Cybersecurity Trends

Edizione italiana, N. 1 / 2023

INTERVISTE VIP:

- LUIGI MARACINO
- ROBERTO TIOZZO
- MATTIA FANTINATI
- FABIO LAZZINI

Folder centrale: Penetration Test & Automation Security

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

Quando il gioco si fa duro.

Autore: Nicola Sotira

È sempre più evidente che i temi di sicurezza informatica rappresentino un aspetto che non può più essere trascurato. Il cybercrime si sta dimostrando sempre più capace e abile nel superamento delle difese aziendali e nazionali facendo leva su vulnerabilità, che continuiamo a vedere in aumento, e su problematiche organizzative insieme al fattore umano che fa da sfondo a questo ecosistema digitale in fermento. Molti ancora gli aspetti da migliorare, a partire da una semplificazione e maggiore integrazione della sicurezza, l'inserimento di misure strutturali atte a colmare il divario culturale, in ambito digitale, diminuendo contestualmente le problematiche afferenti all'errore umano e soprattutto cercando di avere una copertura più ampia rispetto alle minacce cyber. In questo contesto si è visto come i temi di resilienza cibernetica vengano attenzionati e messi in alta priorità da Autorità e governi nazionali. Il settore finanziario, in particolare, sembra essere quello più esposto a questo tipo di minacce anche in ragione della numerosità dei soggetti che vi operano, oltre alla stretta interconnessione tra i vari nodi del sistema senza contare la chiara motivazione economica degli attaccanti. Ovviamente, lo scenario nel quale, un attacco a un singolo operatore possa trasmettersi ad altri, è altamente probabile. Proprio in quest'ottica, a livello europeo e nazionale gli Organismi di vigilanza stanno adottando framework e misure volte al rafforzamento sui temi di difesa, prevenzione e reazione dei singoli operatori economici. Proprio in questo contesto l'Unione Europea ha istituito il framework TIBER-EU, acronimo che sta per *Threat Intelligence-Based Ethical Red Teaming*. Il framework è stato creato dalla Banca Europea nel 2018, in risposta ad un quadro di crescenti minacce informatiche con lo scopo di utilizzare un approccio coordinato e sofisticato alla gestione del rischio cybersecurity. Perché le organizzazioni dovrebbero considerare con attenzione questo framework e la sua implementazione, vediamo i principali vantaggi:

- Miglioramento della sicurezza informatica: Il framework provvede un approccio completo alla gestione del rischio di cybersecurity.
- Aumentare la fiducia: implementando TIBER-EU, le organizzazioni possono dimostrare a clienti, stakeholder e autorità di regolamentazione che stanno adottando le misure necessarie per proteggersi dalle minacce informatiche.
- Efficientare la risposta agli incidenti: Il framework indirizza le tematiche di risposta agli incidenti, la ricerca delle minacce e il monitoraggio della sicurezza.
- Verifica della compliance: TIBER-EU è allineato alle normative europee pertinenti, con l'implementazione del framework le organizzazioni possono garantire il rispetto dei requisiti normativi e ridurre il rischio di sanzioni.
- Vantaggio competitivo: Le organizzazioni che adottano TIBER-EU possono ottenere un vantaggio competitivo dimostrando il loro impegno nelle tematiche di cybersecurity e la loro capacità di proteggere i dati dei loro clienti.

Non c'è dubbio, quindi, che TIBER-EU sia un supporto prezioso per tutte le organizzazioni che desiderano migliorare la propria posizione in materia di cybersecurity. Buona lettura… ■

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.

Il testing framework TIBER-IT.

Autore: Mario Trinchera

Il 2 agosto 2022 **Banca d'Italia, Consob** e **IVASS** hanno adottato la Guida nazionale **TIBER-IT** in modo congiunto. La Guida costituisce il recepimento in ambito nazionale del framework **TIBER-EU**, promosso già qualche anno fa dalla Banca Centrale Europea come modello di riferimento per la conduzione di test avanzati di cybersicurezza armonizzati a livello europeo in ambito bancario.

Il TIBER-IT è stato adottato in una prospettiva di stabilità finanziaria, nell'ambito delle competenze affidate alle tre Autorità concernenti la sorveglianza sul regolare funzionamento, affidabilità ed efficienza del settore nel suo complesso.

BIO

Mario Trinchera è Laureato in Ingegneria Informatica presso l'Università di Napoli "Federico II", vanta una lunga esperienza nel settore della Difesa ed ha conseguito diverse certificazioni internazionali in ambito security (tra cui la CISSP). Attualmente è il coordinatore tecnico del CERTFin, il CERT finanziario italiano, la cui mission è aumentare la cyber resilience dell'intero settore finanziario e le attività di cui si occupa spaziano dall'analisi su attacchi informatici e modelli di frode alla gestione delle emergenze derivanti da incidenti cyber. È impegnato in vari progetti europei, finanziati dalla UE, e partecipa a diversi gruppi di lavoro internazionali (EBF, ENISA, EPC, …). Infine, è coinvolto nell'organizzazione di diversi Osservatori di Ricerca (Cyber Security, Artificial Intelligence, Business Continuity, …) in seno ad ABI Lab, Centro di Ricerca e Innovazione per la Banca.

In questa prima fase, di cui non è stata ancora definita la durata, le entità finanziarie decidono di sottoporsi a un test TIBER-IT su base volontaria. Le Autorità assicurano il loro supporto ai soggetti che si sottopongono al test, supervisionano la conformità ai requisiti della Guida Nazionale TIBER-IT e delle altre previsioni rilevanti e curano, quando necessario, le attività per il mutuo riconoscimento a livello transfrontaliero del test.

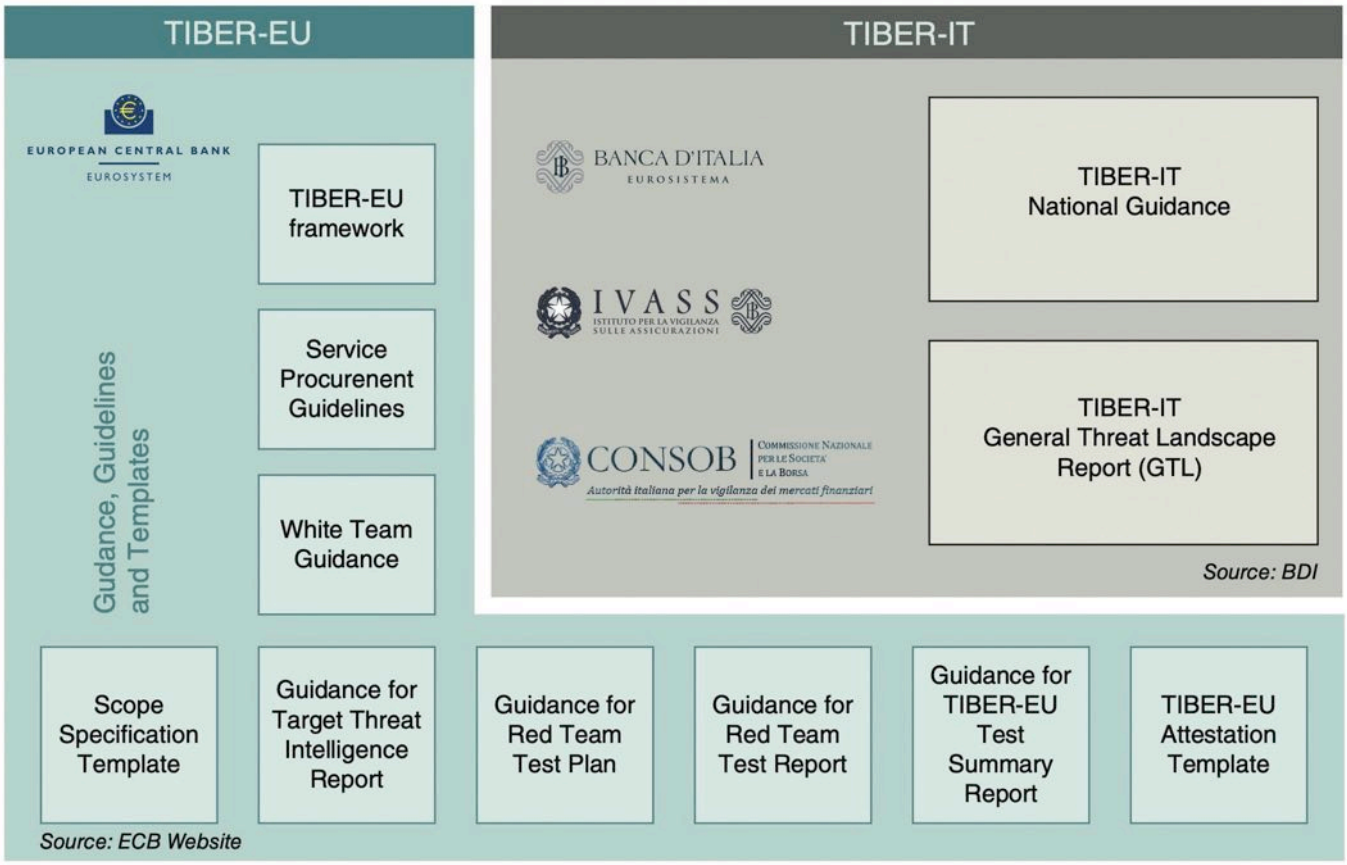
In particolare, la Guida Nazionale TIBER-IT:

- definisce la metodologia e il modello operativo per la conduzione di test di tipo Threat led Red Teaming[1] da parte delle entità finanziarie italiane, in accordo con il framework TIBER-EU;
- individua le fasi in cui si articola il processo di test;
- definisce i ruoli, le responsabilità e le attività dei diversi attori coinvolti presso il soggetto che effettua il test, i fornitori esterni e le Autorità.

In generale, il testing è una parte fondamentale della sicurezza informatica e consente di identificare le vulnerabilità e le falle nel sistema prima che queste possano essere sfruttate dagli attaccanti. TIBER-IT offre una metodologia completa di testing end-to-end che copre tutte le fasi del processo, dalla pianificazione alla valutazione dei risultati.

Il framework si basa sulle best practice del settore e sulle linee guida TIBER-EU adattandole alla realtà italiana e alle specifiche esigenze delle organizzazioni che operano nel nostro paese.

Per supportare le entità finanziarie nell'utilizzo della nuova metodologia e nelle attività di test, le tre Autorità mettono a disposizione un centro di competenza dedicato: il TIBER Cyber Team Italia (TCT), il cui funzionamento è assicurato da esperti di Banca d'Italia, in collaborazione con quelli di Consob e IVASS. Fra le attività di supporto del TCT rientra anche la definizione di un **Generic Threat Landscape** (GTL) quale riferimento sullo scenario delle minacce più rilevanti per il settore nel suo contesto geografico.



Inoltre, tale scenario può essere sviluppato in sinergia con il TIBER Knowledge Center (TKC), istituito presso la BCE per coordinare a livello europeo le attività inerenti all'implementazione del TIBER EU. Per la definizione del GTL il TCT può avvalersi di diverse fonti, fra le quali si segnala il **Threat Landscape Scenario (TLS) for the Italian Financial Sector**, prodotto con cadenza semestrale dal CERTFin.

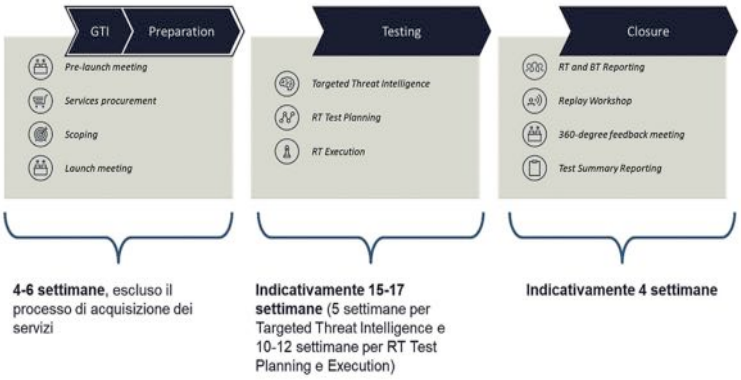
CERTFin

Il TLS è riservato ai membri del CERTFin e, poiché offre una panoramica piuttosto dettagliata sulle minacce emergenti, costituisce un'utile fonte per definire il GTL. In particolare, nella prima parte del report vengono analizzate e discusse le top threats che prendono di mira le organizzazioni, mentre nella seconda parte vengono approfondite le minacce che prendono di mira i clienti.

Gli scenari di minacce delineati in ragione del loro profilo generale devono poi essere proiettati sulla realtà tecnico/organizzativa oggetto di test. A tal fine è prevista un'attività di **Targeted Threat Intelligence** che, intersecando scenari generali di minacce con informazioni relative all'entità oggetto di test (insight), produce un elenco di minacce effettive e concrete sulle quali costruire uno specifico piano di test che simula tecniche, tattiche e procedure di un attaccante reale.

In altre parole, analizzando le peculiarità aziendali (l'infrastruttura, l'organizzazione, i processi, le vulnerabilità, etc.) sarà necessario identificare, tra le tante minacce generiche, quelle che rappresentano realmente il pericolo maggiore perché in grado di sfruttare le debolezze specifiche di quel soggetto.

Nel merito, il framework è stato progettato proprio con il fine di aiutare le organizzazioni a individuare potenziali vulnerabilità, siano esse organizzative, tecniche o di processo, e, di conseguenza, ad aumentare la sicurezza dei loro sistemi informativi e a mitigare i rischi derivanti da attacchi informatici.



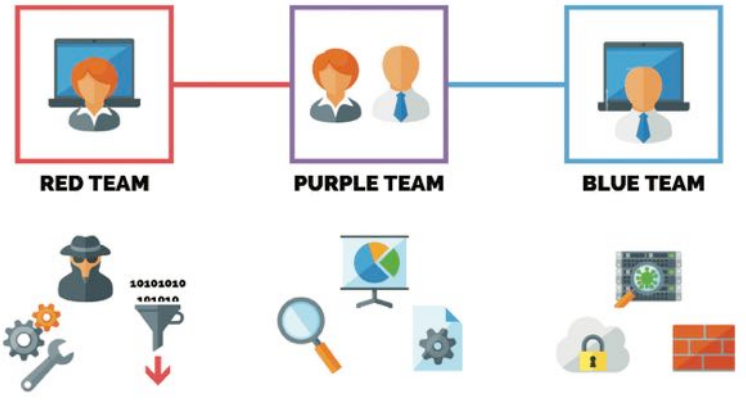
L'obiettivo è quello di aumentare, attraverso una migliore postura dei singoli, la sicurezza dell'intero ecosistema finanziario.

I test consentono di verificare le capacità di *Protection, Detection & Response* dell'entità testata simulando attacchi reali che riproducono tattiche, tecniche e procedure dei Threat Actor e utilizzando metodi di attacco sviluppati di volta in volta in base al contesto.

Il processo di testing si svolge in tre fasi principali: **pianificazione, esecuzione** e **valutazione** dei risultati. Tutte le fasi vanno affrontate con delicatezza e perizia, e spesso la rifinitura di tutti i dettagli preventivi può richiedere settimane; non deve quindi sorprendere che la durata complessiva di un'esercitazione può protrarsi oltre i 6 mesi.

Nella fase di pianificazione si definiscono gli obiettivi del testing, si definisce il perimetro, si identificano le possibili minacce e si stabiliscono le modalità di esecuzione del test. Le prime volte che un'entità si cimenta in simili esercitazioni sarebbe consigliabile tenere fuori dal perimetro servizi e processi core, al fine di contenere "effetti collaterali" non voluti. Nella fase di esecuzione si testano i sistemi e si valutano le loro capacità di risposta a possibili attacchi. Infine, nella fase di valutazione dei risultati si analizzano i risultati del test e si definiscono eventuali azioni correttive da intraprendere.

L'elemento fondamentale affinché il test di Red Teaming sia efficace è che "i rossi" assumano il più possibile la mentalità e l'attitudine dei veri attaccanti, se non in alcuni casi dei veri cyber criminali. Per questo motivo risulta sconsigliabile scegliere i membri del Red Team fra le persone che hanno contribuito o contribuiscono a proteggere l'infrastruttura dell'organizzazione stessa, perché si creerebbe un evidente conflitto di interessi che non garantirebbe l'efficacia dell'attacco (e di conseguenza dell'assessment della postura di sicurezza). Dunque, il Red Team è principalmente messo a disposizione da un provider con comprovata esperienza nell'erogazione di questi servizi. Altro imperativo consiste nel tenere completamente all'oscuro il Blue Team (il team a cui è strutturalmente affidata la difesa aziendale) del fatto che è stata pianificata un'esercitazione di tipo Red Teaming.



Nel caso il Blu Team riesca a identificare e respingere gli attacchi, per non "sprecare" le significative risorse (economiche, ma non solo) impiegate fino a quel momento nell'organizzazione dell'esercitazione il test può proseguire con la variante del **Purple Team**: un componente del team dei blu viene aggiunto al team dei rossi. In questo modo, conoscendo molto bene l'infrastruttura aziendale, le misure difensive e le sue vulnerabilità, può indirizzare al meglio gli attacchi dei rossi.

È molto importante comprendere che una volta messa in moto la macchina è fondamentale che vengano prodotti dei risultati e delle evidenze utili a scoprire ogni possibile debolezza e a porvi adeguato rimedio.

Se ciò non avvenisse, cioè se l'esercitazione non riuscisse a mettere in luce possibili spunti di miglioramento, tecnici e non, lo sforzo sarebbe vanificato.

Il framework include anche la possibilità di eseguire test che aiutino a valutare la capacità del soggetto di ripristinare le funzionalità dopo un attacco informatico. Questo è particolarmente importante in un contesto in cui:

- gli attacchi informatici stanno diventando sempre più sofisticati e persistenti;
- le interdipendenze tra soggetti sono molteplici e l'indisponibilità dei servizi erogati da uno può riverberarsi su altri, causando potenzialmente un effetto domino;
- è necessario assicurare che i servizi identificati come essenziali siano sempre garantiti.

TIBER-IT offre inoltre una serie di vantaggi per le realtà che lo utilizzano, ad esempio:

- pianificare gli investimenti futuri partendo da dati oggettivi ottenuti tramite la simulazione di una situazione reale;
- fare test specifici in modo strutturato per evitare i costi imposti dalle autorità di vigilanza in risposta a incidenti causati dalla mancanza di misure di sicurezza adeguate;
- aumentare la fiducia dei clienti e degli stakeholder, dimostrando l'impegno dell'organizzazione per la sicurezza informatica.

Il framework TIBER-IT è stato sviluppato in collaborazione con un'ampia gamma di stakeholder, tra cui il mondo accademico, il settore bancario e finanziario, i fornitori di servizi di sicurezza informatica e le autorità di regolamentazione. Questa collaborazione ha permesso di sviluppare un framework completo e all'avanguardia, in grado di rispondere alle esigenze delle organizzazioni italiane. A supporto del framework, il CERTFin ha messo a disposizione una metodologia di Threat Intelligence utile per la generazione degli scenari di minaccia, siano essi generici o specifici. Inoltre, contribuisce con le sue attività di Threat Intelligence a monitorare la continua evoluzione delle minacce cyber ed è disponibile a supportare i suoi membri nelle fasi preparatorie dei test TIBER ma anche offrendo, gratuitamente, l'opportunità di verificare il proprio livello di maturità attraverso esercitazioni propedeutiche quali quelle di tipo Table-Top (attraverso le quali viene verificata la robustezza dei processi) e Capture-the-Flag (utili invece a personale più operativo). ■

1 Ricordiamo che il Financial Stability Board ha chiarito, nel suo Cyber Lexicon, che le terminologie "Red Teaming" e "Threat Led Penetration Testing" sono sinonimi.

Attack Breach Simulation: una Componente Chiave della Tua Strategia di Cybersecurity.

Autore: Lisa Ventura

La cybersecurity è una delle preoccupazioni più importanti per aziende, organizzazioni e individui in tutto il mondo. Con il crescente numero di attacchi informatici, le aziende e le organizzazioni devono sviluppare solide strategie di sicurezza per prevenire, rilevare e rispondere a potenziali minacce cyber.

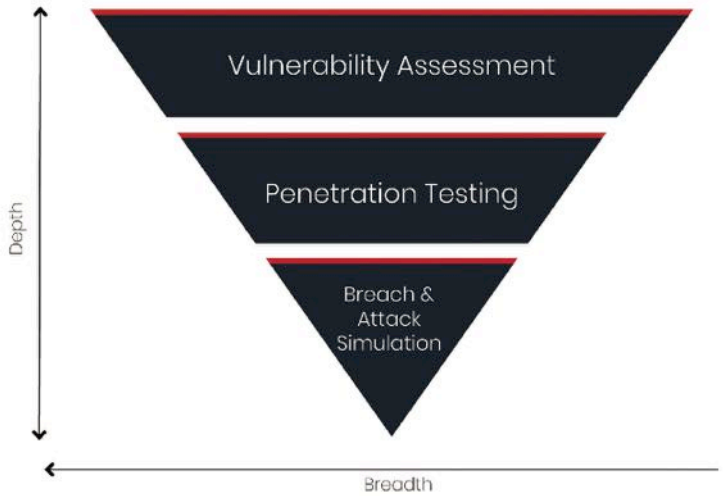
Le simulazioni di un attacco cyber sono uno degli strumenti più efficaci per valutare la postura cyber di un'azienda e identificare le vulnerabilità che possono essere sfruttate dai criminali informatici. In questo articolo, esploreremo il concetto di attack breach simulation e come i cyber-attack simulation tool possono aiutare a rafforzare la postura di sicurezza della tua organizzazione.

BIO

Lisa Ventura è una pluripremiata specialista, scrittrice e relatrice in materia di sicurezza informatica. È la fondatrice di Cyber Security Unity, un'organizzazione comunitaria globale che si dedica a riunire individui e organizzazioni che lavorano attivamente nella cyber security per aiutare a combattere la crescente minaccia informatica. Lisa è anche una mindset e coach per la salute mentale e offre aiuto e supporto a coloro che sono colpiti da stress, burnout e problemi di salute mentale nella cyber security e Infosec.

Cosa è un Attack Breach Simulation?

Un Attack breach simulation, noto anche come red teaming, è progettato per simulare attacchi informatici nel mondo reale per identificare le vulnerabilità e le misure di sicurezza di un'organizzazione. Questo tipo di simulazione viene eseguito da un team di ethical hacker, che tentano di penetrare le difese di un'organizzazione utilizzando le stesse tattiche e tecniche usate dai reali aggressori. Un Attack breach simulation può essere eseguito in vari modi, tra cui network penetration testing, social engineering e test di sicurezza fisica.



I penetration testing della rete prevedono il tentativo di penetrare nella rete di un'organizzazione sfruttando le vulnerabilità nei suoi sistemi software e hardware. Il social engineering implica l'uso di tattiche psicologiche per ottenere l'accesso a informazioni sensibili o a sistemi, come e-mail di phishing o chiamate telefoniche. I test di sicurezza fisica prevedono il tentativo di ottenere l'accesso fisico alle strutture di un'organizzazione bypassando le misure di sicurezza come serrature o telecamere di sicurezza.

L'obiettivo di un attack breach simulation è identificare le vulnerabilità nelle misure di sicurezza di un'organizzazione prima che i reali aggressori possano sfruttarle. In questo modo, le organizzazioni possono migliorare la loro postura di sicurezza e proteggersi meglio dalle minacce cyber.

I Vantaggi di un Attack Breach Simulation

I vantaggi nell'eseguire un attack breach simulation sono molteplici:

Identificare le Vulnerabilità: un attack breach simulation è progettato per identificare le vulnerabilità nelle misure di sicurezza di un'organizzazione. In questo modo, le organizzazioni possono migliorare la loro postura di sicurezza e proteggersi meglio dalle minacce cyber.

Migliorare i Tempi di Risposta: un attack breach simulation può anche aiutare le organizzazioni a migliorare i tempi di risposta in caso di un reale attacco cyber. Simulando gli attacchi del mondo reale, le organizzazioni possono testare le proprie procedure di risposta agli incidenti e identificare le aree che necessitano di miglioramenti.

Valutare i Controlli di Sicurezza: un attack breach simulation può anche aiutare le organizzazioni a valutare l'efficacia dei loro controlli di sicurezza. Identificando le vulnerabilità nei controlli di sicurezza, le organizzazioni possono migliorare il livello generale della loro postura di sicurezza.

Test sui Dipendenti: un attack breach simulation può anche aiutare le organizzazioni a testare la consapevolezza dei propri dipendenti sulle minacce cyber. Simulando attacchi di social engineering, le organizzazioni possono testare la capacità dei propri dipendenti di identificare e affrontare e-mail di phishing o altri tipi di attacchi.

Compliance: un attack breach simulation può anche aiutare le organizzazioni a soddisfare i requisiti normativi di compliance. Molti standard di compliance, come PCI-DSS e HIPAA, richiedono alle organizzazioni di eseguire regolari valutazioni e test di sicurezza.

Come Funziona un Attack Breach Simulation

Un attack breach simulation generalmente comporta diversi step:

Planning: il primo step in un attack breach simulation è la pianificazione. Gli ethical hacker lavoreranno con l'organizzazione per determinare l'ambito della simulazione, compresi i sistemi e le applicazioni che saranno presi di mira.

Reconnaissance: lo step successivo è la reconnaissance. Gli ethical hacker raccoglieranno informazioni sui sistemi e le applicazioni dell'organizzazione, tra cui l'architettura di rete, i sistemi operativi e le versioni del software.

Exploitation: una volta che gli ethical hacker hanno raccolto le informazioni sui sistemi e le applicazioni dell'organizzazione, tenteranno di sfruttare le vulnerabilità nelle misure di sicurezza. Ciò può comportare il tentativo di penetrare nella rete, ottenere l'accesso a informazioni sensibili o aggirare le misure di sicurezza fisica.

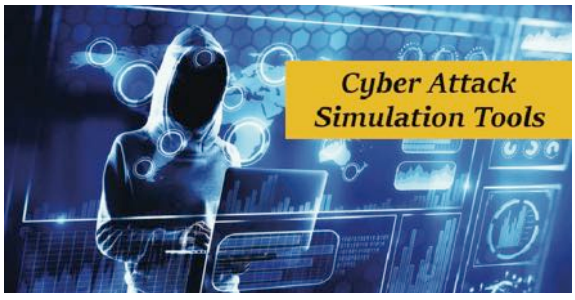
Reporting: una volta completata la simulazione, gli ethical hacker forniranno un report dettagliato sulle vulnerabilità identificate, insieme a raccomandazioni per migliorare la postura di sicurezza dell'organizzazione.

Remediation: lo step finale è la remediation. L'organizzazione utilizzerà il report fornito dagli etichal hacker per risolvere le vulnerabilità identificate durante la simulazione.

Durante ogni fase di un attack breach simulation, il team di sicurezza valuterà l'efficacia dei controlli di sicurezza dell'organizzazione e identificherà eventuali punti deboli o vulnerabilità che potrebbero essere sfruttati dagli aggressori.

Cosa sono gli Attack Simulation Tool e come Funzionano?

I Cyber-attack simulation tool sono programmi software che consentono alle organizzazioni di simulare attacchi informatici in un ambiente controllato. Questi tool possono aiutare le organizzazioni a identificare le



vulnerabilità nei loro sistemi e reti e sviluppare e testare strategie di risposta efficaci.

I cyber-attack simulation tool in genere funzionano simulando un ambiente che riproduce i reali sistemi e le reti dell'organizzazione. Il tool simula quindi una serie di scenari di attacco, come campagne di phishing, attacchi malware e attacchi Denial of Service (DoS), per testare le difese dell'organizzazione e identificare le vulnerabilità.

Durante la simulazione, il tool tenterà di sfruttare i punti deboli nella security posture dell'organizzazione, come software obsoleti o password deboli. L'obiettivo è identificare questi punti deboli prima che possano essere sfruttati dagli aggressori nel mondo reale.

Una volta completata la simulazione, il tool genera un report che descrive le vulnerabilità identificate e fornisce raccomandazioni per affrontarle. Il report può anche includere metriche come il tempo impiegato per rilevare e rispondere all'attacco simulato.

I cyber-attack simulation tool possono essere utilizzati da organizzazioni di tutte le dimensioni e in tutti i settori. Sono particolarmente utili per le organizzazioni che hanno un alto rischio di essere prese di mira da attacchi cyber, come istituzioni finanziarie, fornitori di servizi sanitari e agenzie governative.

Sono disponibili diversi tipi di cyber-attack simulation tool, ciascuno con i propri punti di forza e di debolezza. Alcuni tool sono progettati per simulare tipi specifici di attacchi, come campagne di phishing o attacchi ransomware, mentre altri sono più generici e possono simulare un'ampia gamma di scenari di attacco.

Una considerazione importante quando si sceglie un cyber-attack simulation tool è il livello di customizzazione e flessibilità che offre. Il tool dovrebbe essere in grado di simulare scenari di attacco rilevanti per il settore e il profilo di rischio specifici dell'organizzazione e dovrebbe essere in grado di adattarsi ai cambiamenti nel panorama delle minacce nel tempo.

Nel complesso, i cyber-attack simulation tool sono uno strumento prezioso per migliorare la resilienza informatica di un'organizzazione. Simulando scenari di un attacco cyber del mondo reale in un ambiente controllato, le organizzazioni possono identificare le vulnerabilità e sviluppare strategie di risposta efficaci, riducendo in ultima analisi il rischio di un attacco informatico riuscito.

In che modo i cyber-attack simulation tool possono aiutarti con la tua postura di sicurezza?

I cyber-attack simulation tool sono programmi software che simulano gli attacchi alla rete o all'infrastruttura di un'organizzazione. Questi tool possono aiutare ad aumentare la postura di sicurezza dell'organizzazione fornendo una simulazione realistica di ciò che farebbe un attaccante e identificando i punti deboli e le vulnerabilità che potrebbero essere sfruttate.

Ecco alcuni modi in cui i cyber-attack simulation tool possono contribuire ad aumentare la postura di sicurezza della tua organizzazione:

Identificare punti deboli e vulnerabilità: i cyber-attack simulation tool possono identificare punti deboli e vulnerabilità nella postura di sicurezza della tua organizzazione che altrimenti non sarebbero stati scoperti. Simulando una varietà di scenari di attacco, questi tool possono identificare i punti deboli nella rete, nelle applicazioni e nei processi dell'organizzazione.

Valutare l'efficacia dei controlli di sicurezza: i cyber-attack simulation tool possono aiutare a valutare l'efficacia dei controlli di sicurezza della tua organizzazione. Simulando attacchi che bypassano o eludono i controlli di sicurezza, questi tool possono identificare le aree in cui è necessario migliorare i controlli di sicurezza dell'organizzazione.

Formare il personale di sicurezza: i cyber-attack simulation tool possono essere utilizzati per formare il personale di sicurezza su come rispondere a diversi tipi di attacchi cyber. Simulando attacchi che imitano scenari del mondo reale, il personale addetto alla sicurezza può acquisire esperienza nella risposta agli attacchi e sviluppare strategie per mitigarli.

Testare i piani di risposta agli incidenti: i cyber-attack simulation tool possono essere utilizzati per testare il piano di risposta agli incidenti

dell'organizzazione. Simulando un attacco cyber, puoi valutare l'efficacia del piano di risposta agli incidenti della tua organizzazione e identificare le aree in cui deve essere migliorato.

Validare i requisiti di conformità: i cyber-attack simulation tool possono essere utilizzati per validare i requisiti di conformità. Simulando attacchi che testano i requisiti di conformità, le organizzazioni possono assicurarsi di rispettare i propri obblighi di conformità.

Alcuni esempi di esercitazione di una simulazione di un attacco includono:

Campagne di phishing: una campagna di phishing è un email o un messaggio di testo simulato che tenta di indurre gli utenti a divulgare informazioni sensibili, come username e password. L'esercizio può essere personalizzato per imitare le tattiche utilizzate dagli attaccanti reali e può aiutare a formare i dipendenti su come riconoscere ed evitare attacchi di phishing.

Esercitazioni di Red Teaming: le esercitazioni di Red Teaming coinvolgono un team di ethical hacker che tentano di penetrare le difese di un'organizzazione e ottenere l'accesso a informazioni sensibili. Il team può utilizzare una varietà di tecniche, come il social engineering e network explotation, per simulare attacchi il più possibile vicini a quelli reali.

