Cybersecurity Trends

Edizione italiana, N. 2 / 2023

INTERVISTE VIP:

- GABRIELE FAGGIOLI
- LUCIANO VIOLANTE
- MICHELE PETROCELLI
- DAVIDE GIRIBALDI

Folder centrale: Rischio Dinamico e Terze Parti

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

Cyber e Supply Chain ancora molto da fare.

Autore: Nicola Sotira

Appare ormai più che assodato che il tema della supply chain e della cybersecurity costituiscono aspetti sempre più collegati e fondamentali nell'ambito dell'industria e dei servizi. Il tema della sicurezza è ormai di importanza crescente in una gestione efficace della catena di approvvigionamento, in quanto la tecnologia digitale è diventata sempre più pervasiva in ogni fase dei processi di approvvigionamento e distribuzione. La gestione della supply chain coinvolge diverse parti interessate, come fornitori, produttori, distributori e clienti. Ogni punto della catena di approvvigionamento può rappresentare un'opportunità o un rischio per la sicurezza dei dati e delle informazioni. È essenziale garantire la sicurezza e la protezione delle informazioni per preservare la fiducia tra le parti coinvolte e prevenire potenziali minacce. In questo numero si è cercato di fare il punto, di capire come diverse realtà abbiano approcciato la tematica nei suoi vari punti che riassumiamo:

Valutazione dei rischi e pianificazione strategica. La gestione efficace della supply chain in termini di cyber security inizia con una valutazione dei rischi. Identificare le vulnerabilità potenziali e le minacce specifiche che possono colpire la supply chain è un passo fondamentale. È necessario condurre un'analisi delle minacce, valutare l'impatto potenziale di tali minacce e sviluppare una pianificazione strategica per affrontare e mitigare i rischi.

Forte collaborazione con i fornitori. Questi possono rappresentare un punto di vulnerabilità sotto il profilo della sicurezza. È fondamentale collaborare con i fornitori per garantire che adottino adeguati protocolli di sicurezza. La valutazione dei fornitori in base alle loro politiche di sicurezza, la condivisione delle migliori pratiche e la stipula di accordi contrattuali chiari sulla sicurezza dei dati sono tutte azioni importanti.

Sicurezza dei dati. La protezione dei dati è essenziale per prevenire le violazioni della sicurezza nella supply chain. Occorre verificare che le misure di sicurezza siano implementate e verificate lungo questa filiera, inserendo clausole nei contratti di fornitura, gestendo il ciclo di vita del fornitore e tenendosi aperta anche la possibilità di effettuare delle verifiche.

Formazione. La formazione e la consapevolezza dei dipendenti sono elementi fondamentali per prevenire le violazioni della sicurezza. Devono trovare spazio in questo dominio e formare la filiera sulle modalità di identificazione e gestione delle minacce potenziali. Promuovere una cultura della sicurezza in cui i dipendenti siano consapevoli dei rischi e siano attivamente coinvolti nella protezione dei dati può fare la differenza.

Risposta agli incidenti e piano di continuità aziendale. Nonostante le migliori misure di prevenzione, è possibile che si verifichino violazioni della sicurezza. È fondamentale avere un piano di risposta agli incidenti ben definito e un piano di continuità aziendale per mitigare gli effetti di tali incidenti.

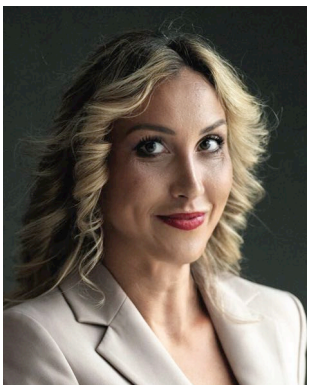
Conformità normativa Le leggi e i regolamenti in materia di sicurezza. Fondamentale il rispetto delle normative rilevanti e garantire la conformità alle stesse.

In conclusione, una gestione efficace della supply chain in termini di cyber security richiede un approccio olistico che consideri la valutazione dei rischi, la collaborazione con i fornitori, la sicurezza dei dati, la formazione dei dipendenti, il monitoraggio costante, la risposta agli incidenti e la conformità normativa. L'adozione di queste migliori pratiche contribuirà a rinforzare la supply chain, mitigandone i rischi garantendo il corretto funzionamento dell'azienda. Le materie di sicurezza devono essere considerate come una priorità strategica e integrata in tutti gli aspetti della gestione della supply chain. ■

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.

