabilità DDoS con MazeBolt RADAR

Affrontare la causa principale dei tempi di inattività DDoS richiede un cambio di paradigma dai tradizionali approcci di sicurezza reattivi a un modello di test automatizzato e continuo. È qui che MazeBolt RADAR™ interviene per cambiare le carte in tavola.

RADAR™ è una soluzione brevettata che elimina le vulnerabilità DDoS prima che si verifichi un attacco. A differenza dei test DDoS tradizionali, che sono periodici e dissuasivi, RADAR™ opera senza problemi senza impattare sulle operazioni aziendali. Identifica continuamente le configurazioni errate sull'intera superficie di attacco, dà priorità alle vulnerabilità e facilita la correzione automatica per garantire che le protezioni rimangano ottimizzate.

Come funziona il RADAR

1 **Visibilità completa della superficie di attacco:** RADAR™ fornisce alle organizzazioni una visione in tempo reale delle vulnerabilità DDoS su tutti i livelli di protezione della rete.

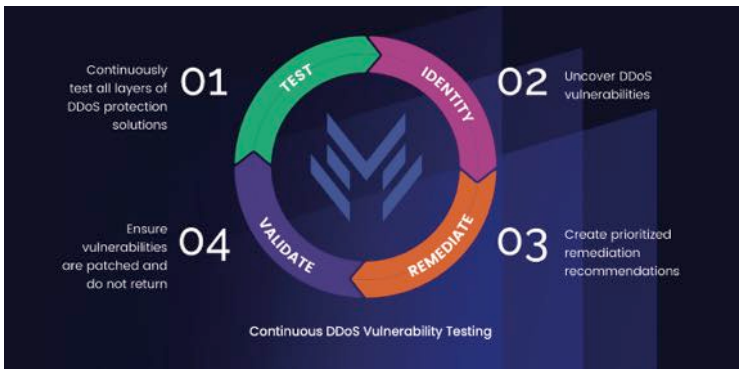
2 **Test continui:** A differenza dei tradizionali e infrequenti test DDoS, RADAR™ opera senza interruzioni e in modo continuo, garantendo che le posizioni di sicurezza rimangano aggiornate.

3 **Rimedio automatico:** Una volta rilevate le vulnerabilità, RADAR™ stabilisce le priorità e le corregge automaticamente, eliminando la necessità di una configurazione manuale e riducendo gli errori umani.

4 **Preparazione alla conformità:** Attenuando in modo proattivo le vulnerabilità DDoS, le organizzazioni possono garantire la conformità con DORA, NIS2 e altre normative di settore, evitando rischi finanziari e di reputazione.

Il futuro della protezione DDoS: Un approccio proattivo e automatizzato

Gli attacchi DDoS non accennano a diminuire e le organizzazioni non possono più permettersi di affidarsi a una risposta reattiva agli incidenti. Con la crescente complessità delle minacce informatiche, l'unica soluzione possibile è il test e la remediation continui e automatizzati.



RADAR™ di MazeBolt rappresenta la prossima evoluzione nella protezione DDoS, passando da difese manuali obsolete a un modello di sicurezza completamente automatizzato e basato sui dati. Integrando RADAR™, le organizzazioni possono finalmente andare oltre gli SLA e i tempi di risposta della mitigazione per passare a una vera strategia di difesa proattiva.

In un'epoca in cui i tempi di inattività equivalgono a perdite finanziarie e di reputazione, la necessità di innovazione nella gestione delle vulnerabilità DDoS non è mai stata così forte. Il momento di agire è adesso: adottando test continui, remediation automatizzata e visibilità della superficie di attacco completa, le aziende possono garantire operazioni resilienti e senza interruzioni di fronte a un panorama di minacce informatiche in continua evoluzione. ■

Comprendere gli attacchi DDoS e le moderne strategie di mitigazione.

radware

Autore: Ron Meyran

Gli attacchi DDoS (Distributed Denial-of-Service) sono una forma diffusa e dirompente di criminalità informatica. Questi attacchi mirano a sommergere la rete, il servizio o il sito web di un obiettivo con un'ondata di traffico Internet, rendendolo inaccessibile agli utenti legittimi. A differenza di altri attacchi informatici che sfruttano le vulnerabilità, gli attacchi DDoS si basano semplicemente sul volume per interrompere i servizi.

Caratteristiche degli Attacchi DDoS

Gli attacchi DDoS sono caratterizzati dall'utilizzo di più dispositivi compromessi, che spesso formano una botnet, per generare quantità massicce di traffico. Questa natura distribuita li rende particolarmente difficili da difendere. I tipi più comuni di attacchi DDoS includono:

1. Attacchi volumetrici: Mirano a consumare la larghezza di banda della rete bersaglio, sovraccaricandola di dati.
2. Attacchi di protocollo: Sfruttano le debolezze dei protocolli di rete per esaurire le risorse del server.
3. Attacchi al livello di applicazione: Questi attacchi prendono di mira applicazioni specifiche, rendendole indisponibili per gli utenti.

L'impatto di un attacco DDoS riuscito può essere grave, con perdite finanziarie, danni alla reputazione e interruzione dei servizi.

Strategie di Mitigazione

Per combattere gli attacchi DDoS, i fornitori di soluzioni utilizzano diverse strategie:

1 Limitazione delle richieste: I provider standard si concentrano sul Source-based Rate Limiting. Questa tecnica limita il numero di richieste che un server accetta dalla stessa fonte in un determinato periodo, contribuendo a ridurre il traffico eccessivo di richieste. Questa strategia è efficace per ridurre il traffico eccessivo e mantenere vitale l'infrastruttura applicativa. Tuttavia, blocca il traffico degli utenti legittimi insieme a quello degli attacchi ed è inefficace contro le tecniche sofisticate di attacco DDoS, come i flood HTTPS, i flood DNS o gli attacchi altamente distribuiti.

2 Rilevamento basato sul comportamento: per combattere le tecniche di attacco avanzate, alcuni fornitori di soluzioni utilizzano l'intelligenza artificiale e l'apprendimento automatico. Queste soluzioni possono identificare e rispondere rapidamente alle minacce, generando regole di blocco in tempo reale. I vantaggi di queste tecnologie sono che mitigano tutti i tipi di attacchi DDoS di rete e applicativi (compresi gli attacchi HTTPS/DNS flood) riducendo il rischio di falsi positivi.

Entità degli attacchi

NoName057(16) ha causato la stragrande maggioranza di questi incidenti, rivendicando oltre l'85% degli attacchi, mentre Z-Pentest ha contribuito per quasi il 10%, concentrandosi principalmente sulle violazioni industriali. L'industria manifatturiera è stata la più colpita, con il 27% del totale, seguita da vicino dalla finanza con il 24%. Le agenzie governative hanno registrato il 12% delle interruzioni, mentre i settori dell'ospitalità e dei trasporti hanno registrato circa il 9% degli attacchi totali.

Gestiscono il progetto DDoSia, una botnet finanziata da volontari e utilizzata per lanciare attacchi DDoS contro istituzioni governative, infrastrutture critiche, entità finanziarie e media nei Paesi membri della NATO. Per sostenere l'efficacia di questi attacchi condotti da volontari, NoName057(16) aggiorna frequentemente la sua infrastruttura di comando e controllo. Z-Pentest Alliance è un gruppo informatico filorusso specializzato in test di penetrazione, hacking e sabotaggio informatico.

BIO

Ron Meyran è a capo di un team globale di Threat Intelligence, Analysts Strategy e Technology & Partner Marketing di radware. Il team di intelligence sulle minacce raccoglie dati e segue gli attori delle minacce per fornire approfondimenti su motivazioni, obiettivi e comportamenti di attacco degli attori delle minacce. Nel suo ruolo di responsabile del marketing delle alleanze strategiche, Ron è stato il responsabile del riconoscimento di Radware nel settore e della leadership di marketing con i partner di canale e i partner OEM come Cisco e Check Point. Meyran è un esperto del settore della sicurezza informatica che rappresenta Radware in vari eventi di settore e sessioni di formazione. La sua leadership di pensiero e le sue opinioni sono state ampiamente pubblicate nelle principali riviste del settore IT e della sicurezza. Meyran ha conseguito una laurea in ingegneria elettrica presso l'Università Ben-Gurion e un MBA presso l'Università di Tel Aviv.

Caratteristiche degli attacchi

NoName057(16) sfrutta attacchi DDoS di livello 7 basati su HTTP, progettati per inondare i siti web con richieste POST e GET apparentemente legittime che sovraccaricano la capacità del server. Queste tattiche sono particolarmente efficaci perché sfruttano le debolezze dei tradizionali firewall per applicazioni web (WAF), utilizzando dati di richiesta casuali che sembrano normali ma servono a paralizzare i servizi online. Gli aggressori utilizzano reti VPN anonime e a una botnet gestita da volontari per nascondere la loro posizione, rendendo difficile rintracciare l'origine degli attacchi. Il numero di sessioni al secondo può variare notevolmente, da 10.000 a oltre 100.000, a seconda del numero di soggetti coinvolti in un determinato momento.

In sintesi

In conclusione, sebbene gli attacchi DDoS rappresentino una minaccia significativa per le applicazioni aziendali critiche, le organizzazioni devono effettuare una valutazione del rischio e adottare un'efficace strategia di mitigazione DDoS per mitigare efficacemente questi rischi e garantire la business continuity. ■

Attacchi DDoS.

Autore: Alberto Perini

La minaccia persistente alle infrastrutture digitali

Gli attacchi Distributed Denial of Service (DDoS) rappresentano una delle minacce più diffuse e sofisticate nel panorama della cybersecurity. Questi attacchi sfruttano reti di dispositivi compromessi, noti come botnet, per generare un traffico anomalo e massivo verso un obiettivo specifico, con l'intento di esaurire le risorse di rete o di elaborazione e rendere il servizio inaccessibile agli utenti legittimi.

Negli ultimi anni, con la crescente digitalizzazione e l'espansione delle infrastrutture critiche online, il numero e la portata degli attacchi DDoS sono aumentati esponenzialmente e le aziende, le istituzioni governative e persino i fornitori di servizi essenziali come banche, ospedali ed enti pubblici sono sempre più nel mirino di queste minacce informatiche. Gli aggressori spesso utilizzano gli attacchi DDoS come strumenti di ricatto, sabotaggio economico o guerra informatica,

dimostrando come la sicurezza informatica sia diventata un tema di rilevanza strategica a livello globale.

Un aspetto critico di questi attacchi è la loro evoluzione costante, i criminali sviluppano continuamente nuove tecniche per aggirare le difese esistenti e massimizzare l'efficacia degli attacchi e tra i metodi più diffusi vi sono gli attacchi volumetrici, che saturano la larghezza di banda di una rete; gli attacchi a livello di protocollo, che sfruttano le vulnerabilità nei protocolli di comunicazione e gli attacchi a livello applicativo, che mirano direttamente ai servizi web e alle API.

Negli ultimi mesi le tensioni geopolitiche e gli interessi economici hanno favorito un incremento significativo di attacchi DDoS, con impatti devastanti su aziende, enti governativi e infrastrutture critiche e dove anche le nostre infrastrutture hanno recentemente subito attacchi di questa natura, evidenziando l'urgenza di adottare misure preventive e strategie di mitigazione efficaci.

Per approfondire le modalità possiamo dire che gli attacchi DDoS si possono classificare in diverse categorie, ciascuna con specifiche metodologie di esecuzione:

- Attacchi volumetrici che mirano a saturare la banda disponibile della vittima inviando un elevato numero di pacchetti o richieste. Esempi includono attacchi UDP flood, ICMP flood e DNS amplification. Questi attacchi sono tra i più devastanti in termini di impatto sulla rete e spesso vengono eseguiti sfruttando dispositivi IoT compromessi che amplificano il traffico generato. La loro velocità e potenza di esecuzione rendono difficile

BIO

Alberto Perini è il CISO di Azimut Holding e STIM Tech Group, con una consolidata esperienza nella cybersecurity a livello internazionale. Guida il Team GRC e supporta il Risk Management, affrontando sfide complesse in diverse regioni europee e implementando le più avanzate normative di settore, tra cui DORA e NIS2. Nel corso della sua carriera, ha lavorato su progetti strategici per la protezione di infrastrutture critiche e la conformità a standard globali, contribuendo all'innovazione nel settore della sicurezza informatica.

una risposta tempestiva se non si dispone di adeguati sistemi di protezione.

- Attacchi a livello di protocollo che sfruttano vulnerabilità nei protocolli di comunicazione, come nel caso del SYN flood, che esaurisce le connessioni disponibili su un server. Attacchi come il TCP SYN flood si basano su un'elevata quantità di richieste che iniziano la procedura di handshake con il server senza mai completarla, lasciando le connessioni aperte e impedendo ad altri utenti di connettersi. Questo tipo di attacco è particolarmente insidioso poiché può essere difficile da distinguere dal traffico legittimo.
- Attacchi a livello applicativo che colpiscono applicazioni e servizi web attraverso richieste HTTP, simulando traffico legittimo ma in volumi tali da sovraccaricare il sistema. Gli attacchi Layer 7 sono tra i più difficili da rilevare perché utilizzano richieste che sembrano provenire da utenti reali, come il caricamento di pagine web o l'invio di moduli. Questi attacchi possono essere devastanti per le piattaforme di e-commerce e i servizi online che si basano su un funzionamento continuo e senza interruzioni.

Vorrei evidenziare il fenomeno TsuNAME, una nuova minaccia, ovvero una delle tecniche emergenti più pericolose, che sfrutta dipendenze circolari nei record DNS per generare un loop infinito di richieste tra server DNS autoritativi. Questo porta a un aumento esponenziale del traffico, sovraccaricando i server coinvolti e causando un'interruzione dei servizi digitali. Questo attacco è difficile da individuare e richiede una gestione attenta delle configurazioni DNS per evitare tali vulnerabilità. Secondo un recente rapporto dell'Agenzia per la Cybersicurezza Nazionale (ACN), gli attacchi DDoS sono in costante crescita e sempre più sofisticati, l'analisi ha evidenziato come molti attacchi siano coordinati e spesso legati a gruppi

di cybercriminali o a operazioni sponsorizzate da Stati. Il rapporto sottolinea l'importanza di un approccio strategico alla cybersecurity per mitigare questi rischi e proteggere le infrastrutture critiche.

Strategie di mitigazione e difesa

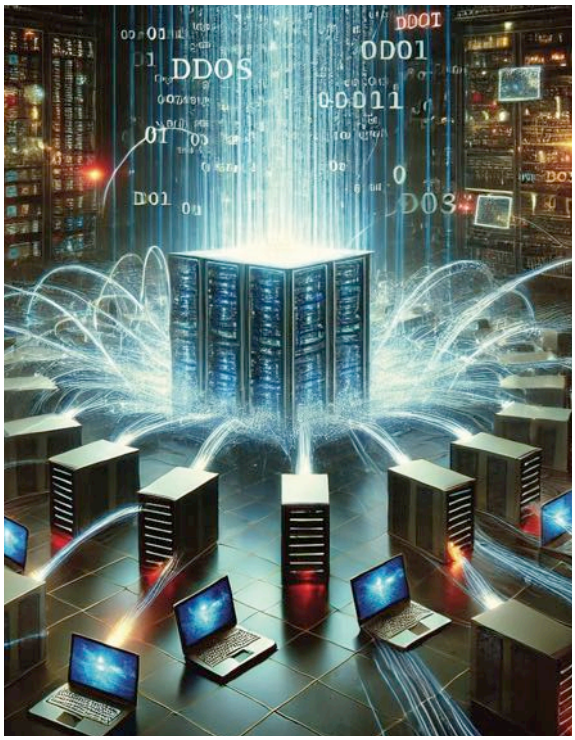
Contrastare un attacco DDoS richiede un approccio multilivello che integri soluzioni tecnologiche avanzate e strategie di risposta tempestive. Filtraggio del traffico con utilizzo di firewall e sistemi di prevenzione delle intrusioni (IPS) per identificare e bloccare pacchetti malevoli, rate limiting, ovvero limitazione del numero di richieste per unità di tempo per prevenire sovraccarichi, Anycast e Content Delivery Network (CDN) ovvero la distribuzione del traffico su più server per ridurre la pressione su singoli punti della rete. Soluzioni cloud anti-DDoS con servizi specializzati in grado di assorbire grandi volumi di traffico malevolo.