Attacchi ransomware: un'esercitazione di simulazione di un attacco ransomware prevede l'implementazione di un attacco ransomware simulato sui sistemi di un'organizzazione. L'esercitazione può aiutare a identificare le vulnerabilità nei processi di backup e di ripristino dell'organizzazione, nonché formare i dipendenti su come rispondere a un attacco ransomware.

Attacchi Denial of Service (DoS): un'esercitazione di simulazione di un attacco DoS comporta l'interruzione intenzionale della rete o dei sistemi di un'organizzazione, con l'obiettivo di renderli inutilizzabili. L'esercitazione può aiutare a identificare le vulnerabilità nell'infrastruttura di rete dell'organizzazione e può essere utilizzata per testare le procedure di risposta.

Violazioni della sicurezza fisica: un'esercitazione di simulazione di una violazione della sicurezza fisica comporta il tentativo di ottenere l'accesso non autorizzato alle strutture fisiche di un'organizzazione, ad esempio aggirando i controlli di accesso o utilizzando tecniche di social engineering. L'esercitazione può aiutare a identificare i punti deboli nelle misure di sicurezza fisica dell'organizzazione e può essere utilizzata per formare i dipendenti su come rispondere alle violazioni della sicurezza.

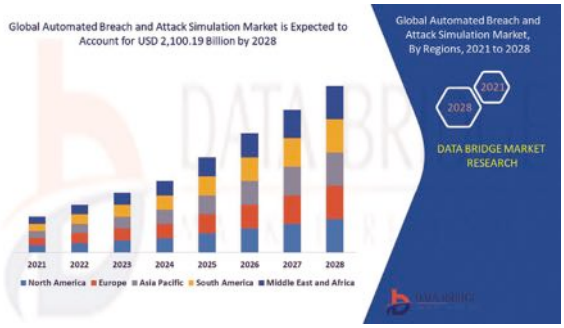
Attacchi alla catena di approvvigionamento: un'esercitazione di simulazione alla supply chain prevede la simulazione di un attacco contro un fornitore di terze parti, con l'obiettivo di ottenere l'accesso ai sistemi dell'organizzazione attraverso una supply chain vulnerabile. L'esercitazione può aiutare a identificare

i punti deboli nei processi di gestione dei fornitori dell'organizzazione e può essere utilizzata per istruire i dipendenti su come riconoscere e rispondere agli attacchi alla catena di approvvigionamento.

Questi sono solo alcuni esempi delle numerose esercitazioni di simulazione di attacco che le organizzazioni possono utilizzare per testare la propria resilienza informatica. È importante condurre queste esercitazioni regolarmente e applicare le lezioni apprese nei continui miglioramenti della sicurezza.

Esempi di attack breach simulation tool

Sul mercato sono disponibili numerosi attack breach simulation tool e alcuni di questi includono:



Cobalt Strike: questo tool viene spesso utilizzato da penetration tester e red team per simulare attacchi cyber avanzati. Include funzionalità come beaconing, fileless malware e social engineering.

Metasploit: Metasploit è un framework popolare per condurre penetration test e simulare attacchi cyber. Include un'ampia libreria di exploit e payload per testare le vulnerabilità nei sistemi e nelle reti.

CANVAS: Sviluppato da Immunity Inc., CANVAS è un tool commerciale per la simulazione di attacchi cyber avanzati. Include un'ampia gamma di exploit e payload, nonché un'interfaccia personalizzabile per la creazione di attacchi personalizzati.

Core Impact: Core Impact è un tool commerciale che include un'ampia libreria di exploit e payload, oltre a funzionalità per la simulazione di attacchi di social engineering e campagne di phishing.

BeEF: BeEF (Browser Exploitation Framework) è un tool per testare e simulare web-based attack. Include funzionalità per testare le vulnerabilità nelle applicazioni Web e condurre attacchi XSS (cross-site scripting).

OWASP Zed Attack Proxy (ZAP): ZAP è un tool gratuito e open source per testare le vulnerabilità delle applicazioni Web. Include funzionalità per la simulazione di attacchi come SQL injection, cross-site scripting e buffer overflow.

Nmap: Nmap è un popolare tool per la scansione della rete che può essere utilizzato anche per eseguire port scans e vulnerability assessments. Include funzionalità per la simulazione di attacchi come attacchi Denial of Service (DoS) e attacchi di brute force.

Questi sono solo alcuni esempi dei numerosi cyber-attack simulation tool disponibili. È importante utilizzare questi strumenti in modo responsabile e solo in conformità con le linee guida etiche e legali.

Come utilizzare un attack breach simulation tool in un ambiente reale?

Immaginiamo che un grande istituto finanziario sia preoccupato per il rischio di un attacco ransomware, dato il recente aumento degli attacchi ransomware contro altre organizzazioni del settore finanziario. Per valutare la propria preparazione a un simile attacco, l'istituto decide di condurre una simulazione di un attacco ransomware utilizzando un attack breach simulation tool.

La simulazione inizia con la creazione di un ambiente virtuale che replica la rete e i sistemi dell'istituto. Il tool di simulazione avvia quindi un attacco ransomware simulato, con l'obiettivo di crittografare quanti più dati possibile e richiedere un pagamento di riscatto in cambio della chiave di decrittazione.

Durante la simulazione, il tool utilizza una varietà di tecniche per tentare di penetrare le difese dell'istituto, come lo sfruttamento di vulnerabilità prive di patch nel software o l'utilizzo di tattiche di social engineering per indurre i dipendenti a scaricare software malevolo.

Man mano che la simulazione procede, il tool identifica diverse vulnerabilità nelle difese dell'istituto, inclusi software obsoleti, password deboli e procedure di backup dei dati insufficienti. Il tool evidenzia anche le aree in cui la formazione dei dipendenti potrebbe essere migliorata, come riconoscere ed evitare le e-mail di phishing.

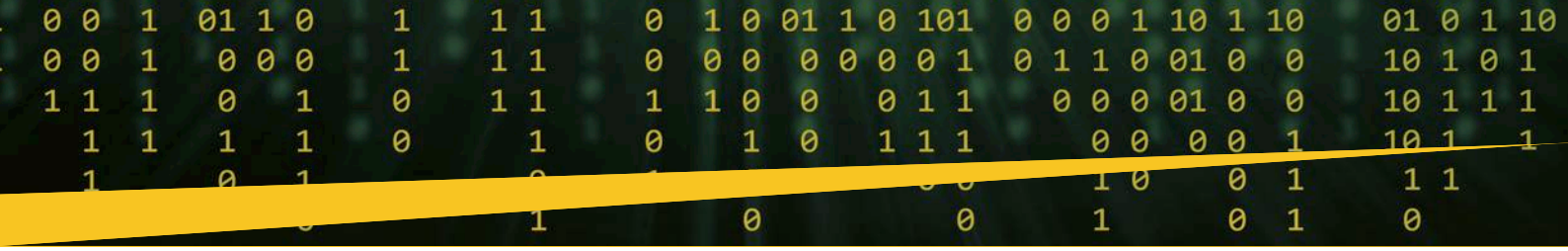
Al termine della simulazione, l'istituto riceve un report dettagliato che delinea le vulnerabilità identificate e fornisce raccomandazioni per affrontarle. Sulla base dei risultati della simulazione, l'istituto aggiorna le proprie politiche e procedure di sicurezza, implementa ulteriori controlli di sicurezza e conduce ulteriore formazione dei dipendenti per migliorare la loro preparazione a un attacco ransomware nel mondo reale.

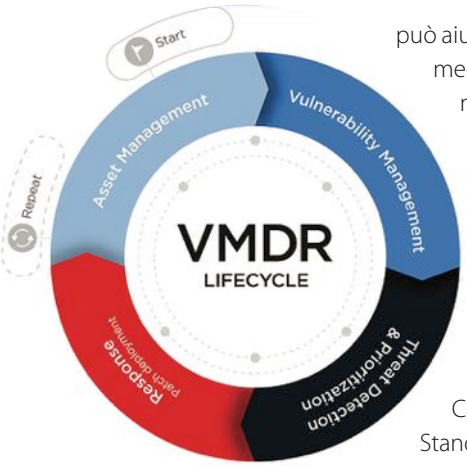
Sebbene questo scenario sia ipotetico, illustra come un attack breach simulation tool potrebbe essere utilizzato per simulare un attacco reale e identificare le vulnerabilità nelle difese di un'organizzazione. Utilizzando questo strumento per condurre simulazioni regolari, le organizzazioni possono identificare e affrontare in modo proattivo le vulnerabilità, riducendo in ultima analisi il rischio di un attacco informatico riuscito.

Perché le organizzazioni dovrebbero utilizzare un attack breach simulation?

Un attack breach simulation può aiutare le organizzazioni a identificare le falle e le vulnerabilità della sicurezza prima che vengano sfruttate dagli aggressori del mondo reale. Simulando vari tipi di attacchi, le organizzazioni possono ottenere una migliore comprensione di come i loro sistemi e reti potrebbero essere compromessi e possono adottare misure per migliorare la loro sicurezza.

Un attack breach simulation può anche aiutare le organizzazioni a migliorare i loro piani di risposta agli incidenti, offrendo opportunità per esercitarsi e testare la loro risposta a diversi tipi di incidenti di sicurezza. Ciò





può aiutare le organizzazioni a essere meglio preparate a rispondere in modo rapido ed efficace alle violazioni della sicurezza, riducendo al minimo l'impatto di tali incidenti.

Inoltre, può aiutare le organizzazioni a rispettare vari requisiti normativi e di conformità. Molte normative e standard, come il Payment Card Industry Data Security Standard (PCI DSS), richiedono test e assessment di sicurezza regolari. Un attack and breach simulation può aiutare le organizzazioni a soddisfare questi requisiti e dimostrare il loro impegno per la sicurezza.

Sono spesso visti come uno strumento importante per le organizzazioni che cercano di migliorare la propria postura di sicurezza e proteggere i propri sistemi e dati dalle minacce cyber.

Quando le organizzazioni dovrebbero utilizzare gli attack breach simulation tool?

Le organizzazioni dovrebbero utilizzare regolarmente gli attack simulation tool come parte della loro strategia generale di test e assessment della sicurezza. Ecco alcuni casi specifici in cui le organizzazioni potrebbero voler utilizzare questi strumenti:

Dopo l'implementazione di nuovi sistemi o applicazioni: ogni volta che vengono aggiunti nuovi sistemi o applicazioni all'infrastruttura di un'organizzazione, è importante eseguire test di sicurezza per identificare eventuali vulnerabilità che potrebbero essere sfruttate dagli aggressori.

Prima di modifiche importanti a sistemi o applicazioni esistenti: se sono previste modifiche importanti per sistemi o applicazioni esistenti, le organizzazioni devono eseguire test di sicurezza per garantire che le modifiche non introducano nuove vulnerabilità.

Regolarmente, come parte dei test e degli assessment di sicurezza in corso: le organizzazioni dovrebbero eseguire regolarmente test e assessment di sicurezza per identificare eventuali nuove vulnerabilità che potrebbero essere state introdotte o scoperte dopo l'ultimo assessment.

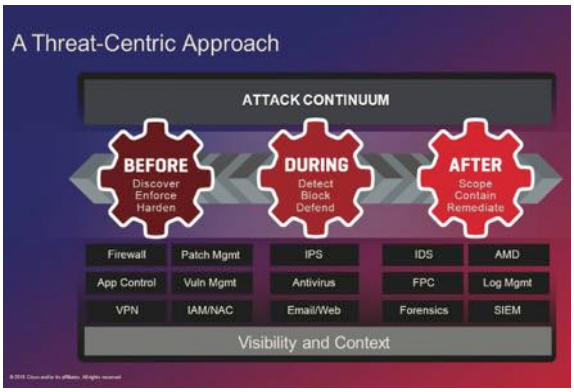
Dopo un incidente di sicurezza: se un'organizzazione subisce una violazione o un incidente di sicurezza, è importante eseguire test di sicurezza per identificare come si è verificata la violazione e prevenire incidenti simili in futuro.

Le organizzazioni dovrebbero considerare di adottare un approccio incentrato sulle minacce?

Il raggiungimento di un approccio incentrato sulle minacce è un obiettivo fondamentale per qualsiasi organizzazione che desideri migliorare le sue difese cybersecurity. Un approccio incentrato sulle minacce comporta lo spostamento dell'attenzione da misure reattive come firewall e software antivirus a un approccio proattivo che si concentra sull'identificazione e la mitigazione delle potenziali minacce prima che possano essere sfruttate. Questo approccio tiene conto dell'evoluzione del panorama delle minacce e delle tattiche, tecniche e procedure (TTP) utilizzate dagli aggressori.

In un approccio incentrato sulle minacce, le organizzazioni si concentrano sulla comprensione delle motivazioni, degli obiettivi e dei metodi dei potenziali aggressori. Ciò include l'identificazione degli attaccanti più probabili, i loro vettori di attacco preferiti e le vulnerabilità che potrebbero sfruttare.

Comprendendo potenziali minacce e vulnerabilità, le organizzazioni possono adottare misure proattive per prevenire o mitigare gli attacchi cyber. Ciò può includere l'implementazione di controlli e misure di sicurezza per



affrontare le vulnerabilità note, l'esecuzione regolare di test e assessment di sicurezza e lo sviluppo di piani di risposta agli incidenti efficaci.

Un approccio incentrato sulle minacce comporta anche il monitoraggio e l'analisi continui dell'attività di rete e dei feed di informazioni sulle minacce per identificare potenziali minacce e indicatori di compromissione (IoC). Ciò consente alle organizzazioni di rispondere rapidamente alle minacce e di intraprendere le azioni appropriate per prevenire o mitigare l'impatto di un attacco.

Conclusioni

Un attack breach simulation e l'utilizzo di tool pre eseguire le simulazioni sono degli strumenti importanti per le organizzazioni che cercano di migliorare la propria postura di cyber security e proteggere i propri sistemi e dati dalle minacce cyber. Forniscono un approccio proattivo alla cybersecurity che può aiutare le organizzazioni a identificare le vulnerabilità, testare i piani di risposta agli incidenti, soddisfare i requisiti di conformità, ridurre i rischi e migliorare la security awareness.

Tutte le organizzazioni dovrebbero prendere in considerazione l'integrazione di esecitazioni di attack breach simulation al proprio arsenale di cyber security. Più siamo preparati contro la crescente minaccia cyber e contro gli exploit di potenziali aggressori, più sicuri saranno i nostri sistemi dagli attacchi cyber. ■

Gestione continua delle minacce e delle esposizioni: un nuovo approccio per ridurre il rischio verso gli asset critici.

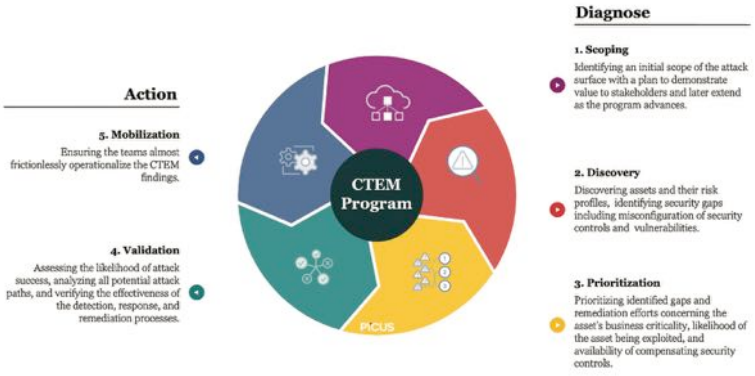
Autore: Davide Rivolta

La gestione corretta e proattiva delle minacce e delle esposizioni è un obiettivo che sembra diventare sempre più difficile da realizzare. Secondo il recente report di Gartner "Implement a Continuous Threat Exposure Management (CTEM) Program", le aziende fanno sempre più fatica a ridurre la propria esposizione alle minacce a causa di approcci irrealistici e focalizzati su strumenti spesso isolati tra di loro.

I responsabili della sicurezza e della gestione del rischio devono quindi iniziare a maturare un programma di gestione continua dell'esposizione alle minacce per riuscire a gestire e ridurre in modo continuativo il livello di rischio.

Data la complessità delle moderne infrastrutture, amplificata ancora di più dalla trasformazione digitale delle infrastrutture in hybrid e multi-cloud, risulta quindi indispensabile un approccio che permetta di identificare e rimediare in modo **automatico** e **continuativo** le proprie esposizioni.

In quest'ottica di analisi continuativa dell'esposizione ai rischi dell'infrastruttura, in opposizione rispetto a controlli sporadici o su specifiche aree, si è recentemente espressa anche l'Unione Europea con l'entrata in vigore



del Digital Operational Reslience Act (DORA) applicata a oltre 22.000 società nell'ambito dei servizi finanziari.

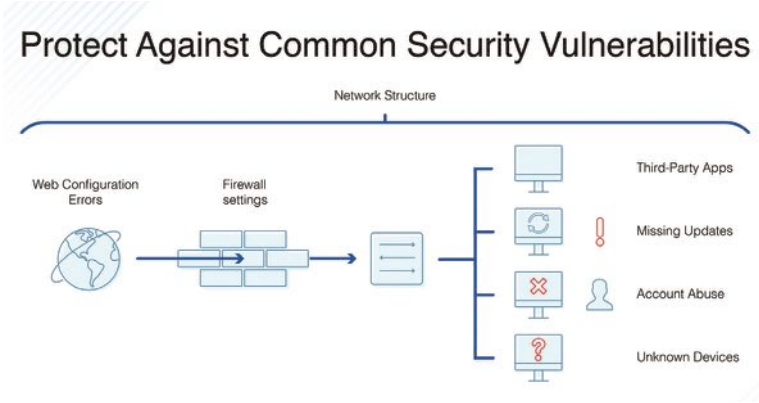
È bene tenere presente che il concetto di esposizione non si ferma alle sole vulnerabilità, ma dal punto di vista dell'attaccante include anche misconfigurazioni e problematiche relative a utenze e permessi che possono essere sfruttate per arrivare a compromettere gli asset critici.

Quali opzioni offre il mercato?

I responsabili della sicurezza hanno a disposizione molteplici opzioni per affrontare la problematica, ma molti di questi approcci hanno delle limitazioni che non permettono di affrontare in modo efficace il problema.

Le classiche attività di Vulnerability Scanning, in rete o tramite agenti, coprono in modo quasi completamente automatico la maggior parte degli asset dell'infrastruttura, ma generano un numero ingestibile di risultati e spesso un elevato numero di falsi positivi.

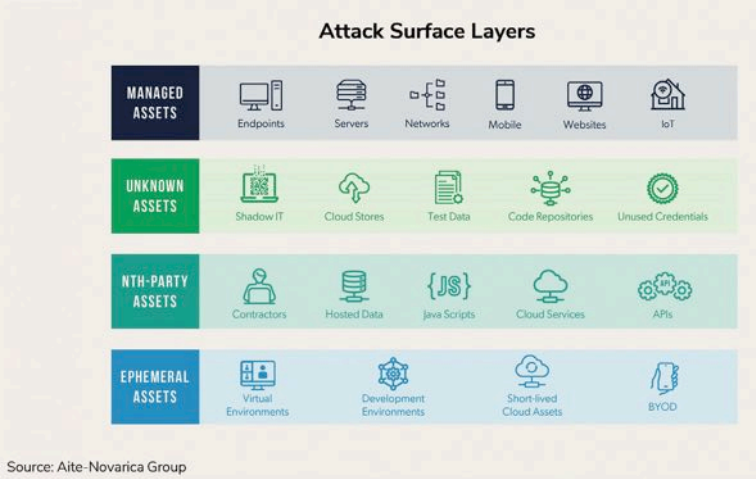
Le attività di Penetration Test manuali forniscono invece risultati accurati ed approfonditi, ma sono spesso limitati ad uno scope molto specifico e



richiedono uno sforzo manuale significativo, che non può quindi essere applicato trasversalmente a tutta l'infrastruttura in modo continuativo.

Soluzioni di Breach and Attack Simulation (BAS) permettono di verificare in modo continuativo e automatico se i controlli di sicurezza implementati sono in grado di identificare e bloccare le minacce note, ma sono limitati a percorsi di attacco prestabiliti e non garantiscono che la copertura sia analoga nel resto dell'infrastruttura.

Le soluzioni di Attack Surface Management sono spesso focalizzate sulle risorse esposte verso l'esterno, che è una parte sicuramente importante, ma non tengono conto della facilità con cui gli attaccanti possano trovarsi già all'interno dell'infrastruttura tramite phishing, compromettendo workstation o addirittura comprando credenziali legittime o asset compromessi sul dark web.



Source: Aite-Novarica Group

Vi sono poi soluzioni specializzate in Penetration Test Automatici, ma seppure eseguiti in modo automatico e continuativo, sono limitati nello scope e considerano solo alcuni punti di partenza e alcune parti dell'infrastruttura durante ogni esecuzione, anziché individuare in modo metodico tutti i possibili percorsi di attacco disponibili ogni giorno da qualsiasi punto di partenza. Inoltre, data la lentezza nell'aggiungere nuovi exploit, il Mean-Time-To-Detect delle esposizioni è più elevato, in quanto devono essere scritti in modo specifico per limitare il più possibile i disservizi e testati adeguatamente, lasciando comunque un rischio residuo di causare disservizi eseguendo exploit reali in ambienti di produzione. L'attività invasiva può lasciare inoltre degli artefatti sfruttabili da attaccanti reali (es: credenziali in cache) e generare molti falsi positivi nei SOC, sovraccaricando le già limitate risorse disponibili.

BIO

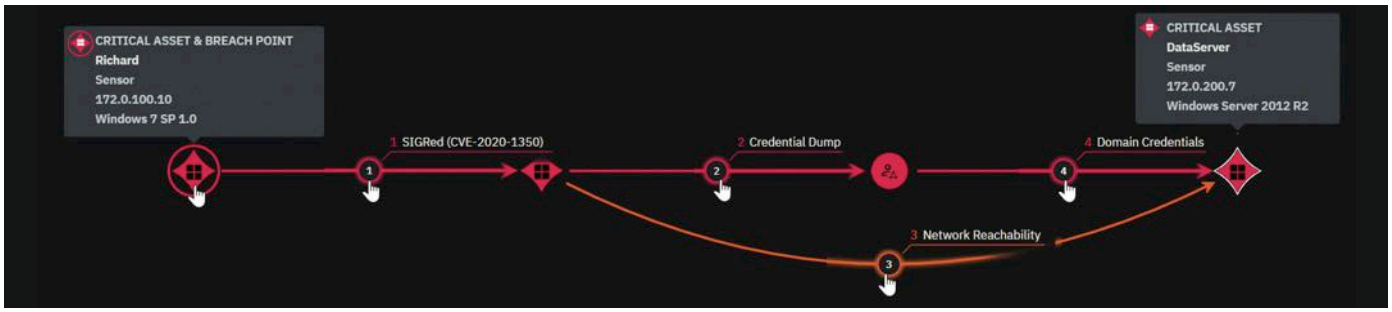
Davide Rivolta è Technical Director per l'Italia in XM Cyber, dove è responsabile per tutte le attività di prevendita e punto di riferimento tecnico per i partner. Da sempre appassionato di cybersecurity, si è laureato nel 2011 in Sicurezza dei Sistemi e delle Reti Informatiche e ha maturato più di 10 anni di esperienza nel settore, lavorando con differenti tecnologie, tra cui Next-Generation e Web-Application Firewalls, strumenti di Vulnerability Assessment, soluzioni anti-APT/Sandbox e soluzioni NAC. Davide ha iniziato la sua carriera come Professional Service Engineer presso un system integrator, maturando esperienza sul campo su varie tecnologie e completando più di 50 deployment su differenti soluzioni, dopodiché ha ampliato le sue soft skill lavorando come Presales Engineer, Channel System Engineer e istruttore certificato per differenti vendor, lavorando presso il distributore Exclusive Networks. Prima di entrare in XM Cyber, Davide è stato Technical Director per Skybox Security, dove ha fortemente ampliato il mercato italiano e reso autonomo il canale dal punto di vista tecnico. Grazie alla sue conoscenze e ruoli ricoperti in molteplici aree della cybersecurity e alla sua forte esperienza sul campo, Davide ha adottato un approccio consulenziale per comprendere le necessità del cliente e fornire le soluzioni ottimali.

Continuous Threat and Exposure Management: un nuovo approccio

Per affrontare in modo olistico la problematica è necessario creare un processo continuo che permetta di identificare i **percorsi di attacco** sfruttabili per raggiungere gli **asset critici** e permetta alle organizzazioni di focalizzarsi sulle esposizioni che comportano un livello di rischio maggiore, indipendentemente che si tratti di misconfigurazioni, utenze a rischio, permessi eccessivi o vulnerabilità.

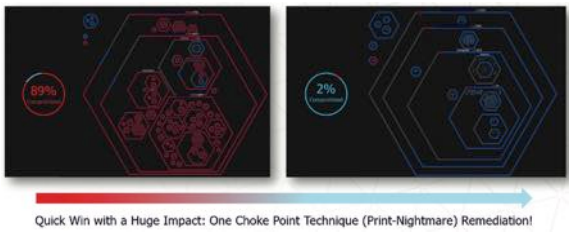
Con questo approccio è possibile simulare in modo continuativo ed automatico tutti i possibili percorsi di attacco che possono portare un attaccante da una compromissione iniziale a compromettere gli asset più critici dell'azienda, senza eseguire attacchi reali sull'infrastruttura e garantendo al tempo stesso la miglior copertura possibile, anche in ambienti hybrid e multi cloud.

Il processo inizia con l'identificazione dei possibili punti di compromissione, come ad esempio utenti o workstation a rischio (in base all'attività o alla mancanza



di adeguata protezione), qualsiasi asset esposto su internet, terze parti e vittime delle campagne di phishing; dopodiché occorre identificare gli asset critici per l'azienda, che possono essere machine, utenze, applicazioni, servizi, ecc. al fine di focalizzare l'attenzione su ciò che è davvero critico per il business.

A questo punto avviene l'identificazione di tutte le possibili esposizioni, come problemi relativi alle identità e ai permessi, vulnerabilità e misconfigurazioni, che una volta correlate tra di loro permettono di costruire un grafo con tutte le possibili combinazioni di attacco. Questa operazione va ovviamente eseguita in modo trasversale su tutta l'infrastruttura, compresi gli ambienti hybrid e multi-cloud.

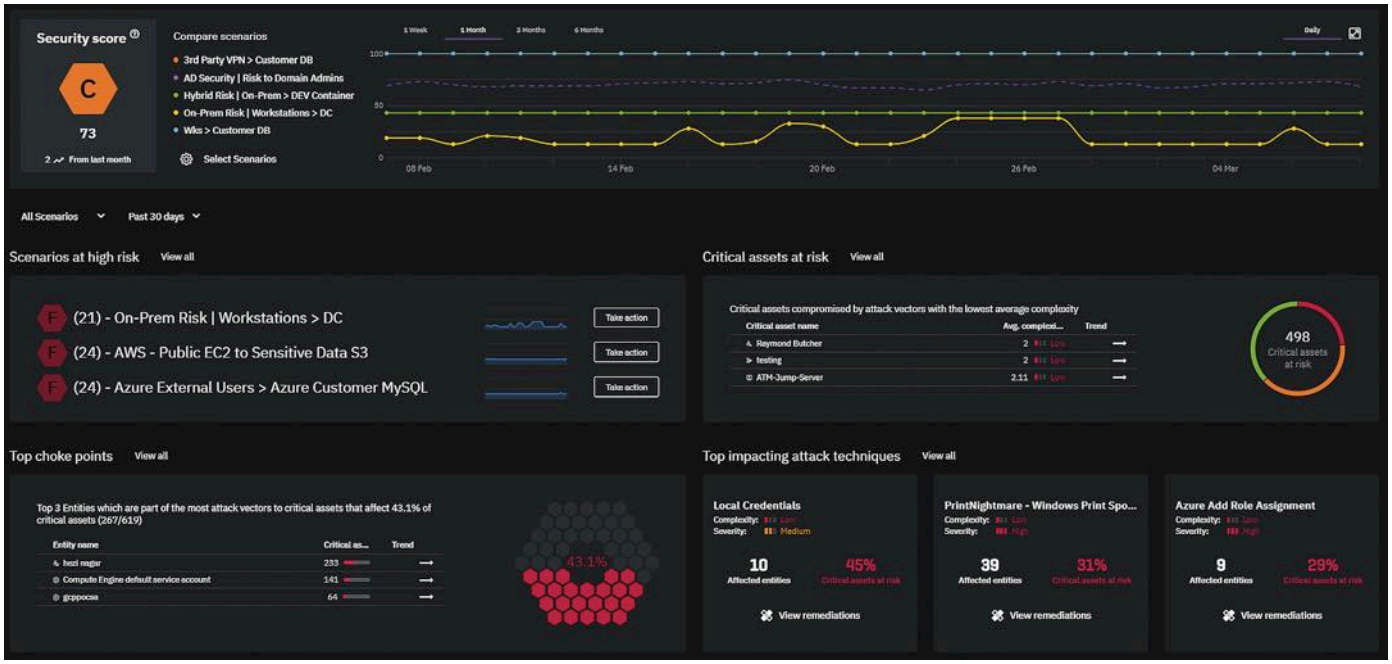


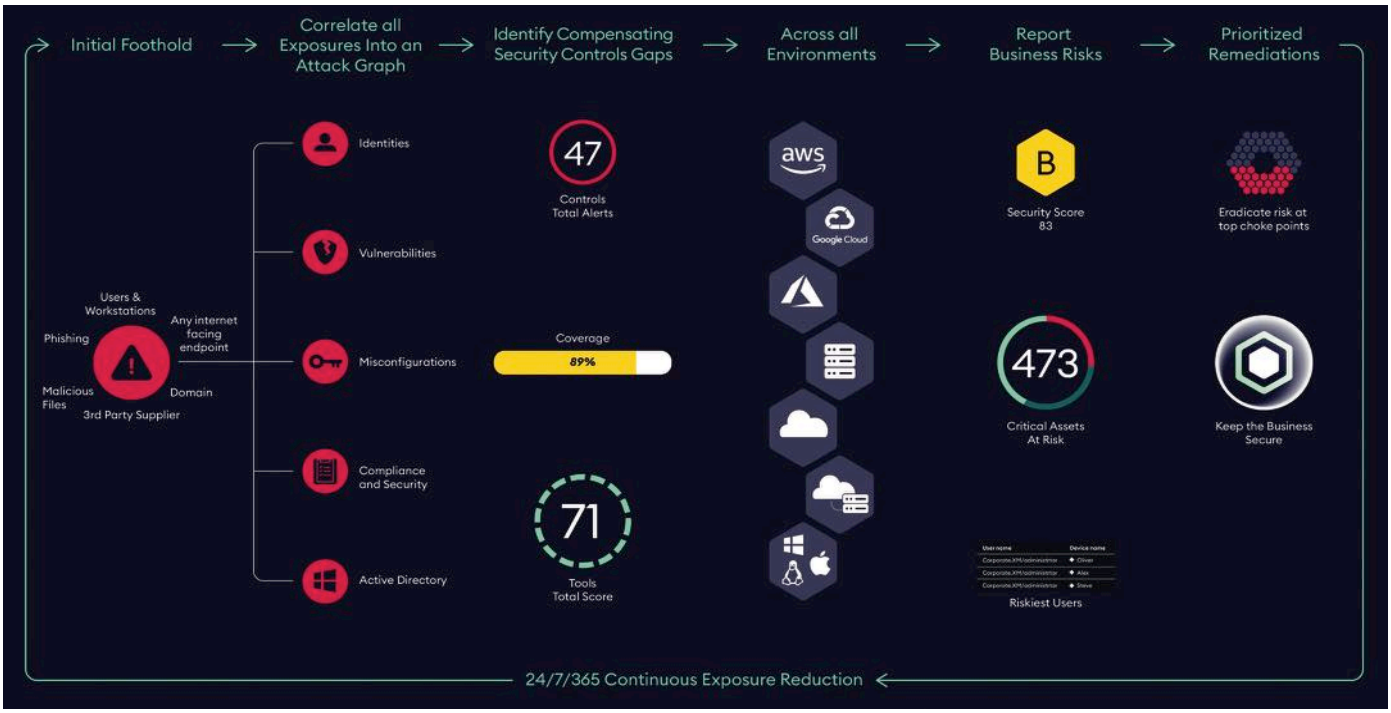
Una volta ottenuto il grafo con tutti i possibili percorsi di attacco, è possibile identificare i **"choke points"**, cioè i colli di bottiglia o strozzature attraverso le quali passano la maggior parte dei percorsi di attacco diretti verso gli asset critici. La corretta identificazione dei "choke points", che può avvenire solo tramite un approccio omnicomprensivo, permette di focalizzare le attività di remediation per ottenere la migliore **riduzione del rischio** con il minor sforzo o numero di azioni, massimizzando così il **ritorno dell'investimento**.