Tutela della Supply Chain Globale: Rischi Cyber, Incidenti, e Misure di Mitigazione.



Autore: Jelena Zelenovic Matone

Organizzare la scena

Qualche tempo fa, il gruppo di servizi di trading finanziario, ION, si è trovato alle prese con un attacco ransomware perpetrato dal gruppo di hacker Lockbit. Nonostante lo sfortunato evento, ION ha ripristinato la sua piattaforma di derivati compensati, consentendo ai clienti di riprendere le attività di trading.

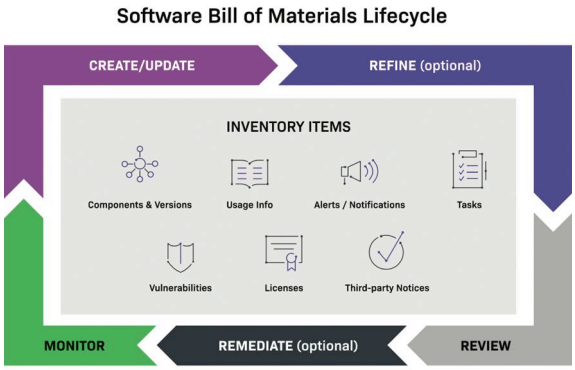
Tuttavia, questo incidente ha portato alla ribalta l'allarmante realtà delle minacce cyber che impattano in maniera diretta sulla supply chain, le quali possono avere effetti devastanti sul settore finanziario, comprese le principali banche, broker e hedge fund. L'esperienza di ION evidenzia la vulnerabilità delle organizzazioni nella gestione delle minacce informatiche provenienti dai loro partner, fornitori e vendor. L'attacco ha provocato interruzioni significative nel trading e nei processi di liquidazione, richiedendo interventi manuali con conseguenti ritardi nella registrazione delle negoziazioni. Inoltre, ci sono state notevoli difficoltà nella compilazione delle statistiche di trading e delle corrispondenti transazioni in borsa.

Recentemente un'altra società, Zellis, fornitore per l'elaborazione delle buste paga, ha subito un attacco alla supply chain di software che ha colpito diverse aziende importanti. In risposta, Zellis ha agito prontamente, disconnettendo il server interessato e ingaggiando un Incident Response Team. Responsabile dell'attacco che ha esposto i dati dei dipendenti è stato il gruppo ransomware Clop. Questo incidente sottolinea, ancora una volta, la vulnerabilità delle supply chain del software.

Alla luce dei recenti attacchi alla supply chain, che hanno attirato una diffusa attenzione, il presidente Biden ha emanato un ordine esecutivo (EO) sulla cybersecurity, volto a migliorare il modo in cui i dipartimenti federali, i fornitori e le altre agenzie collaborano con il governo.

Inoltre, una delle soluzioni chiave introdotte nel 2018 per affrontare la sicurezza della supply chain è stata la "Software Bill of Materials" (SBOM).

SBOM offre un inventario dettagliato delle parti costitutive del software, inclusi i componenti open source e di terze parti, insieme alle relative versioni e ai metadati associati. A causa della crescente complessità dello sviluppo del software e della crescente dipendenza da componenti open source in numerosi settori, SBOM ha preso significamente piede. Negli Stati Uniti, la National Telecommunications and Information Administration ha rilasciato linee guida che raccomandano l'utilizzo di SBOM per migliorare la sicurezza della supply chain del software attraverso un processo aperto che affronta la trasparenza dei componenti software.



Introduzione

La supply chain globale, una complessa rete di entità interconnesse, è sempre più suscettibile alle minacce informatiche. Con la crescente digitalizzazione delle operazioni e la dipendenza dalla tecnologia, le organizzazioni devono dare priorità alla cybersecurity per mitigare i rischi.