Monitoraggio e rilevamento avanzato con sistemi di analisi del traffico basati su intelligenza artificiale per identificare schemi anomali e rispondere in tempo reale.

Queste sono le principali metodologie e soluzioni per rispondere in modo adeguato ad un attacco DDOS che ha l'obiettivo di sovraccaricare un sistema fino a renderlo inutilizzabile, interrompendo il normale funzionamento di siti web, servizi online e infrastrutture critiche. Sebbene nella maggior parte dei casi non causino danni permanenti, il loro impatto può essere significativo, sia in termini di disservizi che di conseguenze economiche e geopolitiche.

DDoS vs DoS, l'evoluzione della minaccia

Gli attacchi DoS (Denial of Service) sono stati i primi a comparire nel panorama informatico e consistono nel sovraccaricare un server con un numero eccessivo di richieste provenienti da un'unica fonte. Questo tipo



di attacco, sebbene fastidioso, è relativamente facile da bloccare: il server può identificare la fonte malevola e chiudere la connessione.

Con il tempo, però, i criminali hanno sviluppato strategie più sofisticate, dando origine agli attacchi DDoS, in cui il traffico malevolo non proviene più da una singola fonte, ma da migliaia di dispositivi compromessi in tutto il mondo. Questo rende l'attacco molto più difficile da arginare, poiché il traffico dannoso si mescola con quello legittimo, complicando l'individuazione e la difesa.

Alla base di molti attacchi DDoS ci sono le botnet, reti di dispositivi infettati da malware e controllati da remoto da criminali informatici, che possono includere computer, server, router e dispositivi IoT e vengono reclutati senza che i loro proprietari ne siano consapevoli e utilizzati per lanciare attacchi su larga scala. Il processo avviene in tre fasi principali tramite: infezione, il malware viene diffuso tramite phishing, exploit di vulnerabilità o download da siti infetti;

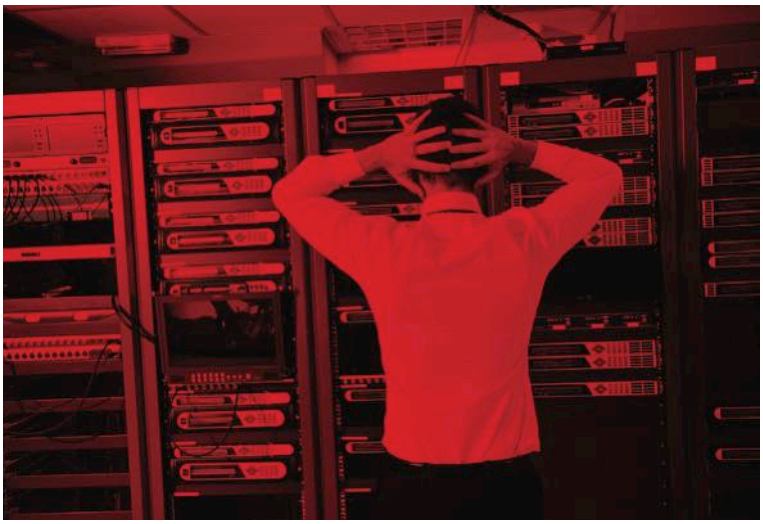
reclutamento, i dispositivi infetti entrano nella botnet e rimangono in attesa di istruzioni e infine attacco coordinato, i criminali, attraverso un centro di comando e controllo (C&C), ordina alla botnet di inondare il server bersaglio con milioni di richieste. A questo punto, la vittima si trova a fronteggiare un traffico insostenibile, con CPU e memoria sovraccaricate e larghezza di banda satura con l'interruzione dei servizi, rallentamenti e danni economici e reputazionali ingenti. Un attacco particolarmente insidioso è il DDoS di amplificazione, che sfrutta server intermedi per moltiplicare il traffico malevolo come, ad esempio, il DNS Reflection Attack, in cui i server DNS vengono indotti a rispondere con volumi di dati molto più grandi rispetto alla richiesta originale, creando un effetto a catena devastante.

DDoS come arma geopolitica e strategica

Se inizialmente i DDoS erano utilizzati per sabotaggi aziendali o atti di vandalismo informatico, oggi sono sempre più spesso strumenti di pressione politica e intimidazione digitale. La loro capacità di interrompere servizi critici e generare allarmismo li rende particolarmente efficaci in un contesto di guerra cibernetica.

Attacchi di questo tipo hanno colpito infrastrutture governative, aeroporti e servizi pubblici, spesso con l'obiettivo di testare le difese informatiche di un Paese, lanciare un messaggio politico o seminare insicurezza nell'opinione pubblica. Anche se nella maggior parte dei casi i disservizi sono temporanei, la frequenza e la durata di questi attacchi possono compromettere la fiducia nei sistemi digitali.

Parallelamente, cresce il dibattito sulla sovranità tecnologica, infatti, molti paesi stanno valutando la possibilità di sviluppare reti autonome e indipendenti per ridurre la propria esposizione a minacce esterne anche se il cyberspazio non ha confini rigidi, e nessuna nazione può considerarsi del tutto immune da queste minacce.



Un esempio concreto dell'uso strategico dei DDoS è l'attacco condotto dal gruppo Killnet, una rete di cybercriminali filo-russi, contro diversi aeroporti statunitensi.

L'attacco ha colpito i siti web di numerosi aeroporti, tra cui LAX (Los Angeles), Atlanta Hartsfield, Chicago O'Hare, Orlando International e LaGuardia, rendendoli temporaneamente inaccessibili. Sebbene nessun volo sia stato interrotto, il disservizio ha causato difficoltà ai passeggeri e ha evidenziato la vulnerabilità delle infrastrutture digitali.

Secondo esperti si è trattato di un'operazione di hactivism piuttosto che di un vero attacco strategico, ma l'evento ha dimostrato quanto gli attacchi DDoS possano essere usati per destabilizzare e creare tensioni internazionali.

Molte aziende si affidano a soluzioni cloud anti-DDoS per una protezione scalabile e senza investimenti in hardware costoso. Con l'evoluzione continua delle tecniche di attacco, la cybersecurity rimane una sfida costante, un equilibrio dinamico tra difesa e minaccia. ■

Intervista VIP a Padre Paolo Benanti.

Autore : Massimiliano Cannata

La fine del "sogno" di Internet

Nell'era del sintetico dobbiamo restare umani. Internet è stata una grande illusione di libertà che rischia di implodere. La pandemia ci ha detto che abbiamo trasformato molti processi analogici in digitale, questo ha spostato *il locus of control*. Domina oggi un potere computazionale, in mano a pochissimi soggetti. Padre Benanti consigliere del Papa ed esperto dell'ONU è divenuto un ambasciatore dei valori dell'umanesimo integrale in una società che sembra aver affidato tutto al potere infinitesimale dell'algoritmo. Nel suo ultimo saggio *Il crollo di Babele* (ed. San Paolo) si può trovare la *summa* di un pensiero forte, che tematizza le grandi questioni legate allo sviluppo della tecnoscienza, senza pregiudizi, con razionale consapevolezza.

BIO

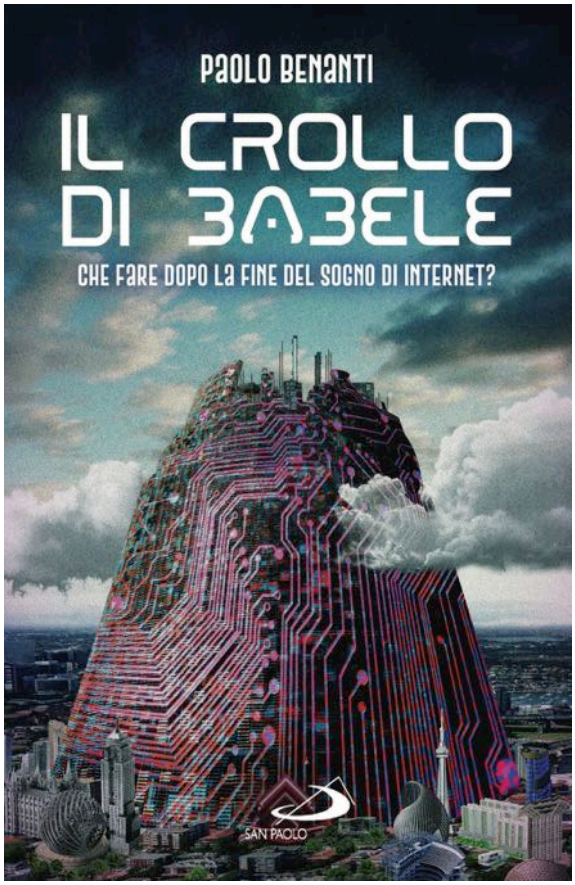
Frate francescano del Terzo Ordine Regolare - TOR - sono nato il 20 luglio del 1973. Docente alla Pontificia Università Gregoriana, mi occupo di etica, bioetica ed etica delle tecnologie. In particolare i miei studi si focalizzano sulla gestione dell'innovazione: internet e l'impatto del Digital Age, le biotecnologie per il miglioramento umano e la biosicurezza, le neuroscienze e le neurotecnologie. Cerco di mettere a fuoco il significato etico e antropologico della tecnologia per l'Homo sapiens: siamo una specie che da 70.000 anni abita il mondo trasformandolo, la condizione umana è una condizione tecno-umana. Autore di una quindicina di libri ed un centinaio di articoli scientifici. (www.paolobenanti.com)

Padre Benanti dopo la "Rivoluzione Internet" siamo già alla restaurazione? Cosa sta avvenendo?

Che già a partire dalla seconda decade del 2000 il vento è cambiato. La crescita delle grandi piattaforme che governano il web, la necessità di monetizzare i dati degli utenti, il nuovo "petrolio" che fa gola ai "signori della Rete", il proliferare delle *fake news,* hanno generato una nuova "Babele" di incomprensioni, equivoci, solitudini togliendo di fatto agli utenti quella libertà che dovrebbe sostanziare un mezzo straordinario, quale è Internet. Comanda chi possiede i server. Il 70% è di proprietà di due compagnie di Seattle, il 100% di sole cinque compagnie al mondo. Un poter immenso a disposizione di pochi. Quanto è avvenuto nel 2021 negli USA con le rivolte di Capitol Hill e l'assalto al Campidoglio ha svelato il potere delle piattaforme digitali capaci di mobilitare le masse e di trasformare la disinformazione on line in azioni reali, drammaticamente violente. Sono eventi fissati nella nostra memoria che sollevano interrogativi etici e giuridici sulla censura e sulla regolamentazione dei contenuti in rete, rimasti in larga parte insoluti.

Lei usa l'immagine della Torre di Babele, che l'umanità vive come castigo. Non Le pare eccessivamente negativa questa visione?

Il racconto di Babele è divenuto nei secoli emblematico della nostra cultura. La costruzione della torre evoca il sogno dell'umanità di trovare un'unica lingua, un canale universale di scambio e di intesa per tessere relazioni e creare un'alleanza tra popoli di diverse etnie e culture. Internet ha espresso, soprattutto nel primo decennio di questo millennio, lo stesso desiderio di costruzione di una piazza universale, che è storicamente culminata con le *Primavere arabe* del 2011, che ci avevano fatto credere che gli strumenti digitali fossero adatti a unire anche le realtà geograficamente più lontane. In realtà questo non è avvenuto, ci siamo esposti al rischio che le macchine decidano per noi, pensando che l'algoritmo fosse la soluzione.



Ho portato un esempio in un recente colloquio con Walter Veltroni pubblicato dal Corsera, quello di aver chiesto all'intelligenza artificiale: "Come faccio a eliminare il cancro dalla faccia della terra?" La risposta è stata: "Eliminando tutti gli uomini". Evidentemente qualche cosa non funziona, i processi di argomentazione e riflessione dell'uomo non possono essere demandati a questa forma particolare di "sapiens" telematico, che abbiamo messo al mondo.

Dobbiamo definire meglio le regole per lo sviluppo di strumenti straordinari come il sistema di intelligenza artificiale generativa?

L'Europa lo sta facendo, bisogna andare avanti su questa strada. La nostra civiltà possiede gli enzimi che provengono da una radicata cultura del diritto. Esiste l'associazionismo, gli enti intermedi, certo non basta, servirebbe una sorta di *brain helmet* un caschetto che aiuti a difenderci dal pensare oltre.

Si fa strada una nuova età dei diritti

Appare evidente che siamo di fronte a un "salto quantico" che vede sempre più alleate tecnologia e potere. La rielezione di Trump, che ha messo in campo equilibri e dinamiche nuovi, basti pensare al ruolo di Elon Musk, si può considerare come la fotografia di un profondo cambiamento d'epoca?

Elon Musk, psicopolitica e potere digitale costituiscono il trinomio che ha scandito il crollo del sogno di Internet e l'avvento di una nuova era guidata dall'intelligenza artificiale. Capitol Hill ha manifestato il primo alert sul futuro della democrazia nello spazio digitale computazionale. La diffusione dello *smartphone* ha fatto sì che ognuno di noi si ritrovasse in tasca un potere, mai avuto prima. Questo di fatto ci ha tolto autonomia, perché da quel momento la tecnologia che alberga dentro di noi, si interpone tra il soggetto e le cose condizionando le nostre conoscenze e relazioni.

La digitalizzazione del quotidiano non avrebbe dovuto rendere la vita più semplice?

Il digitale è uno strumento ambivalente. Pensiamo a quello che i social ci hanno consentito di fare abbattendo le barriere spazio-temporali, facilitando la condivisione di informazioni, opinioni e la creazioni di vere e proprie "comunità" di interessi. Ma non scordiamoci che i server sono anche imprese che coprono costi di esercizio e ingenerano guadagni grazie alla *like economy*, che prevede la monetizzazione dei contatti degli utenti. È evidente che tutto questo ha stravolto il profilo originale dell'utopia, che concepiva la Rete come l'agorà di uno scambio disinteressato tra soggetti liberi di agire e di pensare. Social network e tecnocrazia in una espansione incontrollata stanno invece schiacciando l'individuo. È questo il terreno di sfida, su cui si ruota il futuro di tutti.

"Noi e la macchina" verso la *sostenibilità* digitale

Intanto il prepotente sviluppo della tecnoscienza e la diffusione delle piattaforme digitali stanno modificando i linguaggi della democrazia. Quali sono i rischi cui andiamo incontro?

I rischi li stiamo già vedendo. Si sta affermando una plutocrazia delle piattaforme che agisce sui governi condizionandone le scelte. L'America, come è spesso accaduto nella storia, fa da apripista su determinati fenomeni, che appaiono destinati a replicarsi in altre aree del Pianeta. Dobbiamo pensare che la nostra stessa esistenza e capacità di agire sono state ormai riconfigurate in forma digitale, ne discende che anche il nostro diritto e potere di cittadinanza è divenuto computazionale. L'IA con il suo prepotente impatto si è aggiunta, complicando il quadro.

A cosa si riferisce, può spiegarcelo meglio?

Alle applicazioni dell'intelligenza generativa che sfumano la linea di demarcazione tra il potere computazionale personale e il potere centralizzato del *cloud*, la "nuvola" che contiene informazioni e dati sensibili che ci riguardano. Questa centralizzazione ha a che fare con la democrazia e il bilanciamento dei poteri su cui si basa. Per intenderci: stiamo correndo il rischio che si formi una oligarchia del *cloud* che può far collassare la democrazia.

I politologi parlano a proposito di* tech right *cercando di dare un nome all'ideologia emergente, nata nella Silicon Valley, che si fonda sulla stretta alleanza tra conservatorismo politico e potere tecnologico. Qual è il suo giudizio in merito?