Con questo tipo di visibilità è possibile riportare al board in modo semplice ed efficace il rischio per il business e al tempo stesso ottenere una lista di attività di correttive prioritizzate in base alla loro efficacia in termini di riduzione del livello di rischio e complessità, tramite la quale è possibile instradare correttamente le attività con il sistema di ticketing in uso nell'azienda.

I benefici di questo approccio

Gli obiettivi principali di questo approccio sono la possibilità di rispondere in qualsiasi momento a domande critiche come "Quali minacce comportano il rischio maggiore per la mia azienda?", "Quale azione correttiva fornisce il maggior ritorno dell'investimento?", **"I miei asset critici sono protetti?"**. Un altro obiettivo è individuare con esattezza le esposizioni che devono necessariamente essere rimediate per mantenere sicuro il business e adottare un processo per un monitoraggio automatico e continuo al fine di individuare e ridurre il livello di rischio a fronte delle modifiche che avvengono ogni giorno nell'infrastruttura.





L'azienda che meglio sostiene questo approccio è XM Cyber, che sta aiutando le organizzazioni in tutto il mondo ad adottare questo nuovo approccio al rischio informatico. XM Cyber cambia il modo in cui le aziende gestiscono le esposizioni dimostrando visivamente in che modo gli attaccanti sfruttano e combinano configurazioni errate, vulnerabilità, identità e altro ancora in AWS, Azure, GCP e gli ambienti on-premise allo scopo di compromettere gli asset critici.

XM Cyber consente di visualizzare i vari vettori di attacco e apprendere le best practice per interromperli, individuando con precisione le aree in cui applicare misure correttive con il minimo sforzo. Fondata da alti dirigenti della community di cyber-intelligence israeliana, XM Cyber è presente sul territorio italiano e ha sedi in America del Nord, Europa e Israele.

L'adozione di questo approccio con XM Cyber permette quindi di supportare vari tipi di iniziative, tra cui:

- Hybrid Cloud Security: identificazione delle esposizioni in base alle modifiche, minimizzando il costo legato ai penetration test, controllando se vi sono rischi critici che impattano la trasformazione digitale e riducendo le risorse e le skill necessarie per mitigarli;
- Ransomware Readiness: visualizzazione della superficie di attacco interna per capire il raggio di compromissione di un eventuale ransomware, focalizzazione delle risorse sulle modifiche che impattano maggiormente il rischio, comunicazione al board del rischio per il business;
- Supply Chain e 3rd Party Risk Management: simulazione continua dei possibili attacchi provenienti dalle interconnessioni con le terze parti, identificazione delle esposizioni e delle attività correttive, comunicazione al board del rischio legato alle terze parti;
- Vulnerabiity Prioritization: focalizzazione delle attività correttive per bloccare i percorsi di attacco verso gli asset critici in base all'impatto sul business, ottimizzando le risorse a disposizione;
- Cyber Risk Reporting: quantificazione del livello di cyber risk con semplificazione della reportistica e della comunicazione delle informazioni al board;
- Mergers & Acquisitions: valutazione della postura di sicurezza della società acquistata, riducendo il rischio prima dell'integrazione e simulando continuamente potenziali attacchi sia nel corso dell'integrazione, sia una volta completata;
- OT Security: simulazione continua degli scenari di attacco verso gli strumenti di gestione della rete OT, con verifica della corretta segmentazione dell'infrastruttura e rimozione proattiva dei rischi verso il mondo OT;
- Zero-Day Vulnerability Assessment: rapida valutazione dell'impatto di nuove vulnerabilità eclatanti (es: Log4J), identificando quali occorrenze possono permettere agli attaccanti di compromettere gli asset critici per il business, focalizzando quindi le attività correttive e facilitando la comunicazione del rischio al board.

Da un'analisi condotta da Forrester (Economic Impact of XM Cyber Exposure Management Platform) l'approccio con XM Cyber è risultato vincente anche in termini economici, fornendo un ROI del 394%, dato da una riduzione dei costi associati alle attività correttive, multe, perdita di business e brand reputation, da una riduzione dei costi legati alle attività di penetration test manuali e da una riduzione del 90% della probabilità di subire un attacco agli asset critici dell'azienda. ■

Un Approccio Ibrido tra i Requisiti Cyber e il Framework TIBER-EU.

Autore: Jelena Zelenovic Matone

Il crescente numero di minacce cyber e la carenza di professionisti della cybersecurity indica che le organizzazioni devono essere proattive nel loro approccio alla cybersecurity. I professionisti della cybersecurity devono adottare un approccio a più livelli che includa: controlli, normative, direttive e test per ridurre al minimo il rischio di attacchi cyber.

Inoltre, il panorama della cybersecurity sta cambiando rapidamente e le organizzazioni devono rimanere aggiornate con gli ultimi trend, minacce e best practice. Ad esempio, il cloud computing ha introdotto nuovi rischi e sfide, tra cui la protezione dell'infrastruttura e dei dati basati su cloud. L'Internet of Things (IoT) è un altro settore che ha prodotto nuove vulnerabilità man mano che sempre più dispositivi si connettono a internet. E poi con l'edge computing sorge un altro rischio significativo, come i data breach. E potremmo continuare.

Di conseguenza, i professionisti della cybersecurity devono adottare un approccio flessibile e agile, aggiornando continuamente le proprie competenze e conoscenze per stare al passo con le ultime minacce cyber. Ciò richiede un impegno costante per favorire la formazione, l'istruzione e lo sviluppo professionale.

Inoltre, da tempo abbiamo visto (compreso) che le organizzazioni devono dare priorità alla cybersecurity ai più alti livelli del management. Non è più un argomento tabù nei consigli di amministrazione, ma uno dei maggiori rischi di qualsiasi organizzazione. I dirigenti e i membri del consiglio di amministrazione devono comprendere i rischi e avere un ruolo attivo nello sviluppo e nell'attuazione di una strategia di cybersecurity. La strategia di cybersecurity include l'allocazione delle risorse, del budget e del personale

necessari per salvaguardare i sistemi e i dati critici. Tutte le sfide che, più o meno, tutti noi attualmente dobbiamo affrontare.

La cybersecurity è un aspetto cruciale delle organizzazioni moderne. Man mano che la dipendenza dalla tecnologia continua a crescere, aumenta anche il rischio di attacchi informatici. Inoltre, una maggiore attenzione alla cybersecurity da parte degli alti livelli del management è fondamentale per garantire che le organizzazioni possano proteggere efficacemente i propri sistemi e dati.

Approfondire controlli, standard, regolamenti e direttive

Consapevoli che la frequenza e la gravità degli attacchi informatici continuano ad aumentare, è sempre più evidente che i controlli cyber e gli standard IT da soli potrebbero non essere sufficienti per proteggere le organizzazioni da minacce sofisticate e persistenti. Oltre a implementare una solida serie di controlli cyber, le organizzazioni devono anche assicurarsi di testare e aggiornare regolarmente le proprie misure di sicurezza per stare al passo con le minacce in evoluzione. Ciò comporta l'esecuzione combinata di assessment vulnerability, penetration testing e Red Teaming, nei quali vengono condotti attacchi simulati per identificare i punti deboli nelle difese di un'organizzazione.

Inoltre, le organizzazioni devono dare priorità alla cybersecurity awareness e alla formazione per tutti i dipendenti, perché l'errore umano e il comportamento negligente possono contribuire in modo significativo alle violazioni della sicurezza. La security awareness può aiutare i dipendenti a identificare ed evitare truffe di phishing e attacchi di social engineering.

Infine, le organizzazioni devono restare informati sulle tendenze e sulle best practice della cybersecurity. Ciò significa tenersi aggiornati sulle novità del settore e partecipare a conferenze e programmi di formazione per conoscere i nuovi tool e le tecniche per la protezione dalle minacce cyber. Le organizzazioni possono ridurre significativamente il rischio di un devastante data breach adottando un approccio proattivo e olistico alla cybersecurity.

Iniziamo da ISO, NIST, GDPR, NIS e NIS2

Con l'aumento delle minacce cyber, le aziende sono alla ricerca di modi per proteggere sé stessi e i dati dei propri clienti. Un modo per raggiungere

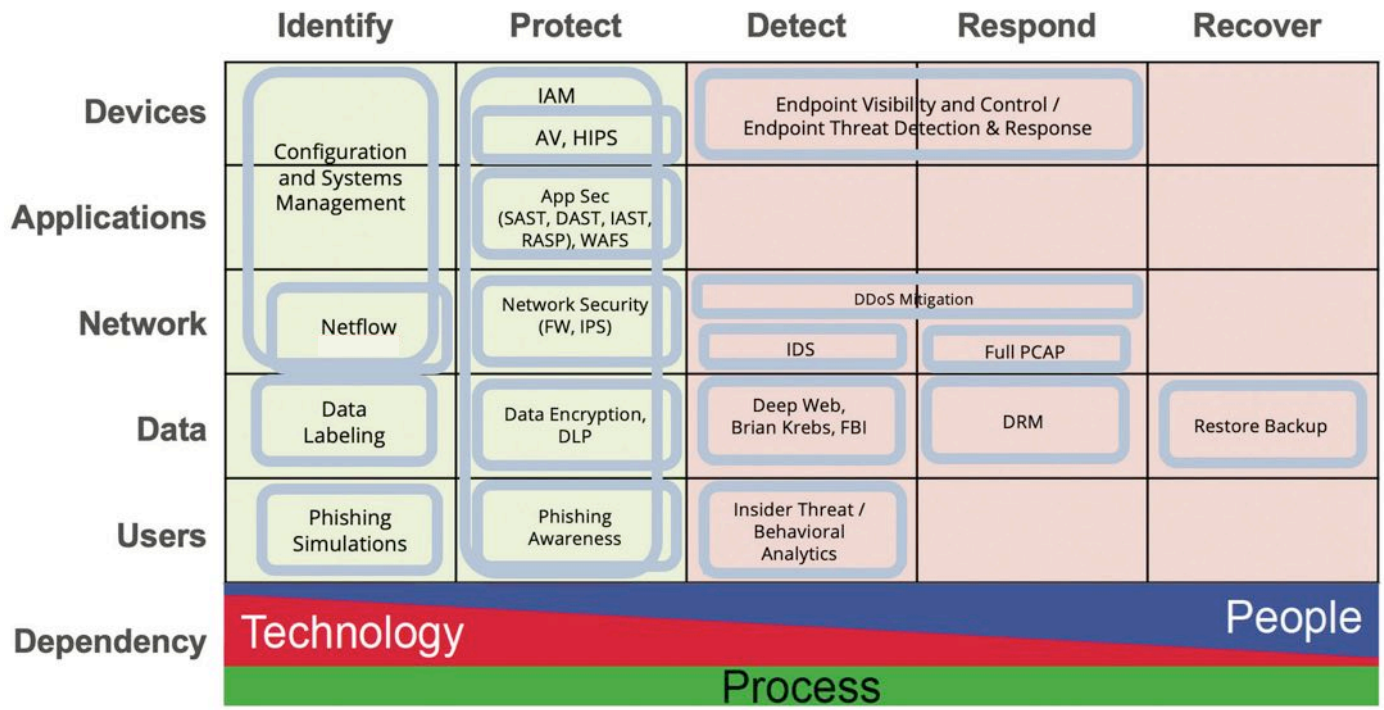
BIO

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.

questo obiettivo è seguire gli standard di cybersecurity come l'International Organization for Standardization (ISO) 27001 e il National Institute of Standards and Technology (NIST) Cybersecurity Framework.

ISO 27001 è uno standard ampiamente riconosciuto che fornisce controlli e processi completi per gestire la sicurezza delle informazioni. Lo standard comprende la gestione dei rischi critici, il controllo degli accessi e la gestione degli incidenti. Seguendo questo standard, le organizzazioni possono stabilire un approccio sistematico alla gestione della sicurezza delle informazioni, la quale può essere ulteriormente rafforzata ottenendo la certificazione ISO.

NIST Cybersecurity Framework è un insieme di linee guida incentrate sulla riduzione e la gestione dei rischi della cybersecurity. Il framework fornisce un approccio



basato sul rischio incentrato su cinque funzioni principali: identificazione, protezione, rilevamento, risposta e ripristino. Seguendo questo framework le organizzazioni possono stabilire un linguaggio comune per segnalare i rischi e sviluppare un approccio flessibile e adattabile alla gestione della cybersecurity.

La Cyber Defense Matrix, sviluppata da un rispettato collega, è uno strumento utile che integra il NIST Cybersecurity Framework. Questo framework fornisce un costrutto logico che aiuta i professionisti a organizzare i loro sforzi per la cybersecurity. Utilizzando questo framework, possono individuare rapidamente quali prodotti di sicurezza risolvono particolari problemi e comprendere le funzioni principali di ciascun prodotto.

Seguendo questi standard di cybersecurity, le organizzazioni possono rafforzare la propria postura di sicurezza e mitigare i rischi associati alle minacce cyber. I framework di cybersecurity ISO 27001 e NIST forniscono una serie completa di controlli e processi che le organizzazioni possono utilizzare per gestire sistematicamente la sicurezza delle informazioni. La Cyber Defense Matrix integra ulteriormente il framework NIST fornendo un costrutto logico che i professionisti possono utilizzare per organizzare i loro sforzi di cybersecurity.

Inoltre, l'Unione Europea ha adottato diverse misure per migliorare la cybersecurity e proteggere le infrastrutture critiche. Uno di questi regolamenti è il General Data Protection Regulation (GDPR), che mira a garantire la protezione dei dati e gli standard sulla privacy. Invece, la direttiva sulle reti e sui sistemi informativi (NIS) è un altro regolamento efficace che

stabilisce i requisiti minimi di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali.

Questo regolamento ha svolto un ruolo cruciale nel migliorare la cybersecurity all'interno dell'Unione europea. Ai sensi della direttiva NIS, le organizzazioni sono tenute ad attuare varie misure di sicurezza per salvaguardare i propri sistemi dagli attacchi informatici. Queste misure includono l'implementazione di procedure di gestione degli incidenti, svolgere periodicamente valutazioni del rischio, test e aggiornamenti dei propri sistemi di sicurezza.

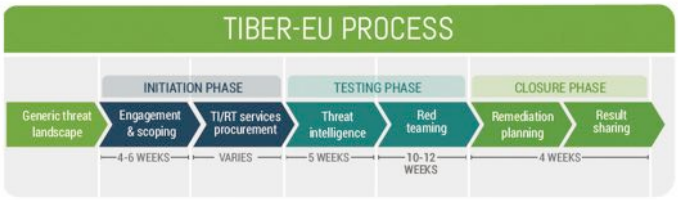
La direttiva NIS2 richiede alle organizzazioni di stabilire una serie completa di misure di sicurezza per prevenire e rispondere agli attacchi informatici. Inoltre, impone alle organizzazioni di segnalare sistematicamente gli incidenti di sicurezza significativi alle rispettive autorità nazionali. Inoltre, la Direttiva NIS2 che si basa sulla Direttiva NIS, migliora ulteriormente le misure di sicurezza che le organizzazioni devono implementare.

Questi regolamenti stabiliscono vari requisiti di sicurezza per le organizzazioni e hanno svolto un ruolo fondamentale nel mitigare le minacce informatiche dei rispettivi paesi.

Sebbene tutti questi controlli svolgano un ruolo fondamentale nella protezione delle infrastrutture critiche e nella riduzione del rischio di attacchi informatici, ci si chiede se è sufficiente. La maggior parte degli esperti risponderà che abbiamo bisogno ancora di altro. Implementando standard come ISO 27001, NIST Cybersecurity Framework, NIS Directive e NIS2, le organizzazioni possono migliorare la loro resilienza informatica e proteggere meglio i loro sistemi informativi, questo è certo. Le organizzazioni che adottano un approccio proattivo alla sicurezza informatica e valutano e aggiornano regolarmente i propri controlli, saranno meglio preparate a proteggersi dalle minacce informatiche. Tuttavia, pongo nuovamente la domanda: È sufficiente? Quanti controlli mi permetteranno di dire di essere protetto se non applico un approccio "ibrido" ai miei test? E anche in questo caso, nessun rischio può essere mitigato al 100%. Tuttavia, dobbiamo sforzarci di fare di più.

Sebbene tutte le procedure menzionate in precedenza forniscano una solida base per la sicurezza informatica, è necessario altro per preparare le organizzazioni a contrastare le minacce in continua evoluzione. È qui che entra in gioco TIBER-EU (Threat Intelligence-Based Ethical Red Team Exercises).

Qualcuno potrebbe chiedere: "Ma qual è la differenza tra i penetration test e il framework TIBER-EU? Perché dovrei spendere tempo e risorse dell'organizzazione in questo test?"



Molti professionisti stanno già eseguendo attivamente penetration test, noti anche come "pen test", attacchi informatici simulati che valutano la sicurezza dei sistemi informativi di un'organizzazione. Questi test sono essenziali per qualsiasi organizzazione per comprendere le vulnerabilità dei propri sistemi e identificare le aree che necessitano di miglioramenti. È qui che un team di esperti di sicurezza utilizza varie tecniche per penetrare nel sistema specifico, incluso lo sfruttamento delle vulnerabilità. L'obiettivo di un pen test è fornire una valutazione realistica della postura di sicurezza di un'organizzazione. Tuttavia, TIBER-EU, almeno per me, fornisce un livello aggiuntivo e una simulazione "step-up". Sebbene i pen test supportino una strategia globale di sicurezza informatica, è necessario di più. L'UE ha istituito il programma TIBER-EU per fornire una valutazione completa della cybersicurezza al di là del tradizionale pen test. TIBER-EU è progettato per aiutare le organizzazioni a identificare e mitigare i rischi informatici valutando in modo completo la loro postura in materia di sicurezza informatica.

Alcune informazioni interessanti su TIBER-EU

Prima di iniziare, ecco alcune rapide informazioni su TIBER-EU:

TIBER-EU è l'acronimo di "Threat Intelligence-Based Ethical Red Teaming - European Union".

Il framework è stato sviluppato in risposta alla crescente minaccia di attacchi informatici alle istituzioni finanziarie e per aiutare queste istituzioni a identificare e affrontare le vulnerabilità nelle loro difese informatiche.

Il framework è progettato per essere flessibile e adattabile alle esigenze specifiche dei singoli istituti finanziari. Può essere personalizzato in base alle dimensioni, alla complessità e al profilo di rischio cyber dell'istituto.

Il framework TIBER-EU prevede una serie di attacchi informatici controllati e personalizzati progettati per simulare attacchi informatici nel mondo reale.

Il framework TIBER-EU è comunque su base volontaria e le istituzioni finanziarie possono scegliere di sottoporsi a un test a loro discrezione.

I test TIBER-EU sono condotti da fornitori di terze parti indipendenti e coordinate internamente con i White e Blue Team.

Il test coinvolge tre Team importanti: il White Team, il Blue Team e il Red Team.

White Team: il White Team è responsabile della progettazione e della supervisione del test, della creazione degli scenari e degli obiettivi, del monitoraggio dei progressi e della guida degli altri team.

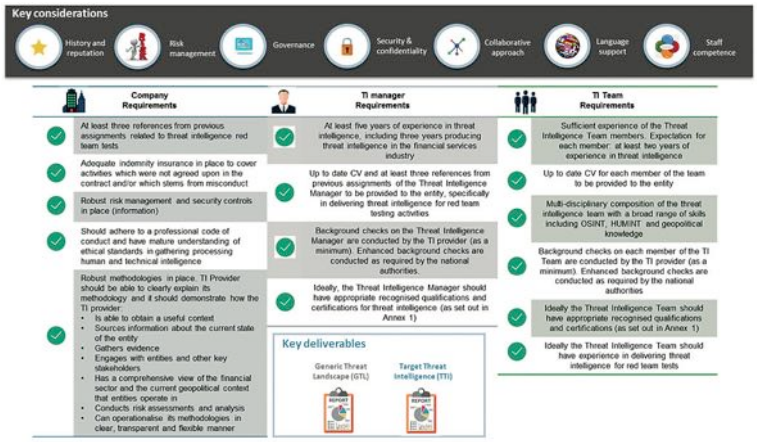
Blue Team: il Blue Team è il difensore in questo test. Il suo ruolo è proteggere i sistemi, le reti e i dati dagli attacchi del Red Team. I membri sono responsabili dell'implementazione dei controlli di sicurezza, del monitoraggio dei sistemi per le vulnerabilità e della risposta agli incidenti utilizzando la loro esperienza di sicurezza informatica. Il Blue Team aiuta a identificare e correggere eventuali punti deboli nella postura di sicurezza del sistema.

Red Team: il Red Team è l'attaccante nel test. Il suo ruolo è simulare attacchi cyber nel mondo reale e testare l'efficacia delle difese del Blue Team. I membri usano le loro conoscenze dell'hacking e del social engineering

per individuare vulnerabilità nel sistema e sfruttarle al fine di raggiungere i loro obiettivi.

TIBER-EU

TIBER EU è un'iniziativa dell'UE abbastanza nuova, volta a migliorare la resilienza del settore finanziario dell'UE alle minacce informatiche. A differenza dei tradizionali penetration test e degli esercizi del Red Team, TIBER-EU si concentra sulla verifica della capacità delle istituzioni finanziarie di rilevare e rispondere alle minacce informatiche del mondo reale. Mira a fornire un approccio completo alla cybersecurity, coprendo tutte le fasi del ciclo di vita dell'attacco e simulando minacce persistenti avanzate. TIBER-EU è progettato per valutare in modo completo la postura di cybersecurity di un'organizzazione, coprendo molte aree, tra cui la sicurezza fisica, logica e organizzativa; inoltre è stato progettato per essere più completo rispetto ai tradizionali pen test andando oltre la semplice identificazione delle vulnerabilità. Fornisce, invece, una visione completa della postura di sicurezza di un'organizzazione e del potenziale impatto di un attacco informatico.



I vantaggi di utilizzare TIBER-EU sono numerosi. In primo luogo, un tale esercizio aiuta le organizzazioni a identificare le falle nelle loro attuali difese di sicurezza informatica e consente loro di testare e migliorare le loro procedure di risposta agli incidenti. Inoltre, la partecipazione a TIBER-EU consente a un'organizzazione di dimostrare il proprio impegno per la sicurezza informatica a clienti, organi di controllo e stakeholder, il che può migliorare la propria reputazione e creare fiducia nel proprio brand.

Come affermato, le organizzazioni possono trarre vantaggio dalle esercitazioni TIBER-EU testando la loro capacità di rilevare, rispondere e contrastare le minacce informatiche, migliorando così la loro postura di sicurezza informatica. Ecco alcuni esempi di quali enti potrebbero trarre vantaggio dall'utilizzo degli esercizi TIBER-EU:

1 Istituzioni finanziarie: forse obiettivo principale degli attacchi informatici. Le esercitazioni TIBER-EU possono aiutare queste istituzioni a identificare potenziali punti deboli nei loro sistemi e processi e migliorare la loro capacità di rilevare e rispondere alle minacce informatiche.

2 Organizzazioni sanitarie: gestiscono informazioni sanitarie riservate e sensibili e sono ad alto rischio di attacchi informatici. Gli esercizi TIBER-EU possono aiutare queste organizzazioni a valutare la loro capacità di proteggere i dati dei pazienti e garantire la conformità con HIPAA, GDPR, ecc.

3 Aziende di vendita al dettaglio e di e-commerce: gestiscono grandi quantità di informazioni riguardanti clienti e transazioni finanziarie, rendendole un bersaglio per i criminali informatici. Le esercitazioni TIBER-EU possono aiutare queste aziende a identificare le vulnerabilità nei loro sistemi e migliorare la loro capacità di rilevare e rispondere agli attacchi informatici.

4 Agenzie governative: gestiscono informazioni sensibili e riservate e sono ad alto rischio di attacchi informatici. Gli esercizi TIBER-EU possono aiutare queste agenzie a valutare la loro capacità di proteggere le informazioni sensibili e garantire la conformità alle normative.

5 Società energetiche e di servizi pubblici: controllano le infrastrutture critiche, rendendole un bersaglio per i criminali informatici. Le esercitazioni TIBER-EU possono aiutare queste società a valutare la loro capacità di rilevare e rispondere agli attacchi informatici e garantire il funzionamento delle infrastrutture critiche.

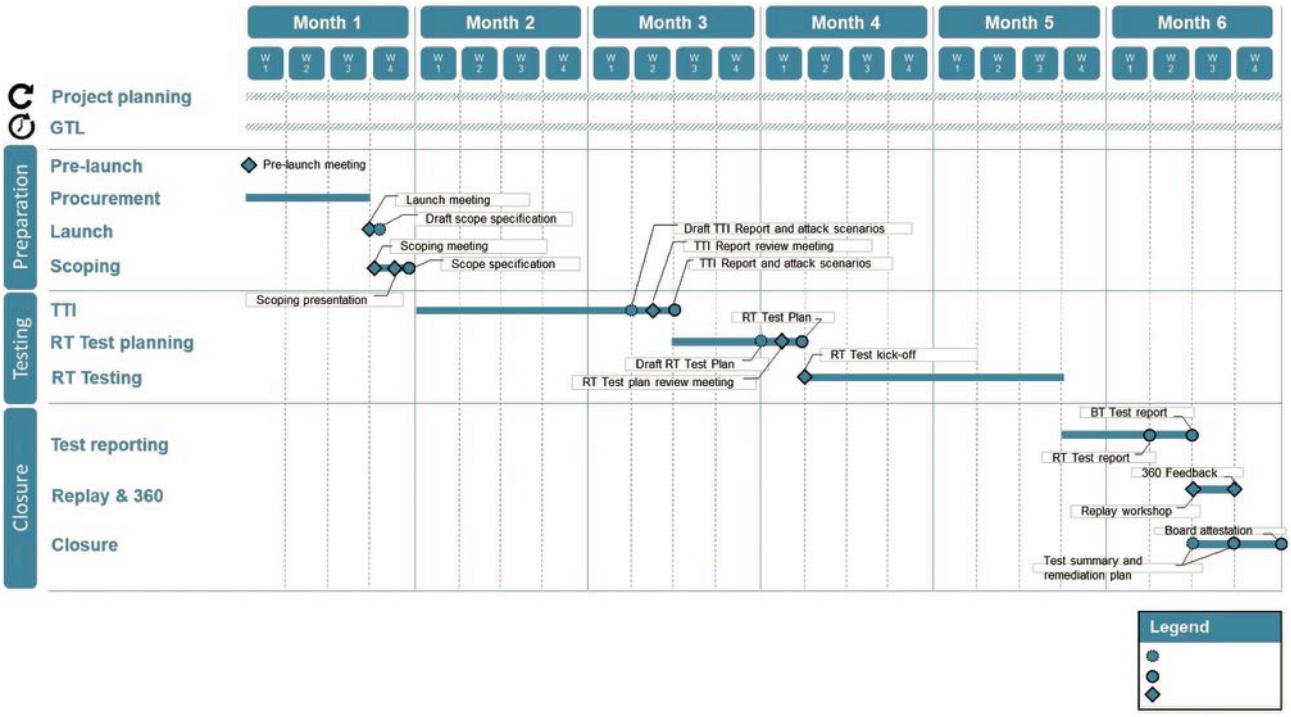
Perché è necessario sottoporsi a un test TIBER-EU?

Come accennato in precedenza, TIBER-EU può aiutare le organizzazioni a valutare la loro postura della sicurezza informatica e a identificare le aree che richiedono attenzione e miglioramento. Il carattere complessivo di TIBER-EU lo rende uno strumento efficace per le organizzazioni per comprendere la loro situazione generale di sicurezza e identificare le aree che necessitano di miglioramenti. TIBER-EU fornisce inoltre alle organizzazioni un punto di riferimento rispetto al quale possono confrontare il proprio livello di sicurezza rispetto ad altre organizzazioni del loro settore.

Le diverse fasi del processo da prendere in considerazione durante l'esercitazione TIBER-EU:

1 Preparation: durante questa fase, l'organizzazione si prepara per il test TIBER-EU, compreso lo sviluppo di un piano di test dettagliato e l'identificazione di sistemi e dati critici. La fase di preparazione potrebbe includere anche il rapporto sul panorama delle minacce in termini generali in modo che tutti i soggetti coinvolti sappiano quali minacce attuali sono specifiche, ad esempio, per un particolare settore o paese. Da lì si potrebbe creare uno specifico panorama delle minacce, molto specifico per i controlli e le attività attuali dell'organizzazione. Questa fase include anche una corretta gestione del progetto, i ruoli e le linee di comunicazione giusti e i vari piani d'azione di cui si occuperà il Red Team.

Di seguito alcuni esempi di tipi di attacchi che possono essere utilizzati per simulare gli attacchi del Red Team TIBER-EU. Tuttavia, bisogna tenere in considerazione lo specifico contesto della tua organizzazione e il panorama delle minacce che deve affrontare.



- Attacchi di rete: il Red Team può utilizzare la scansione delle porte, la scansione delle vulnerabilità e lo sfruttamento di sistemi privi di patch per ottenere l'accesso non autorizzato alla rete dell'organizzazione.
- Attacchi di social engineering: il Red Team può utilizzare e-mail di phishing, telefonate o altre tattiche per indurre i dipendenti a divulgare informazioni sensibili o scaricare software dannoso.
- Violazioni della sicurezza fisica: il Red Team può tentare di accedere ai locali fisici dell'organizzazione sfruttando i punti deboli della sicurezza, ad esempio seguendo un dipendente o fingendosi un addetto alle consegne.
- Attacchi interni: il Red Team può tentare di accedere a dati sensibili prendendo di mira i dipendenti con accesso a sistemi o informazioni critici.
- Minacce persistenti avanzate (APT): il Red Team può simulare un attacco persistente e sofisticato contro l'organizzazione, utilizzando una combinazione di tattiche e tecniche per eludere il rilevamento e mantenere la persistenza nella rete.

2 Assessment: durante questa fase, il team di TIBER-EU valuta in modo completo la postura di sicurezza dell'organizzazione. Ciò include una serie di attività. Ci si potrebbe aspettare solo test tecnici, ma come ho detto prima è anche utile prestare attenzione ai test di sicurezza fisica. Inoltre, aspetti essenziali sono l'esecuzione di attacchi simulati di social engineering attraverso test fisici e tecnologici. Vorrei sottolineare un aspetto molto importante: il White Team deve assicurare una comunicazione costante con i Blue e Red Team. È, inoltre, importante assicurare che il test si svolga senza problemi da entrambe le parti e che, dove necessario, il flusso di comunicazione sia sempre efficace e trasparente.

3 Evaluation: durante questa fase, il team TIBER-EU valuta i risultati del test e identifica le aree che necessitano di miglioramenti. L'obiettivo è valutare l'efficacia della simulazione del Red Team e identificare eventuali aree di miglioramento. Gli alti rischi devono essere segnalati immediatamente ai responsabili dei team non appena vengono scoperti. L'analisi dei risultati è necessaria per identificare eventuali lacune o punti deboli nelle difese informatiche dell'organizzazione e nei piani di risposta agli incidenti. Tali falle possono comportare rischi alti per le organizzazioni. Pertanto, i rischi alti non devono essere solo segnalati, ma dovrebbero essere trattati il prima possibile. L'esecuzione di sessioni di debriefing è di fondamentale importanza in questa fase. Tale debriefing dovrebbe includere tutti i partecipanti, i Blue e White Team. Ciò consente ai team di capire cosa ha funzionato bene e cosa potrebbe essere migliorato. Valutare i tempi di risposta del Blue Team è un'altra questione che dovrebbe essere discussa. Ad esempio, se il tempo di risposta è stato lento, dovremmo individuare il motivo, identificare la causa principale e assicurarci di segnalare alle persone giuste.

Ecco alcune potenziali idee KRI che potrebbero essere impostate per valutare l'efficacia del test TIBER-EU:

- Tempo di rilevamento: la misurazione del tempo necessario affinché un attacco del Red Team venga rilevato dal Blue Team può aiutare a identificare i punti deboli nelle capacità di rilevamento di un'organizzazione.