La protezione delle imprese dal ransomware ha ricevuto una notevole attenzione, ma la questione della protezione delle supply chain rimane relativamente inesplorata. Sarebbe vantaggioso se tutti i fornitori implementassero solidi protocolli di sicurezza per proteggersi dal ransomware e garantire una resilienza affidabile. Tuttavia, come abbiamo osservato con altri pericoli, questo scenario ideale è realizzabile solo a volte.

Nell'ambito della gestione della supply chain esiste una gamma di misure di cybersecurity, ciascuna con vari gradi di forza. Questa realtà rappresenta una potenziale fonte di rischio per le imprese. Per affrontare questo rischio, i Risk Manager hanno il fondamentale compito di valutare la sicurezza della supply chain, in particolare nei confronti del ransomware, e di identificare i fornitori con il livello di rischio più elevato. Questi manager devono quindi adottare misure appropriate per mitigare questi rischi. Tuttavia, questo compito può essere particolarmente impegnativo a causa delle risorse limitate disponibili e dell'incapacità di valutare completamente i fornitori dall'interno.

Una domanda cruciale è perché le aziende più piccole all'interno della supply chain non sono soggette agli stessi standard di conformità normativa delle organizzazioni più grandi. Purtroppo, nel nostro settore, le misure di sicurezza informatica di base tendono a essere trascurate abbastanza frequentemente a causa delle risorse/budget limitati.

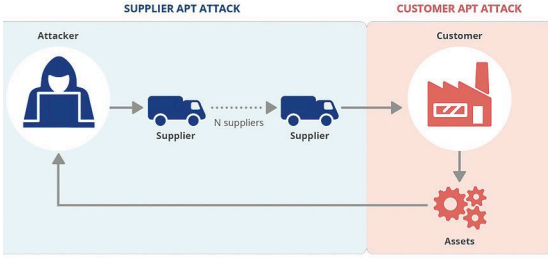
Un rapporto pubblicato dall'ENISA nel marzo 2023 indica che la supply chain è considerata una delle principali minacce alla sicurezza informatica per il 2030. Questo perché quando parti e servizi diversi vengono combinati per creare nuovi prodotti, potrebbero esserci vulnerabilità dovute a interazioni e interfacce non monitorate. Tali vulnerabilità possono aumentare il rischio che attori malintenzionati ottengano l'accesso alla supply chain attraverso lo sfruttamento delle vulnerabilità del software, hardware, e attacchi tramite configurazioni software), iniezione di malware o tentativi di phishing. Pertanto, è indispensabile che i soggetti interessati capiscano quanto la sicurezza dipenda dal software, in particolare dalle librerie open source, e siano consapevoli di potenziali compromissioni drive-by e attacchi di social engineering. Inoltre, è importante notare che esiste anche il rischio che soggetti di altri Stati si infiltrino negli impianti di produzione tramite addetti ai lavori per compromettere dati o sistemi, come si è visto nell'incidente di SolarWinds. Inoltre, c'è una crescente preoccupazione per l'uso improprio della tecnologia deepfake, che potrebbe portare a persecuzioni, inquinamento delle prove e disordini sociali. Mentre si prevede che la verification software migliori, potrebbero essere prese scorciatoie per soddisfare la domanda del mercato, rendendolo ancora più vulnerabile a coloro che desiderano utilizzare i deepfake per scopi illegali o non etici.

ENISA Threat Landscape for Supply Chain Attacks

È fondamentale riconoscere il ruolo cruciale della tecnologia nell'industria della produzione alimentare. In quest'ottica, il settore si è sempre più affidato ai sistemi digitali, il che lo rende suscettibile di interferenze da parte di soggetti che possiedono le risorse necessarie. Atti deliberati di sabotaggio, come la manomissione delle attrezzature di produzione o degli impianti di confezionamento, possono avere gravi implicazioni, tra cui la possibilità di carenza di cibo, instabilità economica e problemi di contaminazione.

Diversi recenti sondaggi condotti da organizzazioni rispettabili come il World Economic Forum (WEF) e Anchore hanno rivelato statistiche allarmanti sull'impatto degli incidenti informatici di terze parti sulle imprese. Incredibilmente, questi sondaggi indicano che molte organizzazioni, che vanno dal 39% al 62%, sono state colpite da tali incidenti. Inoltre, nel 2021 le compromissioni della supply chain sono diventate un comune vettore di infezione iniziale, rappresentando il 17% delle intrusioni, rispetto a meno dell' 1% di quelle dell'anno precedente.