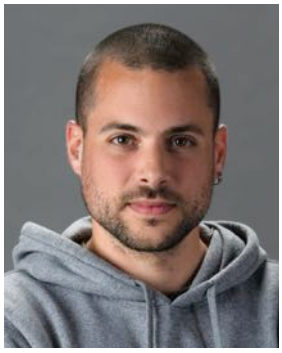
Non entro nelle valutazioni politiche che esulano dal mio studio. Una cosa è certa: attualmente è in corso una guerra cognitiva che si svolge

nel cyberspazio, che include anche i media tradizionali e la tv destinata a modificare gli equilibri geopolitici. La guerra in Ucraina combattuta con armi non convenzionali basata su strategie militari sulla manipolazione delle percezioni e delle decisioni del nemico attraverso l'uso delle tecnologie digitali è la dolorosa prova che sono cambiate le regole nel gioco del potere. Questo non può che avere riflessi sulla salute della democrazia.

Tra le contromisure possibili alla deriva del potere schiacciante dei colossi del web, Lei insieme al filosofo della politica Sebastiano Maffettone individua nel saggio* "Noi e la macchina" *(Luiss University Press) il possibile percorso di una "sostenibilità digitale". Di che cosa si tratta?

Di mettere dei paletti normativi, etici e giuridici per istruire correttamente la macchina, L'*algoretica* è la disciplina che impone dei *guardrail* proprio come avviene con le automobili perché non sbandino. Di certo nessuno può dire come vivremo in questi anni Trenta del secolo e cosa lasceremo alle generazioni future dopo il crollo della Babele digitale. Una cosa, in ultimo, appare evidente: lo scenario analogico-digitale di una contemporaneità segnata dalla post verità, dalle fake news, attraversata da complottismi e populismi di diversa estrazione, impone, di fronte allo strapotere degli attori digitali, la collaborazione tra pubblico e privato, quale strumento necessario per rafforzare le difese collettive contro le minacce cyber che stanno mettendo in ginocchio la democrazia a tutte le latitudini e con essa i più elementari principi dello stato di diritto. Le classi dirigenti farebbero bene a tenerlo bene a mente. ■

Orientarsi tra i rischi crittografici: Perché i CISO devono agire ora.



SANDBOXAQ™

Autori: Marc Manzano,
Mo Aboul-Magd

Crittografia: Il Fondamento della Digital Security

La crittografia è la base della moderna protezione dei dati, in quanto protegge le comunicazioni, le transazioni e le informazioni sensibili in tutti i settori. Garantisce la riservatezza, l'integrità, l'autenticazione e la non-repudiation, tutti principi fondamentali che garantisco la fiducia nelle transazioni digitali. Negli ultimi trent'anni, la crittografia si è evoluta di pari passo con la trasformazione digitale, passando da un settore di nicchia come quello accademico e militare a una realtà diffusa, base del commercio elettronico, della messaggistica sicura e della sicurezza aziendale.

Tuttavia, nonostante il suo ruolo fondamentale, la crittografia è spesso una vulnerabilità trascurata all'interno delle organizzazioni. A differenza di altre misure di cybersecurity come i firewall o la protezione degli endpoint, le risorse crittografiche sono distribuite negli ambienti IT, nascoste nei sistemi operativi, nei dispositivi hardware e nelle applicazioni legacy. Questa frammentazione rende difficile per le organizzazioni mantenere visibilità e controllo sulle proprie implementazioni crittografiche, creando rischi nascosti che gli avversari possono sfruttare.

Le Crescenti Sfide della Gestione Crittografica

Molte organizzazioni gestiscono ancora manualmente la propria infrastruttura crittografica, affidandosi ad approcci obsoleti o frammentari che non sono né scalabili né efficaci. Questa mancanza di visibilità lascia i team di sicurezza in difficoltà nell'identificare le vulnerabilità, soprattutto dopo aggiornamenti del software, integrazioni IT o aggregazioni e acquisizioni. Il risultato è un aumento della superficie di attacco e una maggiore esposizione alle violazioni dei dati.

Una delle sfide principali che le organizzazioni devono affrontare è la complessità e la frammentazione delle implementazioni crittografiche. Quanto più estesa è l'infrastruttura IT di un'organizzazione, tanto più difficile diventa tracciare e gestire le risorse crittografiche su più piattaforme, applicazioni software e ambienti cloud. Per risolvere questo problema, stanno emergendo moderne soluzioni di gestione crittografica che aiutano le aziende a centralizzare la visibilità e la valutazione dei rischi, garantendo controllo, conformità e sicurezza. Inoltre, vi è una carenza di professionisti qualificati nella sicurezza crittografica. La crittografia richiede competenze approfondite, spesso acquisite attraverso specializzazioni e, data la carenza di talenti nel campo della cybersecurity, poche organizzazioni dispongono di specialisti in grado di supervisionare efficacemente la sicurezza crittografica.

Una delle sfide principali che le organizzazioni devono affrontare è la complessità e la frammentazione delle implementazioni crittografiche. Quanto più estesa è l'infrastruttura IT di un'organizzazione, tanto più difficile diventa tracciare e gestire le risorse crittografiche su più piattaforme, applicazioni software e ambienti cloud.

Per risolvere questo problema, stanno emergendo moderne soluzioni di gestione crittografica che aiutano le aziende a centralizzare la visibilità e la valutazione dei rischi, garantendo controllo, conformità e sicurezza. Inoltre, vi è una carenza di professionisti qualificati nella sicurezza crittografica. La crittografia richiede competenze approfondite, spesso acquisite attraverso specializzazioni e, data la carenza di competenze nel campo della cybersecurity, poche organizzazioni dispongono di specialisti in grado di supervisionare efficacemente la sicurezza crittografica.

L'Urgenza della Modernizzazione della Crittografia

Visto che le organizzazioni che si trovano ad affrontare minacce informatiche sempre più sofisticate, compresi i rischi incombenti posti dal quantum computing, garantire la sicurezza dei dati sensibili non è mai stato così critico. Di conseguenza, è fondamentale dare priorità alle soluzioni che migliorano la visibilità crittografica, l'automazione e la mitigazione del rischio per rimanere al passo con l'evoluzione delle minacce. L'arrivo di computer quantistici di grandi dimensioni a tolleranza di errore minaccia i metodi crittografici ampiamente utilizzati, in particolare la crittografia a chiave pubblica, che è alla base di molte soluzioni di sicurezza esistenti. L'esigenza di crypto-agility - la capacità di adattarsi rapidamente e di passare ad algoritmi quantum-resistant - non è mai stata così pressante.

Le organizzazioni devono adottare misure proattive per modernizzare la propria infrastruttura crittografica. È essenziale ottenere una visibilità crittografica completa. Le aziende devono implementare soluzioni

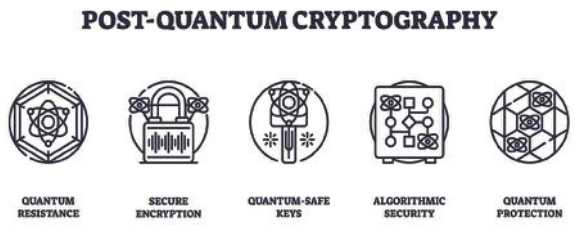
BIO

Marc Manzano dirige il gruppo di cybersecurity di SandboxAQ. Con oltre dieci anni di esperienza, ha guidato lo sviluppo di una serie di prodotti di sicurezza informatica, librerie crittografiche e protocolli. In precedenza, è stato Senior Staff Software Engineer presso Google e vicepresidente del Centro di ricerca sulla crittografia presso il Technology Innovation Institute (UAE). Ha conseguito un dottorato di ricerca in Computer Network Security presso l'University di Girona e la Kansas State University. Ha contribuito ampiamente alla ricerca, con oltre 25 pubblicazioni in conferenze, riviste e libri scientifici. La sua formazione accademica comprende istituzioni in Spagna, Regno Unito, Danimarca e Stati Uniti.

BIO

Mohammed è VP of Product per il gruppo di cybersecurity di SandboxAQ, dove guida lo sviluppo di soluzioni di sicurezza innovative. Prima di SandboxAQ, ha ricoperto il ruolo di vicepresidente del prodotto presso Snyk, la piattaforma di sicurezza per sviluppatori leader del settore, dove ha guidato il lancio di Snyk Code, un prodotto SAST alimentato dall'intelligenza artificiale che ha rapidamente raggiunto un ARR di 100 milioni di dollari. Ha anche ricoperto un ruolo di leadership di prodotto presso Akamai, guidando la sua piattaforma di Edge Computing. Mohammed si è laureato in Ingegneria dei sistemi informatici presso la Carleton University di Ottawa, in Canada.

che forniscano un quadro completo del loro panorama crittografico, consentendo loro di identificare le vulnerabilità e di ridurre i rischi prima che diventino dei problemi. L'automazione della gestione crittografica è un'altra misura chiave. Il monitoraggio manuale della crittografia è inefficiente, costoso e soggetto a errori. L'automazione dell'individuazione, del monitoraggio e della correzione delle risorse crittografiche garantisce alle organizzazioni di mantenersi sicure e conformi.



Anche la migrazione verso algoritmi crittografici post-quantistici è imperativa. La transizione verso metodi crittografici quantum-resistant sarà necessaria per salvaguardare i dati dalle future minacce quantistiche. Le aziende devono prepararsi a questo passaggio implementando soluzioni di crypto-agility che consentano una migrazione senza soluzione di continuità man mano che emergono nuovi standard. Inoltre, le politiche crittografiche devono essere integrate in strategie di cybersecurity più ampie. La crittografia non deve essere una funzionalità distaccata, ma parte integrante della postura di sicurezza di un'organizzazione. L'allineamento della gestione crittografica ai principi di Zero Trust aumenta la resilienza complessiva contro le minacce informatiche.

Il Ruolo delle Moderne Piattaforme di Gestione Crittografica

Per anni non sono state disponibili soluzioni complete per la gestione complessiva delle risorse crittografiche. Oggi le moderne piattaforme di gestione crittografica stanno colmando questo gap, consentendo alle organizzazioni di centralizzare il controllo, automatizzare le operazioni crittografiche e garantire la conformità alle normative di settore. Uno dei punti chiave per i team di sicurezza è la realizzazione di un archivio crittografico completo, che garantisca la visibilità delle risorse di crittografia su reti, applicazioni e infrastrutture.

SandboxAQ ha sviluppato AQtive Guard, una piattaforma di gestione crittografica unificata che aiuta le organizzazioni a scoprire, monitorare e proteggere le proprie risorse crittografiche in ambienti IT complessi. AQtive Guard fornisce un sistema di inventario crittografico a livello aziendale, identificando e mappando le risorse crittografiche su reti, applicazioni e infrastrutture. Esegue controlli sui rischi e sulla conformità, garantendo

l'allineamento con le policy di sicurezza aziendali, i requisiti normativi e gli standard crittografici in evoluzione. La piattaforma si integra perfettamente con gli strumenti di sicurezza esistenti, accelerando la creazione di un primo sistema di inventario e migliorando la visibilità e il controllo crittografico. Inoltre, AQtive Guard prepara le organizzazioni al futuro, consentendo una transizione agevole verso algoritmi crittografici quantum-resistant.

Già oggi, organizzazioni come la U.S. Air Force, il Department of Health & Human Services, la Defense Information Systems Agency (DISA), Vodafone, SoftBank, Informatica, e le principali banche mondiali hanno sfruttato le nostre soluzioni per migliorare la loro sicurezza crittografica. SandboxAQ collabora anche con organizzazioni di settore come il NIST, National Cybersecurity Center of Excellence (NCCoE), il GSMA Post-Quantum Telco Network (PQTN), la Fondazione Linux Post-Quantum Cryptography Alliance (PQCA), e il MITRE PQC Coalition. Queste partnership guidano gli sforzi globali per promuovere la formazione delle imprese e degli enti governativi sulle strategie di sicurezza crittografica proattive.

Il Futuro della Sicurezza Crittografica

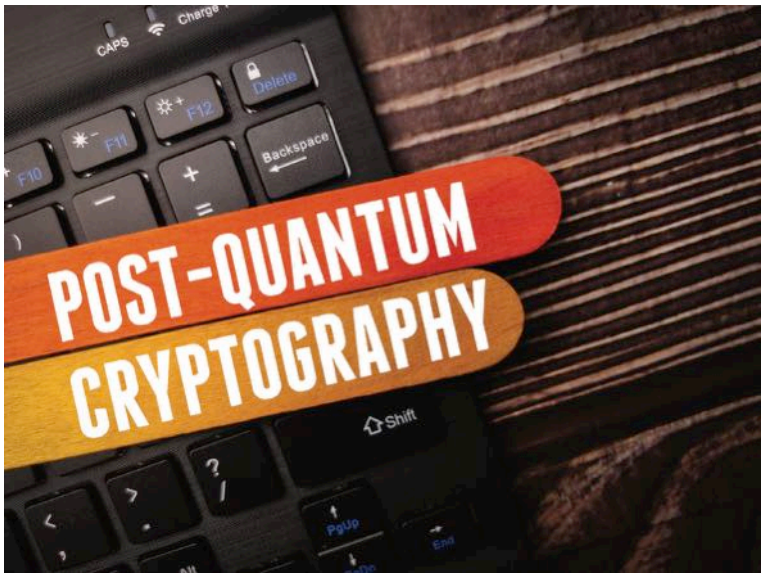
In un'era in cui gli attaccanti si avvalgono di strumenti sempre più sofisticati, e la rivoluzione del quantum computing che incombe, la sicurezza crittografica non può essere un elemento secondario. Le organizzazioni devono dare priorità alla visibilità crittografica, all'automazione e all'agility per salvaguardare le basi di qualsiasi postura di cybersecurity, ovvero le loro risorse crittografiche più sensibili.

Implementando moderne soluzioni di gestione crittografica, le aziende possono proteggersi dalle minacce informatiche emergenti, compresi gli attacchi quantistici. L'adozione di misure proattive per valutare e modernizzare l'infrastruttura crittografica sarà essenziale per le organizzazioni che intendono mantenere la resilienza in un ambiente di sicurezza sempre più complesso. Garantire la conformità ai requisiti normativi in evoluzione diventerà più facile, riducendo i rischi operativi associati a una cattiva gestione della crittografia. In questo modo le aziende potranno concentrarsi sui loro obiettivi principali, mantenendo la fiducia nella sicurezza dei dati.

Il futuro della cybersecurity è intrinsecamente legato alla resilienza crittografica. Le organizzazioni devono agire ora, prima che le vulnerabilità nascoste diventino violazioni catastrofiche. La prossima fase della sicurezza crittografica sarà definita dalla gestione proattiva del rischio, dall'automazione e dalla prioritizzazione guidate dall'intelligenza artificiale e dalla transizione senza soluzione di continuità agli standard di crittografia post-quantum. Adottando una gestione crittografica moderna, le aziende possono mettere a prova il futuro della loro infrastruttura di sicurezza e rimanere all'avanguardia in un panorama di minacce in continua evoluzione. ■

L'Urgente necessità di una migrazione alla crittografia post-quantun (PQC).

Autore : Jelena Zelenovic Matone



Introduzione

Questo articolo è rivolto a CISO, CIO, esperti della sicurezza e responsabili IT che hanno sentito parlare di termini come quantun computing, crittografia post-quantum (PQC) e minacce quantistiche, ma non sanno da dove partire. Se la vostra organizzazione ha appena iniziato il suo percorso PQC (o sta ancora discutendo se sia il caso di interessarsene o meno), non siete soli. Il problema è che aspettare troppo a lungo equivale a ignorare un asteroide che si muove lentamente verso la Terra: potrebbe impiegare del tempo per colpire, ma quando lo farà, i danni saranno catastrofici.

Con la pressione normativa in aumento e le discussioni a livello globale sulla quantum security che prendono sempre più piede, è il momento di passare dai dibattiti teorici all'azione concreta. Questa guida semplificherà la complessità della migrazione PQC in una strategia strutturata e attuabile, garantendo che la vostra infrastruttura crittografica rimanga sicura anche nel futuro quantistico.