- Tempo di risposta agli incidenti: misurare il tempo impiegato da un'organizzazione per rispondere a un attacco simulato può aiutare a identificare potenziali gap nelle procedure di risposta agli incidenti.

- Gestione delle vulnerabilità: il monitoraggio del numero e della gravità delle vulnerabilità identificate durante gli esercizi di Red Team può aiutare a identificare potenziali aree di debolezza che devono essere affrontate.

- Consapevolezza dei dipendenti: misurare l'efficacia della formazione sulla security awareness dei dipendenti può aiutare a identificare potenziali gap nella comprensione e nel comportamento che gli aggressori potrebbero sfruttare.

- Postura del rischio: misurare la postura del rischio complessiva di un'organizzazione prima e dopo un esercizio di Red Teaming può aiutare a valutare l'efficacia delle misure di sicurezza e identificare le aree di miglioramento.

- Tattiche, tecniche e procedure degli attori delle minacce (TTP): il monitoraggio dei TTP utilizzati dagli attori delle minacce simulate durante un esercizio di Red Teaming può aiutare le organizzazioni a comprendere meglio i potenziali attacchi del mondo reale.

- Tasso di successo: misurazione del tasso di successo di un esercizio di Red Teaming può aiutare a valutare l'efficacia complessiva delle misure di sicurezza e identificare le aree di miglioramento.

Ovviamente, la selezione di KRI specifici dipenderà dagli obiettivi specifici dell'esercitazione e dalla natura degli attacchi simulati.

4 Recommendation: durante questa fase, il Red Team fornisce raccomandazioni per migliorare la postura di sicurezza dell'organizzazione, insieme a discussioni precedenti con i team operativi (principalmente il Blue Team) sul campo, quelle che proteggono quotidianamente le nostre preziose informazioni. I piani di remediation dovrebbero identificare i compiti e le responsabilità di ciascun team coinvolto in questa fase. Inoltre, dovrebbe essere seguito uno stretto monitoraggio del White Team per garantire che i punti deboli identificati vengano affrontati in modo efficace.

La frequenza con cui le organizzazioni dovrebbero praticare i test TIBER-EU dipende da molti fattori. Tuttavia, alcuni di quelli importanti sono le dimensioni e la complessità dell'organizzazione, il livello di minaccia e il profilo di rischio complessivo dell'organizzazione.

Alcune organizzazioni conducono il test una volta ogni due anni, anche se possono essere necessarie esercitazioni più frequenti per le organizzazioni che operano in ambienti ad alto rischio o con sistemi informativi complessi. Inoltre, si raccomanda alle organizzazioni di incorporare TIBER-EU nei loro processi standard di gestione del rischio, utilizzando i risultati delle esercitazioni di TIBER-EU per informare le loro valutazioni del rischio in corso e le procedure di risposta agli incidenti.

Poiché in molti casi utilizziamo i penetration test, le organizzazioni potrebbero ora prendere in considerazione l'esecuzione di test TIBER-EU dopo modifiche significative ai loro sistemi informativi, come l'implementazione di nuove tecnologie o l'introduzione di nuovi processi aziendali. Ciò può aiutare a garantire che le loro difese di sicurezza informatica rimangano aggiornate ed efficaci di fronte alle minacce in continua evoluzione.

Lo svolgimento regolare delle esercitazioni TIBER-EU può aiutare le organizzazioni a identificare le falle nelle loro difese di sicurezza informatica, migliorare le loro procedure di risposta agli incidenti e migliorare la loro resilienza informatica complessiva. La frequenza con cui le organizzazioni dovrebbero praticare le esercitazioni TIBER-EU dipende da diversi fattori. Le organizzazioni dovrebbero valutare il proprio profilo di rischio, la propensione al rischio definita dal management e il livello di minaccia per determinare la frequenza appropriata delle esercitazioni TIBER-EU.

Mappare le best practice sul framework TIBER-EU

D'altro canto, mappando questi regolamenti, direttive e quadri su una esercitazione TIBER-EU, è possibile garantire che la postura di cybersecurity sia in linea con i requisiti legali e normativi e le best practice, da qui i modi "ibridi" e creativi di difendere un'organizzazione:

1 Control Objectives for Information and Related Technology (COBIT): un framework per la governance e la gestione dell'IT che fornisce una serie completa di best practice per la gestione delle informazioni e della tecnologia.

2 General Data Protection Regulation (GDPR): le regole per la protezione dei dati personali e si applicano alle organizzazioni che trattano tali dati.

3 Network and Information Systems (NIS): mira a migliorare la sicurezza delle reti e dei sistemi informativi e si applica agli operatori di servizi essenziali e ai fornitori di servizi digitali.

4 La Cybersecurity Act mira a migliorare la resilienza e la cybersicurezza dell'UE e a garantire un elevato livello di sicurezza delle reti e dei sistemi informativi.

5 Payment Services Directive (PSD2): stabilisce le regole per i servizi di pagamento e si applica ai prestatori di servizi di pagamento e agli intermediari.

6 NIST Cybersecurity Framework (CSF): framework sviluppato dal National Institute of Standards and Technology (NIST) per aiutare le organizzazioni a gestire e ridurre i rischi di sicurezza informatica.

7 ISO/IEC 27001: uno standard internazionale per i sistemi di gestione della sicurezza delle informazioni (ISMS) che fornisce un quadro per implementare, mantenere e migliorare continuamente la sicurezza delle informazioni.

Alcune cose da FARE e da non FARE:

FARE:

1 Assicurati di pianificare accuratamente il test in anticipo, inclusa lo scopo della tua organizzazione, quindi traducilo in ambito, obiettivi ed elementi attuabili, con una tabella di marcia chiara e i risultati desiderati.

2 Coinvolgere le parti interessate e i relativi team nel test. In primo luogo, ottenere il consenso dal management, quindi dal team di sicurezza IT (Blue Team), dal team di risposta agli incidenti e dal team della business continuity.

3 Definire i ruoli e le responsabilità per ogni membro del team e mapparli sulle attività previste. Assicurarsi che le capacità dei membri del team siano coerenti alle attività previste, garantendo l'efficienza del test.

4 Importante: documentare e analizzare i risultati del test per identificare le aree di miglioramento e sviluppare piani attuabili, insieme al team di progetto e agli stakeholder sopra menzionati.

5 Assicurarsi di utilizzare scenari e metodi di attacco realistici e applicabili. Per far questo è necessario far riferimento al panorama delle minacce e a ciò che preoccupa maggiormente la tua organizzazione per testare le capacità di difesa e risposta dell'organizzazione.

NON FARE:

1 Ricordarsi di non compromettere la riservatezza, l'integrità o la disponibilità delle informazioni o dei sistemi dell'organizzazione. Lo scopo non è sfruttare le debolezze e le vulnerabilità o interrompere in alcun modo le attività aziendali.

2 Assicurarsi di non interferire con le attività aziendali critiche o compromettere la sicurezza di qualsiasi persona. Simula gli attacchi reali ma assicurati che non venga arrecato alcun danno alla business continuity o alla sicurezza fisica di qualcuno.

3 Ricordarsi di non tentare di accedere, alterare o compromettere alcuna informazione o sistema senza la dovuta autorizzazione. Se stai per farlo o stai eseguendo test su informazioni sensibili, informa il management e allineati su cosa puoi fare e fino a che punto puoi arrivare.

4 Non essere troppo tranquilli: le organizzazioni che si sottopongono a un test TIBER-EU e lo superano possono pensare di essere completamente al sicuro contro gli attacchi informatici, il che potrebbe portare all'autocompiacimento e all'incapacità di continuare a investire nelle loro difese di cybersecurity.

5 Non sottovalutare il costo: il processo del test TIBER-EU può essere costoso e gli istituti finanziari più piccoli potrebbero aver bisogno di più risorse per sottoporsi a un test.

6 Non ignorare o archiviare i risultati del test. Analizza seriamente i risultati e utilizzali con gli stakeholders interessati per migliorare la postura di sicurezza.

7 Ricorda, come con qualsiasi altro test, questo è un processo continuo e che il panorama delle minacce cambia, i controlli possono diventare obsoleti e le competenze possono diventare irrilevanti. Pertanto, bisogna eseguire regolarmente il test TIBER-EU per mantenere la postura di sicurezza dell'organizzazione aggiornata e pertinente. Questo vale sia per gli aspetti tecnici che per quelli relativi alle risorse.

La cybersecurity è un problema fondamentale nell'attuale era digitale, poiché la frequenza e la sofisticazione degli attacchi informatici continuano a crescere. Di conseguenza, le organizzazioni di tutte le dimensioni sono sottoposte a crescenti pressioni per garantire che i propri sistemi informativi siano sicuri e protetti da attività dannose. Il futuro del framework TIBER-EU continuerà probabilmente a essere influenzato dall'evoluzione del panorama delle minacce, dai requisiti normativi e dai progressi tecnologici. Non sorprenderà vedere i test TIBER-EU diventare più diffusi man mano che le organizzazioni si sforzano di migliorare la loro postura di cybersecurity e conformarsi ai requisiti normativi. Alla luce di ciò è naturale che le posizioni aperte e i profili nel campo della cybersecurity siano effettivamente in ascesa, alimentati dalla crescente richiesta in questo campo e dall'aumento minacce informatiche. In conclusione, è necessario che i professionisti della cybersecurity siano flessibili e adattabili verso metodi nuovi e "ibridi" per testare la loro postura di sicurezza e proteggere le informazioni preziose delle loro organizzazioni. ■

Cambiare l'approccio: Threat Exposure Management.

Autore: Giovanni Assolini

Nel corso di poco più di un decennio due grandi eventi hanno caratterizzato la completa trasformazione dei rapporti tra persone e tecnologia e la vertiginosa crescita del mercato dell'IT nel mondo.

La nascita del web ha segnato un cambio radicale nel modo di fruire le informazioni ed ha creato un mercato di prodotti e servizi totalmente nuovo che ha letteralmente rivoluzionato la vita e la quotidianità di ognuno di noi.

In modo estremamente più invasivo, la nascita degli smartphone e del nuovo mercato rappresentato dalle app mobile ha consolidato, in modo definitivo, la completa dipendenza delle persone dalla tecnologia a cui affidano quotidianamente interi ambiti della propria vita, dal benessere fisico ai contatti con il mondo, dai propri asset finanziari alla propria sicurezza fisica e digitale.

A differenza di ambiti altrettanto pervasivi come ad esempio la medicina, dove enti internazionali di

controllo regolamentano e garantiscono la qualità dei prodotti, nel mondo dell'informatica si è, più o meno consapevolmente, deciso di accettare la mancanza di un regolatore e di uno standard qualitativo di riferimento. Come diretta conseguenza di questa decisione ci si trova oggi a dover convivere con prodotti dichiaratamente inadeguati che obbligano ciascuno di noi a convivere con i concetti di "patch management" e "bug fixing" o, per chi si occupa di sicurezza, con il processo di "vulnerability management".

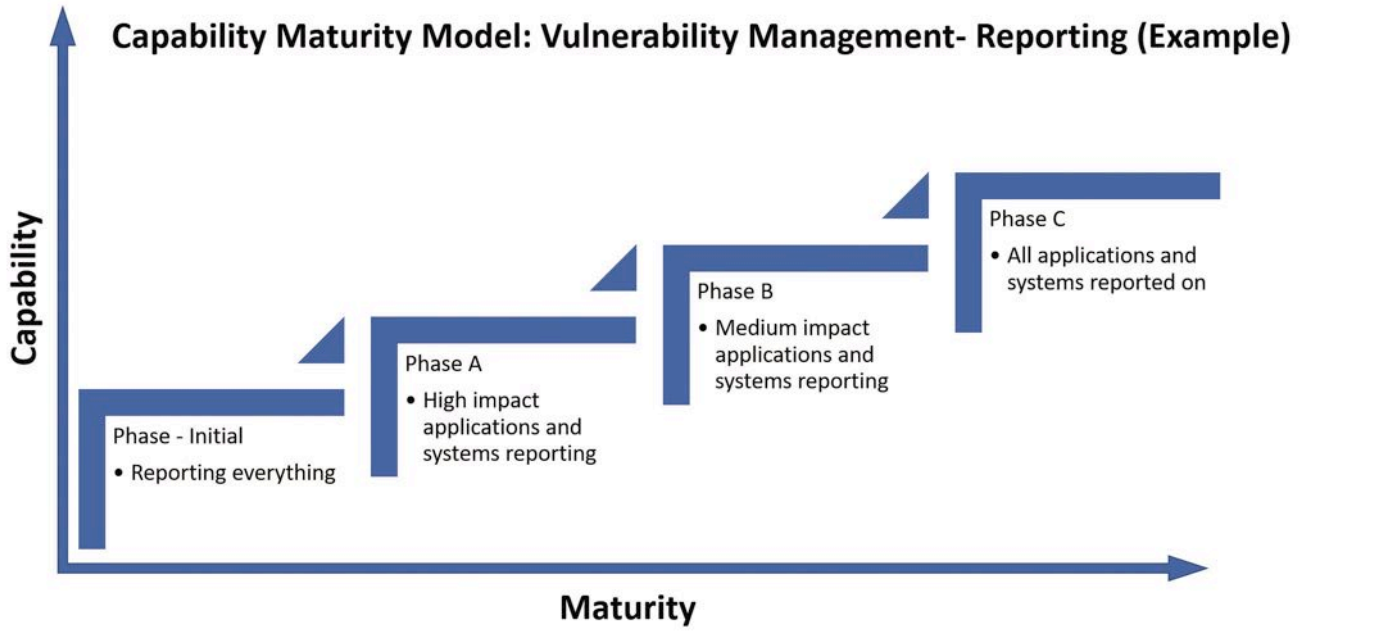
Questa differenza è una caratteristica sostanziale e unica del mondo dell'Information Technology. In nessun altro ambito della vita di ciascuno di noi sarebbe ritenuto accettabile pagare per un prodotto di cui si sa che non sono garantiti funzionalità, stabilità o il rispetto delle misure minime di qualità e sicurezza.

Vulnerability Management

Il Vulnerability Management è un processo circolare di verifica, identificazione e correzione di tutte le debolezze dei sistemi che

BIO

Giovanni Assolini inizia il proprio percorso occupandosi per oltre un decennio della progettazione di datacenter e reti geografiche complesse nelle telecomunicazioni per poi passare al mondo finance dove da 15 anni sviluppa ed approfondisce le proprie conoscenze in ambito continuità operativa cybersecurity e antifrode.



compongono la propria infrastruttura informatica. In quanto tale è un processo per definizione infinito e per questo fondamentalmente frustrante. Nuove vulnerabilità appaiono quotidianamente, la complessità crescente dei sistemi pongono sempre maggiori vincoli rendendo più complesso risolverle. A causa di questi elementi il numero di vulnerabilità ed il backlog sono in perenne aumento.

Troppo spesso inoltre, nell'immaginario comune, la gestione delle vulnerabilità viene confusa con il Patch Management sminuendo l'intero processo e riducendolo a un sottoinsieme di prodotti e misure correttive incompleto e spesso vano.

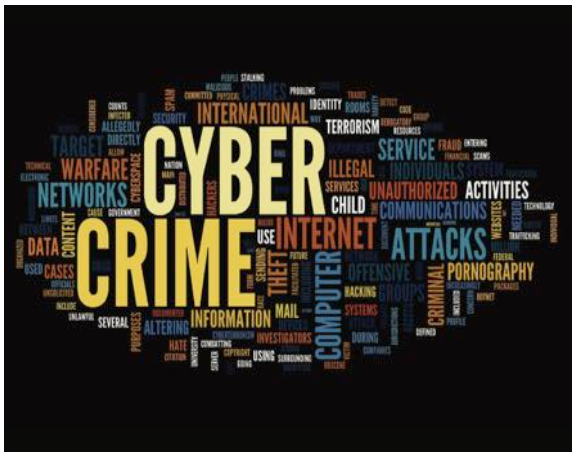
La maggior parte delle soluzioni disponibili sul mercato restituisce lunghissimi elenchi di vulnerabilità classificate sulla base di criticità oggettive ed arbitrarie, lasciando gli addetti alla sicurezza con un senso di impotenza dato da un carico di lavoro sempre crescente, non valorizzato e spesso vano perché si pone, come fine principale, non la vera risoluzione delle vulnerabilità ma la mera creazione di KPI e viste di sintesi che trasmettano un messaggio positivo verso il management aziendale.

Il risultato è la diffusione di un falso senso di sicurezza non sostenuto da una reale riduzione del rischio ed aggravato dal disinteresse collettivo e dalla convinzione che quello della sicurezza sia l'unico team all'interno dell'organizzazione responsabile dell'implementazione e della gestione dei presidi di sicurezza.

Il punto di vista dell'attaccante

L'inefficacia dell'attuale impostazione nella gestione delle vulnerabilità risulta ancora più evidente se si considerano gli elementi chiave che differenziano attaccanti e difensori.

Il divario di risorse a disposizione di un numero crescente di vere e proprie organizzazioni criminali che dispongono di risorse economiche sempre maggiori, anche grazie a recenti metodi di attacco come i Ransomware che garantiscono flussi di cassa rapidi ed immediati; l'importante differenza di competenze a disposizione di queste organizzazione che hanno accesso diretto ad un immenso numero di esperti di informatica, oltre che di sicurezza, attratti da facili guadagni; la sostanziale disparità di motivazione alla base dei due



attori principali: da una parte un team di attaccanti composto da centinaia di migliaia di persone a cui basta un solo colpo andato a segno per vanificare gli sforzi profusi nel proteggere i sistemi aziendali e portare a termine il proprio obiettivo e vincere la partita; dall'altra, un team risicato di cavalieri che, dal canto loro, sono obbligati a garantire un success rate pari al 100% per poter aspirare, al massimo, ad ottenere un pareggio.

La motivazione e le risorse a disposizione portano chi attacca ad avere un punto di vista totalmente diverso; facendo leva su ogni possibile elemento e sfruttando non le singole vulnerabilità ma una combinazione di più elementi (tra cui errori di configurazione e malcostumi di utenti ed amministratori) chi attacca è in grado di sfruttare, con estrema facilità, ogni debolezza nascosta nelle complessità dei sistemi aziendali.

E la situazione risulta ancora più aggravata dall'aumento della superficie di attacco introdotta dai servizi cloud che hanno, di fatto, esteso a dismisura i confini digitali delle aziende.

È pertanto evidente la necessità di ripensare completamente l'approccio introducendo nuove metodologie e processi per validare i presidi di sicurezza e ridurre sensibilmente i rischi.

La soluzione però va ricercata in un vero e proprio cambio di paradigma: non più una gestione delle singole vulnerabilità ma la loro valorizzazione e combinazione con elementi di contesto che aiutino ad identificare i rischi ed indirizzino sforzi e risorse verso l'applicazione di soluzioni realmente efficaci e risolutive.

L'arricchimento delle vulnerabilità con elementi di contesto è il vero game changer quando si parla di riduzione del rischio perché permette di avere una visione oggettiva e di ricreare veri e propri percorsi di attacco potenziali, evidenziando proattivamente percorsi nascosti, punti deboli dell'impianto e gap nei controlli di sicurezza che rappresentano le vere debolezze esposte e sono per questo una minaccia reale.

In quest'area molte aziende stanno facendo i primi passi verso l'adozione di nuovi strumenti di automazione per la fase di simulazione o Breach & Attack Simulation (BAS) con l'obiettivo di arrivare a pensare e agire come un attaccante e validare in questo modo i presidi di sicurezza.

Purtroppo, affidare interamente all'automazione il processo di analisi e remediation porta inevitabilmente al fallimento del processo.

Continuous Threat Exposure Management

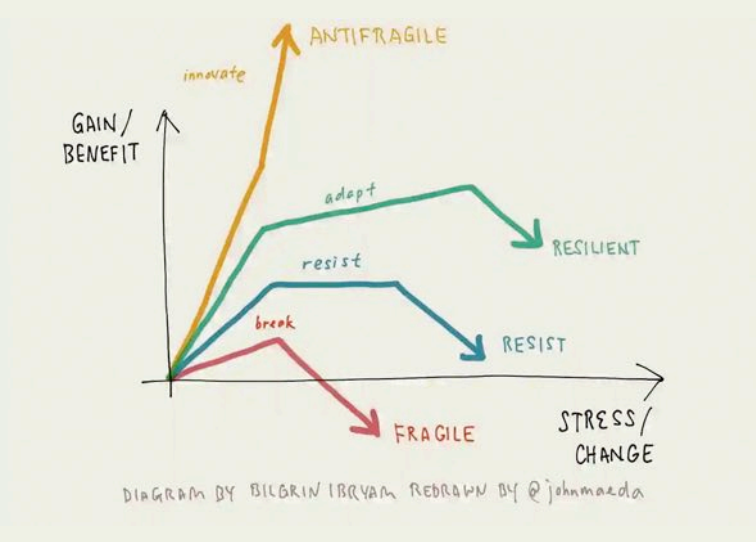
Il nuovo paradigma da introdurre è rappresentato dal concetto di Continuous Threat Exposure Management (CTEM) che non deve essere sminuito a semplice prodotto ma va invece considerato come un vero e proprio programma, strutturato e formalizzato, che si differenzia dal Vulnerability Management proprio perché considera elementi aggiuntivi di contesto nella valutazione del rischio e nell'individuazione delle remediation.

Il CTEM si pone quattro principali obiettivi a breve e medio termine:

- Aiutare il team focalizzato ai presidi di sicurezza difensivi (Blue Team) a rilevare e rispondere agli attacchi in tempo reale fornendo contesto e conoscenze del perimetro e delle vulnerabilità;
- Ridurre al minimo i rischi aiutando a stabilire l'ordine di priorità con cui mettere in atto le azioni più efficaci alla riduzione del rischio ottimizzando al contempo tempo e risorse;
- Aumentare il livello di resilienza nell'immediato creando un quadro più chiaro ed indirizzando la strategia generale;
- Impiantare l'attitudine al continuo miglioramento attraverso l'integrazione delle "Lessons Learned".

Antifragilità

In un mondo sempre più digitalizzato e informatizzato l'intero contesto in cui si opera è in continua mutazione e presuppone l'importanza di dotarsi di un sistema di gestione della resilienza sempre più efficace. L'evoluzione



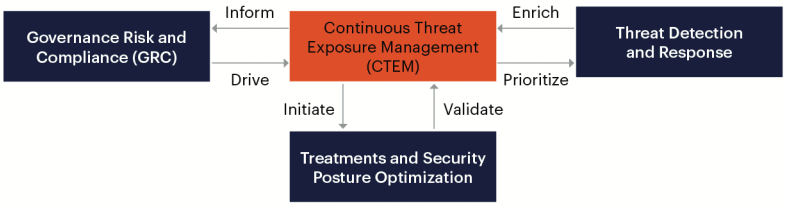
regolamentare e normativa suggerisce di predisporre una strategia ben definita per fronteggiare le nuove minacce e per gestire i rischi emergenti. Il CTEM va esattamente in questa direzione agevolando l'introduzione del principio di antifragilità raccontato da Nassim Nicholas Taleb.

L'antifragilità va al di là del concetto di resilienza o robustezza.

Ciò che è resiliente è strutturato per resistere agli shock e tornare allo stato iniziale rimanendo identico a sè stesso; ciò che è antifragile invece è in grado di modificarsi a fronte di sollecitazioni esterne migliorando ogni volta la propria struttura.

E questa attitudine al continuo miglioramento deve essere posto alla base del nuovo approccio dato dal concetto di Threat Exposure Management. ■

Continuous Threat Exposure Management



Source: Gartner
763954_C

Gartner.

Il cyber crimine può "spegnere" le nostre città. Sventare questo rischio è il nostro mestiere.

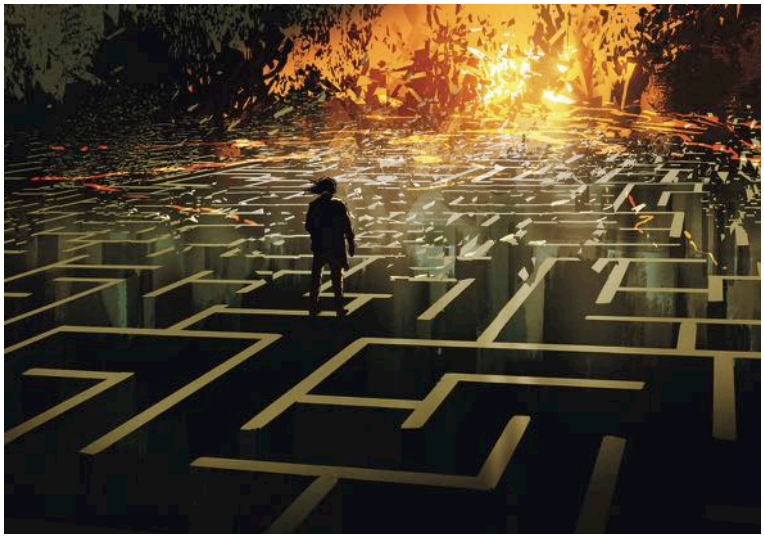
Intervista VIP a Luigi Maracino.

Autore: Massimiliano Cannata

"Nella Cyber security niente si può improvvisare, sono tante le declinazioni di un'attività strategica da cui dipende sempre più l'equilibrio e la tenuta di governi, istituzioni e imprese. Bisogna stare vicino ai cittadini, per dare un servizio competente, responsabile. Il sistema di protezione deve estendersi alle reti e ai sistemi che fanno funzionare le nostre città, non dobbiamo pensare solo alle infrastrutture critiche e alle grandi realtà produttive perché le aree potenzialmente esposte riguardano ormai tutti gli ambiti della vita quotidiana. I target di oggi sono indefiniti, chiunque può essere esposto a un attacco soprattutto perché in larga scala viene condotta una attività di scanning indiscriminato, rispetto a cui dobbiamo saper alzare le nostre difese". Luigi Maracino, *General Manager di Atlantica Cyber Security*, dirige il SOC aziendale, struttura all'avanguardia per competenze, strumenti, attività di formazione e recruiting.

Dott. Maracino, a giudicare da quello che sta avvenendo in ogni angolo del Pianeta siamo tutti sotto "attacco". Come dobbiamo valutare il nostro grado di esposizione in quella che il celebre sociologo tedesco Ulrich Beck ha definito la "società del rischio"?

Il livello di esposizione alle minacce reali e virtuali in una società sempre più permeata da sistemi hi-tech è innegabilmente molto alto. Questa condizione che tutti sperimentiamo corre di pari passo alla generale sensazione di fragilità esistenziale crescente che sta segnando un'epoca



BIO

Luigi Maracino è il Direttore Generale di Atlantica Cyber Security, la società di sicurezza informatica di Atlantica Digital.
Possiede un solido background tecnico/ imprenditoriale e una pluriennale esperienza nella gestione aziendale.
E' un interprete e conoscitore profondo dello scenario della Cybersecurity.

come quella che viviamo densa di paure e contraddizioni. Questo obbliga a mantenere alta la soglia di attenzione, non si tratta di rallentare lo sviluppo della tecnologia, esercizio miope e fuori dal tempo, piuttosto di rafforzare la nostra capacità di lettura delle fenomenologie del cambiamento. Venendo alla sua domanda, va detto che esiste uno status di pericolo diffuso connesso alla complessità stessa delle reti e dei sistemi entro cui viviamo ormai immersi, ma vi sono anche, ed è su questo che dobbiamo soffermarci, "attacchi targettizzati" che hanno caratteristiche peculiari che finiscono sulle prime pagine dei giornali.

Prima di approfondire i tratti distintivi che connotano le attività di Atlantica Digital nel campo della cyber security, può darci una chiave interpretativa di questi eventi che colpiscono l'opinione pubblica, condizionando comportamenti collettivi?

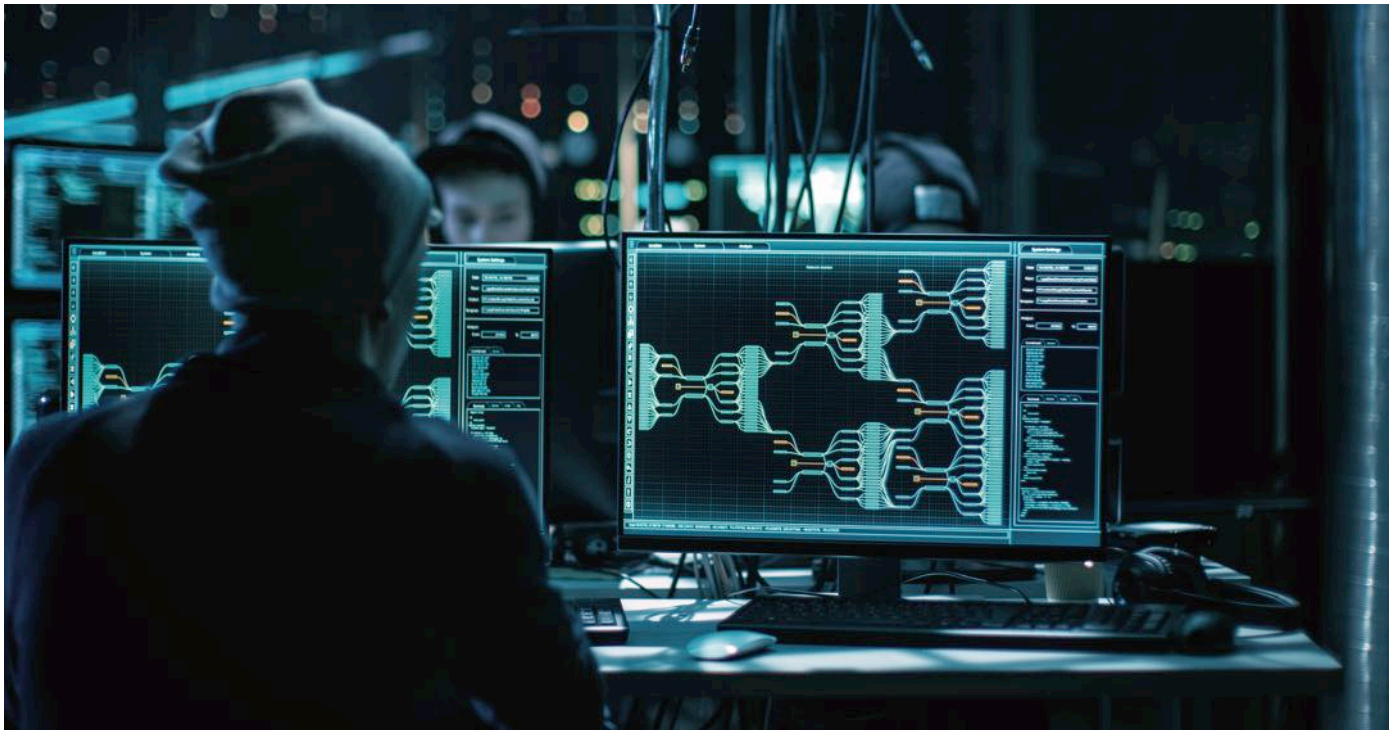
Quando si ha di fronte un obiettivo preciso la minaccia diventa più temibile. In questi casi, per dirla in gergo tecnico, non "si fa massa ma sostanza". L'infrastruttura critica sotto scacco, sia un ospedale, una impresa, un partito politico come sempre più sovente avviene, deve essere in grado di reagire, che significa esser pronta a fronteggiare un'azione organizzata. Fino a quando penseremo che il pericolo sia remoto, non faremo mai il salto di qualità. Sottovalutare il grado di rischio informatico è un errore grave. Dobbiamo, infatti, pensare che questi gruppi attaccanti sono strutturati e abili, non danno scampo, scelgono bene i potenziali target da colpire, le loro azioni sono incisive e problematiche, dense di conseguenze.

Quali azioni di contrasto vanno messe in campo per limitare i danni?

Quello che fa la differenza, rispetto alla continua evoluzione delle minacce è il *framework* che siamo in grado di costituire e alimentare; la sicurezza, come mi capita spesso di ripetere, è un ecosistema non un concetto astratto. La tecnologia, dico sempre ai miei collaboratori, deve essere per noi una commodity, nostro compito è analizzare e sondare l'intera catena del valore. Non tutte le organizzazioni possono avere le skills per colmare le vulnerabilità, per questo devono delegare ad attori terzi la governance della sicurezza, cosa sempre delicata. *L'outsourcing* può essere praticato in condizioni di sostenibilità economica, ma soprattutto quando la reputazione della struttura che assicura un servizio gestito abbia competenza, reputazione accertata e credibilità. Il SOC deve possedere questi requisiti per affiancare grandi e piccole realtà in un percorso evolutivo, che oltre a ridurre le superficie esposte agli attacchi renda più competitiva l'organizzazione.