La gravità della situazione è ulteriormente evidenziata dal rapporto ENISA sul panorama delle minacce per il 2021, il quale indica che nel 66% dei attacchi alla supply chain analizzati i fornitori devono essere trasparenti su come sono stati compromessi. Tuttavia, il dato preoccupante è che meno del 9% dei clienti compromessi tramite attacchi alla supply chain non era a conoscenza del metodo di attacco. Ciò indica un divario significativo nei livelli di maturità tra i fornitori e le aziende che si rivolgono agli utenti finali per quanto riguarda la segnalazione degli incidenti di sicurezza informatica.



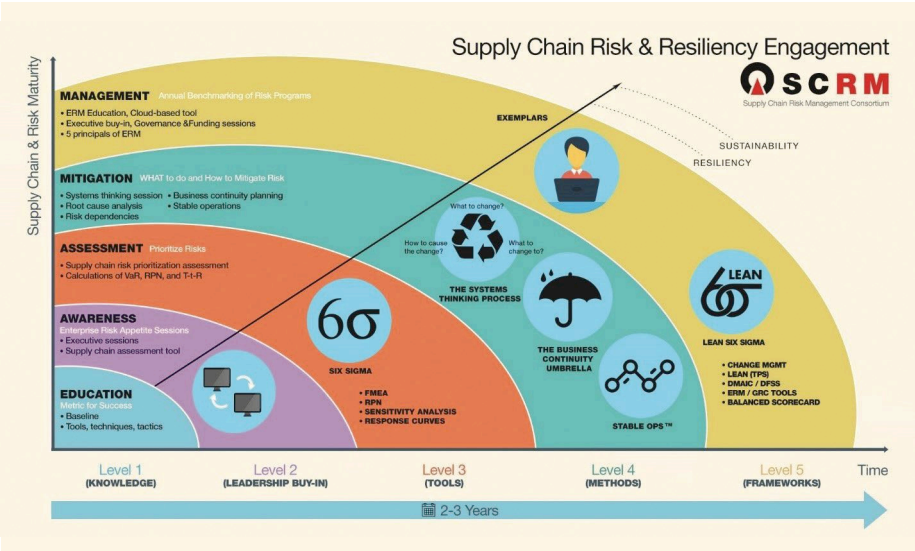
Il malware è la tecnica di attacco più comunemente utilizzata, con circa il 62% degli attacchi agli utenti che sfruttano la loro fiducia nei

loro fornitori. Gli attaccanti spesso compromettono gli utenti che sono oggetto di attacco concentrandosi sulla compromissione del codice dei fornitori. Inoltre, vale la pena notare che anche i ricercatori di sicurezza e i famosi repository open source, come Python, non sono stati immuni dalla minaccia degli attacchi informatici. In alcuni casi, questi gruppi sono stati presi di mira da malintenzionati, portando a iniezioni di malware non rilevate per periodi prolungati.

Le implicazioni sistemiche dei rischi informatici derivanti da partner, fornitori e vendor sono evidenti. Quasi il 40% degli intervistati in un recente sondaggio condotto tra cyber leader e CEO afferma aver sperimentato gli effetti negativi derivati da incidenti di sicurezza informatica che avevano colpito fornitori di terzi parti/supply chain. La maggior parte dei CEO ha espresso preoccupazione per la resilienza dei propri partner e fornitori, pensano, infatti, che essi siano meno resilienti delle loro organizzazioni.