Perché la Migrazione PQC è Importante: la Minaccia Quantistica è Reale

Il quantum computing non è più solo un concetto fantascientifico: è una realtà tecnologica che avanza a un ritmo inquietante. A differenza dei computer tradizionali che elaborano informazioni in binario (0 e 1), i computer quantistici sfruttano i qubit, consentendo loro di eseguire calcoli a una velocità esponenzialmente superiore. Ottime notizie per le scoperte scientifiche! Pessime notizie per la crittografia.

Per decenni, la crittografia RSA ed ECC sono state l'equivalente digitale di un fortezza inespugnabile. Ma il quantum computing le trasformerà da fortezza a semplice cartapesta. La sicurezza di qualsiasi cosa, dalle operazioni bancarie online alle comunicazioni governative, dipende da questi metodi crittografici e, una volta che i computer quantistici raggiungeranno una soglia di potenza sufficiente, potranno violarli con facilità.

Ancora peggio, gli attaccanti stanno già adottando una tattica sinistra chiamata **Store Now, Decrypt Later (SNDL)** – archiviano dati crittografati oggi, pianificando di decifrarli quando la potenza quantistica sarà matura. Immaginate se qualcuno rubasse oggi i vostri segreti più intimi, sapendo che potrebbe leggerli tra un decennio. Agghiacciante, vero? Le organizzazioni

devono agire ora prima che i loro dati diventino un facile bersaglio per i futuri cybercriminali.

Pressione Normativa: DORA, TIBER-EU e Quantum Readiness

Se le minacce esistenti non sono una motivazione sufficiente, le autorità di regolazione stanno intervenendo per garantire che le organizzazioni non si facciano trovare impreparate.

DORA e PQC

Il Digital Operational Resilience Act (DORA) è il modo in cui l'UE dice: «Niente più scuse». Questo regolamento impone a istituzioni finanziarie, banche e fornitori di servizi ICT di rafforzare la loro resilienza informatica, compresa la preparazione ai rischi quantistici.

- **Articolo 8:** richiede che i framework di risk management ICT considerino le minacce emergenti come il quantum computing.
- **Articoli 14 & 15:** pongono l'accento sui test di resilienza operativa e la risposta agli incidenti, entrambi elementi che dovrebbero integrare la crittografia quantum-safe.
- Le **Autorità di Vigilanza Europee (ESA)** stanno già lavorando su standard che potrebbero rendere obbligatoria la conformità PQC in futuro.

TIBER-EU e Test di Quantum Security

TIBER-EU

TIBER-EU, il framework **Threat Intelligence-Based Ethical Red Teaming**, porta i test di cybersecurity a un livello superiore. Le istituzioni finanziarie sono incoraggiate a simulare attacchi informatici sui propri sistemi (perché aspettare quelli reali?). Questo dovrebbe ora includere anche le vulnerabilità quantistiche:

- **Le esercitazioni di red-teming** dovrebbero testare la tenuta dell'infrastruttura crittografica contro le minacce post-quantistiche.
- **Le valutazioni della prontezza PQC** dovrebbero essere integrate nei test di resilienza.
- **Le soluzioni dei fornitori** dovrebbero essere valutate per la conformità alla quantum security.

Queste normative non sono solo caselle da spuntare, ma segnali luminosi che indicano il futuro della cybersecurity. Le organizzazioni che le ignorano rischiano non solo data breach, ma anche sanzioni normative, interruzioni operative e danni reputazionali.

Approccio in Tre Fasi alla Migrazione PQC

Data la complessità della migrazione PQC, le organizzazioni necessitano di un piano strutturato. Ecco un approccio in tre fasi per affrontare la transizione senza impazzire:

1. Analisi delle Vulnerabilità Quantistiche

Prima di sistemare qualcosa, bisogna sapere cosa è rotto o a rischio di rompersi nell'era quantistica.

- **Creare un inventario di tutti gli asset crittografici** (perché non si può proteggere ciò che non si conosce).
- **Identificare i sistemi critici** che sarebbero maggiormente impattati dagli attacchi quantistici.
- **Valutare le dipendenze crittografiche** per comprendere come come sarà influenzata la vostra architettura di sicurezza.

2. Pianificazione

Una volta identificate le vulnerabilità, è tempo di definire una strategia.

- **Sviluppare una roadmap dettagliata** con tempistiche e priorità.
- **Allinearsi ai requisiti normativi** per garantire la conformità a framework come DORA e TIBER-EU.
- **Coinvolgere gli stakeholder** di sicurezza, IT e business per garantire una transizione fluida.

3. Esecuzione

Questo è il momento dell'azione (o dove le organizzazioni spesso si scontrano con la burocrazia).

- **Implementare soluzioni PQC in modo graduale**, garantendo l'interoperabilità con i sistemi legacy.
- **Testare e validare le implementazioni crittografiche** per evitare problemi di sicurezza o prestazioni.
- **Monitorare continuamente gli sviluppi PQC** e adattare le strategie di conseguenza.

Sfide e Riflessioni: Non è così semplice come premere un pulsante

Passare alla PQC è come passare da una bicicletta a un jet: emozionante, ma pieno di sfide:

- **Compatibilità Tecnica** - I sistemi legacy non sono affatto stati progettati per la crittografia quantum-safe.
- **Impatto sullePrestazioni** - Gli algoritmi PQC sono spesso più impegnativi dal punto di vista computazionale.
- **Conformità Normativa** - Le organizzazioni devono allinearsi agli standard PQC globali in continua evoluzione.
- **Supporto dei Fornitori** - Molti fornitori non hanno ancora integrato completamente soluzioni compatibili con PQC.

Il report **Protecting Payments in the Quantum Era** del NIST evidenzia che i servizi finanziari, in modo particolare, dovranno affrontare ostacoli notevoli a causa della loro dipendenza dalla crittografia sicura per i pagamenti e la verifica dell'identità.

Il Futuro: Tre Principali Standard Crittografici

1. FIPS 203 (ML-KEM) - Uno standard di crittografia a reticolo basato su CRYSTALS-Kyber.

2. FIPS 204 (ML-DSA) - Algoritmo di firma digitale basato su CRYSTALS-Dilithium.

3. FIPS 205 (SLH-DSA) - Algoritmo di firma digitale stateless basato su hash (Sphincs+).

Questi standard sostituiranno RSA ed ECC, garantendo che la crittografia e le firme digitali siano quantum-resistant.

Indicazioni principali: Cosa fare ora?

1. Iniziare Oggi - La migrazione della PQC richiede anni, quindi non aspettate la resa dei conti quantum.

2. Seguire un Approccio Graduale - Date priorità alle aree ad alto rischio e pianificate di conseguenza.

3. Integrare il Crypto Asset Discovery - Utilizzare gli strumenti CADI per fare un inventario e valutare l'infrastruttura crittografica.

BIO

Rispettata leader CISO, insignita del CISO dell'anno per il 2019 in Lussemburgo, Sentinel CISO Global 2020, EU CISO 2020 e Ambasciatore dell'anno 2021 in Lussemburgo, Jelena è esperta di Cybersecurity versatile e innovativa con enfasi sulla gestione del rischio di sicurezza informatica/ risk management, creazione di policy e procedure, sicurezza IT/ IS, operazioni IT, audit, mitigazione del rischio, miglioramento dei processi aziendali, governance IT, business process improvement, IT governance. Appassionata di partecipazione e incoraggiamento delle donne alla cybersecurity e ai programmi STEM. Prima del ruolo attuale, ha ricoperto il ruolo di Senior Operational Risk e ISO manager per un'altra istituzione dell'UE. All'inizio della carriera, ha gestito IT Audit and Compliance per Sobey's, uno dei due rivenditori nazionali di generi alimentari in Canada e Audit, Corporate Development, M&A e strategie di crescita e IT Audit per George Weston, una delle più grandi società di trasformazione e distribuzione degli alimenti in Canada quotata in borsa.

4. Collaborare e Tenersi Aggiornati - Impegnarsi con le autorità di regolamentazione, i rappresentanti del settore e i fornitori.

5. Prepararsi per il Lungo Periodo - La crittografia è un campo in evoluzione; la PQC non comporterà un unico aggiornamento.

Conclusione

La crittografia post-quantum non è più una preoccupazione astratta: è una bomba a orologeria. I computer quantistici avranno presto il potere di violare la crittografia attuale, mettendo a rischio transazioni finanziarie, comunicazioni governative e identità digitali. Le organizzazioni che non agiscono ora si ritroveranno a rincorrere il problema in futuro, e a quel punto potrebbe essere troppo tardi.

La soluzione? Un approccio strutturato e proattivo alla migrazione PQC. Che siate già in fase di pianificazione o che vi stiate appena rendendo conto della minaccia, ora è il momento di proteggere il vostro futuro crittografico. Perché quando la tempesta quantistica arriverà l'unica cosa peggiore dell'essere impreparati è rendersi conto di aver avuto anni per prepararsi… e non aver fatto nulla.

Allora, siete pronti per l'era quantistica o state aspettando che l'asteroide si abbatta su di voi? ■

Nasce Associso asset importante per la sicurezza digitale.

Autore : Igor Kranjec

Nel panorama in continuo divenire della sicurezza informatica, la figura del **Chief Information Security Officer (CISO)** ha assunto un ruolo ormai centrale. Se questa possiamo considerarla una consapevolezza ormai diffusa non solo tra gli addetti ai lavori, quello che continuava a risultare deficitario era il riconoscimento ufficiale della specificità di un ruolo che oggi agisce a fianco delle istituzioni e del top management.

Associso, è l'associazione di categoria che nasce con questa precisa mission, grazie all'immediato riscontro di un primo corposo nucleo

di sottoscrittori che hanno generato in poco tempo un'importante reazione a catena tra i professionisti del settore. Grazie alla dedizione dei suoi membri e alla visione strategica dei suoi fondatori, l'associazione si è rapidamente affermata come un punto di riferimento indispensabile per il settore, tanto che si può affermare che un pezzo importante del futuro della sicurezza digitale passerà da «questa casa comune», dentro cui si potranno affrontare con spirito di squadra le grandi sfide della contemporaneità.

Offrire una voce autorevole ai responsabili della difesa cibernetica, favorendo il dialogo intersettoriale e inter istituzionale, promuovendo nel contempo standard e best practice condivise, è un aspetto cruciale dell'attività dell'associazione, la cui rapida crescita dimostra quanto fosse sentita la necessità di individuare un punto di riferimento per chi si trova quotidianamente impegnato a bilanciare esigenze di business e requisiti di sicurezza.

Un paese che impara a proteggere i propri asset digitali crea fiducia, attrattività per gli investitori e benessere diffuso nei cittadini. La sicurezza è un valore trasversale alla base della stabilità del sistema economico e sociale. L'equilibrio tra innovazione e protezione richiede capacità strategica che va oltre una mera gestione tecnica degli apparati e degli strumenti della sicurezza informatica, perché si estende alla sensibilizzazione del management aziendale, alla capacità di definire i criteri di conformità normativa e all'affinamento di azioni di difesa e di sostegno del business.

I fattori di contesto tra sfide e opportunità: «la voce dei CISO»

Tenuto conto di questi fattori di contesto non bisogna stupirsi se le aspettative che hanno accompagnato la nascita di Associso sono molto alte, non solo riguardo agli aspetti inerenti la tutela dei professionisti del settore, ma più in generale per il futuro stesso dell'information security.

Favorire la crescita di una nuova generazione di professionisti, attraverso programmi di mentorship e collaborazioni con il mondo accademico, che possa fare da catalizzatore del percorso di crescita, che va di pari passo con l'identificazione di sempre nuove competenze è l'obiettivo sfidante che i CISO aderenti si sono posti. In un'epoca in cui le minacce informatiche sono divenute sempre più sofisticate e interconnesse, va ribadito che i compiti e le attività che porta avanti **Associso** assumono notevole delicatezza e rilevanza, come risulta nell'impegno messo in campo per la definizione degli standard professionali e nel supporto assicurato alle istituzioni e alle aziende. Affrontare insieme le sfide del cambiamento contribuendo a costruire un ecosistema digitale più sicuro rimane la stella polare, verso cui dovranno convergere gli investimenti in know-how e capitale umano. Nella volontà di promuovere il confronto e il dialogo tra punti di vista ed esperienze diverse, l'Associazione curerà una nuova rubrica «La Voce del CISO» che amplierà la proposta editoriale di Cybersecurity Trends trattando dei nuovi orizzonti della sicurezza digitale. ■

BIO

Igor Kranjec è Co-Founder & Secretary General at Associazione Nazionale Chief Information Security Officer - AssoCISO ETS. La curiosità e il rifiuto di schemi e soluzioni predefinite lo ha spinto a un approccio non accademico al mondo della sicurezza. Prima come ricercatore, poi ricoprendo con lo stesso spirito pragmatico il ruolo di CEO in aziende di consulenza internazionali e altri ruoli corporate come Group Chief Security Officer e Head of Cyber Security Business Unit del Gruppo Engineering.
Oggi è Segretario Generale dell'Associazione Nazionale Chief Information Security Officer - Asso CISO ETS, l'associazione nazionale che rappresenta e riunisce le figure CISO e di Cyber e Information Security, aziendali e istituzionali. Inoltre è CISO e Senior Advisor di organizzazioni internazionali come European Cyber Security Organisation (ECSO).

Cybersecurity e sanità: asset strategico di sviluppo per il Sistema Paese.

Autore: Massimiliano Cannata

"Cybersecurity e diritto alla salute corrono su un unico filo: potente e fragile. Sviluppo tecnologico ed evoluzione normativa dovranno essere accompagnati da una maturazione culturale che deve diffondersi in tutto il Paese, per garantire la privacy degli utenti, la sicurezza delle infrastrutture sanitarie e, allo stesso tempo, una migliore performance del sistema sanitario. Dobbiamo rafforzare gli strumenti della conoscenza, al fine di comprendere il fitto intreccio di interdipendenze in un settore, quello della Sanità, che segna un ambito delicato per la vita dei cittadini e per gli equilibri della convivenza democratica".

Molto chiaro il messaggio emerso nel corso di un Seminario di Studi promosso dalla **Fondazione ICSA**, sintetizzato dal direttore della stessa Fondazione **Italo Saverio Trento**. *"Cybersecurity e infrastrutture sanitarie nell'era della transizione digitale e dell'intelligenza artificiale"*, il tema attorno a cui manager e studiosi si sono confrontati aprendo la strada per una serie di incontri futuri. *"L'evento non si è concluso lo scorso dicembre* – prosegue l'analisi di Trento – *farà infatti parte di un programma tecnico-scientifico che produrrà in futuro ulteriori step di approfondimento da parte della Fondazione ICSA, non solo sul piano dell'analisi del fenomeno ma anche su quello della formazione destinata al management e al personale sanitario in genere". "A guardare bene l'attualità si può vedere come quello della sanità sia un mondo tra i più martoriati quello della sanità pubblica* – commenta il Presidente ICSA, gen. **Leonardo Tricarico** - *che necessita di attenzione, responsabilità, investimenti per contrastare efficacemente gli attacchi informatici di natura malevola. Che i dati sanitari abbiano acquisito una rilevanza notevole lo dimostra il caso della cattura di Matteo Messina Denaro, localizzato proprio mediante la raccolta dei suoi dati clinici. Grazie a indagini e intercettazioni i ROS sapevano di quali patologie soffriva Matteo Messina Denaro e incrociando le informazioni sulle visite specialistiche, gli interventi chirurgici e le cure mediche a cui si stava sottoponendo, gli investigatori sono risaliti alla sua localizzazione. Aspetti pragmatici e visione strategica hanno trovato un punto di convergenza che ha permesso l'arresto del celebre latitante, adottando un modello collaborativo di knowledge-sharing che dobbiamo seguire se vogliamo ottenere risultati con quella rapidità che la società dell'informazione, in continuo divenire, oggi richiede".*

Una nuova modalità di conflitto

La cyberwar è la nuova modalità di conflitto e che nessuno può permettersi di sottovalutare, portata avanti con armi invisibili, schieramenti

BIO

Massimiliano Cannata (Palermo, 1968), Filosofo, giornalista Professionista, autore televisivo, svolge attività di consulenza nell'ambito della comunicazione d'impresa. Membro del Comitato scientifico di "Anfione e Zeto",collabora con"TechnologyReview", "L'impresa", "Il Giornale di Sicilia", "Centonove Press".E' autore di numerosi saggi sui temi della social innovation, della formazione, dello sviluppo organizzativo e manageriale.

fluidi, in "trincee virtuali" e comporta la sottrazione di informazioni sensibili e la manipolazione della verità. Quando questo avviene nella sanità i rischi diventano esponenziali per la complessità e la ricchezza intrinseca dei dati che vengono elaborati. Appare devastante quello che, con sempre maggior frequenza sta avvenendo, ossia l'accesso incondizionato a patrimoni di know-how e dati sensibili che mettono a rischio il diritto alla salute, violando rispetto e dignità della persona umana. Un fenomeno rispetto a cui bisogna correre ai ripari. Venire a conoscenza dello stato di salute di leader e capi di stato è un "piatto particolarmente ghiotto" per i servizi di un'attività di intelligence che risulta sempre più ibridata di competenze cyber. L'interesse crescente di hacker esperti e di una criminalità organizzata capace ormai di manipolare software e banche dati e di entrare in reti e sistemi documentali non può dunque stupire.