Lei parlava di* governance *della sicurezza, non basta il "controllo" come i teorici della complessità ci hanno dimostrato. Le nostre aziende sono pronte ad applicare questo nuovo paradigma?

Dobbiamo compiere un salto culturale molto forte per comprendere i nuovi scenari che la sua domanda fa intravedere. Fare una diagnosi è il primo passo che gli analisti del SOC devono compiere, serve a comprendere



la postura di sicurezza dell'organizzazione. Gli strumenti del *risk assessment e del vulnerability assessment* ci danno la possibilità di fare un'anamnesi precisa. La metafora, tratta dalla medicina, rende l'idea della delicatezza di questa fase che deve portare a un documento di rischio condiviso, che permette di aggiornare i sistemi e di modificare le configurazioni. Per dirla in sintesi: il cliente deve acquisire consapevolezza del livello di esposizione, per poter valutare i potenziali danni derivati dall'azione di uno o più attaccanti organizzati. Compito del SOC è, in particolare, il monitoraggio, il riconoscimento della minaccia e la verifica della portata dell'azione malevola in corso.

Senza allenamento corale non c'è sicurezza

Dalla sua disamina si capisce che gli analisti devono essere "medici competenti" avendo "in cura" la salute di reti e sistemi da cui dipende il benessere della collettività in senso ampio. Il tema centrale di questo numero di Cybersecurity Trends è costituito dal binomio: **penetration test e security automation.** ***Qual è il livello di impegno di Atlantica Digital su questo versante?***

Molto elevato, come dimostra l'assetto organizzativo di cui ci siamo dotati. All'interno del nostro SOC opera, infatti, un *"blue team"* costituito dal gruppo di difesa votato ad analizzare la tipologia delle minacce, le possibili falle e le fragilità, affiancato da un *"red team",* il gruppo di attacco che ha il compito di validare in maniera continuativa le azioni di contrasto sperimentate dalla struttura. La reattività del sistema, come dicevo all'inizio, è un aspetto cruciale che deve essere messa alla prova senza sosta, attraverso l'applicazione del *continuous assessment*.

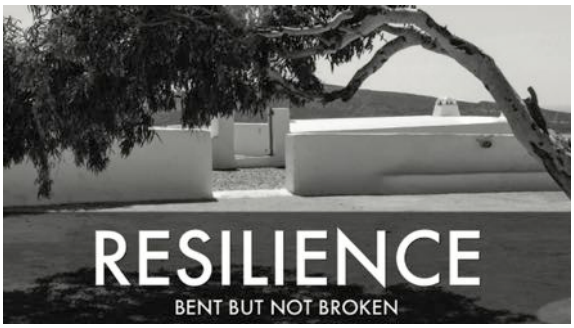
Dal linguaggio della medicina a quello dello sport, il passo è breve…

Lo sport ci insegna che per essere competitivi serve costanza negli allenamenti e che molto spesso la miglior difesa è l'attacco. Un'efficace *compliance* deve basarsi sulla continuità non sulla sporadicità, che non permetterebbe di acquisire quella capacità predittiva essenziale per chi opera nella *cyber security*. Entra in gioco il fattore umano. Infatti, presidiare le piattaforme, i *marketplace* e le regioni più "nascoste" del web, che sono tutte aree di scambio dei dati che oggi assumono rilevanza strategica, utilizzare

gli strumenti tecnologici più avanzati come la *threat intelligence* e il *machine learning,* risulta di importanza decisiva a patto che ci siano analisti validi, pronti a dosare interventi, strategie e metodologie di intervento.

Quando si parla di organizzazioni resilienti, che cosa si intende esattamente?

Resiliente è colui che sa adattarsi. Un SOC fa bene il suo compito se è in grado di allenare istituzioni, imprese, grandi e piccole, rendendole non solo reattive, ma anche capaci di ripensare azioni e strategie di contrasto rispetto all'emersione di minacce sempre diverse e in perenne evoluzione. Ho lavorato progettando uno dei primi SOC in Italia (presso BNL n.d.r.) eravamo ai primordi, non esistevano ancora tecnologie in grado di correlare ed aggregare eventi automaticamente, come i SIEM ad esempio, si cominciava a sperimentare un metodo di analisi e di messa in relazione di eventi potenzialmente pericolosi, con lo scopo di affinare le strategie di contrasto. Adesso il mio impegno è volto alla creazione di un *Threat Operation Center*, utilizzando un nuovo acronimo sarei tentato di parlare di "TOC", orientato a praticare il tracciamento di una fragilità che va seguita dal punto di origine lungo tutto il percorso evolutivo. Un team di abili analisti ed *ethical hacker,* terminologia che certo non amo, ma che utilizzo solo a scanso di equivoci, ci stanno già aiutando in questo compito.



Cosa non Le piace di un certo vocabolario, per altro molto in uso?

Gli equivoci che può generare. Ricordiamoci che l'hacker ha per sua natura una spinta etica, dettata dalla curiosità che porta alla conoscenza. La sete di profitto di comuni delinquenti digitali ha purtroppo fatto saltare gli equilibri snaturando il significato di hacker. I gruppi criminali che sono nati negli ultimi anni non hanno niente a che vedere con la nascita e l'evoluzione della figura originaria, che mantiene forse un alone nobile e romantico, ma che è servita e continua a servire alla scienza per affinare le azioni di contrasto. L'*hacker* è un creativo difficile da prevedere, perché riesce a vedere oltre, cosa che per chi fa il nostro mestiere è molto importante.

Per mantenere gli occhi aperti serve l'apporto dei talenti. Di quali profili ha bisogno la cyber security per rispondere ai bisogni crescenti del mercato?

Il *recruiting* è un fronte che impegna sempre più la struttura che dirigo. Se pensiamo all'evoluzione che ha avuto questo settore ci possiamo rendere conto di quanto sia importante l'aggiornamento del know-how per sostenere la sfida di una competizione senza frontiere. L'analista è ormai una figura trasversale, non risponde a nessuno standard tradizionale. Va costruita su

un mix di competenze. Consapevoli di questo abbiamo sviluppato dei rapporti molto stretti con l'Università, li vanno cercati i cervelli e i nuovi saperi, che sono il motore dello sviluppo e dell'innovazione, a qualsiasi latitudine.

Quello* cyber *è un universo mutante, non si fa in tempo a scattare una fotografia che subito ci si accorge che è resa sfocata dal susseguirsi degli eventi. Si può essere al passo con i tempi?

Sì, aggiornandosi continuamente, non vedo altra strada. La formazione è il valore numero uno che deve guidare ogni passo. I nostri neoassunti sperimentano il loro "battesimo di fuoco" misurandosi con un *trainer* che opera per l'esercito israeliano nella formazione dei team che, a livello governativo, sono chiamati ad affrontare le azioni di cyber war. In pochi anni il mondo è cambiato. Ricordo che negli anni Novanta l'enfasi era posta sull'information technology, tutto era IT, l'acronimo scandiva non solo un tempo di sviluppo delle tecnologie, ma una condizione potrei dire "esistenziale". Con la stesura dell'"allegato B", voluta da Stefano Rodotà nella qualità di Presidente dell'Autorità Garante della Protezione dei dati Personali, si aprì un percorso che non avevamo mai battuto prima. Dovevamo abituarci all'idea che la protezione doveva ampliarsi al dato immateriale, il "recinto" posto a difesa del perimetro fisico dell'organizzazione era solo una parte del lavoro che bisognava fare. Persone, strutture, reti e sistemi andavano protetti con nuovi strumenti e metodi.

Il Documento Programmatico della Sicurezza, che tutte le aziende avrebbero dovuto da quel momento stilare, avrebbe conferito la stessa dignità alla dimensione reale e alla componente virtuale; il dato fisico e il corpo elettronico erano due facce della nostra stessa identità. Sono tutti passaggi decisivi che fanno comprendere la portata del cambiamento d'epoca, rispetto a cui il nostro processo di adeguamento è ancora ai primi passi.

L'attacco alle RTU, un rischio crescente per la collettività

Tecno-scienza e filosofia si toccano nel suo ragionamento. Sconvolgente tutto questo, non crede?

Lo sarebbe nella misura in cui non provassimo nemmeno ad allargare la nostra capacità di lettura di fatti e fenomeni. La fase sanzionatoria, che abbiamo vissuto nella prima fase IT cui facevo riferimento, definita dagli obblighi normativi pur necessari, è ormai superata. Oggi quella componente, che fa parte del corredo delle nostre conoscenze, si intreccia con l'esigenza di proteggere la sicurezza delle informazioni, che apre una serie di implicazioni la cui portata è ancora in larga parte difficile da misurare e prevedere.

Dicevamo all'inizio che i target potenzialmente esposti si stanno ampliando a dismisura. Parlare di sicurezza diventa utopia?

Non esiste una sicurezza assoluta, quello che possiamo fare e cercare di ridurre il rischio il più possibile. Non si può tralasciare nulla. I sistemi industriali sono divenuti il primo obiettivo del cyber crimine perché possiedono un'anima tecnologica che ne permette il funzionamento. Gli attacchi maggiormente dirompenti vengono sferrati alle *Remote Terminal Unit*, il fulcro elettronico che regola l'operatività delle reti industriali, ferroviarie, elettriche, infrastrutturali. Manomettere una RTU vuol dire spegnere le città, dirottare treni, fermare catene produttive. Vi sono vere e proprie academy che formano degli specialisti nell'utilizzazione di questa nuova, sofisticata strategia. Il nostro SOC sta lavorando su questo versante, nella consapevolezza che il fine dei criminali è quello di portare a termine una *kill chain*, una catena di azioni che ha l'obiettivo di acquisire il comando e il controllo di un dispositivo o sistema di una organizzazione. Il nostro lavoro è quello di impedire l'installazione, la modifica o la cancellazione di codice o eseguibile non autorizzato o potenzialmente dannoso, attuando una protezione passiva, *secure by design,* che ha l'obiettivo di validare (o negare), anche a livello *firmware*, azioni di tipo persistente. Attuando poi un *continuous assessment*, reiterando nel tempo attività di Vulnerability Assessment e Penetration Test (VA-PT), definiamo le scale di priorità delle azioni di mitigazione del rischio cyber, mettendo in evidenza quelle falle entro cui il nemico può farsi strada, suggerendo le contromisure più rapide ed efficaci a contrasto.

Sulla base di questa rivoluzione da Lei ben descritta possiamo in conclusione definire che il dato è divenuto un "asset sociale" come ha recentemente scritto Michele Mezza nel brillante pamphlet* Algoritmi di libertà *(ed. Donzelli n.d.r)?

Si può essere d'accordo in considerazione dell'importanza che il trattamento dei dati riveste nella *digital society. Disponibilità, integrità, riservatezza,* sono le regole che presiedono all'utilizzazione delle informazioni, per me hanno coinciso con delle precise regole di condotta, rivestendo, ci tengo a sottolinearlo, una valenza etica oltre che normativa. ■

Il capitale umano nella società del rischio.

Intervista VIP a Roberto Tiozzo.

Autore: Massimiliano Cannata

Dott. Tiozzo, la figura dell'hacker ha assunto un rilievo essenziale nella società dell'informazione. Avvolta da un alone quasi "mitico" nella prima fase dello sviluppo del web, oggi ha una valenza rilevante sul piano dello studio delle vulnerabilità. Cosa dobbiamo pensare al riguardo?

Se in passato l'hacker poteva essere pensato come l'ingegnere informatico circoscritto in un ambito ristretto, oggi con l'accesso facilitato alle informazioni, hacker può diventare chiunque sia animato da curiosità e da voglia di imparare. Questa figura credo debba essere intesa nella connotazione originaria di colui o di coloro che esplorano un sistema per individuarne i punti di debolezza o di vulnerabilità, al fine di fornire delle soluzioni o creare dei vettori ottimali per analizzare la natura degli attacchi. L'hacker è una componente professionale decisiva nella dinamica di sistemi sociali dinamici e in evoluzione. La visione statica dell'ottenimento di una referenza professionale fine a sé stessa non si addice più a una figura che si costruisce con un continuo aggiornamento. Il quadro attuale è reso ancora più complicato dal fatto che in Italia e nel resto del mondo abbiamo ancora pochi specialisti informatici al cospetto del numero crescente di fruitori di strumenti tecnologici sempre più diffusi.

La Cyber Security è un ambito che sta generando un interesse crescente. Quali sono le ragioni di questa attenzione?

Posso parlare della mia esperienza. Il mio interesse particolare per l'hacking etico, aspetto importante della cyber sicurezza, nasce dalla necessità vitale di accedere alle informazioni in un sistema ostile, come quello cinese in cui sono vissuto. Per me come per altri "stranieri", lì residenti, dialogare senza essere osservati dal "Grande Fratello" era di importanza vitale. Per questa ragione ho iniziato ad utilizzare una navigazione che gli addetti ai lavori definiscono "stealth" o tramite "proxy".

BIO

Roberto Tiozzo, 55 anni, consulente nel mondo della digitalizzazione e dell'innovazione, coltiva da sempre tre grandi passioni: l'informatica, le arti marziali e la filosofia. Nei primi anni 2000 in Cina dove, dove ha vissuto per 20 anni a Shanghai, ha lavorato come project manager per le startup innovative di un noto incubatore tecnologico della città. Ha seguito lo sviluppo di soluzioni tecnologiche per software hardware per il mondo del digitale e delle telecomunicazioni. Ha fondato una startup anche in Inghilterra, operando tra Hong Kong e Regno Unito. Sta ultimando un percorso di specializzandone in cyber security e Data Analysis con l'obiettivo di ottenere la certificazione internazionale in questi ambiti strategici e fornire un supporto specialistico alle organizzazioni complesse che operano in Italia e all'estero.

Allargando lo sguardo, come va interpretato il fenomeno?

Se si parla del fenomeno più generale, l'interesse in Occidente nasce probabilmente dalla presa di consapevolezza, individuale e collettiva che abbiamo ormai una seconda identità digitale che va tutelata

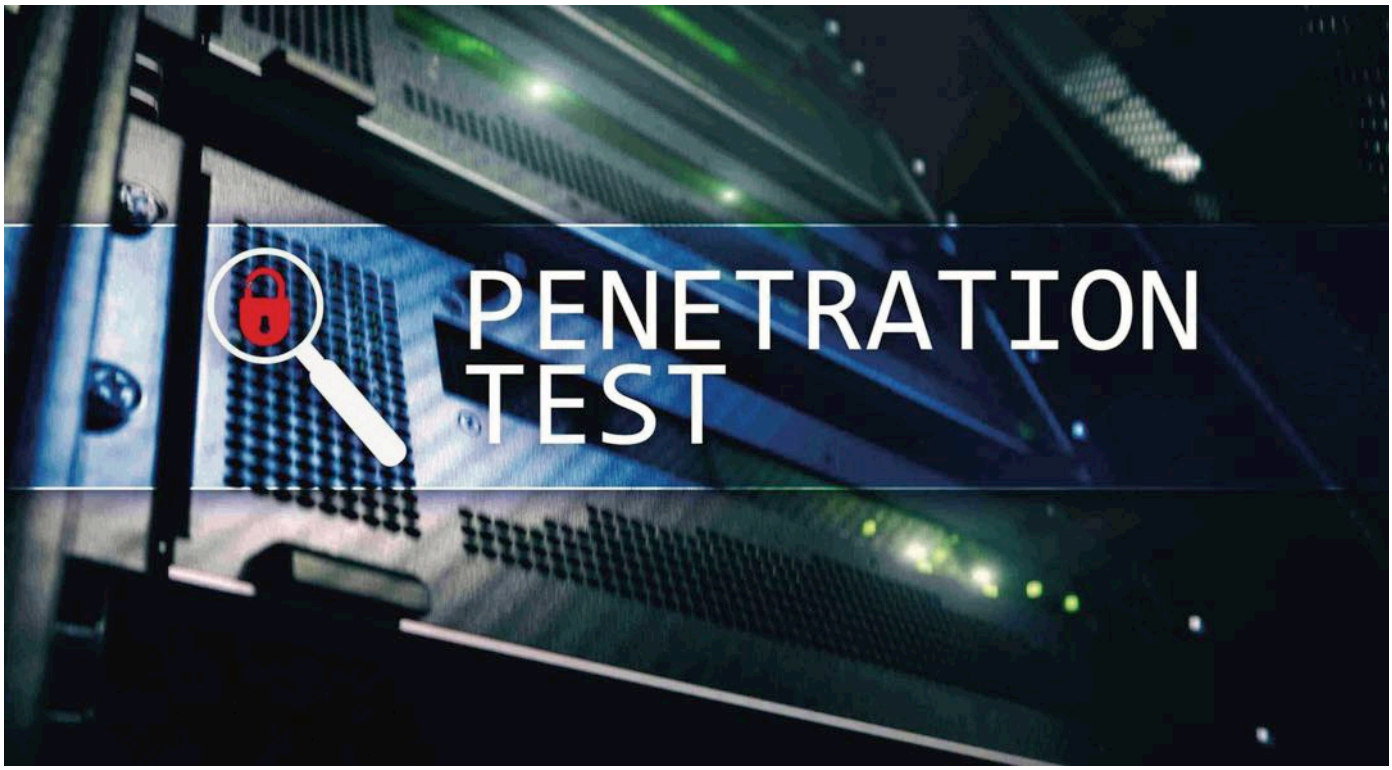
e protetta. Le informazioni generate su di noi sono disponibili in rete e una semplice indagine Osint può bastare per ricostruire non solo l'identikit di un criminale ma le abitudini di un normale cittadino ponendolo in una situazione di fragilità. Se queste vulnerabilità esistono per gli individui, valgono tanto più per i target istituzionali o strategici; questo fa capire la delicatezza della materia. Per il cyber security expert, dunque, lavoro ce n'è abbastanza, non solo quando è posto a difesa del "recinto virtuale" di un'organizzazione aziendale, di una banca o di una istituzione, ma anche quando si occupa di simulare degli attacchi al fine di allenare le organizzazioni ad adottare modelli e strategie efficaci di riduzione della vulnerabilità.

Si discute molto del rapporto che esiste tra tecnologie informatiche e creatività. In questo numero ospitiamo un'intervista ad Alessandro Curioni che oltre ad essere un apprezzato esperto di cyber security è già al secondo romanzo. Un dato sorprendente non crede?

Vi sono molti luoghi comuni leganti al mondo dell'informatica. Uno di questi è che sia un mondo formato da cervelloni o da nerds infarciti di matematica. In realtà non è proprio così, anche se alcune basi di matematica possono servire. Conosco molte figure che si sono formate sul campo apprendendo da vari ambiti disciplinari, questo perché, come dicevo, è un mondo in perenne evoluzione, che richiede grande passione e dedizione. Non esistono soluzioni uniche e sempre valide, né metodi infallibili. Trovandoci perciò di fronte a soluzioni interpretabili e soggettive, il linguaggio o il metodo di approccio a una macchina possiamo definirlo a tutti gli effetti creativo. La "distruzione" è un termine chiave dal ruolo ambivalente che, riconducendo al processo di innovazione, impone il superamento di vecchi schemi. Il vero pericolo in questa partita è la nostra paura di abbandonare sistemi di riferimento tradizionali, una paura che diviene acerrima nemica dell'hacker o, più in generale, dell'innovatore.

Questo ragionamento ha a che fare con quello che una certa letteratura, in voga qualche anno fa, definiva "pensiero laterale". Siamo capaci di coltivarlo, al di là dei facili slogan?

Mi viene in mente una tra le tante strategie di Sun Tzu che consiste nell'osservare silenziosamente che il nemico faccia qualche passo falso prima di sferrare l'attacco. Noi occidentali, figli della logica aristotelica, tendiamo a pianificare secondo un definito modello teorico mentre nel mondo orientale le azioni vengono portate avanti in maniera trasversale, un po' come fanno gli hacker. Nella cyber security un ruolo fondamentale viene giocato dai pentester, sono gli hacker buoni, coloro che testano la resilienza delle organizzazioni violando i sistemi in maniera calcolata. Per fare questo occorre lavorare in maniera strategica adottando tattiche offensive che per



essere efficaci, presuppongono approcci indiretti che vanno dall'assunzione di informazioni sull'asset da colpire, all'individuazione di strategie di attacco primarie e secondarie molto specifiche. Il tempo impiegato ha un ruolo importante, mentre l'osservazione gioca a favore dell'hacker. Bisogna ricordarsi che non è mai come nei film dove un singolo colpo va a buon fine. Servono tentativi multipli, che vanno portati a termine senza fare "troppo rumore".

Un aspetto oggi allo studio della psicologia è la possibilità di canalizzare la devianza. Oltre la "gabbia della frustrazione" che spinge molti soggetti a "bucare" i sistemi, ci può essere un recupero positivo e socialmente utile di chi si muove ai margini della legalità?

Il malcontento, l'insoddisfazione, l'idea di aver subito un torto, si sa, è una leva fondamentale che può spingere a mettere in moto comportamenti devianti. "Rompere il giocattolo" è anche il modo migliore per capirne il funzionamento. L'hacker gioca in un'area marginale o di confine. Si astrae dalla realtà, per immergersi nel virtuale. Ha un senso di rifiuto del sistema e proprio perché non è parte dell'ingranaggio vuole comprenderne nel dettaglio i meccanismi. Bisogna comprendere che operando dalla periferia del sistema può meglio identificare i meccanismi interni che lo governano e conseguentemente le vulnerabilità. Quando si ha consapevolezza di questa dinamica, tante devianze oltre ad essere sanate, possono tramutarsi paradossalmente in valore socialmente utile.

Quali strategie le imprese devono adottare nell'orizzonte della società del rischio?

L'istituzione e le imprese gestiscono informazioni che hanno un valore inestimabile, nel momento in cui diventano accessibili ad altri per la presenza di un Ransomware o di un DDos Attack cominciano i guai. Gli agenti primari dell'attacco in molti casi possono anche essere persone che lavorano all'interno dell'azienda e che per qualche ragione hanno maturato dei conflitti con l'organizzazione o più semplicemente non hanno introiettato i comportamenti adeguati a ridurre il rischio. Trattare con cura e attenzione i dipendenti per non istigare comportamenti anomali è sempre importante, così come dotarsi di strumenti di controllo interno. Far testare periodicamente i propri sistemi con attacchi simulati di specialisti addestrati e ben pagati è un ulteriore aspetto di cui tenere conto: bisogna essere esercitati per vincere questa guerra continua tra "guardie" e "ladri".

Possiamo, alla luce di questa conversazione, concludere che il fattore umano deve rimanere al centro di ogni riflessione?

Il capitale umano non può essere unicamente valorizzato dallo strumento remunerativo, è altresì importante creare le condizioni per far vivere meglio ogni attore che opera all'interno dell'organizzazione. È giusto che ogni persona si senta apprezzata sperimentando

un percorso di crescita conforme ad aspettative crescenti. Il singolo deve sempre sentirsi parte attiva, contribuendo al progetto comune di sviluppo. Se questo non si verifica, le risorse più brillanti cercheranno nutrimento altrove. Questo succede anche nella cyber security. La suddivisione in red team e blue team è la rappresentazione schematica di una guerra tecnologica, che fotografa i fronti contrapposti di chi protegge lo status quo e di chi, al contrario, vuole cambiare gli assetti. Per andare alla radice dei problemi va cambiata la cultura della sicurezza, aprendosi ai valori della collaborazione e dell'innovazione, fattori che incidono sull'evoluzione della società considerata nel complesso delle sue articolazioni. ■

Il metaverso imporrà un nuovo modo di stare sul pianeta.

Intervista VIP a Mattia Fantinati.

Autore: Massimiliano Cannata

"La comunicazione è sempre più preponderante nelle nostre vite, che ormai sono esse stesse trasformate a volte in medium, a volte in messaggio e a volte incarnano entrambi. Internet ha ridotto gli spazi tra le persone e ha accelerato il fenomeno. Organizziamo sessioni, incontri e seminari soprattutto per fornire strumenti di lotta contro le *fake news* e il *deepfake* che mettono a rischio le nostre democrazie. I bisogni e i diritti e le prerogative dell'uomo devono essere sempre al centro di tutta l'internet *governance*. Questa la mission di IGF Italia, Internet Governance Forum, organismo che fa capo all'Onu e che sostiene con il suo impegno la democratizzazione etica del governo della rete. Dobbiamo insomma arrivare a un corpus di norme che tuteli i diritti online esattamente come accade per la realtà offline". Mattia Fantinati, presidente di IGF Italia tratteggia in questa intervista il delicato rapporto tra diritto, etica e i ritmi evolutivi del progresso tecnologico, sempre più serrati e dirompenti.

BIO

Mattia Fantinati è presidente del IGF Italia (Internet Governance Forum) dal 2021 e partecipa all'organizzazione di EuroDIG dal 2019. Alle Nazioni Unite Mattia rappresenta l'Italia alle tavole rotonde dell'HLPDC (High Level Panel of Digital Cooperation). È stato Membro del Parlamento Italiano, alla Camera dei Deputati e Sottosegretario della Funzione Pubblica. Le sue principali aree di interesse sono la Trasformazione Digitale nei Governi e la Gestione dell'Innovazione nel Pubblico e nel Privato. È stato nominato dal Segretario Generale delle Nazioni Unite membro del MAG (Multistakeholder Advisory Group) che ha lo scopo di fornire consulenza al Segretario Generale sull'IGF (Internet Governance Forum). Regolarmente partecipa a convegni e seminari sulla Digitalizzazione tenuti dalle più importanti agenzie pubbliche e private (ITU, WSIS, CES,E-Leaders, OECD).

Presidente Fantinati, Stefano Rodotà vagheggiava una Costituzione per Internet, sottolineando la visione globale e una reale collaborazione tra gli Stati, necessaria per regolare uno strumento per definizione senza confini. L'intuizione del grande giurista è desinata a rimanere utopia?

Vediamo che oggi non tutti gli Stati hanno un identico approccio sui diritti umani. Così capita anche nel regno del digitale. Forse è utopia immaginare una legge uguale per tutti, ma a livello Onu o di Unione europea un coordinamento tra nazioni che firmano intese e le rispettano rappresenta già un buon punto di partenza. IGF ha fatto la mappatura di tutti i 38 accordi inter-stakeholder a livello mondiale e osserviamo due temi ricorrenti: il rispetto dei diritti umani e poi l'importanza della cooperazione digitale tra Paesi. Ovviamente poi gli Stati devono mettere questi principi

in pratica, ma la consapevolezza sta aumentando e noi facciamo la nostra parte. Dopotutto, tocca alle aggregazioni sovranazionali bilanciare il peso delle grandi piattaforme e dei colossi della rete.

Il secondo tempo di Internet

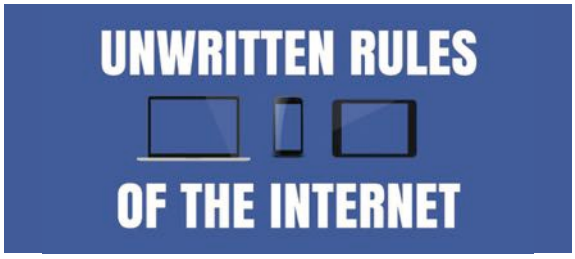
Gli studiosi parlano di un secondo tempo di Internet. Dopo la prima fase che ha aperto un universo nuovo per il mondo della comunicazione e della produzione, si sono fatti strada i social, l'IOT, fino ad arrivare a "Quella quarta rivoluzione" ben descritta da Luciano Floridi in cui reale e virtuale si mescolano, sostanziando la dimensione "on life" entro cui tutti siamo immersi.

Come si fa a regolare questo duplice piano di realtà?

Lo spunto dato dalla domanda mi porta a parlare del metaverso, tecnologia giovane che però lascia già intravedere i suoi risvolti futuri, in cui dal 2D si passa al 3D e la persona viene proiettata dentro un mondo virtuale. Ciascuno di noi può fare molte cose nel metaverso. Si può partecipare a delle riunioni, formarsi o lavorare a distanza con grandi benefici, perché l'esperienza è resa più coinvolgente grazie al passaggio dai pixel ai voxel, versione tridimensionale dei pixel stessi. Si può imparare a usare oggetti o fare *training* in molti settori senza le pericolosità intrinseche all'offline. Certo, il metaverso non può sostituire la realtà, le emozioni di un viaggio, ad esempio. Però è sbagliato spaventarsi e il legislatore non deve inseguire il mondo che cambia.

In concreto quali strategie andrebbero adottate?

Credo sia giusto che un regolatore a livello multistakeholder si sieda con i creatori di queste piattaforme per provare a delineare lo scenario a partire da alcuni *pillar* legislativi chiari e stabili, così da lasciare poi l'assetto delle norme immutato per più tempo possibile. Bisogna, infatti, evitare una schizofrenia regolatoria che genera solo incertezza ed eccesso di burocrazia. Tra le



direttrici fondamentali tornano ovviamente la centralità dell'uomo, la formazione, il rispetto della privacy e dell'identità individuale e infine il miglioramento dei presidi di cybersecurity. In fondo, funziona come le regole della mobilità e il codice della strada: io mi affido a determinate convenzioni vincolanti, ad esempio i colori del semaforo, perché so che più o meno tutti le rispettano. Stessa cosa deve accadere quando uso un device: ho bisogno di sapere che c'è un complesso di norme che mi protegge.

Metaverso, democrazia e Internet

Democrazia e Internet costituiscono uno snodo cruciale. In un recente saggio Michele Mezza ha denunciato l'oligopolio delle piattaforme, che mettono a rischio le libertà fondamentali. A che punto siamo su questo delicato versante che ha a che fare con quel capitalismo della sorveglianza, teorizzato da Shoshana Zuboff, che tanti interrogativi ha generato?

Queste piattaforme hanno fatturati pari al Pil di un piccolo Stato. Quindi la singola nazione non può

bilanciarle in solitudine, mentre le unioni di Paesi, facendo massa critica, possono limitarne gli abusi, ad esempio dal punto di vista dell'utilizzo dei dati. Soltanto l'Unione europea ha 600 milioni di abitanti e dunque può avere voce in capitolo. Non a caso, la Commissione Ue con provvedimenti come il Digital Markets Act (DMA) e il Digital Services Act (DSA) ha un approccio regolatorio forte e integrato sulle piattaforme. Come ha detto Roberto Viola, direttore generale della Dg Connect della stessa Commissione, le piattaforme sono importanti, ma non sono Stati, non hanno una legislazione indipendente. Devono anzi rispettare le regole di un mercato sano. E poi c'è un irrinunciabile piano etico: i grandi player del digitale hanno fatto enormi profitti e ora hanno il dovere di reinvestire per fare in modo che internet sia un posto sempre più sicuro e fruibile.

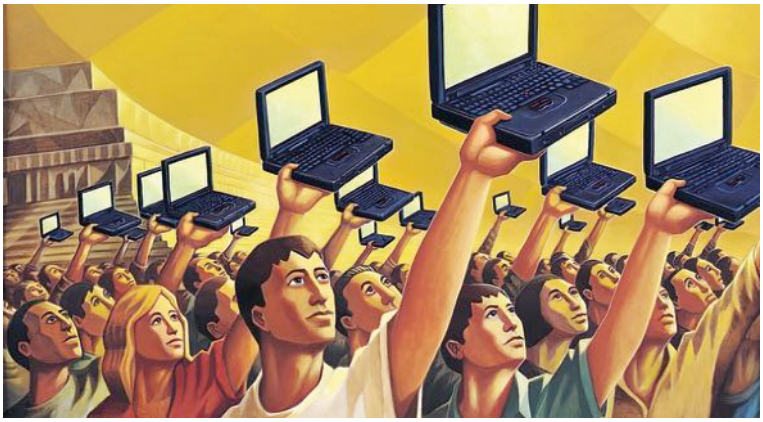
Lei ha parlato della prospettiva legata al metaverso. Il Garante in occasione della giornata europea della Privacy ha dichiarato:* «Non è tanto la novità concettuale che deve sconvolgerci, di virtuale ci hanno parlato Pierre Levy, Negroponte e i primi teorici della Rete - quanto le problematiche legate all'impatto che questo nuovo "habitat" digitale avrà sulle relazioni sociali e sui comportamenti dei singoli, sulle loro libertà e diritti, così come sui processi decisionali della collettività". *Siamo di fronte a un nuovo banco di prova per giuristi, politici e uomini delle istituzioni.