"Un tema come la sicurezza – il parere di **Ivano Gabrielli, Direttore della polizia postale e delle Comunicazioni** – *occupa una posizione di assoluta priorità nell'ambito istituzionale e nell'agenda dei governi. La Fondazione ICSA ci ha offerto l'opportunità di calarci in un contesto operativo e altamente a rischio come la Sanità, e questo ci consente di sporcarci veramente le mani sul piano tecnico e investigativo. La sicurezza cibernetica si costruisce sull'integrazione di una serie di competenze: difesa, intelligence, investigazione e resilienza. Saranno circa 40 mila i soggetti che rientreranno dentro il perimetro delle direttive NIS1 e NIS2 (Network and Information Security Directive), soggetti destinati ad assumere una responsabilità di tipo pubblicistico, affiancando lo Stato nei compiti di ordine pubblico e sicurezza nazionale. Diritto, tecnologie, metodi investigativi e presidi tecnologici devono dunque evolversi in modo armonico, razionalizzando gli strumenti, evitando repliche e inutili ridondanze".*

Sulla stessa lunghezza **Domenico Vulpiani, Presidente Osservatorio *Health Cybersecurity* ICSA:** *"I servizi sanitari sono un'infrastruttura a largo spettro, la cui tutela si presenta particolarmente complessa, perché tocca molteplici aspetti: dalla privacy del paziente, alle vulnerabilità che più in generale si possono manifestare nella supply chain che governa una grande struttura ospedaliera. Il nostro osservatorio intende promuovere un confronto tra tutti i soggetti pubblici e privati che possono essere oggetto di attacchi informatici, al fine di individuare delle soluzioni praticabili, che possano migliorare gli aspetti che attengono alla prevenzione del rischio. La NIS 2 è uno strumento normativo molto importante, perché individua per la prima volta i soggetti destinatari delle misure di prevenzione e protezione, classificandoli in essenziali e importanti. L'Italia emanando il decreto 138 è stata tra le prime in Europa a recepire i criteri della NIS 2, dimostrando di comprendere lo spirito di una legge che intende creare una regia unica a livello continentale di azione e contrasto del cyber crimine".*

Cybersecurity nella Sanità e Cyber Threat intelligence (CTI)

Molti studiosi parlano ormai di *software defined reality, un regno delle non cose* che impone diverse categorie della conoscenza. Studiare gli attaccanti per cercare di capire gli impatti sulle infrastrutture complesse, come fa la Cyber Threat intelligence (CTI), può aiutare, così come può aiutare fare memoria di fatti ed eventi. **Emanuele Gentili, co-direttore dell'area Cybersecurity della Fondazione ICSA**, ha ricordato l'attacco del 2023 all'ospedale israeliano Ziv Medical Cente da parte di un avversario cibernetico statuale, alleato di Hezbollah, con finalità di bloccare i servizi sanitari e sottrarre le cartelle cliniche dei pazienti. *"La lezione che se ne trae presenta le potenzialità di una vera e propria Cyber kill chain, in cui strutture parastatali e cyber crime si muovono all'unisono per preparare gli attacchi cibernetici. Appare chiaro che stiamo andando oltre la dinamica di azioni combinate da malware isolati, occorre fronteggiare fasi ben precise di attacchi architettati tramite sfruttamento e ricognizione delle vulnerabilità. Il software malevolo si muove sempre più individuando molto bene la realtà del target di riferimento. Statistiche sui ransomware che hanno colpito il settore sanitario forniscono una idea molto concreta del fenomeno: 278 incidenti gravi registrati a livello globale nel 2024, con gli Stati Uniti il Paese più colpito, seguito dal Brasile Regno Unito e Canada. Quello che più preoccupa riguarda la crescita di organizzazioni complesse, dotate di*

business plan, che si muovono con un modello piramidale con tanto di help desk e che consente la negoziazione in caso di richiesta di riscatto.

"Dobbiamo crescere in consapevolezza – ha ribadito **Gianluca Ignagni, Capo di gabinetto dell'Agenzia Cybersicurezza Nazionale (ACN)** – *soprattutto quando ci muoviamo in settori esposti come quello sanitario. Dalla frode allo spionaggio al sabotaggio, sono tutti fenomeni che la nostra struttura ha sotto osservazione. La commissione europea interverrà su un asset strategico come la Sanità, considerando che il diritto alla salute passa dall'affidabilità di reti e sistemi digitali. 66 incidenti che hanno generato un blocco dei servizi a livello nazionale negli ultimi due anni facendo ben comprendere quanto esteso e grave sia il pericolo, con rischi altissimi per la salute collettiva. La ricerca di un bilanciamento tra esigenze investigative e di resilienza del sistema paese costituisce pertanto l'obiettivo più sfidante di questa delicata fase. La legge 90 e le direttive NIS1 e NIS2 che danno delle indicazioni su come "organizzare" la sicurezza sono espressione dello sforzo in termini di governance del rischio che si sta compiendo e che vedrà in futuro una collaborazione sempre più efficace tra pubblico e privato. Sicurezza della catena di approvvigionamento, capacità di gestione degli incidenti, necessità di garantire la business continuity e di gestire l'obsolescenza degli strumenti sono tutti step necessari da traguardare per fare un salto di qualità".*

Lo strumento di contrasto dell'intelligenza collettiva

Ma la sicurezza è anche sviluppo, non solo governance dell'esistente. Concetti molto bene espressi da **Mario Nobile, Direttore Generale Agenzia per l'Italia Digitale.** *"In Italia* - ha affermato – *il problema non è tanto gestire 39 milioni di spid, 16 milioni di PEC, 5 milioni di certificati di firma, quanto piuttosto trovare un punto di convergenza tra 23 mila Pubbliche amministrazioni -un calcolo per forza approssimativo- tra comuni regioni, USL, concessionari di pubblico servizio, etc. Data la specifica complessità degli attori in gioco, quindi, il tema cyber assume in Sanità contorni molto particolari. Da qui la necessità di tessere una "intelligenza collettiva" per usare la celebre definizione del filosofo Pierre Levy, intessuta dalla collaborazione istituzionale tra Polizia Postale, ACN, AGID; PSN e AGENAS. Un presupposto necessario, se ci teniamo a diventare non solo bravi consumatori e gestori di infrastrutture critiche, ma protagonisti di una transizione digitale che deve generare percorsi virtuosi di crescita".*

Al riguardo, **Emanuele Iannetti, CEO del Polo Strategico Nazionale**, ha sottolineato come il PSN *"si rivelerà centrale per la sicurezza delle infrastrutture e del dato sanitario, attraverso la migrazione in Cloud delle Aziende Sanitarie e l'utilizzo al riguardo dei fondi PNRR. Il tutto all'interno di un quadro più ampio in cui il PSN sta perseguendo l'innovazione e la trasformazione digitale italiana attraverso la gestione sicura dei dati e dei servizi dell'intera Pubblica Amministrazione".*

"Attenzione però: parlare di sicurezza nelle reti digitali è un ossimoro perché con molta leggerezza tendiamo a sbattere sul web "pezzi" della nostra vita privata senza alcuna cura e attenzione", il monito arriva da **Cosimo Comella, Direttore tecnologie digitali e sicurezza informatica del Garante per la Protezione dei dati personali**. *"L'attività ispettiva e di vigilanza che spetta all'Autorità Garante – prosegue l'analisi di Comella – impatta sul mondo della Sanità in maniera determinante relativamente al sistema delle banche dati. Capitolo delicatissimo che ha delle peculiarità quando si parla di salute. Il dato sanitario fa gola non solo perché svela aspetti identitari, ma perché ci informa sullo stato di salute e persino, cosa che in futuro avverrà sempre di più, sulla genetica dei soggetti. Conoscere lo stato di salute di leader politici, pensiamo a quello che in passato è avvenuto con Gorbaciov e con i suoi predecessori, a quello che avviene oggi con Putin e Trump, solo per fare degli esempi eclatanti, può cambiare il corso della storia. D'altro canto, anche l'iperconnessione presenta aspetti di potenza ma anche di fragilità. Non dobbiamo stupirci se attualmente l'Autorità registra circa 2000 notifiche di violazioni l'anno, di cui il 10% riguarda la sanità, che comprende, aspetto non trascurabile, le aziende di servizio che gravitano in questo mondo, ponendo un'altra grande questione che stiamo cercando di affrontare la responsabilità delle terze parti".* ■

Geopolitica degli attacchi cyber.

Autore: Francesco Corona

SCENARI GEOPOLITICI ATTUALI - Nel 2010 Sergey Ulasen della società di sicurezza informatica bielorussa VirusBlockAda, consulente per la cybersecurity, scoprì su infrastrutture tecnologiche operanti in Iran un nuovo virus che fu chiamato "Stuxnet", il quale colpiva impianti industriali di tipo SCADA (Supervisory Control And Data Acquisition) basati sul protocollo PLC. Diversi esperti di cybersecurity analizzarono e scoprirono che era stato progettato per attaccare segretamente la centrale nucleare iraniana di Natanz, e in particolare il sistema delle centrifughe per l'arricchimento dell'uranio, facendole lavorare sotto soglia operativa, ritardandone così il processo di arricchimento, fondamentale per la preparazione di ordigni nucleari. La natura del virus era tale, infatti, da poter controllare e manipolare le apparecchiature industriali senza essere rilevato. L'ipotesi più accreditata, confermata poi da fonti autorevoli, fu che Stuxnet, era stato sviluppato tramite una collaborazione tra le agenzie, l'NSA americana e Unit 8200 israeliana, raggiungendo con successo gli obiettivi prefissati.

BIO

Francesco Corona è docente e direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome, già docente a contratto presso la Facoltà di ingegneria gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca in ambito MIUR e attività professionale d'impresa nel settore della sicurezza per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria. f.corona@unilink.it

La situazione geopolitica globale attuale è la risultante di un nuovo frenetico riposizionamento delle potenze economico-militari mondiali, dalle più grandi alle più piccole, dopo il secondo mandato di Trump a presidente degli Stati Uniti d'America, potenze a caccia di nuovi mercati e "terre rare" ovvero risorse per sviluppi tecnologici strategici soprattutto nel continente africano ma anche in Ucraina e Sud America. Da un lato assistiamo alla cercata pace tra Ucraina e Russia, pubblicamente voluta da Trump e con un'Europa confinata a giocare un ruolo marginale (almeno in apparenza), ricordiamo che l'Europa è attualmente tenuta fuori dai negoziati di pace in Arabia Saudita. Dall'altro la stabilizzazione del conflitto arabo-israeliano con un Iran sempre più minaccioso, dotato di un considerevole arsenale missilistico e droni (UAV) molto efficaci. L'Iran è da considerare una nuova potenza nucleare emergente nell'area medio orientale, in netta competizione e deterrenza nei confronti di Israele. Ricordiamo inoltre al lettore che Israele, nel 2019, fu la prima nazione al mondo a rispondere in modalità cinetica agli attacchi cyber lanciati dagli hacker di Hamas, abbattendo con un missile la palazzina di Gaza dove operava il gruppo in questione.

Tralasciando per un momento l'attacco dei miliziani di Hamas al *rave party* dell'ottobre 2023 (10) e l'escalation di morte e distruzione che ne è conseguita: bombardamenti israeliani a Gaza ridotta ormai ad un cumulo di macerie con decine di migliaia di morti civili, poi gli attentati contro personaggi di spicco delle milizie di Hamas e l'esplosione simultanea dei cercapersone avvenuta nel settembre 2024 cui seguirono, nell'ottobre delle stesso anno , piogge di missili iraniani su Israele per lo più intercettati dal sistema US Iron Dome. Come antefatto riportiamo che i vertici militari della Repubblica Islamica dell'Iran, nel gennaio 2024 divennero più audaci e per la

prima volta nella storia rivendicarono attacchi missilistici con razzi di lunga gittata, compiuti nel Kurdistan iracheno, nella Siria nord-occidentale e nord-orientale e nel Pakistan nord-orientale. Alcune basi americane della Siria e dell'Iraq furono colpite provocando numerosi feriti. Stiamo parlando dello stesso Iran apertamente schierato con Hamas e Hezbollah che da alcuni anni fornisce armi e appoggio ai combattenti Houti dello Yemen, i quali compiono attacchi con droni iraniani alle navi commerciali occidentali in transito da e verso il Mar Rosso.

Trump si è sempre schierato contro l'Iran e contro gli Houti yemeniti dando appoggio ad Israele nel confitto contro Hamas ed Hezbollah e imponendo a marzo 2025 due azioni specifiche:

1. Trasformare la costa marina prominente la striscia di Gaza in un luogo attrattivo per investimenti nel settore turistico, con nuovi alberghi e numerosi visitatori lungo le sponde del Mediterraneo. Famoso il suo filmato creato con l'IA generativa. (https://youtu.be/PslOp883rfI)

2. Portare avanti attacchi alle postazioni Houti sino alla totale riapertura delle rotte commerciali marittime nel Mar Rosso.

Sempre nella stessa area geopolitica, in Arabia Saudita, l'azione "contro corrente" del principe Mohammed bin Salman, manifestatamente eclatante nei confronti dell'amministrazione Biden sembrerebbe oggi svanita del tutto, dopo l'ascesa al potere di Trump e la scelta, insieme a Putin, della capitale Riad come sede dei negoziati di pace per Russia-Ucraina.

L'Arabia Saudita risulta essere ad oggi il primo partner commerciale dei Paesi BRICS (Brasile, Russia, India, Cina, Sudafrica) (5) che, ricordiamo, si prefiggono una multipolarità economica indipendente, contro una visione strettamente unipolare e globalista della precedente amministrazione USA e della BCE. L'Arabia Saudita è ora candidata a farne parte, come pure Iran ed Emirati Arabi Uniti (EAU), ma se da un punto di vista strettamente economico le scelte saudite non incontrano più elementi ostativi, anche in virtù di una possibile quanto morbida apertura di Trump ai BRICS, dal punto di vista militare le basi militari dell'US Army sono operative sul territorio saudita. Il Principe saudita aveva precedentemente minacciato Biden di chiuderle ma ora con l'assunzione a paese scelto da Russia e Stati Uniti per i negoziati di pace, tutto sembrerebbe volgere per il meglio nei rapporti USA - Arabia Saudita e USA - Russia. Ricordiamo al lettore che l'ingresso del Regno Saudita nei BRICS è favorito non solo da un risentimento antiamericano dei paesi del Golfo e dell'Africa, ma anche dalle crescenti relazioni economico-commerciali sempre più forti con la Cina, come risulta dall'ultimo *Arab-Chinese Business Forum*, nonché dalla ripresa delle relazioni diplomatiche con l'Iran mediate proprio da Pechino.

الدورة العاشرة لمؤتمر رجال الأعمال العرب والصينيين

10TH ARAB - CHINA

BUSINESS CONFERENCE

中阿合作论坛第十届企业家大会

Chiaro è che le relazioni internazionali non prescindono dal contenimento economico esercitato dagli Stati Uniti verso Cina, Europa, Russia e altri paesi (alleati e non alleati) in virtù degli obiettivi del MAGA (Make America Great Again) trumpiano attraverso logiche di deterrenza sia economica (dazi) sia militare. Sul fronte interno USA non possiamo omettere la proclamata guerra trumpiana al Deep State neocons, alla corruzione dilagante e alle derive gender della precedente amministrazione. Tutto questo si inserisce in un contesto geopolitico in continua evoluzione che coinvolge in primis il Medio Oriente con la velata volontà di Trump a creare i presupposti per un riavvicinamento degli States verso le politiche economiche dei BRICS dopo che la pace tra Russia e Ucraina sarà raggiunta non escludendo le aree calde asiatiche del mar meridionale cinese, di Taiwan.

GEOPOLITICA CYBER - Sappiamo bene che le tensioni internazionali si riflettono direttamente sulle strategie di cybersecurity dei paesi coinvolti e loro alleati: il 70% delle organizzazioni riconosce un impatto significativo della geopolitica sulle proprie scelte di sicurezza. L'analisi di scenari geopolitici e di cyber intelligence è inoltre diventata cruciale per prevenire attacchi futuri e attribuire responsabilità; come dimostrato dai recenti casi di attacchi cinesi contro gli Stati Uniti, contrastati sia dal punto di vista cyber

sia con sanzioni mirate. Le crisi globali inoltre (es. pandemia, cambiamento climatico, conflitti di varia natura) hanno reso urgente una stringente cooperazione internazionale, ma la frammentazione degli interessi nazionali dei singoli attori ostacola soluzioni condivise. Al contempo, l'evoluzione delle minacce cyber spinge verso l'adozione di strumenti che integrano analisi geopolitiche e di intelligence per diffondere *alert* preventivi in modalità condivisa. Stati Uniti, Russia e Cina emergono pertanto come protagonisti di un conflitto cibernetico globale, con reciproci attacchi mirati a infrastrutture critiche, istituzioni governative e settori strategici. La Cina ha dimostrato capacità avanzate attraverso operazioni come quelle della rete "Volt Typhoon", che ha infiltrato sistemi statunitensi a Guam e in altri Paesi.

"Volt Typhoon" è una organizzazione APT (Advanced Persistent Threat) filo Repubblica Popolare Cinese attiva dal 2021, che ha preso di mira principalmente organizzazioni di infrastrutture critiche sia negli Stati Uniti sia nei suoi territori. Il targeting e il modello di comportamento di Volt Typhoon sono stati valutati come pre-posizionamento per consentire i movimenti laterali verso risorse di tecnologia operativa (OT) per potenziali esfiltrazioni di dati e successivi attacchi distruttivi. Volt Typhoon, nel 2024, ha evidenziato la furtività nelle operazioni utilizzando web shell, codici binari living-off-the-land (LOTL) (14), attività manuali e credenziali rubate (4).

La Corea del Nord sta invece impiegando migliaia di hacker per finanziare il regime di Kim Jong-un attraverso attacchi ransomware e furti di criptovalute, che generato miliardi di euro all'anno.

Russia e Ucraina invece rappresentano un caso emblematico: il conflitto ha scatenato un'escalation di attacchi state-level (+24% nel 2022) e operazioni di *information warfare* (+119,2%), spesso legate a campagne di disinformazione.

Come dicevamo, in affiancamento alle agenzie governative abbiamo i famigerati gruppi APT alcuni con spiccata propensione ad azioni filo governative e geopolitiche (https://attack.mitre.org/groups/).

Dall'inizio della guerra in Ucraina, ad esempio, sono emersi vari gruppi identificati come "hacktivisti nazionalisti", in particolare da parte russa, in

Logo dei principali enti governativi ufficiali di cyber security & intelligence © Autore

forza allo scontro tra Kiev e Mosca. Tra queste entità, il gruppo filo-russo NoName057(16) ha suscitato interesse attraverso il Progetto DDoSia, uno sforzo collettivo filo russo volto a condurre attacchi DDoS (Distributed Denial-of-Service) su larga scala, prendendo di mira entità (società private, ministeri e istituzioni pubbliche) appartenenti a paesi che sostengono l'Ucraina, prevalentemente Stati membri della NATO.

A partire dal 2024, il Progetto DDoSia e il gruppo che lo gestisce (Sekoia.io) continua a monitorare in modo proattivo l'infrastruttura di comando e controllo (C2) acquisita per meglio finalizzare gli attacchi DDoS. In particolare, ha implementato un sistema automatizzato per la raccolta di dati dai target in tempo reale e il monitoraggio regolare dei canali di comunicazione in cui NoName057(16) rivendica la responsabilità dei suoi attacchi (11)(12).

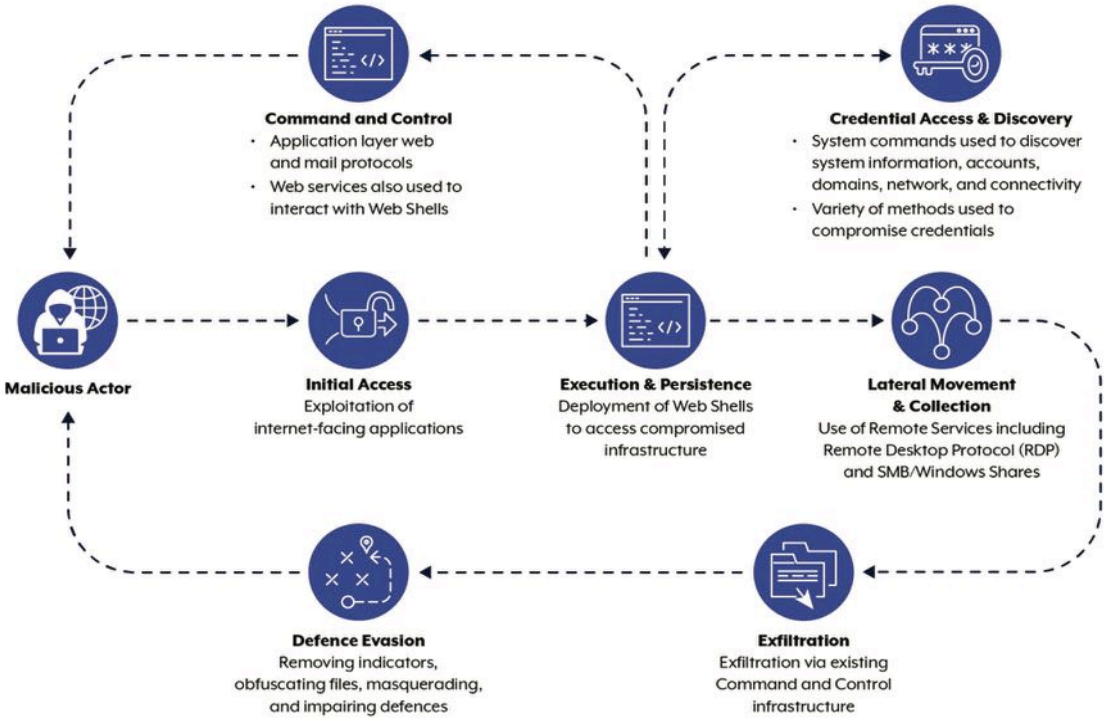


Fig. 1 - Schema classico di un attacco APT – Fonte Cisa.gov (7)

I gruppi APT allineati alla Cina sono per lo più concentrati sulle infrastrutture critiche del Giappone ma anche occidentali e hanno fatto sempre più affidamento sul controllo malevolo delle VPN (Virtual Private Network) di tipo open source e sulle piattaforme per mantenere l'accesso alle reti delle vittime. Sono quindi stati rilevati utilizzi estensivi anomali di VPN da parte del già citato gruppo APT Volt Typhoon, osservando il transito di Webworm tramite backdoor sul SoftEther VPN Bridge e sui computer di organizzazioni governative europee e server SoftEther VPN presso operatori di telecomunicazioni in Africa. (vedi Volt Typhoon, BRONZE SILHOUETTE, Vanguard Panda, DEV-0391, UNC3236, Voltzite, Insidious Taurus, Group G1017 | MITRE ATT&CK®).

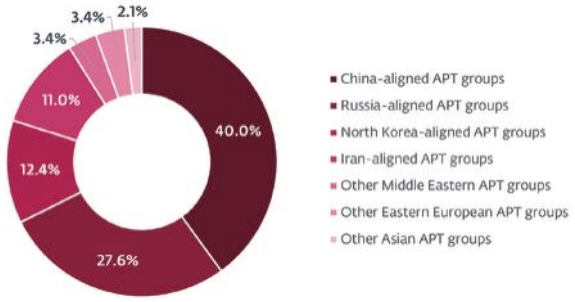


Fig. 2 - Fonte ESET APT Activity Report APT groups Q2 2024–Q3 2024 (6)

In questo report emerge chiara l'attività dei gruppi APT nord coreani (12,4%) e iraniani (11,0%) rispettivamente al terzo e quarto posto.

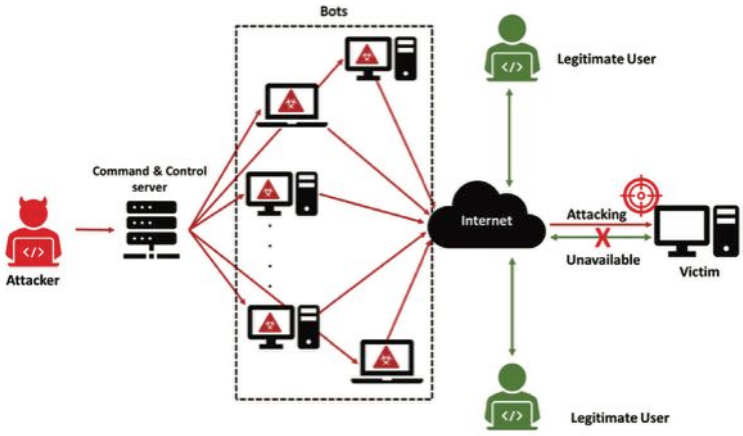


Fig. 3 – Tipico schema di attacco DDoS

ATTACCHI DDoS - Gli attacchi cyber alle infrastrutture critiche, in particolare gli attacchi DDoS (Distibuted Denial of Service), hanno un impatto significativo sulla geopolitica globale. Questi attacchi possono essere utilizzati come strumenti di coercizione politica e strategia militare, influenzando la stabilità economica e la sicurezza nazionale dei paesi coinvolti.

Country	APT Group Name / Alias	Primary Motive	Key Targets
China	APT1 (Comment Crew), APT3 (Buckeye), APT10 (Stone Panda), APT41 (Winnti), Volt Typhoon	Cyberespionage, Economic Gain	Government, defense, telecom, healthcare, tech
Russia	APT28 (Fancy Bear), APT29 (Cozy Bear), Sandworm, Noname57(16)	Cyberespionage, Political Influence	Governments, NATO, critical infrastructure
Iran	APT33 (Elfin), APT34 (OilRig), APT39 (Chafer)	Cyberespionage, Regional Influence	Energy, financial services, government, telecom
North Korea	APT37 (Reaper), APT38 (Lazarus Group)	Financial Theft, Cyberespionage	Banks, cryptocurrency exchanges, defense
USA	Equation Group (linked to NSA)	Cyberespionage	Global infrastructure, communication systems
Vietnam	APT32 (OceanLotus)	Cyberespionage, Political Influence	Government, private sector, dissidents
Pakistan	APT36 (Transparent Tribe)	Cyberespionage, Political Influence	Indian government, defense sector
India	SideWinder, Dark Basin	Cyberespionage, Political Influence	Pakistan, China, Bangladesh, NGOs
Kazakhstan	Nomadic Octopus	Cyberespionage, Regional Influence	Central Asian governments
Turkey	StrongPity	Cyberespionage	Dissidents, Kurdish groups, government agencies
South Korea	Kimsuky	Cyberespionage	North Korean defectors, NGOs, journalists
Syria	Syrian Electronic Army	Political Influence, Hacktivism	Media, political opponents
Israel	OilRig (linked to Iran-Israel conflict)	Cyberespionage	Regional adversaries

Tab.1 - Principali gruppi APT nel mondo. Fonte: Comprehensive List of APT Threat Groups, Motives, and Attack Methods (8)

Settori come energia, sanità e trasporti, sono diventati bersagli privilegiati per attacchi che minano la sicurezza nazionale e la vita quotidiana. La digitalizzazione accelerata ha aumentato la vulnerabilità di questi sistemi, con conseguenze potenzialmente catastrofiche.

L'intelligenza artificiale generativa sta inoltre rivoluzionando gli attacchi, permettendo la creazione di malware più sofisticati e campagne di phishing personalizzate.

Parallelamente, lo scontro tecnologico tra Cina e Stati Uniti alimenta una corsa agli armamenti cibernetici, con attacchi finalizzati al furto di know-how o al sabotaggio di rivali economici.

In sintesi, un tipico attacco DDoS è un tentativo ostile di bloccare il normale traffico di un server, di un servizio informatico o rete internet sovraccaricandoli con flussi di traffico proveniente da più font in contemporanea. Per generare un DDoS è necessario:

1. **Creare una botnet:** utilizzo il malware per creare una rete di dispositivi infettati, chiamata botnet. Questi dispositivi possono includere smartphone, computer, router e dispositivi IoT;
2. **Inviare istruzioni:** Una volta creata la botnet, i criminali inviano istruzioni ai dispositivi infettati per generare traffico verso il sistema preso di mira;
3. **Sovraccaricare il sistema:** Il traffico generato dalla botnet sovraccarica il sistema, impedendo agli utenti legittimi di accedere ai servizi.

Si distinguono le seguenti tipologie di attacco:

- **Attacchi volumetrici:** Sono diretti ai livelli 3 e 4 del modello OSI e sovraccaricano il sistema con un afflusso di traffico, esaurendo la larghezza di banda disponibile;
  - ***DNS Flood:*** Utilizza server DNS aperti per inviare una grande quantità di risposte DNS al target;
  - ***UDP Flood:*** Inonda le porte dell'host target con pacchetti UDP.
- **Attacchi al protocollo:** Sfruttano punti deboli nello stack del protocollo di livello 3 e 4, come l'attacco SYN;
- **Attacchi a livello di applicazione:** Colpiscono le applicazioni Web, ad esempio con attacchi HTTP flood, che sovraccaricano il server con richieste http;
  - ***Slowloris:*** Mantiene aperte più connessioni HTTP sul server preso di mira, assorbendo le risorse;
- **Distributed Reflected Denial of Service (DRDoS):** Utilizza server esterni per inviare risposte al bersaglio, amplificando l'effetto.

Per proteggersi, è importante utilizzare servizi di mitigazione DDoS, come quelli offerti da ottimi apparati di rete e firewall che possono rilevare e bloccare il traffico di attacco. Inoltre, è fondamentale attestare questi apparati difensivi sfruttando una banda superiore a quella dalla quale si ricevono gli attacchi dopodiché mantenere aggiornati i sistemi e le reti per prevenire la creazione di botnet.

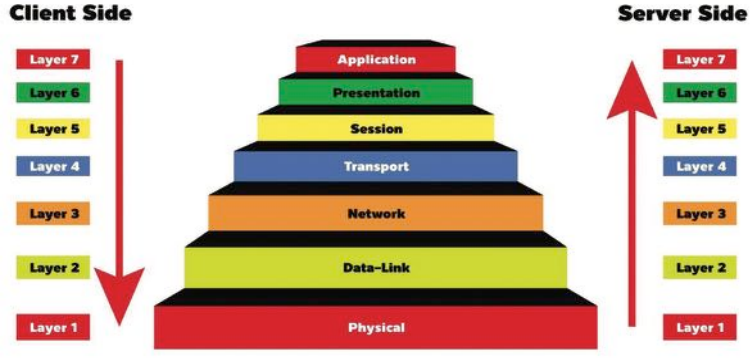


Fig. 4. Modello ISO/OSI Client/Server – Fonte Fastweb Plus (13)]

INTELLIGENZA ARTIFICIALE GENERATIVA E ATTACCHI DDOS - L'Intelligenza Artificiale generativa (GenAI) è un tipo di intelligenza artificiale in grado di creare contenuti originali come testi, immagini, audio, video, codice software o musica, partendo da richieste specifiche (prompt) e sfruttando modelli statistici addestrati su enormi quantità di dati. GenAI è basata su modelli di deep learning come i *foundation models* o i *modelli linguistici di grandi dimensioni* (LLM) che analizzano distribuzioni probabilistiche dei dati di addestramento per generare output coerenti.