Qual è il suo giudizio in merito?

Abbiamo già affrontato in questa conversazione l'aspetto giuridico. Sul piano economico, è chiaro che la corsa alla nuova "modalità dell'essere" potrà provocare squilibri, bolle e rischi speculativi. Qualcuno si lancerà alla ricerca di un nuovo Eldorado, sperando di intercettare grosse fette di una inedita torta di mercato e consumo, per cui è chiaro che una regolazione non potrà che impattare anche sulle attività economico-finanziarie, immobiliari e sui vari mercati "virtuali" e decentralizzati che dovessero affermarsi. Tuttavia, come sostiene il filosofo digitale Cosimo Accoto, probabilmente la virtualità è solo uno dei possibili *output* del metaverso, mentre l'internet immersivo sarà incorporato anche negli oggetti, nei corpi stessi, nei nostri ambienti, a partire dalla realtà aumentata, e vivremo dentro le tante simulazioni che stanno trasformando il mondo e stanno generando una "terraformazione", che impone un nuovo modo di stare sul pianeta.

In questo scenario c'è naturalmente grande attenzione e grande inquietudine attorno ai temi della cybersecurity, un terreno ormai cruciale sul quale si combattono battaglie criminali per il profitto economico, ma anche guerre di presunto carattere "etico" da parte di gruppi transnazionali e di attivisti militanti delle più svariate cause. A queste si aggiungono le schermaglie tra Stati sovrani per la supremazia geopolitica globale. Cosa può dire in merito?

L'Europa sta togliendo potere alle piattaforme e investendo sulla sovranità digitale e sulla difesa di istituzioni e cittadini. Le vecchie regole del mercato dell'informatica sono tarate su una realtà di 50 anni fa e quindi vanno aggiornate. Oggi bisogna badare al management dei dati e appunto alle piattaforme: dunque la legislazione va riscritta in chiave innovativa, come sta accadendo con i già citati DSA e DMA. Sono appena tornato da un viaggio di lavoro in Israele e da quelle parti sono attentissimi all'avanzamento della tecnologia in ottica militare.



Cosa può insegnarci lo stato di Israele in una delicata materia come la cyber security?

Sono molto progrediti sia sul versante hardware che software. Investono tanto in formazione: un comparto che è soggetto a continue mutazioni e che necessita di una robusta formazione scolastica, soprattutto secondaria. Bisogna inoltre saper spingere sulla capacità dei giovani di fare impresa innovativa, creando un ambiente favorevole alle start-up. A Tel Aviv sono bravissimi e noi, malgrado alcune eccellenze, abbiamo molto da imparare.

Sulla cybersicurezza, infatti, la sensibilità in Italia non è ancora altissima, ma l'IGF ha aderito da poco a "Repubblica Digitale", l'iniziativa strategica del Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei Ministri, proprio per sostenere il rafforzamento delle competenze digital. Infine, stiamo portando avanti una scuola *sull'Internet* governance per insegnare a imprese, enti e associazioni cosa sono e come funzionano le diverse tecnologie di cui disponiamo. Abbiamo celebrato l'evento zero ad Ancona, nello scorso novembre e proseguiremo sicuramente su questa strada. ■

Etica digitale e intelligenza artificiale. I rischi per la protezione dati.

Intervista VIP a Fabio Lazzini.

Autore: Massimiliano Cannata

Lo sviluppo dell'IA è al centro dell'attenzione non solo degli studiosi, ma dell'intera società. A detta di molti osservatori siamo alla vigilia di un'ulteriore rivoluzione che riguarda il nostro modo di vivere la contemporaneità. Ne parliamo con Fabio Lazzini, ingegnere delle telecomunicazioni, esperto di sicurezza delle informazioni, DPO di Soegi SPA, che ha pubblicato per l'editore Giappichelli, *Etica digitale e Intelligenza Artificiale.*

Ingegnere l'innovazione tecnologica sta cambiando i nostri asset di riferimento. Orientarsi non è facile, cosa consiglia di fare nel suo studio che sta suscitando un ampio dibattito non solo nella stretta cerchia degli addetti ai lavori?

La rivoluzione dell'intelligenza artificiale è la diretta conseguenza della continua evoluzione del genere umano, alla continua ricerca di un miglioramento delle condizioni di vita. Le sfide che ci attendono sono diversificate così come innumerevoli le aree di applicazione: dalla ricerca scientifica, all'informatica, alla robotica alla medicina sino al mercato azionario. Dobbiamo infatti pensare che la capacità dei computer di elaborare volumi enormi di dati anche in lingue diverse permette agevolmente di interpretare i dati al fine di ottenere i migliori risultati in ogni settore. L'esempio del settore automobilistico dove lo sviluppo dell'intelligenza artificiale è sotto gli occhi di tutti, rende molto bene la portata dei cambiamenti in atto. Le auto dotate di un sistema di giuda senza conducente sono di già una realtà, e con gradi di sicurezza sempre più elevati per la presenza di sensori e telecamere in grado di capire cosa succede durante la guida, prendere decisioni, effettuare manovre per evitare gli ostacoli.

In un futuro vicino queste automobili probabilmente diventeranno il nostro mezzo di trasporto principale. L'intelligenza artificiale ci permette, inoltre, di generare testi, tradurre lingue e interpretare un discorso, si pensi agli assistenti digitali come ad esempio Alexa o Siri, che sono già presenti nelle nostre case, così come la domotica cablata e il wireless sempre più alla portata di tutti, caratterizzati da servizi in cloud e dall'uso crescente

dell'IA. Oppure agli strumenti di riconoscimento vocale che utilizziamo con i sistemi di sicurezza o con gli smartphone: molti presentano piattaforme basate su sistemi di IA che permettono una vera e propria interazione tra il telefono e il suo possessore. La sfida futura risiede nella capacità nostra di gestire tutte queste trasformazioni ad oggi positive, e far sì che tutta questa tecnologia non ci si ritorca contro.

Nel saggio si parla di un "contesto etico" che va rafforzato e difeso. Quali strategie vanno adottate?

Ad oggi non conosciamo una definizione univoca di intelligenza artificiale. Quello che ci è dato conoscere è il fatto che la macchina è in grado di compiere in modo automatico e in piena autonomia un compito, che si esplica nella caratteristica propria di elaborare una quantità di dati, in un processo continuo di aggregazione e disaggregazione degli stessi. Il tutto a una velocità incomprensibile per l'uomo, secondo una particolare formula preconfezionata il c.d. algoritmo. Diventa così centrale la problematica relativa ai dati che vengono elaborati da macchine sempre più sofisticate in grado di apprendere autonomamente, (si parla non a caso di machine learning n.d.r.) o persino di sviluppare nuovi percorsi di acquisizione come nel caso del deep learning.

Se questo è possibile da realizzare per la macchina è invece difficile poter calcolare le numerose variabili impreviste e imprevedibili, cioè il discernimento. Quest'ultima è una caratteristica tipicamente umana così come propriamente umana è la capacità di esprimere emozioni, pensieri, attitudini e preferenze. Sarà dunque sempre più necessario porsi delle domande in merito al diritto e all'etica dell'algoritmo. Sarà quindi compito dell'uomo, del legislatore esaminare e sorvegliare i processi evolutivi dell'IA, affinché le enormi capacità della macchina siano sempre utilizzate in modo saggio per la stessa sopravvivenza della specie. Su questa linea si sta muovendo l'Unione Europea stillando delle linee giuda etiche nell'utilizzo della IA.

Governance giuridica e sviluppo della tecno-scienza

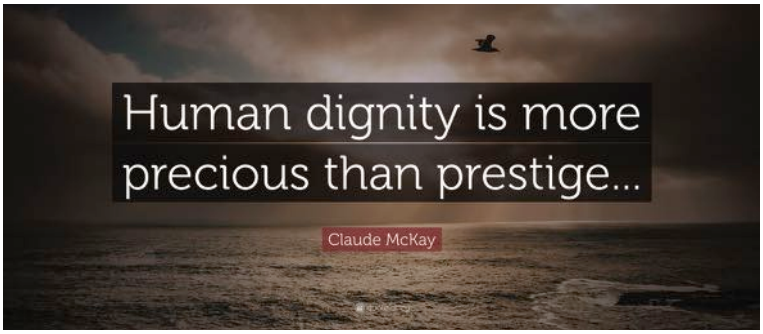
A proposito di regole, quale governance giuridica andrà pensata per strumenti potenti come l'intelligenza artificiale?

In un contesto di tecnologie sempre più traccianti, profilanti e predittive diventa sempre più necessario apportare strumenti in grado di tutelare gli individui, dalla violazione dei diritti dei dati personali. Questa esigenza è ancor più necessaria in vista della tutela degli individui dagli usi potenzialmente scorretti delle neurotecnologie, in grado di condizionare il pensiero e l'agire umano.

Si parla di neurodiritti, categoria di diritti umani attinenti alla sfera mentale e neurocognitiva. Si tratterebbe di una rivoluzione neurotecnologica, che crea nuovi contorni che sfuggono all'attuale quadro normativo vigente. La più comune delle neurotecnologie è l'elettroencefalografia una tecnica di registrazione elettrica del cervello, che è la più comune tecnica di monitoraggio in tempo reale dell'attività funzionale del cervello. Questa sarebbe in grado di condizionare il pensiero e addirittura l'agire: la cosiddetta interfaccia cervello-macchina, un canale di comunicazione diretta tra cervello e computer.

Di neurodiritti ha parlato recentemente Pasquale Stanzione, Presidente dell'Autorità Garante per la Protezione dei dati Personali, il suo saggio Ginevra Cerrina Feroni, si apre con la prefazione della giurista Ginevra Cerrina Feroni che fa parte della stessa Authority che sottolinea il ruolo del GDPR nell'evoluzione del delicato binomio: scienze giuridiche – evoluzione tecnologica. Cosa dobbiamo aspettarci su questo delicato fronte?

Diventa sempre più attuale la necessità di proteggere l'individuo dal pericolo di un uso scorretto di queste tecniche. L'attenzione del Garante non è solo opportuna, direi necessaria, in un quadro socio-tecnologico così in divenire. Attorno ai neurodiritti è importante che venga definito uno statuto



giuridico ed etico, in base a cui coniugare l'innovazione con la dignità della persona. Il rischio, altrimenti, è che innovazioni scientifiche potenzialmente preziose per la cura di stati neurodegenerativi divengano lo strumento per fare dell'uomo una non-persona, da addestrare o classificare, normalizzare o escludere.

"Algrograzia" e "algoretica" ambiti delicati e ancora poco conosciuti. Può dirci qualcosa in più in merito?

Algocrazia significa letteralmente "potere degli algoritmi", tutti noi siamo ormai circondati dalle più avanzate tecnologie, sia di informazione che di intelligenza artificiale. Queste, infatti, hanno assunto un peso sempre più rilevante nella società e nell'economia globale. e spaziano in settori molto diversi tra loro, che vanno dalla sanità, all'istruzione, alla giustizia, fino a toccare persino la politica. Tutta la nostra quotidianità è intrisa di tecnologia, si pensi agli assistenti vocali, al riconoscimento facciale, presenti nelle fotocamere dei nostri dispositivi o sui social network, strumenti tutti invisibili nell'interfaccia di app e programmi, che usiamo giornalmente senza neppure rendercene conto. Si basano su algoritmi anche le transazioni finanziarie e le geolocalizzazioni, i motori di ricerca dei nostri computer, la prenotazione di un posto in aereo o in treno, la firma elettronica. Tutto è basato su algoritmi e le prospettive di sviluppo futuro sono inimmaginabili.

Ed è qui che entra l'algoretica?

Certamente perché tutta questa tecnologia di cui abbiamo parlato bisogna saperla governare ed indirizzare, affinché non diventi volano di discriminazioni, fino a tramutarsi in una dittatura dell'algoritmo. L'algoritmo deve, per capirci, prestarsi (uso un termine per semplificare) a una dimensione etica che non significa che dei valori possano essere inseriti nelle logiche algoritmiche, caratteristiche proprie solo dell'uomo, ma prevedere e programmare dei sistemi in grado di orientare la macchina, consentendo di misurare il rischio che le cose possano andare in una direzione sbagliata, ciò vuol dire ledere il diritto o la dignità dell'individuo.

Un terreno delicato, difficile da praticare per chiunque, non crede?

Proprio per questo occorre codificare principi e norme, ripeto, etiche capaci di agire dentro la macchina. Questa è la sfida che dobbiamo portare avanti, affinché quella delle IA sia davvero una rivoluzione che porta a un autentico sviluppo, e l'etica possa accompagnare questo straordinario sviluppo della scienza e della tecnologia che sta segnando questo cambiamento d'epoca.

La figura del DPO nella società dell'informazione

Come si definisce il ruolo del DPO, figura che assumendo una valenza importante, mentre nelle aziende si sta assistendo a una ridefinizione di profili, competenze, assetti organizzativi?

Il Regolamento (UE) 2016/679 fornisce un rilevante contributo alla tutela dell'individuo e dei propri diritti fondamentali all'interno del nuovo mondo digitale. In questo contesto la figura del DPO assume un ruolo di primo piano, contribuendo a salvaguardare le libertà e la dignità degli individui - nell'utilizzo di processi decisionali automatizzati - da potenziali trattamenti discriminatori connessi all'illusoria neutralità degli algoritmi e a un uso distorto e non etico dell'Intelligenza Artificiale. Tale impostazione, per altro, risulta coerente con i principi di trasparenza e di accountability che permeano l'intero Regolamento, assicurando una maggiore visibilità dell'algoritmo e favorendo l'appello delle decisioni da parte dei soggetti direttamente interessati dal processo automatizzato. Il DPO come figura di controllo può altresì contribuire monitorare le regole e le logiche attraverso cui vengono implementati gli algoritmi che incidono sulle nostre vite consigliando che prima

BIO

Fabio Lazzini, laureato in Ingegneria delle Telecomunicazioni all'Università di Pisa, ha conseguito il Master universitario in Tecnologia dell'Informazione presso il CEFRIEL - Politecnico di Milano. Sin dall'inizio si è appassionato ai temi della sicurezza informatica e della privacy, delle architetture di rete e applicazioni IT, ricoprendo ruoli di responsabilità sia in ambito progettuale che di consulenza presso aziende di Information and Communication Technology. Ha contribuito alla progettazione e alla realizzazione di soluzioni tecnologiche ed organizzative in termini di analisi e ridisegno di processi aziendali, di sistemi di metodologie e di sviluppo informatico, per la Pubblica Amministrazione e per il settore privato. Conoscitore di standard e framework internazionali inerenti i sistemi di gestione della sicurezza e delle informazioni, è esperto della normativa sulla protezione dei dati personali, e attualmente, svolge la propria attività in una azienda italiana di Information Technology. Attualmente ricopre il ruolo di DPO e CISO di Sogei Spa. Autore di articoli e relatore in convegni, conferenze e seminari. Autore della pubblicazione *"La sfera pubblica e privata nell'era digitale. Il valore dei nostri dati"* e *"Etica digitale e Intelligenza artificiale. I rischi per la protezione dei dati"*. Cultore della Sicurezza Informatica presso l'Università di Foggia e l'Università di Roma Tre– Dipartimento di Giurisprudenza.

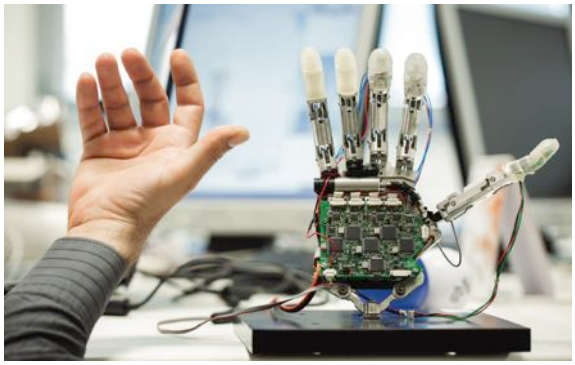
dell'esecuzione di un'attività di trattamento ne venga accertata la conformità ai valori etici e sociali condivisi anche attraverso una DPIA in modo da responsabilizzare i titolari e i responsabili circa le potenziali conseguenze etiche e sociali derivanti dall'utilizzo dei dati.

Vi è anche un interessante processo di ridefinizione delle responsabilità nell'impresa di oggi che deve essere preso in esame. Siamo pronti al riguardo?

Siamo sulla strada giusta. Rimanendo sull'analisi del DPO, va aggiunto che con il suo apporto garantisce una conformità normativa e un approccio aziendale etico e completo alla gestione del rischio IA migliorandone la fiducia nell'utilizzo. Per questo ritengo che all'interno delle organizzazioni sia necessario istruire comitati ad hoc per assumere le responsabilità chiare legate al rischio IA di cui il DPO deve essere parte attiva ed integrante. L'IA può essere inoltre utilizzata nell'ambito di protezione dati per le attività di audit e assessment sull'attuazione dei controlli di privacy e sicurezza facilitando l'analisi e la gestione di un eventuale data breach. La digitalizzazione dei controlli tramite l'intelligenza artificiale rende, infatti, possibile la condivisione degli obiettivi e le risultanze. Portando di fatto all'integrazione di diverse funzionalità e rendendo così più efficiente il processo.

Qual è il livello di consapevolezza che la società ha maturato sul livello rischio che la "potenza della tecnica" per sua stessa natura implica?

Stefano Rodotà parlò per la prima volta in Italia di "corpo elettronico" vent'anni fa. Il grande giurista s'interrogava sulle trasformazioni di un'identità umana che vivesse la realtà attraverso un corpo dotato di potenziamenti tecnologici applicati direttamente su di esso. Oggi tutto questo è diventato realtà, basti pensare ai dispositivi posti sui telefoni cellulari in grado di rilevare lo stato di salute generale della persona, e la possibilità di condividere tutto quanto col proprio medico curante e perché no, anche con l'assicuratore.



La biorobotica attraverso sofisticati dispositivi è in grado di creare braccia che possono sollevare pesi impensabili fino a poco tempo fa, oppure ai microchip che rendono superflui la carta d'identità o agli indumenti intelligenti che ci dicono come vestirsi a seconda dell'ambiente circostante. Il nostro corpo non è più materiale, ma diventa un insieme di dati sparsi in una molteplicità di banche dati, con profili che su queste basi vengono costruiti. La nostra conoscenza si sposta in un territorio nuovo. Questo mutamento di orizzonte incide sull'eguaglianza, sulla libertà di comunicazione, di espressione e circolazione, sul diritto alla salute. Dal principio giuridico dell'habeas corpus su cui si è per secoli fondata la libertà personale, siamo proiettati nell'area di pertinenza dell'habeas data. Si passa dalla tutela dell'integrità della persona alla tutela del corpo elettronico, considerando alla stregua di quello fisico, ed estendendo ad esso, con le dovute differenze, le medesime tutele. Emergono in questa dimensione profili "inediti" di responsabilità, perché anche il corpo elettronico ha un'anima che fa parte della nostra identità più intima e segreta.

Un capitolo del libro è dedicato allo sviluppo della cyber security. Quali strategie vanno messe in atto in questo delicato ambito che vede in particolare i minori particolarmente esposti?

Lo sviluppo crescente della tecnologia ha esposto qualsiasi azienda come ogni persona, alle minacce che provengono dalla rete internet. Gli attacchi informatici in Italia, così come nel resto del mondo, sono in forte crescita e la cyber security si trova di fronte a una minaccia persistente dovuta ai continui tentativi di penetrare la sicurezza aziendale da parte di malware, phishing, sociale engineering e altre tipologie di attacchi informatici. L'entrata in vigore del GDPR ha inciso in materia importante sugli investimenti nella sicurezza informatica, mettendo in evidenza quanto sia importante per le aziende che operano nel settore mantenere livelli di sicurezza adeguati per le informazioni, le quali costituiscono un valore da difendere.

Tocca però ai vertici aziendali valutare quali sono i rischi che possono verificarsi in materia di privacy di dati e informazioni e, quali sono le contromisure adeguate da prendere tenendo conto che la gestione della cyber security varia in base alle esigenze e alla struttura di ogni organizzazione. I rischi presenti sulla rete sono infatti molteplici, specialmente quando a subirli sono i minori, che possono essere vittime inconsapevoli di veri e propri reati, che vanno dall'adescamento dei minori, reato punibile penalmente, ai pericoli in caso di giochi pericolosi col rischio di emulazione. Basti pensare al caso più diffuso dei c.d. selfie estremi, ossia gli autoscatti fatti in luoghi pericolosi o al problema dell'accesso dei minori a contenuti non adatti alla loro età.

Molte sono a tal fine, le strategie poste in campo dai fornitori per la tutela di questi fenomeni che hanno subito ultimamente una crescita esponenziale. Si va dalla predisposizione agli utenti dei c.d. sistemi di parental control ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto. Ricordiamoci però che risulterà di importanza decisiva fondare la gestione di tali meccanismi su principi di chiarezza e trasparenza delle informazioni, nonché di semplicità e intuitività, in modo tale da dare a tutti la possibilità di metterli in pratica. Molto comunque c'è molto ancora da fare. La "sicurezza informatica" è un valore che riguardare tutti noi, nessuno può chiamarsi più fuori, siamo tutti coinvolti nella costruzione di una civiltà digitale che possa essere degna di questo nome. ■

Bloccare i moderni attacchi alla sicurezza informatica richiede XDR basata sull'identità.

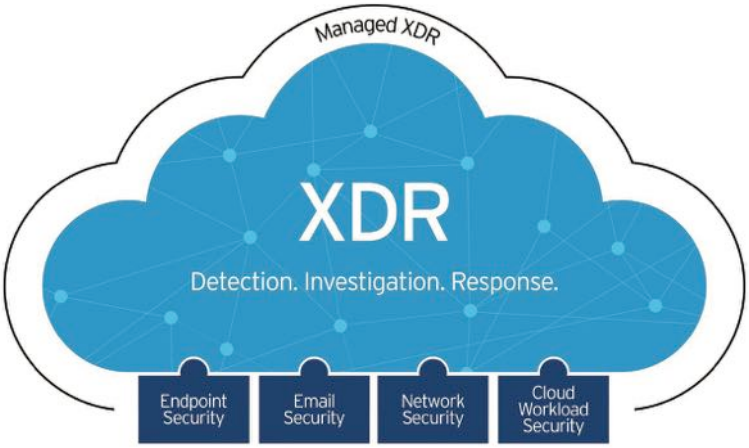
CROWDSTRIKE

Autore: Kapil Raina

Questo articolo offre una panoramica sul ruolo fondamentale della protezione dell'identità, su come questa differisce da ciò che i fornitori di IAM mettono a disposizione e su ciò che le aziende devono sapere quando si trovano a valutare i vendor di sicurezza.

Le aziende stanno rafforzato il proprio livello di protezione delle reti e degli endpoint, ma la compromissione delle identità è diventata un punto nodale in materia di infiltrazioni negli ambienti aziendali. Infatti, è stato rilevato un rapido aumento degli attacchi basati sull'identità: quasi l'80% sfrutta gli attacchi basati sull'identità per compromettere le credenziali legittime e usare tecniche come il movimento laterale per evadere velocemente il rilevamento. In questo scenario, le aziende devono comprendere gli avversari e le loro motivazioni, così da poter intercettare e rispondere tempestivamente a tali minacce.

Seppur la cybersecurity attribuisca all'XDR diverse definizioni e funzioni, secondo Gartner è bene optare per uno strumento di XDR che includa come minimo, gli endpoint, i data lake, strumenti di orchestrazione, dati delle "identità" per la correlazione e la threat intelligence.



BIO

Kapil Raina è VP Zero Trust & Identity Marketing in CrowdStrike. Con oltre 20 anni di esperienza nel settore della cybersecurity, è diventato una delle voci più importanti del settore della sicurezza informatica. E' un speaker molto attivo e autore di numerosi libri su argomenti tra cui PKI, biometria e altri argomenti di sicurezza.

Tuttavia, il problema è che la maggior parte dei fornitori di XDR non riesce ad integrare la protezione dell'identità in modo significativo. Seppur l'identità e la gestione degli accessi (IAM) siano importanti, non consentono una difesa totale dagli attacchi basati sull'identità. I fornitori di XDR non sono infatti stati progettati, fin dall'inizio, con la telemetria necessaria a identificare i moderni attacchi basati sull'identità in tempo reale tra ambienti ibridi, lavoratori che operano da remoto e archivi di identità multiple, senza incorrere in interruzioni delle attività degli utenti.

Dove e perché l'IAM fallisce?

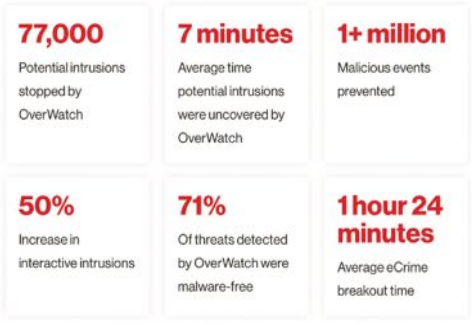
L'obiettivo finale di un avversario è sempre quello di ottenere l'accesso ai dati critici, in genere come utente privilegiato, e di muoversi eludendo il rilevamento.

I fornitori di IAM sono estremamente efficaci nella gestione delle identità digitali lungo i cicli di vita, dal provisioning al de-provisioning, consentendo alle aziende di gestire le identità digitali degli utenti e assicurando loro di avere accesso alle risorse necessarie per procedere con le proprie attività. Molte aziende si affidano a questi fornitori a supporto del loro impegno nel Zero Trust.

Il problema è che queste soluzioni di IAM presentano alcuni punti ciechi. In alcuni casi i fornitori di IAM hanno infatti difficoltà a proteggere la propria infrastruttura. Quando gli autori delle minacce usano credenziali compromesse, possono infiltrarsi nella rete ed aggirare le soluzioni di sicurezza adottate dalle aziende. Per prevenire questi rischi, le aziende devono essere in grado di coniugare perfettamente rilevamento e applicazione.

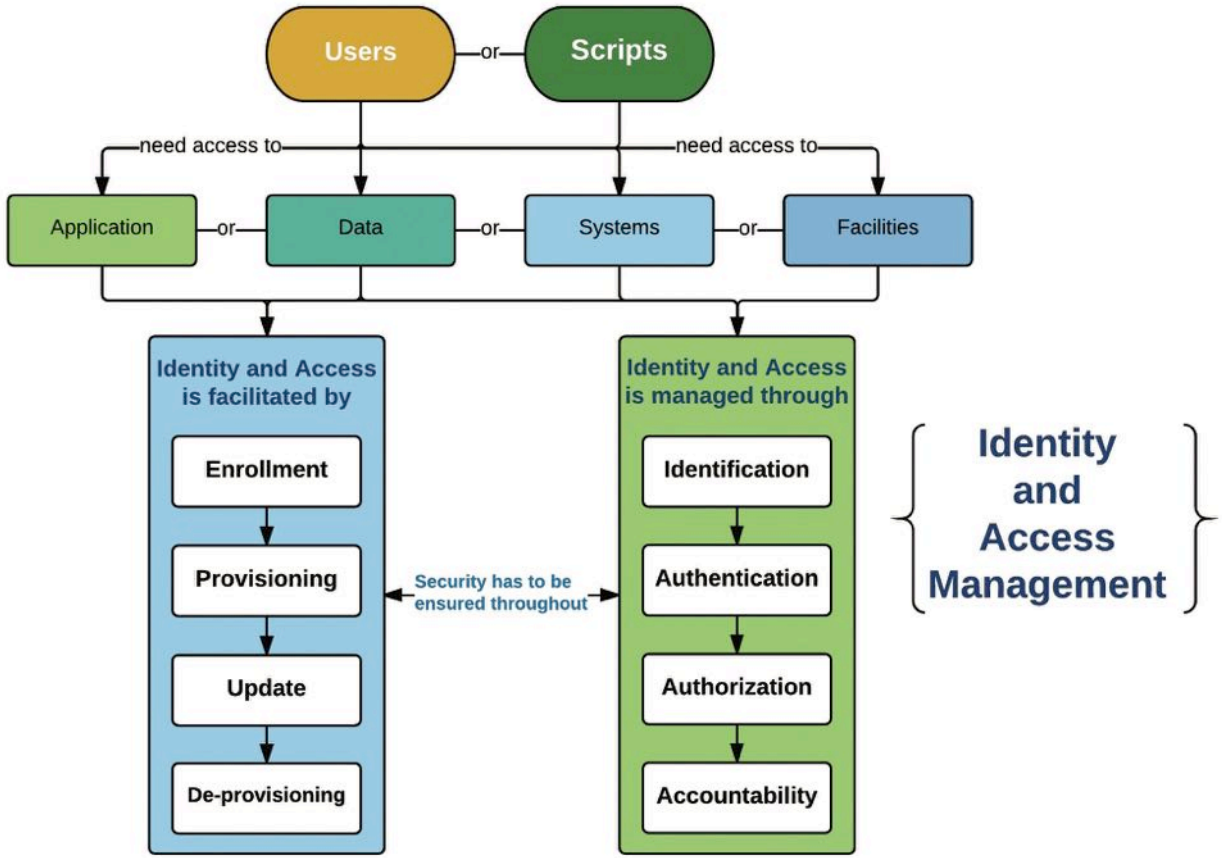
Protezione dell'identità: porre le giuste domande

Gli attacchi basati sull'identità stanno aumentando la velocità con cui gli avversari informatici ottengono l'accesso e si muovono negli ambienti aziendali. In media, gli attaccanti impiegano un'ora e venti minuti per muoversi lateralmente all'interno di un'azienda, in genere usando attacchi basati sull'identità. Se un avversario usa una credenziale valida, è molto più difficile determinare che si tratti di un malintenzionato. È importante disporre di una visibilità completa in tempo reale su tutto lo stack di sicurezza, al fine di identificare comportamenti potenzialmente anomali e agire rapidamente.



È possibile rilevare e difendersi da attacchi basati sull'identità? Innanzitutto, è fondamentale che le aziende si domandino se:

- hanno informazioni sufficienti da fonti native e terze parti, incluse le analisi comportamentali;



- riescono a elaborare ciò che sta succedendo e a bloccarlo in tempo reale e se sfruttano l'accesso condizionato basato sul rischio per ridurre al minimo i falsi positivi;
- riescono ad avere visione (e a proteggere) su tutto ciò che riguarda il proprio ambiente, inclusi i sistemi non gestiti o legacy;
- riescono ad agire proattivamente per contenere una violazione; ciò può includere la valutazione del rischio per bloccare un'identità compromessa su altri endpoint o consentire la segmentazione per prevenire il movimento laterale.

La maggior parte delle soluzioni di XDR odierne presenta delle lacune e non dispone delle capacità necessarie ad aiutare le aziende a rispondere alle precedenti domande. Gran parte dei fornitori di XDR si concentra su una determinata area di competenza, che si tratti di iniziare dalla rete o di far apparire più interessante una soluzione SIEM o SOAR.

Tuttavia, sebbene l'XDR estenda il rilevamento e la risposta dall'endpoint a tutti gli ambienti, è importante tenere conto anche dell'utente e dell'identità, nonché di tutto ciò che riguarda la threat intelligence. Le ultime soluzioni di XDR presentano dei problemi nel processo di correlazione degli schemi di attacco per determinare se un'identità è stata compromessa (ad esempio, identificando in tempo reale un endpoint non gestito, ma con un'identità nota). Per comprendere dove e se si è verificato un attacco, è necessario disporre della telemetria dell'endpoint e dell'identità, ma anche di una conoscenza approfondita dell'avversario con cui confrontare il vettore della minaccia.

XDR con protezione dell'identità: l'unione vincente

L'identificazione e la risposta agli attacchi in tempo reale sono davvero complesse, soprattutto se si guarda soltanto ad un piccolo aspetto di essi. L'IAM, infatti, è soltanto una piccola parte del grande puzzle della protezione dell'identità. Una soluzione di XDR completa, che dunque tenga conto di endpoint, identità e threat intelligence, consente una copertura a 360 gradi (dal cloud all'on-premise, ma anche mobile, dispositivi non gestiti e molto altro) ed è l'unica in grado di risolvere efficacemente questo problema.

Una volta fatto ciò nel modo corretto, le aziende dispongono di capacità di rilevazione ed investigazione cross-domain unificata per unire in modo efficace tutti i punti salienti, comprendere il contesto e automatizzare il rischio di risposta per fermare o contenere gli attacchi degli avversari informatici. L'XDR con la protezione dell'identità non soltanto blocca le minacce, ma migliora anche i profitti. Ad esempio, il CISO di un'azienda di vetri per auto ha riscontrato risparmi sulle spese operative: una riduzione del 75% delle reimpostazioni delle password di supporto, una riduzione dell'8% della suscettibilità al phishing e una riduzione del 32% dei diritti di accesso degli utenti non necessari. In conclusione, una soluzione XDR completa, in grado di correlare la telemetria cross-domain nativa e di terze parti, che abbraccia rete, e-mail, endpoint, identità, applicazioni web, applicazioni cloud e SaaS, workload, sistemi e strumenti di sicurezza di terze parti e altro ancora, è la scelta vincente.

A prescindere dall'approccio, è bene non trascurare l'importanza della protezione dell'identità nella vostra soluzione di XDR. ■

Fragilità e resilienza: attenti all'effetto "semaforo".

Intervista VIP a Alessandro Curioni.

Autore: Massimiliano Cannata

Dopo "Il giorno del Bianconiglio", Alessandro Curioni manda in libreria un secondo romanzo. Metodo narrativo e Cyber security costituiscono un interessante metodo per innalzare la consapevolezza di istituzioni, imprese e cittadini su un grande tema del nostro tempo. Ne abbiamo parlato con l'autore, esperto di formazione e docente di "Sicurezza dell'informazione" presso l'Università Cattolica di Milano.

Prof Curioni, qual è il messaggio che vuole dare al grande pubblico un esperto di cyber security utilizzando la leva potente e immaginifica del racconto?

La dedica spiega molto bene: *"A tutti quelli che non smettono di dubitare"*. Tutte le volte che qualcuno ci presenta una soluzione miracolosa, un'innovazione che ci porterà magicamente in un mondo migliore, una medicina senza controindicazione che guarirà la malattia; in ognuna di queste situazioni dobbiamo porci delle domande. Oggi siamo travolti dalle straordinarie opportunità che ci offre l'intelligenza artificiale e proprio per la loro eccezionalità in ogni campo dello scibile umano dovremmo porci più di una domanda. Spero raccontando una storia, magari intrigante, di indurre le persone al pensiero critico.

"Tante morti non fanno rumore, eppure ci inquietano". Quelle del Suo romanzo aprono il sipario su un mondo complesso, in cui il fitto intreccio di tecnologie e fattore umano genera inquietudine. Dobbiamo avere paura della rivoluzione digitale, che sta modificando l'individuo, la società e il contesto produttivo?

Dobbiamo riconoscere che laddove ci sono grandi opportunità ci sono rischi di pari dimensione. Gli orizzonti che ci aprono le nuove tecnologie sono straordinari e da esse dipende gran parte della transizione ambientale di cui tanto si parla e di conseguenza tanto del nostro futuro, ma se non riusciamo a gestire i rischi potremmo non avere quel futuro. Per la seconda volta nella storia dell'umanità, dopo la svolta nucleare, una tecnologia potrebbe portarci all'estinzione. Il primo segnale sarà quando non saremo più in grado di comprenderla, questo determinerà la nostra impossibilità di controllarla e a quel punto affronteremo il peggiore dei rischi: quello di cui non sappiamo l'esistenza.

Senza investimenti in cultura non potremo ridurre il rischio informatico

Cybersecurity Trends si focalizzerà, in questo numero, su due aspetti: Penetration Test e Automation Security. Alla luce della sua esperienza, su quali aspetti si dovrà insistere per rafforzare la capacità di difesa di aziende e istituzioni, riducendo i margini del rischio informatico?

Senza una cultura in materia non assisteremo mai a una riduzione sostanziale del rischio informatico. È la cultura che porta allo sviluppo della consapevolezza e senza di essa non sarà certo una tecnologia a metterci al riparo dai pericoli. Più di due decadi orsono, il celebre hacker Kevin Mitnick, durante un'udienza di fronte a una commissione del Senato statunitense, ebbe a dire: "si possono spendere milioni di dollari in tecnologie di sicurezza ma è del tutto inutile se è sufficiente chiamare una persona al telefono per convincerla a fare qualcosa che rende vana qualsiasi tecnologia". Oggi siamo ancora in quella situazione. Purtroppo, le trasformazioni culturali sono lente, mentre la società dell'informazione viaggia veloce.

A seguito del recente attacco causato dal* ransomware *che ha compromesso i server di molti Paesi, dalla Francia che pare sia stato il paese più colpito, alla Finlandia, dall'Italia fino al Canada e agli Stati Uniti, l'Agenzia per la Cybersicurezza Nazionale ha invitato istituzioni e imprese ad aggiornare i sistemi che si sono rilevati più esposti. Come si spiega questa trascuratezza che poteva determinare conseguenze molto gravi per milioni di utenti?

L'aggiornamento dei sistemi è una vera e propria croce, senza alcuna delizia. Le cause possono essere innumerevoli, da fattori molto umani come distrazioni e pigrizia a questioni tecniche che sorgono nel momento in cui l'aggiornamento di un sistema porta al mancato funzionamento di un altro. Vogliamo anche dire che i numeri remano contro? A seconda delle fonti si può stimare che ogni anno si scoprono tra le 20 e le 30 mila vulnerabilità ovvero tra le 50 e le 100 ogni giorno. Credo che queste cifre parlino da sole.

Il report 2022 della Polizia Postale ha mostrato un giro d'affari delle cyber truffe in esponenziale innalzamento. Lo scenario è reso ancora più complicato dalle tensioni geopolitiche di questa difficile fase della storia europea. Quali contromisure andranno adottate su un fronte delicato che presenta implicazioni decisive per il futuro della democrazia?

L'Unione Europea ha scelto la strada della normazione attraverso una serie di interventi legislativi che puntano a regolamentare l'intera società dell'informazione. Da un lato si tratta del tentativo di porre un freno al *"far west digitale"*, dall'altro di compensare l'impossibilità di raggiungere una propria sovranità tecnologica visto il pluridecennale ritardo nell'ambito della ricerca e l'assenza di campioni europei nel settore delle tecnologie dell'informazione. A mio giudizio sarebbe opportuno concentrare gli sforzi su un vasto programma di educazione digitale. Cittadini consapevoli sono il pilastro sui cui è possibile edificare quella resilienza di cui tanto si parla, facendo però ancora piuttosto poco.

Il metaverso? La coperta di cui disponiamo per affrontarlo è forse troppo "corta"

Minacce ibride e rivoluzione del metaverso. Sono ambiti ancora poco conosciuti. Quali prospettive si aprono per chi si occupa di sicurezza informatica?

Direi da incubo. Esiste un problema quantitativo. I professionisti sono ancora troppo pochi e vengono richieste loro competenze trasversali al di là di quanto sia umanamente possibile: difficile essere contemporaneamente un bravo cardiologo, neurologo e dermatologo. Questa considerazione ci porta al problema qualitativo. Oggi non è più possibile essere tuttologi nell'ambito della sicurezza delle informazioni e della cybersecurity, è necessario specializzarsi, ma essendo in pochi la questione diventa un circolo vizioso. Insomma, la coperta è troppo corta.

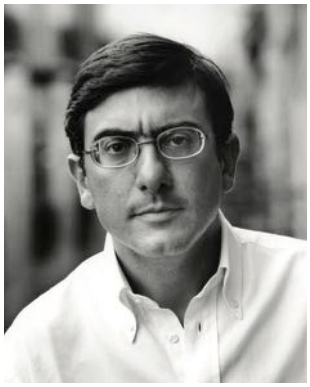
Vita reale e vita digitale si fondono. Le performance di ChatGPT stanno generando, come ha recentemente scritto Federico Rampini su Repubblica, timori e inquietudini in tutto il mondo. C'è una nuova questione della lingua che si fa strada. Il filosofo Eric Sadin parla di lingua industrializzata, che ci parla imponendo scelte e valutazioni. Sul fronte della sicurezza quali indicazioni bisogna trarre da questo nuovo capitolo della "quarta rivoluzione"?

Qualcuno parla di "post-umano", peccato che non abbiamo un'idea precisa di come finirà per configurarsi questa "post-umanità" e non saperlo rende il lavoro di chi si occupa di sicurezza molto difficile. Personalmente, penso che ci siano due questioni interdipendenti con cui dovremo fare i conti: la complessità e la fragilità. La prima deriva dalla fusione di reale e digitale. Parliamo di temi come la convergenza tra le tecnologie dell'informazione e quelle che governano in mondo industriale e degli oggetti, il possibile sviluppo di ambienti come i metaversi e le interazioni tra uomini e intelligenze artificiali. Le relazioni tra miliardi di uomini, macchine e oggetti produrrà triliardi di interazioni. Il risultato finale sarà un sistema in cui risalire la catena causale sarà impresa forse impossibile. Così se Lorenz negli anni Settanta, a proposito delle previsioni metereologiche, parlava dell'effetto farfalla, domani potremmo parlare di quello che ho chiamato "effetto semaforo", ovvero: un guasto a un semaforo a Shangai può causare un black-out a Londra. In questo senso tutto potrebbe essere molto fragile con buona pace della resilienza. ■

BIO

Alessandro Curioni (1967) nasce giornalista e nel 2003, dopo un biennio di studio, pubblica per Jackson Libri il volume *Hacker@tack* dedicato alla sicurezza informatica. Da questa esperienza, e dopo sette anni nel settore, fonda nel 2008 Di.Gi. Academy, azienda specializzata nella formazione e nella consulenza nell'ambito della cybersecurity, della quale è azionista e presidente. È autore di saggi di successo, divulgatore, docente universitario e commentatore presso organi d'informazione come Rai, "Il Sole 24 Ore" e Class Cnbc. *Certe morti non fanno rumore* è il secondo romanzo della serie che vede protagonista l'esperto di cybersecurity Leonardo Artico.

Il virus della disinformazione una minaccia per l'Europa.



Autore: Massimiliano Cannata

Essere giornalisti nell'era di chatGPT: un vasto orizzonte di nuove responsabilità e implicazioni emergono in questo momento storico denso di contraddizioni. La libertà dell'informazione appare minacciata dallo strapotere delle piattaforme, mentre risulta sempre più difficile fare il cronista nell'affollata arena del web, dove vero e verosimile si mescolano in maniera inestricabile. Un interessante seminario che si è svolto nella giornata dell'8 marzo a Roma *"L'Europa alla sfida della disinformazione: #Giornalismo #IA #FakeNews"*, organizzato dall'Osservatorio Tuttimedia e dalla Rappresentanza in Italia della Commissione Europea, ha affrontato questi aspetti destinati a pesare nell'immediato futuro. Al centro del confronto la preoccupazione per il "virus" dilagante della disinformazione, rispetto a cui il miglior antidoto (su questo gli specialisti convenuti si sono trovati d'accordo) rimane, anche nel tempo di Internet, la qualità nell'esercizio della professione giornalistica e il controllo rigoroso e puntuale delle fonti.

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 *"Technology Review"*, *"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.

"L'88% del pubblico che segue l'industria delle notizie per aggiornarsi e capire i segnali dell'attualità considera la disinformazione – ha commentato Carlo Corazza direttore dell'ufficio del Parlamento EU in Italia - come una grave minaccia per la collettività. Un giornalismo robusto può servire ad attenuare il rischio, perché sono i buoni operatori dell'informazione le prime sentinelle della democrazia liberale". Investire nella professionalità è dunque il fattore cruciale, se abbiamo a cuore i diritti universali, che sono patrimonio inestimabile di ogni uomo. Protagonisti del dibattuto sono stati gli specializzandi che frequentano i Master in giornalismo della LUMSA e della Luiss." Il ruolo delle nuove leve – ha sottolineato Antonio Parenti, capo della Rappresentanza italiana della Commissione Europea – oggi si carica di una importante dimensione etica. Individuare con perizia le fonti, privilegiando le più attendibili, vuol dire riaffermare quella funzione di critica e di controllo del potere che è compito del giornalista da sempre "cane da guardia" della democrazia".

Quando parliamo di equilibrio tra i poteri, sono sempre in gioco i principi cardine su cui si regge il pavimento della civile convivenza, fa notare Agnese Pini di rettore del "Quotidiano Nazionale": "Il fatto che l'informazione con l'avvento della rivoluzione hi-tech non sia più elitaria, amplifica l'esigenza di educare tutti ad un uso corretto della strumentazione digitale di cui ormai tutti disponiamo con grande immediatezza". Esiste un'ermeneutica della notizia (non stiamo parlando di un'astratta materia accademica ma di una capacità che il giornalista un professionista deve possedere) che risulta decisiva nella costruzione del racconto giornalistico e che può contribuire

a migliorare il discorso pubblico, troppo spesso superficiale quando non imbarbarito dall'assenza di visione del bene comune. "A questo proposito è utile ricordarsi che "Informazione e comunicazione non sono la stessa cosa - riprende l'analisi della Pini - marcare questa differenza significa comprendere quanto sia importante la lettura critica di fatti ed eventi".

La mediamorfosi irrompe nel cambiamento d'epoca

Il cambiamento d'epoca deve diventare esso stesso fenomeno di studio se non si vuole perdere la bussola di comprensione del presente. "L'arrivo dirompente di quello che gli studiosi definiscono *Large Language Modelling*, linguaggio sofisticato dell'intelligenza artificiale e dalle prime serie di GPT di OpenAI, con l'ingresso in campo di Microsoft e Google con Bing e Bard, segnala un salto quantico: non solo nel processo di trasformazione digitale, ma anche delle categorie epistemologiche e antropologiche", il parere di Derrick de Kerckhove, direttore scientifico di TuttiMedia, allievo di McLuhan, filosofo e massmediologo di fama mondiale, celebre teorico dell'intelligenza connettiva. "Gli esseri umani stanno per delegare alle macchine la loro caratteristica distintiva, cioè il pensiero in tempo reale con parole e immagini. Nella tempesta attuale si cerca, infatti, aiuto nell'IA che si presenta come una soluzione per il controllo sulla verifica dei fatti, per la traduzione linguistica, per il reporting automatizzato e per la personalizzazione.

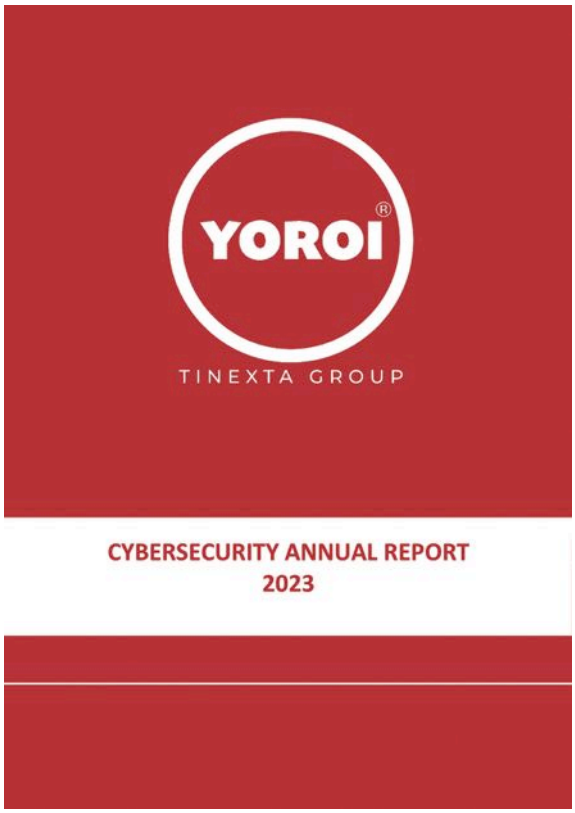
Le tecnologie però non sono ancora pronte o sufficientemente mature, perché non possono andare a sostituire la capacità e il senso critico del giornalista in quanto umano, come mi ha risposto anche lo stesso ChatGPT". Quella descritta dal direttore scientifico di MediaDuemila è una vera e propria "mediamorfosi", che vede l'ingresso dell'algoritmo anche nelle redazioni. Il giornalista è chiamato a non arretrare di un millimetro nel suo ruolo di mediatore, costretto come spesso si trova a regolare il traffico di notizie che corrono su piattaforme multicanale, che tendono a sfuggire a ogni verifica. Anche se abbiamo l'impressione che le fonti si moltiplicano a ritmi vorticosi, bisogna ricordarsi che il fatto rimane nella sua unicità, lasciando al cronista la responsabilità di analizzarlo, sminuzzarlo, raccontarlo. Sovente, lo si sta vedendo molto bene in questo *annus horribilis* della guerra russo-ucraina, l'approvvigionamento delle notizie è inquinato fin dalle origini, le carte vengono mescolate, nella volontà di nascondere la verità. *Slow news, no news,* era l'adagio tradizionale ricordato da Michele Mezza nel recente saggio "Net-War (ed. Donzelli), teso a sottolineare l'importanza del fattore tempo che insegue chi lavora con l'attualità ricercando il nesso plausibile che lega gli accadimenti. La libertà, non deve mai mancare nella tessitura dell'informazione, perché è la libertà il "respiro" della democrazia come solennemente sancito dall'articolo 21 della Costituzione. Oggi si impone una riformulazione di quel detto, nella forma: *"slow analysis, no news",* il giornalista di domani sarà sempre più un analista, che si misura con tecniche di cyber security, muovendosi nell'orizzonte del digitale. Si troverà a maneggiare una diversa sintassi, impegnato a proteggere fonti reali e virtuali, dalle insidie di *hacker,* capaci di giocare con gli eventi, di capovolgerli, proiettandoli in un "metaverso" di significati, difficili da interpretare.

La tecnologia è il messaggio

Ma se la tecnologia è il messaggio, l'algoritmo il vestito su misura che bisogna indossare, il senso critico del soggetto, la sensibilità che si sviluppa con il metodo dialettico e il confronto, che destino avrà? "Informazione e disinformazione sono due facce della stessa medaglia", il parere di Gianni Riotta, direttore del Master della LUISS con un passato di inviato per la televisione e la carta stampata. "Gli organismi europei riuniti a Roma sono impegnati nella battaglia contro la disinformazione ed è una buona notizia, peccato però che i fondi a loro dedicati siano stati dimezzati". Una contraddizione intollerabile denunciata in conclusione del dibattito da Maria Pia Rossignaud, vicepresidente dell'Osservatorio TuttiMedia e direttore responsabile di Media Duemila "Non ci può essere futuro senza visone, nostro compito è quello di tracciare percorsi e pratiche di successo per i giornalisti e il mondo dei media".

La nostra speranza è che il messaggio forte che nel giorno in cui si è celebrata la Festa delle Donne questa giornata di studi ha voluto lanciare all'opinione pubblica, possa diventare priorità nell'agenda dei governi e di quelle élite cosmopolite che hanno in mano il destino del Pianeta. ■

Il Rapporto Yoroi – Tinexta Group 2023 svela il forte rapporto tra geopolitica e cyber security.



Autore: **Massimiliano Cannata**

Il conflitto russo-ucraino evidenzia il forte nesso che lega la Cyber security agli equilibri geopolitici. La rete – ha scritto Michele Mezza in un interessante saggio *Net–war* (ed. Donzelli) - condiziona la guerra. Questo vuol dire in concreto che sono cambiati la dinamica e gli sviluppi del confronto tra le parti, che oltre a presentare una natura strategico militare, presentano un fitto intreccio di tecnologia e informazione. "Chi ha osservato – scrive il giornalista che ha alle spalle una lunga militanza come inviato della RAI - soprattutto la prima fase del conflitto, diciamo i primi cento giorni, avrà notato come si siano confrontati da una parte un modello che qualcuno ha definito ottocentesco di azione militare, simboleggiato dall'ormai famosa sequenza video della poderosa colonna di blindati russi lunga 65 km.

Dall'altra parte un sistema articolato e distribuito che combinava le risorse più ordinarie della rete, dai droni agli *smartphone*, da Telegram a Google street, per localizzare e colpire il nemico mediante la combinazione di informazioni che affluivano dalla popolazione e i sistemi di guerriglia territoriale. L'emblema di questa seconda strategia è l'altrettanto famoso appello del ministro dell'innovazione digitale Fiodorov a ElonMusk di un paio di giorni dopo l'invasione, in cui si chiede di mettere a disposizione della resistenza la sua flotta satellitare, cosa che avviene dopo qualche ora, con una spettacolare capacità di georeferenziare ogni singolo soldato russo che si muoveva sul territorio".

La conferma scientifica delle intuizioni di Mezza arriva dall'ultimo Rapporto Yoroi – Tinexta Group, il quale mette in risalto quanto la situazione geopolitica internazionale stia influenzando l'evoluzione delle minacce cibernetiche, sempre più sofisticate. "Appare sempre più netta – ci dice Marco Ramilli, Ceo e Fondatore di Yoroi - l'intenzione di portare attacchi in grado di mettere a rischio la sicurezza delle nazioni, come dimostra a livello tattico l'impiego di malware avanzati, progettati con il fine di utilizzare vulnerabilità zero-day, ovvero vulnerabilità sconosciute al momento del loro sfruttamento". Si tratta di strumenti particolarmente sofisticati da individuare e prevenire, cui va aggiunto il trend generale che fa vedere una crescita sensibile nell'ultimo anno delle minacce di tipo ransomware, in grado di aggredire i mercati. Il recente allarme lanciato dall'Agenzia Nazionale ha evidenziato il livello di rischio potenziale cui sono esposte reti e sistemi.

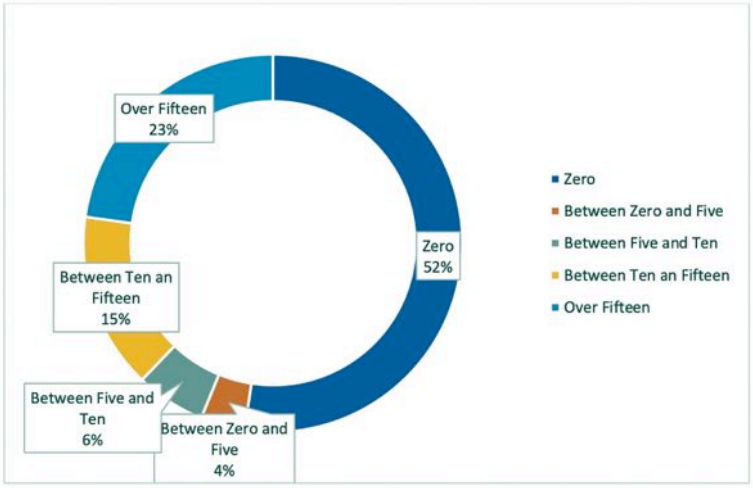


Figura 1: Distribuzione degli n-day malware

I sistemi industriali a rischio: come spegnere le città

Il crimine informatico dimostra grande padronanza degli strumenti digitali; oggi punta a colpire le RTU *(Remote Terminal Unit)*, il fulcro elettronico che regola l'operatività delle reti industriali, ferroviarie, elettriche, infrastrutturali. L'obiettivo, come rivela nell'intervista pubblicata in questo numero Roberto Maracino, General Manager e responsabile del SOC di Atlantica Digital, è quello di spegnere le città, provocando un arresto di tutte le attività produttive. Pensiamo cosa succederebbe se un luna park, gremito di bambini, si arrestasse per un improvviso blackout: smarrimento e paura avrebbero il sopravvento. L'azione di contrasto deve prevenire questa vulnerabilità, difficile da individuare.

Ma le minacce, come si vede dalle fenomenologie prese in esame da Yoroi, presentano molteplici facce. A cominciare dagli attacchi ai "leak" di codice sorgente ai danni di gruppi criminali, come quello subito dal gruppo Conti (cfr. *Il Ransomware nell'economia del cybercrimine,* nello spazio recensioni di questo numero, n.d.r.), che determinano spesso un vero e proprio riassetto nelle gerarchie dei vari gruppi criminali. La Double Extortion rende ancora più articolato l'orizzonte di analisi, che vede la formazione di gruppi strutturati in vere e proprie bande (gang) che hanno sviluppato malware unici per ogni attacco, si potrebbe dire, come si legge nel Rapporto, "attacchi firmati in maniera indelebile".

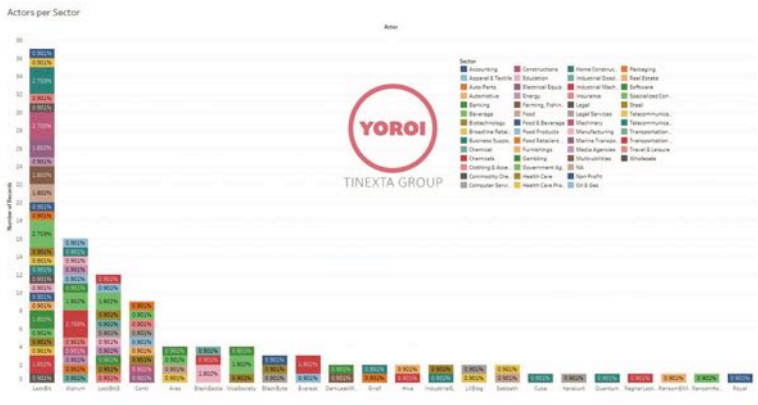


Figura 10: Distribuzione degli attacchi Double Extorsion in funzione del gruppo ransomware

Gli "altri" attacchi

Esistono altre forme di offesa, si tratta di azioni non targettizzate, che si potrebbero definire di tipo opportunistico, diffusi su larga scala, mirati a colpire il maggior numero possibile di aziende e di vittime. "Crimeware" e "Commodity Malware", sono gli strumenti maggiormente usati come per le fasi iniziali di un attacco informatico. Riportiamo, per completezza di informazione, alcuni *highlights* che possono aprire la strada ad approfondimenti futuri.

Il 52,4% dei malware individuati sono di tipo 0day, il che indica che i criminali informatici continuano a preferire la generazione di nuovo codice per colpire i propri bersagli. Interessante da analizzare è la presenza di una specializzazione rispetto ai target industriali. In altre parole, è di interesse riuscire a tracciare la distribuzione delle minacce per settore industriale; si osserva, ad esempio, una forte presenza di minacce di tipo "emotet" in relazione ai settori bancario, assicurativo e finanziario, mentre "AgentTesla" è principalmente presente nei settori industriali (Machinery, Utilities, Fashion) e nel settore Software/IT Services. Si evidenzia una ricorsiva stagionalità di alcune minacce relative a specifici settori industriali e al contempo è possibile osservarne l'indipendenza di altre. Va precisato che nel 2022 la principale minaccia da affrontare è stata quella del phishing, che colpisce in maniera indiscriminata ogni vittima.

La seconda tipologia di attacco utilizzata riguarda i cosiddetti commodity malware, facilmente acquistabili online. Una figura che sta guadagnando terreno e potere nell'universo del cyber crimine è quella del broker di compravendita degli accessi alle aziende. Questo servizio prende il nome di IAaaS, (Initial Access as a Service n.d.r). Gli attacchi operati con la tipologia DDoS (Distributed Denial of Service), "sono una minaccia "cresecente" e inaspettata – commenta in conclusione Ramilli, perché composta da innumerevoli tecniche e tecnologie, finalizzate a specializzare o contestualizzare l'impatto".

Se questo è il quadro, ci sarà da lavorare molto e con certosina continuità, in quanto l'evoluzione delle tecnologie cresce in potenza ma anche in fragilità. Sarebbe importante tenerlo a mente se vogliamo imboccare un percorso di autentico progresso civile e giuridico, elementi fondanti per una crescita sociale ed economica delle nostre comunità. ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

La Sicurezza Informatica

La sicurezza informatica è diventato un argomento sempre più importante nell'era digitale in cui viviamo. La psicologia gioca un ruolo fondamentale nella sicurezza informatica, poiché le vulnerabilità possono derivare da comportamenti umani inconsapevoli o da attacchi mirati a persone che commettono errori comuni.

In questo articolo, esploreremo come la psicologia gioca un ruolo essenziale nella sicurezza informatica. Infatti, per comprendere appieno la sicurezza informatica, non basta concentrarsi solo sulla tecnologia, ma è altrettanto importante tenere in considerazione il ruolo del comportamento umano.

Comportamento umano e Sicurezza Informatica

Il comportamento umano ha un impatto significativo sulla sicurezza informatica, poiché gli attacchi informatici spesso sfruttano le vulnerabilità psicologiche specifiche delle persone per accedere ai sistemi e alle informazioni sensibili.

In particolare, i cyber criminali utilizzano spesso le emozioni per influenzare i comportamenti delle persone e ottenere accesso alle informazioni che cercano.

Tra le emozioni maggiormente usate troviamo:

Per prevenire gli attacchi informatici, è importante che le persone siano consapevoli di queste vulnerabilità psicologiche e imparino a riconoscere le tattiche utilizzate dai cyber criminali.

Consapevolezza e Formazione

La formazione sulla sicurezza informatica aiuta le persone da un lato a comprendere le diverse minacce informatiche e a come poterle prevenire, dall'altro a come poter adottare dei comportamenti più sicuri.

Ad esempio, viene appreso come creare una password robusta, come verificare l'autenticità dei messaggi e delle mail e come evitare il phishing.

In definitiva, la consapevolezza e la formazione sono due fattori chiave per la protezione della sicurezza informatica.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud.cloud

Bibliografia

Camilla Salini, Giuseppe Brando, Marco di Costanzo
Il ransomware nell'economia del cybercrime
Edizioni Themis

Autore: Massimiliano Cannata

Il saggio di Camilla Salini, Giuseppe Brando e Marco di Costanzo nasce con la finalità di far conoscere alla comunità, che va oltre la stretta cerchia degli addetti ai lavori, il livello di rischio informatico cui quotidianamente tutti siamo esposti. "Mentre vi sono – spiega Giuseppe Brando responsabile per ENI di Cyber Threat Intelligence - molte pubblicazioni a livello internazionale che affrontano i temi della Cyber security, in Italia scontiamo un evidente ritardo. Quando parliamo di sicurezza informatica, dobbiamo pensare a un ecosistema molto strutturato, fatto di soggetti molto abili non solo per competenze tecniche, ma anche manageriali".

La trattazione prende in esame, un "caso di specie" emblematico: il "Conti team" gruppo di criminalità informatica, russofono che all'indomani dello scoppio della guerra in Ucraina è stato capace di "gettare un ponte" tra il reale e virtuale, facendo comprendere, a chi fosse ancora scettico, come il conflitto si sarebbe combattuto su due orizzonti strategici: il campo tradizionale di battaglia e l'"arena del web" che ha regole, insidie, linguaggi e meccanismi propri. "Dopo pochi giorni – prosegue il racconto di Brando – la dichiarazione di sostegno di questo gruppo al governo russo ha aperto un fronte articolato di implicazioni, provocando un inevitabile "rottura del vaso di Pandora". Per denuncia probabilmente di alcuni soggetti filo ucraini (sono supposizioni ma molto vicine alla realtà dei fatti) è emerso il fitto tessuto di chat (più di 380 fonti sono state comparate dagli autori) mentre il governo inglese ha postato le foto di molti dei protagonisti della vicenda.

Relazioni, negoziazioni, assunzioni, organigrammi, compiti, un intreccio di cose e persone è finito sotto la lente degli investigatori svelando l'enormità di un fenomeno che sarebbe molto grave sottovalutare. Presumibili i rapporti con i servizi segreti russi di questo gruppo. Non c'è da stupirsi se si considera l'interesse del governo di Putin ad alimentare una densa attività di spionaggio a costo zero. Più di 1000 aziende con il loro patrimonio di dati e informazioni, sono state compromesse. A libro paga anche giornalisti, ingaggiati per mettere pressione ad aziende e istituzioni attraverso la potente arma della disinformazione e della propaganda, che si sa fin dall'antichità, nelle guerre riveste da sempre un ruolo decisivo.

Le implicazioni economiche sono forse l'aspetto più inquietante della vicenda. L'FBI ha stimato – si legge nella ricerca molto ben documentata – introiti totali dovuti ai riscatti pari a 150 milioni di dollari, tanto che la Conti Corporation se non fosse "per le attività illecite perpetrate potrebbe avere le carte in regola per essere considerata come una start up tecnologica di riconosciuta eccellenza".

Quali contromisure, c'è dunque da chiedersi, se il nemico è così oscuro, capace e organizzato?