L'Intelligenza Artificiale generativa introduce inoltre nuove dinamiche:

1. **Supporto agli attaccanti:**
   - **Democratizzazione delle conoscenze:** Utenti senza competenze tecniche possono sfruttare strumenti di IA generativa per ottenere istruzioni dettagliate su come eseguire attacchi DDoS, bypassando limiti di comprensione tecnica;
   - **Personalizzazione degli attacchi:** L'IA aiuta a identificare vulnerabilità specifiche delle reti, adattando gli attacchi per massimizzare l'impatto;
   - **Creazione di contenuti persuasivi:** Strumenti come ChatGPT generano email di phishing o messaggi di riscatto più convincenti, aumentando l'efficacia degli attacchi ibridi (es. DDoS + ransomware).

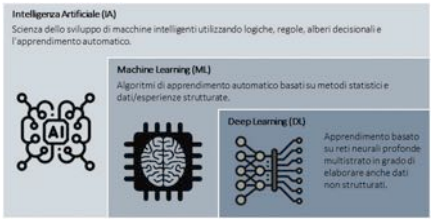


Fig. 6 - Schema relazionale tra IA, ML e DL – Fonte Handelskammer.bz.it (9)

2. **Casi emblematici. TaskRabbit (2018):** Un attacco DDoS assistito da IA ha compromesso i dati di 3,75 milioni di utenti, dimostrando come l'automazione possa amplificare la portata degli attacchi.
3. **Asimmetria tecnologica.** Gli attaccanti sfruttano l'IA per ottimizzare gli attacchi, mentre le autorità faticano a contrastarli efficacemente, soprattutto nell'analisi linguistica delle comunicazioni.
4. **Contromisure.** Le difese basate sull'utilizzo della stessa tecnologia IA consentono:

- **Il monitoraggio predittivo:** sistemi di IA analizzano pattern di traffico per identificare attacchi in tempo reale;
- **L'addestramento di modelli:** le Reti Neurali addestrano dataset su attacchi storici per riconoscere minacce emergenti;
- **La collaborazione tra settori:** ovvero condivisione di dati e best practice tra aziende e istituzioni per contrastare minacce coordinate.

Un Trattato Internazionale Per La Non Proliferazione Di Armi Cyber

Gli attacchi informatici, come quelli DDoS, possono compromettere il funzionamento di reti energetiche, sistemi di trasporto e comunicazioni, centri ospedalieri creando caos e instabilità. Questo tipo di attacchi possono essere particolarmente devastanti per le infrastrutture critiche, come centrali elettriche o sistemi di approvvigionamento idrico, inoltre, le stesse nazioni possono utilizzare le cyberarmi come forma di pressione politica. Ad esempio, durante il conflitto russo-ucraino, la Russia ha utilizzato attacchi informatici per influenzare la sicurezza energetica europea. Gruppi di hacker filorussi come NoName057 hanno condotto attacchi DDoS contro siti istituzionali e aziende strategiche in Italia, dimostrando come questi attacchi possano essere utilizzati per destabilizzare la sicurezza informatica di un paese. Ad esempio, l'attacco alla rete elettrica ucraina del 2015, eseguito tramite il malware BlackEnergy 3, ha mostrato come gli attacchi informatici possano essere utilizzati per compromettere le infrastrutture critiche di un paese, causando blackout e interruzioni dei servizi pubblici.

Gli attacchi cyber possono quindi aumentare le tensioni tra le nazioni, portando ad un'escalation delle misure di sicurezza e delle contromisure. Senza considerare che adesso (per l'Occidente) il Cyberspace è da intendersi come il quinto dominio della conflittualità e avendo Israele nel 2019 interscambiato le aree di conflitto rispondendo cineticamente ad attacchi cyber, gli stessi scenari di conflitto possono degenerare, e nel caso occidentale, si potrà intervenire invocando l'articolo 5 del trattato NATO. Inoltre nella nuova dottrina nucleare russa, la nuova policy afferma che *la Russia potrebbe lanciare armi nucleari in risposta a un attacco sul suo territorio da parte di uno Stato non armato nuclearmente, se sostenuto da uno armato nuclearmente.*

Questi nuovi scenari di conflitto stanno diventando particolarmente significativi nei rapporti tra Stati Uniti, Cina e Russia, dove gli attacchi informatici sono diventati un elemento chiave della strategia geopolitica di questi paesi.

Per affrontare queste sfide, è fondamentale una cooperazione internazionale efficace. Le nazioni non devono limitarsi a condividere informazioni, sviluppare protocolli di sicurezza e lavorare insieme per proteggere le infrastrutture critiche devono invero sviluppare trattati internazionali vincolanti sulla cybersicurezza per stabilire standard minimi di sicurezza e regolamentare l'uso dell'intelligenza artificiale nel cyberspazio. In buona sostanza il mio auspicio è che l'ONU (o chi per essa) predisponga a stretto giro un trattato di non proliferazione di armi cyber con tanto di agenzie pubbliche internazionali di monitoraggio e controllo sulla falsa riga di quanto già accaduto per le armi nucleari strategiche.

Bibliografia Utile

(1) Infrastrutture Critiche e Geopolitica: un'introduzione alla vulnerabilità globale - AIIC (Associazione Italiana esperti in Infrastrutture critiche): https://www.afcearoma.it/news/capitolo-di-roma/infrastrutture-critiche-e-geopolitica-un-introduzione-alla-vulnerabilita-globale-aiic-associazione-italiana-esperti-in-infrastrutture-critiche

(2) Rapporto Clusit 2024 sulla sicurezza ICT in Italia: https://www.quotidianosanita.it/allegati/allegato1739271220.pdf

(3) Attacchi DDoS nel contesto dell'intelligenza artificiale generativa: un'indagine sperimentale: https://www.teichmann-it.com/it/pubblicazioni/Attacchi-DDoS-nel-contesto-dellintelligenza-artificiale-generativa.html

(4) Volt Typhoon: https://attack.mitre.org/groups/G1017/

(5) Così i Brics aprono nuove strade per i Paesi del Medio Oriente: https://formiche.net/2024/11/brics-medio-oriente-med-dialogues/#content

(6) ESET APT Activity Report Q2 2024–Q3 2024 (www.eset.com)

(7) List of APT Threat Groups, Motives, and Attack Methods : https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a

(8) Comprehensive List of APT Threat Groups, Motives, and Attack Methods : https://www.socinvestigation.com/comprehensive-list-of-apt-threat-groups-motives-and-attack-methods/#:~:text=Here%20is%20a%20list%20of%20Advanced%20Persistent%20Threat,are%20typically%20state-sponsored%20or%20highly%20organized%20cybercriminal%20groups

(9) Applicazione dell'intelligenza artificiale nelle imprese: https://www.handelskammer.bz.it/it/servizi/digitalizzazione/conoscenze-pratiche/articoli-specializzati/applicazione-dellintelligenza-artificiale-nelle-imprese

(10) I razzi sul rave. La strage di Hamas al festival israeliano : https://www.ilfoglio.it/esteri/2023/10/09/video/i-razzi-sul-rave-la-strage-di-hamas-al-festival-israeliano-5760460/

(11) Progetto DDoSia NoName057(16): aggiornamenti 2024 e cambiamenti comportamentali : https://blog.sekoia.io/Noname05716-Ddosia-project-2024-updates-and-behavioural-shifts/

(12) NoName057 Threat Actor Profile: https://www.quorumcyber.com/wp-content/uploads/2024/04/TI-NoName057-Threat-Actor-Profile-1.pdf

(13) Che cos'è il modello ISO/OSI e perché è fondamentale nelle telecomunicazioni: https://www.fastweb.it/fastweb-plus/digital-dev-security/che-cos-e-il-modello-iso-osi/

(14) Living Off The Land (LOTL) Attacks And Techniques: https://www.fortinet.com/it/resources/cyberglossary/living-off-the-land-lotl ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

Psicologia comportamentale e resilienza durante un attacco DDos.

L'accoppiata tra psicologia comportamentale e attacchi DDoS non è immediatamente ovvia, ma in realtà c'è un'interessante intersezione.

Un attacco DDoS oltre ad essere una minaccia tecnica è anche un test comportamentale per l'intera organizzazione.

Quando un individuo, o una squadra, si trova improvvisamente sotto attacco, il cervello passa in modalità sopravvivenza. Questa risposta, profondamente radicata nell'evoluzione umana, ha implicazioni dirette sul comportamento e sulla qualità delle decisioni.

La psicologia comportamentale aiuta a capire come le persone reagiscono sotto pressione, in condizioni di incertezza e stress, elementi chiave durante un attacco informatico di questo tipo.

La cultura della Resilienza Psicologica

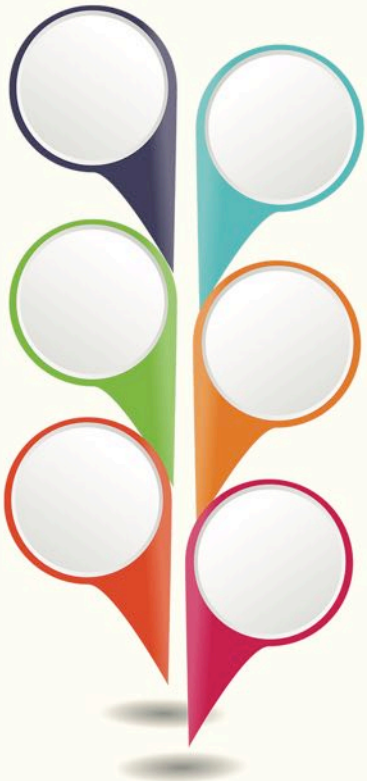
Costruire difese solide significa anche allenare la mente. Preparare il team a gestire momenti di crisi, come un attacco DDoS, permette di ridurre l'effetto del panico, evitare reazioni impulsive e mantenere il controllo anche sotto pressione. La resilienza psicologica nasce anche dalla consapevolezza.

Comprendere le dinamiche emotive legate a questi attacchi aiuta a sviluppare strategie di prevenzione e risposte più efficaci.

Andiamo ora ad esplorare le principali implicazioni psicologiche di un attacco DDos.

VISIONE A TUNNEL
Focalizzarsi su un solo sintomo o soluzione, ignorando il contesto.

BIAS D'AZIONE
Sentirsi obbligati ad agire subito, anche senza informazioni sufficienti.



BIAS DI CONFERMA
Individuare le reazioni emotive aiuta ad agire con più controllo.

FALLACIA DEI COSTI IRRECUPERABILI
Difficoltà ad abbandonare una scelta perché ci abbiamo già speso risorse.

BIAS DI ANCORAGGIO
Dare troppo peso alla prima informazione ricevuta.

BIAS DEL SENNO DI POI
Tendenza a credere, dopo un evento, che fosse ovvio e prevedibile.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud

Bibliografia - Cybersecurity Trends

Mario Caligiuri
Maleducati
Ed. Luiss University Press

Il fitto intreccio che oggi lega educazione, sicurezza e democrazia

Conoscere il mondo per leggere i fenomeni e anticipare i cambiamenti, abbiamo progressivamente smarrito questa fondamentale capacità interpretativa del tempo presente per una ragione tanto semplice quanto evidente: l'educazione ha perso la sua centralità. Da fattore di progresso civile e democratico è stata derubricata nelle agende dei governi, dimostrando la grave malattia di cui sono affette le élite che hanno il futuro dell'umanità. Questa la tesi di fondo dell'interessante e intenso saggio di Mario Caligiuri che continua a suscitare il dibattito. Quanto sia cruciale il tema appare persino superfluo sottolinearlo. In questo cambiamento epocale, bisognerebbe attrezzarsi di un corredo sempre più ampio e articolato di saperi, per sfidare i livelli di complessità crescente che segnano la contemporaneità. Invece, per un'incomprensibile inversione delle priorità, la politica sembra dimenticarsi della scuola e dell'Università, salvo richiamarla in causa in occasione di qualche comizio o programma preelettorale. Così mentre assistiamo all'eccezionale progresso della scienza e della tecnologia che stanno portando le macchine "intelligenti" a dialogare con l'individuo, mimandone anche le facoltà superiori, che credevamo fossero nostra esclusiva prerogativa di specie, si registra, non solo nelle nuove generazioni, un grave deficit cognitivo. "Servirebbero – scrive Caligiuri – risposte visionarie, mentre di fatto restiamo atrocemente fermi, prigionieri di metodi di trasmissione della conoscenza vetusti, costruiti su linguaggi superati, su pratiche obsolete. I cambiamenti sempre più rapidi a cui stiamo assistendo metteranno a dura prova la capacità di adattamento, biologico e cerebrale delle persone, accentuando una dinamica che non è nuova, e che ha preso le mosse dai tempi dell'invenzione della stampa. Tutto questo sembra tracciare uno scontro tra intelligenze: quella umana, formatasi in migliaia di anni, e quella artificiale, in corsa per realizzare l'algoritmo definitivo che programma sé stesso. C'è bisogno, dunque, di strumenti cognitivi che permettano alle persone di comprendere la realtà, diradando le ombre della disinformazione e contrastare la manipolazione dell'intelligenza artificiale".

Tempo educativo e processi del digitale

La ricerca di Caligiuri riguarda uno spettro di analisi molto ampio, che l'autore ha toccato in pubblicazioni orientate a proporre un'autentica riforma dello statuto stesso della disciplina pedagogica. Tutto il sistema educativo è chiamato a compiere un "passo oltre" per interpretare quel passaggio d'epoca che Emanuele Severino definiva "la tendenza fondamentale del tempo che viviamo". L'emergenza educativa è il dato più preoccupante, (Caligiuri lo aveva già denunciato in un altro lavoro edito da Rubbettino: "Disinformare: ecco l'arma" il cui punto di convergenza è sempre il tema dell'emergenza educativa: perché senza un adeguato livello culturale non c'è democrazia, partecipazione, trasparenza, il corpo collettivo si sfalda allontanandosi dalla cosa pubblica, fino a disinteressarsi di quel destino comune che appartiene a tutti.

Il tempo educativo non può andare d'accordo con la fulminea rapidità che regola i processi del digitale. Esiste una discrasia tra il tempo educativo e l'immediatezza dell'informazione. Abbiamo probabilmente dimenticato che la professionalità si costruisce in percorsi lunghi, faticosi, spesso accidentati, che non possono risolversi nel "singhiozzo" di un semplice tweet. La conseguenza di questa grave contraddizione la si può vedere nella progressiva perdita di competitività del nostro sistema–paese. Questo disallineamento è inoltre una delle cause che sta facendo precipitare una fetta molto ampia della popolazione verso un neo analfabetismo, con un decadimento delle capacità di interpretazione di contenuti anche molto semplici che non può lasciare indifferenti. Il pericoloso avanzamento dell'ignoranza diventa, per altro, fatalmente alimento della riluttanza al cambiamento, che caratterizza e ha caratterizzato molte classi dirigenti non solo alle nostre latitudini. Resistere all'innovazione, sfruttando l'assenza di pensiero critico da parte dell'opinione pubblica, consente da sempre al potere di conservare le posizioni e di vivere di rendita. Siamo così precipitati in una "società fantasma", cito testualmente l'autore, che ha ridotto la democrazia ad una semplice procedura, svuotandola di senso. "Siamo tra i paesi occidentali in cui più drammatico si presenta lo scarto tra realtà e percezione della realtà. Nuotiamo come pesci dentro l'acqua di una disinformazione creata ad arte. Come sosteneva **Marshall McLuhan** viviamo dentro la Rete e proprio per questo non sappiamo valutare le caratteristiche del liquido da cui traiamo il nutrimento". Un liquido, va detto, sempre più tossico a giudicare dal crescente fenomeno delle fake news che annebbiano l'orizzonte in un costante e sistematico lavoro di disinformazione, che "avvelena i pozzi" disorientando i cittadini.

In questa drammatica *"Allegria dei naufragi"* la verità rimasta sommersa nella disinformazione entra in crisi. La sua ricerca che aveva orientato tutto il pensiero occidentale fin dalle origini, sembra ormai una pratica passata di moda. Nei regimi autoritari viene calpestata, nelle democrazie, invece di essere il fulcro del dibattito, è stata derubricata ad affare di poco conto. I potentati economici transnazionali hanno altro cui pensare, muovono con più interesse la "macchina del fango" traendo profitti dalla falsificazione della realtà. È così avvenuto che nella "società liquida" di **Zygmunt Bauman**, si è imposta una sorta di "consenso solido" determinato dall'esclusione di una base sociale sempre più ampia, (più del 50% il dato italiano) che non prende parte al gioco democratico, il cui esito risulta scollato dalla volontà del paese reale.

Il paradosso della "Democratura"

Prende, così, corpo quella che molti studiosi definiscono autocrazia elettorale, che dà origine a una grave perdita di interesse per la politica. Il fenomeno, che purtroppo sta investendo numerosi stati dell'Occidente, sostanzia nel filo rosso su cui si regge l'impianto della ricerca: il delicato rapporto che dovrebbe legare educazione, informazione e democrazia. Su questo trinomio si regge la creazione della Scuola Italiana di Intelligence e di un Master dedicato a questa complessa e intricata materia progettato e realizzato da Caligiuri per promuovere non l'attività

degli "spioni" come una certa vulgata vorrebbe, ma "un sapere sociale" al servizio dello Stato e del bene comune.

Solo l'educazione dei cittadini e delle *élites* può rendere effettiva la pratica democratica in un panorama articolato di soggetti e poteri, senza che il voto si riduca a una semplice procedura elettorale, cosa che sta di fatto generando un disequilibrio tra i poteri. Esecutivi pressati dall'efficientismo, mortificano la dialettica parlamentare, che appare limitata e svuotata di senso. Le multinazionali finanziarie e gli Stati autoritari si nutrono della straordinaria capacità di manipolazione delle informazioni, guadagnando, in una sorta di "guerra ibrida" non convenzionale che non ha bisogno apparentemente di nessuna "arma", terreno nello scacchiere geopolitico. Se, per quanto detto appare incerta la comprensione, incerta la descrizione del contesto del cambiamento, instabile diventa l'organizzazione sociale che ne discende, che porta con sé un'inevitabile arretratezza dei sistemi legislativi. L'autore fa riferimento a **Hans Magnus Enzensberger** che ha denunciato in molti scritti l'inanità di una politica che non decide più nulla del futuro. Entra in campo quando fatti e idee diventano banali, oggetto di nutrimento di quella che il grande pensatore tedesco **Martin Heidegger** chiamava "chiacchiera", e che oggi definiamo, in modo ancora più prosaico, gossip. Questa "pericolosa distrazione" delle classi dirigenti è forse l'alert più urgente che lo studioso intende lanciare all'opinione pubblica.

Una pedagogia per il XXI secolo

Nella fluidità dell'universo delle "non cose", per usare una brillante immagine del filosofo **Byung Chul Han**, che ci fa perdere l'abitudine di vivere il reale, bisogna rimettere in sintonia il tempo educativo, cui prima si faceva riferimento, con il tempo dei diritti e del rispetto dei valori democratici, la cui conquista è costata il sacrifico di intere generazioni di donne e uomini. Bisogna mettere in campo una pedagogia per il XXI secolo, da costruire pezzo per pezzo, per sanare un'*"inferma scienza"*, si potrebbe sintetizzare con queste parole il manifesto di impegno culturale che l'autore mette in campo, per sconfiggere la dittatura del "pensiero debole" che ha defocalizzato la *mission* strategica delle agenzie del sapere che dovrebbero amministrare, senza discriminazioni e con universale apertura, il prezioso giacimento delle conoscenze. Se questo non avverrà assumeremo le sembianze degli ***orologi di Dalì "che segnano ore diverse"***, molli, dalle forme fluide, scivolano su piani inclinati, che sembrano rappresentare il precipizio della nostra crescente scarsa consapevolezza e cognizione delle cose del mondo e della storia, incapaci come siamo di intercettare i fenomeni antropologici, sociali ed economici che attraversano il presente che viviamo. ■

Michele Mezza
Connessi a morte
Ed. Donzelli

Viviamo in uno stato permanente di "guerra ibrida"

Il saggio di Michele Mezza, giornalista, inviato per il Giornale Radio Rai in Urss e in Cina, docente dell'Università Federico II di Napoli e direttore del centro di ricerca sul *mobile* PollicinAcademy, è un libro

agile e stimolante che fa riflettere sull'uso dell'informazione nella nostra vita a partire dalla tragica esperienza della guerra ibrida. "Per la prima volta – scrive l'autore – sta avvenendo nella storia che le procedure e le tecniche civili sono divenute la base per il combattimento militare, mentre fino ad oggi era stata la guerra che anticipava le tecnologie che poi sarebbero state adottate nella vita ordinaria. La principale di queste tecnologie è la connettività che rende ogni singolo utente un bersaglio da parte di chi controlla dati e piattaforme, come abbiamo visto nel clamoroso caso dei cerca persone degli Hezbollah". In questa dinamica segnata da una commutazione di codice, lo scambio di notizie si identifica con la logistica militare, con la conseguente manomissione dell'idea che nel senso comune abbiamo dell'avversario. Siamo insomma nel regno delle "non cose" in cui la realtà è ingoiata dal software, una realtà in cui gli stessi giornalisti sono ormai un "capitolo" della cyber security.

Algoritmo è la parola chiave di questa delicata fase dello sviluppo scientifico e tecnologico. L'aspetto delicato riguarda il governo di un potere inedito, che gli studiosi definiscono "computazionale", eccentrico e impalpabile, che condiziona e pianifica le nostre vite. Che fossimo tutti controllati in vario modo lo sapevamo, siamo però andati oltre ogni immaginazione. Lo dimostra la partita aperta da Musk per il controllo politico-strategico dello spazio globale, che coinvolge gli apparati statali e istituzionali, insieme ai grandi player che dominano il mercato della comunicazione digitale. "Nella trattazione non mi sono voluto soffermare – commenta Mezza - su generici giudizi di valore, da cronista sono abituato a guardare ai fatti. Ho cercato piuttosto di far capire che siamo nel mondo della proliferazione militare in cui la cyber security è divenuta un'attività geostrategica di fondamentale importanza. Se tutta la nostra vita è dominata dai file, manometterli è divenuta l'arma principale, lo strumento per prevalere anche nelle attività professionali, tra le aziende, e insisto su questo tra gli Stati. Chi si è appropriato di due fattori che sono i dati e la potenza di calcolo, comanda".

Il mutamento dei codici della comunicazione ha finito col modificare il modo stesso con cui si attua il conflitto. L'autore usa uno slogan per farlo capire: "oggi si combatte come si vive, e si vive come ci si informa, scambiando segni e sogni. Sia in Ucraina che a Gaza noi vediamo come ormai gli aspetti più terribili della guerra siano sempre la conseguenza di un'azione di profilazione del nemico. In duemila anni non era mai successo. Nelle battaglie della contemporaneità ognuno è in condizione di guardare in faccia al suo avversario, per quanto numeroso possa essere. Le armate e le popolazioni sono profilate, uno per uno, e si decide, ferocemente, a mente fredda chi e come colpire". Si combatte una "guerra ibrida" permanente che ha fatto evaporare ogni idea di pace, che sembra sparita dal vocabolario delle cose concretamente perseguibili, rifugiata in un anfratto ha perso la connotazione valoriale che ne fa un ideale per cui bisogna

combattere e sacrificarsi. Questo non vuol dire che dobbiamo rassegnarci a vivere nel terrore ma che la guerra ibrida è il nuovo sistema dominante di convivenza, in cui categorie e interessi di interi paesi, tendono a prevalere alterando ogni nostra percezione.

E "Alice nel paese della meraviglie"? L'imprevedibile e spiazzante citazione in cui ci si imbatte nel corso della lettura? "L'allegoria di Carroll calza anche se riferita alla società contemporanea", viene in nostro soccorso l'autore. "Essa dice all'uomo del nostro tempo che il "sorriso del gatto" stampato nel cielo è il segno di un mondo in divenire dove non si sa chi comanda. Una domanda che dovremmo portarci dietro sempre soprattutto ogni qual volta siamo guidati da file programmati, da parte di qualcuno che vuole manomettere la nostra esistenza. Rimanere passivi significa soccombere, oltre che perdere la partita". ■

Franco Amicucci
Paolo Ferri
Fabrizio Maimone
Francesca Scenini
Tecnologie per la formazione aziendale
Ed. Mondadori Università

Un manuale universitario sulla formazione degli adulti in azienda

"Tecnologie per la formazione aziendale - *Storia, metodologie e futuri possibili del Digital learning in azienda*" è un saggio che nasce dall'incontro tra due ambiti in evoluzione: quello della riflessione e della ricerca accademica sulle sfide della didattica e sui processi di digitalizzazione che incidono sulle pratiche di insegnamento e apprendimento, e quello del know-how delle organizzazioni e dei professionisti della formazione aziendale, costantemente a confronto con le esigenze della formazione degli adulti e chiamati ad applicare le metodologie e le tecnologie più avanzate. Il saggio ha le sembianze di un testo di base per la formazione di giovani studenti universitari che seguono percorsi di specializzazione nell'ambito delle risorse umane e della formazione e dall'altro uno strumento di apprendimento per il formatore aziendale, figura che si è specializzata, finora, principalmente sul campo. Pur essendo migliaia i formatori aziendali, solo recentemente sono stati creati percorsi universitari dedicati a questa figura professionale aziendale.

L'aspetto più interessante, spiegano gli autori, è individuabile nella condivisione e nella sistematizzazione di una solida base di conoscenze e competenze che costituiscono le fondamenta della nuova disciplina accademica: la formazione degli adulti in ambito aziendale, imprescindibile in un mondo del lavoro sempre più complesso che richiede figure professionali in grado di accompagnare le persone, con percorsi di *skilling, upskilling* e *reskilling,* al fine di favorire la crescita e l'innovazione delle aziende.

La formazione è sempre più cruciale per la competitività di aziende e organizzazioni, pubbliche e private, ed è un elemento centrale per il benessere e lo sviluppo delle persone che vi lavorano. Le tecnologie dell'apprendimento sono, oggi, uno strumento essenziale per creare e diffondere conoscenze e competenze. Si tratta di un nuovo campo del sapere organizzativo che è indispensabile padroneggiare e imparare a gestire. Questo manuale parte da una ricostruzione storica dell'affermarsi del digital e del social learning e ne analizza le metodologie e gli strumenti, fino alle tecnologie emergenti come l'intelligenza artificiale, la realtà virtuale e aumentata. L'incontro dei due ambiti che hanno realizzato il testo, quello accademico e quello professionale, ha generato un'opera originale e innovativa sia per il mondo accademico sia per quello professionale, in cui teoria ed esperienze sul campo si alternano continuamente; la dimensione storica del *digital learning* e il quadro normativo europeo e nazionale dell'apprendimento nelle organizzazioni si alternano all'analisi di casi, guide operative e presentazione di metodologie formative applicate nelle aziende.

Il filo conduttore dei vari contributi del testo è quello della formazione continua, di una visione della formazione che vada oltre la dimensione formale per dare piena dignità alla dimensione informale e non formale dell'apprendimento, e della necessità di formare una nuova generazione di formatori con una forte padronanza della cultura e degli strumenti digitali, che sappiano operare negli ecosistemi di apprendimento aziendale e che sappiano padroneggiare una molteplicità di metodologie. ■

XX Rapporto sulla comunicazione del Censis
I media e la libertà
Ed. Franco Angeli

Come cambia il giornalismo e l'informazione nell'era di Internet

I media e la libertà. Il XX Rapporto sulla comunicazione del Censis (ed. Franco Angeli) mette in primo piano questo delicato binomio. Siamo passati dalla spinta alla disintermediazione, epoca in cui ognuno ha cominciato a creare il suo palinsesto, all'era biomediatica, in cui l'individuo ha cominciato a mettere la faccia e le proprie idee sul web passando da fruitore ad attore dell'informazione. Questo mutamento ha fatto da premessa alla successiva esplosione degli *influencer*, abili creatori di mode, seguendo un percorso che arriva alla più stretta attualità, segnata dallo strapotere dell'algoritmo, che sceglie i contenuti informativi per noi, confacendosi ai nostri gusti, in un gioco di specchi difficile da arrestare. La televisione resta regina,

guardata dal 94 per cento degli italiani, la sua non è una sovranità immobile, per reggere il confronto con l'universo cross mediale in costante espansione è divenuta multipolare, ibridata dalle "finestre web" con cui vive ormai in simbiosi, si è aperta a meccanismi nuovi di fruizione. Lo spettatore segue trasmissioni e serie tv sempre più "in differita", è più solo di fronte al teleschermo. Appare conclusa la grande stagione dei programmi *cult* (pensiamo all'epopea dei quiz di Bongiorno o alla "messa cantata del telegiornale delle 20.00) che raccontavano il Paese e che eravamo pronti a condividere in un costante processo di costruzione dell'identità collettiva. Quel mondo si è frammentato, il pubblico di oggi colloca al secondo posto dell'ecosistema dell'informazione un social netwok, come Facebook, che viene percepito come un mezzo molto semplice e rapido di conoscenza di quello che accade. La flessione molto grave della carta stampata testimonia una diffusa scarsa propensione all'approfondimento e alla lettura analitica dei fatti, cui fa da contraltare la progressiva affermazione di quella che i ricercatori definiscono *"platform society"*, territorio virtuale da cui traggono origine consumi culturali e comportamenti. Competenza, verifica rigorosa delle fonti, deontologia, metodo, la "cassetta degli attrezzi" del giornalismo sembra sia divenuta un superfluo, si assiste perciò al paradosso di un giornalismo senza informazione, e di una informazione confezionata senza obbedire ai criteri del giornalismo. I motori di ricerca la fanno da padrone, alimentati dagli algoritmi soddisfano una fame bulimica di curiosità, gonfiando una sorta di *ipernozionismo* da Google, intriso di alta emotività e da un flebile apporto cognitivo. È evidente che l'incrocio di questi fattori mal si concilia con il diritto all'informazione e con il pluralismo delle fonti, principi fondanti dello stato di diritto. Gli italiani sanno di vivere in una condizione di dipendenza da Internet, si sentono controllati e trascinati in una "giostra" multimediale di cui non riescono a controllare movimenti ed esiti, tuttavia non reagiscono, finendo con l'accettare lo stato di subordinazione rispetto a un potere computazionale oscuro, illeggibile. "In questi ultimi venti anni – spiega Giuseppe de Rita – c'è stato un doppio reciproco appiattimento tra sistema sociale e sistema della comunicazione. Mancano dei soggetti *verticali* di rottura, che sappiano spezzare l'andazzo, lo si vede moto bene se personaggi *enormi* come *Papa Francesco* e *Donald Trump*, il primo messaggiando a Sanremo, il secondo trasformando la Casa Bianca in un sito di streaming, hanno deciso di adottare la logica orizzontale e piatta della rete". Il deficit denunciato dalla ricerca riguarda l'assenza della radicalità del nuovo a dispetto della retorica che abusa del termine rivoluzione e che non sa fare i conti con il naufragio di quell'immaginario collettivo che aveva permesso all'Italia di crescere negli anni del miracolo economico, emancipandosi anche grazie all'apporto dei primi media di massa, radio giornali e tv, dalle drammatiche piaghe dell'ignoranza e dell'analfabetismo. ■

Recensioni bibliografiche a cura di
Massimiliano Cannata

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

DONA ORA

Il tuo contributo è prezioso 💎
https://www.cybertrends.it/supportaci/


DDOS
ATTACK