36 paesi e 12 società di cyber security si sono messi in moto costituendo il CRI (International Counter Ransomware Initiative) a dimostrazione che la gravità della minaccia esercita una pressione molto forte sui governi a tutte le latitudini. Il fattore umano rimane centrale, se si vuole vincere questa difficile partita. La sicurezza è infatti un valore trasversale che ha degli impatti decisivi non solo sulla geopolitica, ma in tutti gli ambiti della società.

Bisogna per altro ricordarsi che investire nelle competenze vuol dire anche calibrare gli investimenti. Pensiamo all'Intelligenza Artificiale, al successo e all'interesse che chatGPT sta suscitando, senza valutare tutti profili di rischio nel cammino di un'evoluzione che presuppone un dialogo sempre più stretto tra uomo e macchina, non si potrà andare molto lontano.

Economia, criptovalute, criminologia, psicologia, analisi dei dati, i team che operano nella cyber security dovranno, perciò, caratterizzarsi per il profilo multidisciplinare. "Conoscere il nemico per meglio conoscere sè stessi – prosegue Brando – sarà determinante come ci insegna la sapienza orientale degli scritti di Sun Tzu". Su questa scia di impostazione e di metodo lo studio va oltre, prendendo in considerazione anche l'area, fino a poco tempo fa, sconosciuta del darkweb, regione condensata di illeciti e opacità difficili da dipanare. Ampliando lo sguardo emerge così, ed è un ulteriore messaggio che emerge nella lettura, la necessità di una legislazione comune, che deve portare a una fattiva collaborazione tra gli stati, facilitando lo scambio di informazioni, le estradizioni, ma soprattutto prosciugando quelle zone "franche" che ancora oggi fanno da "scudo ambientale e geografico" di bande organizzate, capaci di muoversi con spietata rapidità sulle rotte reali e virtuali con l'unico convergente obiettivo di arricchirsi a danno della collettività, in spregio delle leggi vigenti e del rispetto dei diritti universali dell'individuo. ■

Italiadecide
Rapporto 2022
La fiducia cresce nelle pratiche di comunità
Ed. Il Mulino

Autore: Massimiliano Cannata

Il valore della fiducia nella società delle reti

Il Rapporto di *Italiadecide 2022* insiste su un termine chiave dalla duplice valenza etica ed economica: la fiducia, perno essenziale dello sviluppo sostenibile e della crescita. La pubblicazione

completa una trilogia iniziata nel 2019 con la Presidenza di Luciano Violante. Con metodo scientifico è stata, nel primo Rapporto, misurata la presenza di questo valore tra istituzioni, associazioni e sistemi di rappresentanza. Il secondo Rapporto si è soffermato sugli effetti che la fiducia genera sulle politiche di *"mutual endorsement"*, creando una convergenza di obiettivi tra gli attori del pubblico, del privato e del terzo settore.

Il lavoro di quest'anno ha come focus il territorio, orizzonte concreto entro cui dovrà attuarsi la transizione ecologica. Molteplici gli ambiti di analisi: l'amministrazione condivisa dei beni comuni, la capacità di incidere sullo sviluppo esercitata dalle organizzazioni non profit nel contesto delle *virtual communities,* la responsabilità sociale che gli attori individuali e collettivi devono sentire rispetto all'ecosistema. Di particolare interesse dal nostro punto di vista il valore della rete e delle connessioni come motore di sviluppo economico e sociale.

I modelli e le esperienze di partecipazione condivisa tra istituzioni, imprese e cittadini, riportati nel volume, sono testimonianza che la *"civitas"*, antica virtù dello spirito italico, storicamente manifestata nella straordinaria fioritura della civiltà comunale, anticipatrice del Rinascimento, non si è liquefatta, ma può ancora riprendere ancora più vigore nella internet society. "Nel tempo della disgregazione del tessuto sociale, del solitario trionfo dell'individualismo, della disaffezione per l'impegno pubblico – spiega nella prefazione la Presidente dell'Associazione Anna Finocchiaro - esperienze di collaborazione diffusa mostrano la possibilità di ritessere legami fondati sul reciproco rispetto piuttosto che sulla sfiducia tra privato e pubblico. Su questa scia il principio della sussidiarietà, sancito dall'Art. 118 della Costituzione sta trovando una sintesi alta nel moltiplicarsi di buone pratiche in 270 comuni italiani, nell'adozione di autonomi Regolamenti locali che incentivano esperienze di partnership a diversi livelli, nella definizione di appositi strumenti legislativi (la regione Lazio e Toscana hanno fatto da apripista) che indirizzano le politiche pubbliche a riconoscere la valenza delle reti civiche, come asset fondanti della ripresa.

La definizione stessa di "bene comune" appare cruciale come dimostra il riconoscimento del Nobel attribuito agli economisti Elinor Ostrom e Richard Thaler. Sulla spinta di una consapevolezza crescente le stesse comunità tendono oggi a identificare nel rispetto dei beni comuni, la qualità della cittadinanza di cui ogni individuo è portatore. Tante realtà vedono i cittadini in prima linea attivarsi per dare maggiore compimento al diritto all'istruzione, affiancando la didattica curriculare con discipline integrative allo scopo di migliorare il corpus di conoscenze delle giovani generazioni, stessa cosa avviene in svariati ambiti: dalla salvaguardia del patrimonio culturale a quello ambientali. È evidente (questo l'aspetto forse più originale che emerge nello studio di Italiadecide) che bisogna uscire dal "duplice inconciliabile dominio tra privatizzazione e pubblicizzazione, perché la difesa del bene comune va oltre ogni schematismo ponendoci di fronte a iniziative strutturate che con l'ausilio di nuovi strumenti di connessione possono ritessere il corpo collettivo slabbrato proiettando – prosegue l'analisi della Finocchiaro - un riflesso positivo sulla qualità democratica del paese". Compito di una politica illuminata può essere dunque quello di mettere insieme i segni di questo senso nascente di comunità, per poi, tentando di ridimensionare la dimensione del conflitto, provare a *"stipulare un contratto sociale senza spada"*, come auspicato dallo stesso Ostrom, che dà voce a una profezia che vorremmo tanto diventasse storia vissuta. ■

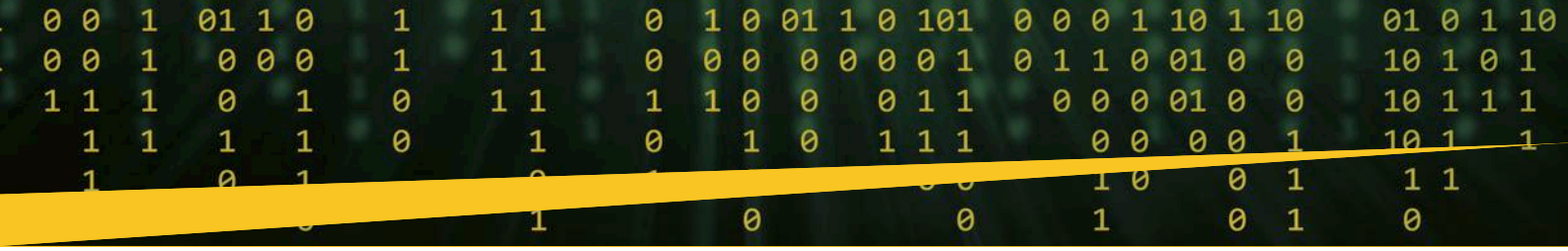
Anil Seth
Come il cervello crea la nostra coscienza
Raffaello Cortina Editore

Autore: **Anil Seth***

Le ferite di Freud

[…] Che siate o no degli scienziati, la coscienza è un importante mistero. Per ognuno di noi, la nostra esperienza cosciente *è tutto ciò che c'è*. Senza di essa, nulla rimane: niente mondo, niente sé, niente di interiore o esteriore. Immaginate che una versione futura di me, magari non molto lontana, vi offra l'occasione della vita. Posso sostituire il vostro cervello con una macchina identica sotto ogni aspetto, in modo tale che nessuno dall'esterno possa notare la differenza. Questa nuova macchina ha molti vantaggi – è immune dal deterioramento e magari vi permette di vivere per sempre.

Ma c'è un inghippo. Poiché nemmeno il futuro-me è sicuro di come il cervello dia origine alla coscienza, non posso garantirvi che avrete alcuna esperienza cosciente, nel caso doveste accettare questa offerta. Magari l'avrete, se la coscienza dipende solamente dalla capacità funzionale, dal potere e dalla complessità della circuiteria cerebrale, o magari no, se la coscienza dipende da un materiale biologico specifico – dai neuroni, per esempio. Ovviamente, poiché il vostro cervello-macchina conduce a un comportamento identico sotto ogni aspetto, quando chiedo al



vostro nuovo-io se è cosciente, il nuovo-io risponde di sì. Ma cosa succederebbe se, malgrado la risposta, la vita – per voi – non fosse più vissuta in prima persona?

Ho il sospetto che non accettereste l'offerta. Senza coscienza, non farebbe alcuna differenza per voi vivere altri cinque anni o cinquecento. Per tutto quel tempo, *non ci sarebbe nulla che si proverebbe a essere voi.*

Al di là dei giochi filosofici, l'importanza pratica di comprendere le basi cerebrali della coscienza è facile da riconoscere. L'anestesia generale è da considerarsi tra le più grandi invenzioni di tutti i tempi. Sfortunatamente, disturbi di coscienza angoscianti possono essere legati a danni cerebrali e malattie mentali per un numero sempre più alto di persone, me incluso, che vanno incontro a tali condizioni. E, per ognuno di noi, le esperienze coscienti cambiano nel corso della vita, dalla confusione rigogliosa e spumeggiante dei primi momenti di vita all'apparente, probabilmente illusoria e di certo non universale, chiarezza della vita adulta, fino alla nostra deriva finale nella graduale – e per alcuni disorientantemente rapida – dissoluzione del sé, allorché si verifica il decadimento neurodegenerativo. In ogni stadio di questo processo esistete, ma l'idea che esista un singolo e unico sé cosciente (un'anima?) che persiste nel tempo potrebbe essere grossolanamente sbagliata. Infatti, uno degli aspetti più coinvolgenti del mistero della coscienza è la natura del sé. La coscienza sarebbe possibile senza autocoscienza, e se lo fosse sarebbe ancora così importante?

Le risposte a domande difficili come queste hanno molte implicazioni sul modo in cui pensiamo il mondo e la vita che esso contiene. Quando arriva la coscienza durante lo sviluppo? Emerge alla nascita o è presente persino nell'utero? E cosa dire della coscienza negli animali non umani – non solo nei primati e negli altri mammiferi, ma in creature eteree come i polpi e magari anche in organismi semplici come i vermi nematodi o i batteri? Esiste un qualcosa che si prova a essere un'*Escherichia coli* o una spigola? E le macchine del futuro? Qui dobbiamo preoccuparci non solo del potere che le forme nuove di intelligenza artificiale stanno avendo su di noi, ma anche del se e quando dovremo assumere una posizione etica nei *loro* confronti. Per me, tali domande evocano l'inspiegabile compassione che ho provato guardando Dave Bowman distruggere la personalità di HAL nel film 2001: Odissea nello spazio, con il semplice gesto di rimuovere le sue banche dati, una per una. Nella maggiore empatia evocata dalle disavventure dei replicanti di Ridley Scott in *Blade Runner,* si trova un indizio sull'importanza della nostra natura di macchine viventi per l'esperienza di essere un sé cosciente.

Questo libro si occupa della neuroscienza della coscienza: il tentativo di comprendere come l'universo interno dell'esperienza soggettiva sia legato a, e possa essere spiegato nei termini di, processi biologici e fisici che si sviluppano in cervelli e corpi. Questo progetto mi ha affascinato per tutto il corso della mia carriera e credo che abbia ora raggiunto un punto in cui dei barlumi di risposte stanno cominciando a emergere […]

Uso il termine "wetware" per sottolineare che i cervelli non sono computer fatti di carne. Sono macchine chimiche tanto quanto sono reti elettriche. Ciascun cervello non è mai esistito senza essere parte di un corpo vivente, immerso nel suo ambiente e in interazione con esso – un ambiente che in molti casi contiene altri cervelli incorporati. La spiegazione delle proprietà della coscienza in termini di meccanismi biofisici richiede la comprensione che i cervelli – e le menti – sono sistemi *incorporati* e *integrati*. Alla fine, voglio lasciarvi con una nuova concezione del sé – l'aspetto della coscienza che è probabilmente per ciascuno di noi il più importante. Una tradizione influente, che risale perlomeno a Cartesio nel XVII secolo, sostiene che gli animali non umani sarebbero privi di ipseità cosciente perché non avrebbero una mente razionale in grado di guidare il loro comportamento. Sarebbero "macchine bestiali": automi fatti di carne, ma privi della capacità di riflettere su se stessi.

Non sono affatto d'accordo […]

Nonostante la sua reputazione sia macchiata tra i neuroscienziati, Sigmund Freud aveva ragione su molte cose. Guardando a ritroso nella storia della scienza, ha identificato tre "ferite" che sono state inferte alla percezione di sé della specie umana, ciascuna delle quali rappresenta un avanzamento scientifico decisivo a cui si è resistito per lungo tempo. La prima ferita si deve a Copernico, il quale, con la sua teoria eliocentrica, ha mostrato che è la Terra a ruotare intorno al Sole, e non viceversa. Così facendo ci ha reso consapevoli di non essere al centro dell'Universo. Siamo soltanto un granello disperso in qualche parte della vastità, un punto celeste sospeso nell'abisso. Poi è venuto Darwin, che ci ha rivelato che condividiamo un antenato comune con tutti gli altri esseri viventi, un'idea che, sorprendentemente, trova ancora oggi resistenza in molte parti del mondo. Immodestamente, Freud imputa la terza ferita contro l'eccezionalismo umano alla sua teoria della mente inconscia, che sfidava l'idea che la nostra vita mentale fosse sotto il controllo cosciente, razionale. Benché si sbagliasse su non pochi dettagli, Freud era nel giusto nel sottolineare che una spiegazione naturalistica della mente e della coscienza avrebbe rappresentato un'ulteriore, se non l'ultima, detronizzazione dell'umanità.

Questi cambiamenti nel modo di vedere noi stessi devono essere salutati con favore. Più avanziamo nella comprensione di noi stessi, più cresce il nostro senso di stupore, nonché la nostra capacità di vedere noi stessi non come separati dal resto della natura, ma come *parte integrante* di essa.

Le nostre esperienze coscienti sono parte della natura proprio come lo sono i nostri corpi e come lo è il nostro mondo. Quando la vita finisce, finisce anche la coscienza. Nel pensare a questo sono riportato alla mia esperienza – alla mia *non* esperienza – dell'anestesia. All'oblio che ne è seguito, forse confortante, ma pur sempre oblio. Lo scrittore Julian Barnes lo dice in modo magistrale nella sua meditazione sulla morte. Quando arriva la fine della coscienza, non c'è più nulla – davvero *nulla* – da temere.

**Per gentile concessione dell'editore pubblichiamo uno stralcio della bellissima prefazione dell'autore.* ■

La compliance integrata per l'attuazione del Modello 231

Mirjana Petrovich
Lucio Gioacchino Insinga
Fabrizio Rossi
Ed. Primiceri

Autore: Massimiliano Cannata

La compliance integrata nel capitalismo di "comunità"

Si viene presi da un senso di positiva armonia dopo la lettura di questo importante lavoro di approfondimento sul Modello 231, che colloca la realtà aziendale nella più vasta cornice di una responsabilità sociale e verrebbe da aggiungere "civile" che gli imprenditori e i manager devono avvertire in una fase drammatica come quella che l'intero pianeta sta vivendo.

Lo studio di **Mirjana Petrovic, *Lucio Gioachino Insinga,* e Fabrizio Rossi** va oltre la connotazione di un manuale d'uso, perché rimette molte cose al loro posto, operazione non semplice in questa fase di cambiamento d'epoca. Il messaggio che gli autori lanciano, non solo al pubblico e agli addetti ai lavori ma al target più ampio del corpo collettivo interessato a sapere qualcosa in più sul futuro che ci attende, è molto chiaro: nella "società delle catastrofi", attraversata da continue emergenze, per reggere l'impatto della tempesta perfetta, che oggi si è materializzata nella pandemia, ma che domani potrà assumere altre imprevedibili sembianze, bisognerà puntare sulla competenza e sulla capacità di leadership se vogliamo uscire dal lungo tunnel fatto di declino e di paura entro cui siamo piombati.

Parlare del D. Leg 231 che ha determinato delle profonde trasformazioni strutturali e tecnico organizzative per milioni di imprese, vuol dire sottolineare l'importanza della responsabilità come valore precipuo dell'impresa. Responsabilità è un termine critico, difficile da maneggiare che ci riconduce nell'alveo del dualismo classico tra *nomos* ed ethos, tra Creonte e Antigone, tra l'imperio della legge che definisce il campo della liceità e la dimensione del dover essere, che mette in campo l'individuo. Sono almeno tre i livelli di analisi, che si possono utilizzare per scandagliare il corpo di questa interessante e ben documentato volume:

- *giuridico* se ci si sofferma sulle parti dedicate alo sviluppo e all'inquadramento normativo;
- *filosofico,* apprezzabile nella capacità di lettura critica del presente, dote che appare molto spiccata nei tre autori;
- *strategico,* appare infatti evidente, che non è in gioco solo l'adempimento della norma, ma l'indirizzo più complessivo che imprese grandi e piccole, dovranno imboccare nella dinamica della competizione, che si gioca su scala globale.

Il *case History* cui è dedicata la parte conclusiva del libro, che racconta l'esperienza della Diddi Dino & Figli S.r.L afferma un principio, che vale la pena esplicitare: *"vogliamo affermare una cultura orientata all'esigenza di correttezza e trasparenza nella conduzione degli affari".* Nella sintesi dell'enunciato è leggibile un manifesto programmatico che contiene una molteplicità di aspetti che sono in questo momento al centro del dibattito pubblico: la trasparenza negli affari come motore del business e l'etica che deve tornare a fare da riferimento. Le azioni messe in atto dalla "Diddi, dalla formulazione del codice etico, alla messa a punto del sistema sanzionatorio, alla definizione di un assetto organizzativo idoneo alla prevenzione dei reati vanno nella giusta direzione, perché frutto di una visione includente che fa ben comprendere come il lavoro di mappatura delle vulnerabilità e di prevenzione dei reati, deve tendere a includere il corpus dell'azienda in tutte le sue componenti.

Va detto che questa visione, comincia a maturare in alcuni scritti precedenti di Lucio Insinga (basti in questa sede ricordare: *Come finanziare l'impresa,* pubblicato dallo stesso Primiceri e *La responsabilità sociale, Ed. Plenum*) rientra in un filone di ricerca che fa vedere molto bene come per fare impresa non basta poter disporre di un elevato corredo di conoscenze tecnico-giuridiche ed economico finanziarie. Serve un *"quid",* un "di più" misurabile nella capacità ermeneutica di lettura del tempo complesso, abilità che l'imprenditore deve imparare ad affinare, perché da essa dipende ogni *chances* di successo. Solo se collocata in quest'ottica trasversale la norma giuridica può contribuire a creare valore, non risolvendosi unicamente in un freddo adempimento burocratico, che l'imprenditore deve subire come un costo, o forse ancor peggio come un peso intollerabile.

È evidente che siamo di fronte a un cambio di passo: non possiamo soffermarci sulla "messa in regola", statica ritualità di un tempo che non esiste più, l'asse della valutazione dell'efficacia ed efficienza della *performance* aziendale va ruotata sugli impatti che ogni scelta economica - finanziaria proietta sugli *stakeholders* e sulla comunità di interessi verso cui si rivolgono le attività del business. Lo sviluppo di un doppio legame tra azienda e territorio, che emerge come uno degli aspetti centrali della trattazione, lascia presagire l'affermazione di una "cultura del confronto", intersettoriale (tra il settore pubblico e privato) e infrasettoriale (tra grandi player e la piccola impresa) destinata a segnare un diverso assetto di sistema, realizzabile nella dinamica di una vera e propria "rivoluzione copernicana" imperniata sul nuovo paradigma di un *"capitalismo comunitario",* come sostiene *Roberto Panzarani*, docente di governo dell'innovazione tecnologica dell'Università Cattolica di Roma, tra i massimi esperti di fenomenologia del cambiamento nelle organizzazioni complesse, in un interessante saggio: *"Il nuovo paradigma (ed. Lupetti).* ■

The Playlist (Per-Olav Sorensen, Netflix 2022)

Dalle fredde lande svedesi approda su Netflix *The Playlist*, la docu-serie (diretta da Per-Olav Sorensen) che racconta in maniera coinvolgente, anche se un po' romanzata, la nascita della celeberrima startup scandinava Spotify e della relativa app musicale, diffusissima nel mondo intero.

La storia di fondo, dunque, è quella facilmente immaginabile: è il racconto, all'inizio degli anni Duemila, dell'ascesa nel mondo imprenditoriale del giovane Daniel Ek (Edvin Endre), che insegue un'idea rivoluzionaria e insieme al socio Martin Lorentzon (Christian Hillborg) lancia sul mercato un rivoluzionario servizio di streaming legale musicale totalmente gratuito, l'ormai famosissimo Spotify. In un mercato musicale in quegli anni in profonda crisi, per via dei sistemi di download non legale e di pirateria legati a software come Napster e Pirate Bay, l'avvento della creazione di Daniel e Martin rivoluziona totalmente la situazione.

Naturalmente, per gli aspiranti imprenditori di successo non sarà una strada in discesa tutta rose e fiori, ma dovranno affrontare avvincenti e impegnative sfide per centrare l'obiettivo.

The Playlist utilizza un metodo originale e innovativo per raccontare una storia che altrimenti, per sommi capi, si conoscerebbe già: in sei puntate la docu-serie svedese racconta sei punti di vista diversi; così, se quello della prima puntata è ovviamente riferibile proprio al protagonista Daniel Ek, dalla seconda vediamo le cose dal punto di vista del suo socio, Martin Lorentzon, altrettanto coraggioso e visionario come lui; la terza è improntata sull'avvocato che si occuperà delle questioni legali, la quarta sul discografico che introdurrà l'idea nel mondo dell'industria musicale, la quinta sul programmatore che dovrà utilizzare tutto il suo genio da "nerd" per realizzare il player (all'epoca apparentemente impensabile) in grado di far partire la musica appena l'utente clicca play, senza alcuna latenza di rete (contravvenendo così uno dei protocolli fondamentali su cui si basava internet).

L'ultima puntata, infine, ha un retrogusto amaro: ambientata in un prossimo futuro, mostra le difficoltà economiche di una cantante, amica d'infanzia di Daniel, che ha raggiunto il successo artistico ma non riesce a stare dietro alle bollette con i soli proventi di Spotify. La puntata, infatti, parla dei criteri di redistribuzione degli introiti (enormi) dell'azienda e del fatto che Spotify è servita soprattutto a introdurre la vecchia industria musicale nel mondo digitale, mentre Daniel, nel suo percorso imprenditoriale, si è via via liberato di tutti coloro che lo avevano aiutato.

Forse la fine un po' triste per una bella storia, ma la bella storia resta. ■

Trust No One: alla ricerca del re delle criptovalute (Luke Sewell, Regno Unito 2022)

Ha suscitato un ampio dibattito e attirato l'attenzione di esperti, tecnici informatici, hacker e semplici curiosi: si tratta di *Trust No One*, il docufilm Netflix dedicato al mondo delle criptovalute e ai rischi che spesso può comportare se non vi si addentra con la dovuta cautela e le giuste competenze. Il documentario, infatti, mostra l'ascesa e il crollo di QuadrigaCX e del suo fondatore, Gerry Cotten, il mago delle criptovalute canadese finito in bancarotta quasi quattro anni fa.

QuadrigaCX era il più grande exchange di criptovalute (ovvero un portale informatico che rappresenta un autentico mercato, dove si vendono, si convertono e si scambiano criptovalute) in Canada, ma quando il suo fondatore, Gerry Cotten, muore (peraltro in modo molto misterioso), 250 milioni di dollari in bitcoin scompaiono come se li avesse portati con sé, come si suol dire, nella tomba.

Gerald Cotten, da tutti ritenuto un genio della finanza e dell'informatica, aveva fondato Quadriga nel 2013, e la sua era stata la prima piattaforma di exchange Bitcoin a ottenere il certificato di trasparenza da parte dell'antiriciclaggio canadese. Ma all'età di 30 anni, con un luminoso futuro davanti e un portafoglio clienti già enorme, il giovane rampante imprenditore muore improvvisamente in India durante il suo viaggio di nozze e da qui inizia lo spettro della rovina per i suoi numerosi clienti: lui era infatti l'unico a conoscere la password per accedere ai conti digitali, che contenevano 250 milioni di dollari in bitcoin.

La vicenda ha assunto toni da film, mediante una feroce e dispendiosa battaglia legale da parte delle decine di migliaia di clienti di Quadriga, per nulla convinti della morte del fondatore e anzi sicuri che Cotten abbia finto la sua morte per truffarli e tenersi tutti i loro soldi. Si è infatti scoperto che, poco prima di morire, l'imprenditore aveva intestato tutti i suoi beni alla (recentissima) moglie: la password viene reperita, ma salta fuori che i conti erano stati tutti svuotati nella stessa data del testamento.

Trust No One si sviluppa attraverso le diverse testimonianze di chi ha preso parte alla vicenda: sia chi è stato truffato da Cotten sia chi ha indagato sulle circostanze della sua morte, giornalisti e investigatori, ma viene intervistato chi lo conosceva personalmente (tranne la moglie Jennifer, forse vedova forse no, che non ha partecipato alla realizzazione del documentario). La truffa di Quadriga è già di per sé una vicenda piuttosto particolare, ma a renderla decisamente più intrigante è il contributo dato dalle vittime, che hanno personalmente indagato su tutti i punti oscuri: si va dalle scoperte più geniali alle teorie più assurde (c'è addirittura chi dice che Cotten si sia sottoposto a una plastica facciale dopo aver simulato la sua morte).

Una storia ricca di mistero, quindi, raccontata con maestria nel documentario Netflix, che fa luce ancora una volta sui rischi degli investimenti online e di quanto sia importante, in questo mercato, scegliere piattaforme sicure e certificate per i propri investimenti e la gestione del proprio portafogli digitale, in modo da essere al sicuro da truffe di ogni genere. ■

Severance (Ben Stiller, Aoife McArdle, USA 2022)

Di quanto aumenterebbe la produttività, se sul lavoro potessimo completamente staccarci da ogni altro pensiero? Un lutto, un dolore, una preoccupazione familiare, una bolletta da pagare: tutto cancellato per otto ore al giorno, nessuna distrazione, la mente totalmente concentrata sulle mansioni d'ufficio. E allo stesso modo, quando si esce, ci si dimentica completamente di quello che si è fatto in ufficio, del proprio lavoro, persino di chi siano i propri colleghi… un sogno o una distopia? Forse entrambe le cose, a seconda dei punti di vista: un sogno magari per i datori di lavoro, che si ritrovano impiegati profondamente dediti al lavoro con nient'altro in mente (e magari senza rischi che in quella stessa mente si portino segreti d'ufficio o industriali, una volta usciti), una distopia per chi sa immaginare i possibili sviluppi negativi di una situazione del genere che è la trama di *Severance*, serie Apple TV+ che fonde il drammatico, il thriller e la fantascienza, diretta da Ben Stiller (primi tre e ultimi tre episodi di nove) e Aoife McArdle (i tre episodi centrali).

Una potente multinazionale richiede ai suoi impiegati di sottoporsi a una avveniristica operazione chirurgica che permette la "severance", la scissione tra due parti del cervello che diventano compartimenti stagni: tutto ciò che riguarda il lavoro da una parte, tutto ciò che riguarda la vita privata nell'altra. Un chip nel cervello si attiva ogni volta che varcano la porta dell'ufficio per entrare o uscire dal lavoro e "spegne" la parte che in quel momento non serve (quella privata quando si entra in ufficio, quella lavorativa quando se ne esce).

Questa è la vita di Mark Scout (Adam Scott), impiegato della potente azienda. Sembra tutto perfetto, ma una serie di misteri coinvolge e stravolge le vite di chi gravita intorno all'azienda e al suo ufficio, mentre i ricordi delle due parti del cervello del protagonista iniziano a mescolarsi: Mark si ritroverà a indagare, ma facendolo sia in orario di lavoro che fuori ed essendo un uomo "scisso", lo farà con strategie e sistemi totalmente diversi a seconda di quale sua parte in quel momento predomina, fino quasi a far sembrare che di "investigatori" ce ne siano due.

Intrigante e coinvolgente, la serie Apple TV+ è in grado anche di inquietare. Non sono solo i colpi di scena, i plot twist, il crescere del thrilling e della tensione a catturare lo spettatore, quanto il senso di angoscia e quasi di claustrofobia che può prendere in certe scene, come quando ad esempio Mark piange in automobile per un suo dolore privato ma nel giro di pochi secondi, una volta varcata la soglia del suo ufficio alla Lumon, si attiva il suo chip, lui dimentica completamente che stesse piangendo e il perché, e diventa un gioviale e allegro impiegato per quegli stessi colleghi di lavoro di cui poi, quando uscirà dall'ufficio, neanche ricorderà l'esistenza.

Profonda è la critica sociale di una serie che dunque si inserisce nell'ormai ricchissimo filone delle distopie non troppo lontane nel futuro da noi. Impreziosita anche dalla presenza di attori del calibro di John Turturro, Patricia Arquette e Christopher Walken, *Severance* ha raccolto un meritatissimo successo di pubblico e di critica, incarnando alcuni timori inconsci che arrovellano la società moderna e soprattutto il futuro a cui potrebbe andare incontro. ■

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

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

www.cybertrends.it

The Innovation Group
Innovating business and organizations through ICT

Cybersecurity SUMMIT 2023

PNRR E CYBERSECURITY, CREARE VALORE CON IL TRUST DIGITALE

ROMA - 10 e 11 Maggio 2023
The Building Hotel

Torna a Roma l'undicesima edizione del **CYBERSECURITY SUMMIT** di **The Innovation Group**, il prossimo **10** e **11 maggio 2023**, il più importante appuntamento annuale dedicato ai Leader e ai professionisti della sicurezza. Un momento unico di scambio, incontro, condivisione sulle tendenze e sulle tecnologie innovative per far fronte al crescente volume di attacchi cyber.

Alcuni dei temi in agenda:

- Il ruolo della Threat Intelligence nella prevenzione e nella preparazione
- Il PNRR per la prevenzione dei rischi, il ruolo della partnership Pubblico-Privato
- Applicare un approccio Risk-Based a Detection, investigazione e risposta
- Rispondere all'allarme Ransomware e alle criticità della Software Supply Chain
- Ripartire velocemente dopo un attacco: le best practice dell'Incident Response
- Dare valore a prodotti e servizi con una sicurezza by-design, aderendo a certificazioni internazionali, rispondendo alla nuova Compliance UE
- Far evolvere nell'organizzazione la governance della cybersecurity
- Difendere le identità digitali, adottare strategie Zero Trust per mitigare gli Insider Threat
- Quantificare il rischio cyber per aiutare a prendere decisioni corrette su investimenti e organizzazione
- Impostare una Security-by-design nell'organizzazione a livello di processi, persone, misure, strumenti, automazione.

INFO
www.theinnovationgroup.it

MAIL
segreteria.generale@theinnovationgroup.it

CERT STAR

Il CERT STAR è un programma di incontri a porte chiuse dedicato ai CERT, SOC e Team della security italiani, finalizzato ad alimentare le competenze, promuovere la cooperazione e la condivisione di esperienze.

Durante gli incontri vengono analizzate a livello tecnico operativo le principali tematiche "core" dei team di security attraverso attività di laboratorio.

Caratteristiche:

- Incontri online e fisici
- Tappe su Milano e Roma
- Competizioni Capture The Flag
- Laboratori hands-on
- Presenza di Guest Star

Sponsor:

paloalto NETWORKS

CYMPIRE DISRUPTIVE CYBER SIMULATION

DARKOWL

CROWDSTRIKE

MANDIANT

XM Cyber

SentinelOne

Le Tappe del CERT STAR

- **07/02/23 - online - Cympire**
- **30/03/23 - Milano - Palo Alto Networks**
- **20/04/23 - Roma - DarkOwl**
- **25/05/23 - Milano - Crowdstrike**
- **20/06/23 - Roma - Mandiant**
- **28/09/23 - Milano - XM Cyber**
- **23/11/23 - Milano - SentinelOne**

Per maggior informazioni scrivere a: info@cybertrends.it

www.cybertrends.it