Direttiva NIS2 e Rischi della Supply Chain

La direttiva NIS2 mira a migliorare il livello di cibersicurezza della supply chain dell'UE in risposta al complesso contesto della supply chain. Questa direttiva elimina la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali, estende la copertura a più settori, affronta la cybersicurezza della supply chain e le relazioni con i fornitori, introduce misure mirate come la risposta agli incidenti e la gestione delle vulnerabilità, sottolinea la responsabilità e consente valutazioni coordinate dei rischi per la sicurezza di servizi TIC critici. La direttiva NIS2 impone agli organismi essenziali e importanti di attuare adeguate misure di gestione del rischio cyber nelle supply chain e nei rapporti con i fornitori, tenendo conto della sicurezza della supply chain, dei rapporti con fornitori diretti o prestatori di servizi, delle vulnerabilità specifiche di ciascun fornitore e della qualità complessiva dei prodotti e delle pratiche di cybersecurity. Gli Stati membri hanno la responsabilità di garantire che i soggetti prendano in considerazione valutazioni del rischio in modo coordinato quando è il momento di definire le misure appropriate. Le organizzazioni devono anche tener conto della dipendenza operativa e garantire che i fornitori abbiano implementato misure di protezione, rilevamento e operazioni di ripristino 24 ore su 24, 7 giorni su 7 contro i ransomware.



BIO

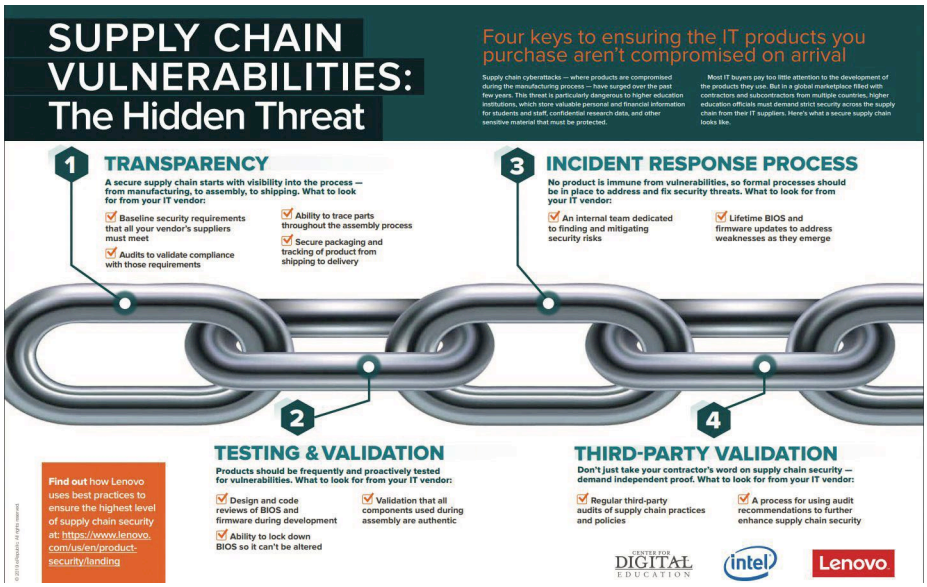
Rispettata leader CISO, insignita del CISO dell'anno per il 2019 in Lussemburgo, Sentinel CISO Global 2020, EU CISO 2020 e Ambasciatore dell'anno 2021 in Lussemburgo, Jelena è esperta di Cybersecurity versatile e innovativa con enfasi sulla gestione del rischio di sicurezza informatica/ risk management, 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.

Effetti degli Attacchi alla Supply Chain

In primo luogo, le vulnerabilità sistemiche possono portare allo sfruttamento di sistemi interconnessi all'interno della supply chain. In altre parole, se i sistemi di un organizzazione presentano delle vulnerabilità, gli attaccanti possono sfruttarle, ottenendo così l'accesso ad altri sistemi della catena e mettendo a repentaglio l'intera catena.

In secondo luogo, i cyber criminali possono compromettere gli scambi di dati come fatture o ordini di acquisto. Possono quindi manipolare le informazioni, commettere frodi finanziarie o interrompere le operazioni lungo la supply chain. Ciò non solo si traduce in perdite monetarie, ma può anche danneggiare la reputazione dell'intera catena.

Inoltre, misure di sicurezza informatica deboli nei fornitori di terze parti o fornitori di servizi possono introdurre rischi che si diffondono lungo tutta la supply chain. Ciò può compromettere l'integrità dei sistemi e dei dati critici, portando in ultima analisi a perdite significative.



Pertanto, le supply chain sono molto vulnerabili ai cyber rischi che risultano essere distruttivi per le imprese. Tra questi pericoli ci sono i data breach, che si verificano quando si ottiene l'accesso non autorizzato a informazioni sensibili. Tali violazioni possono comportare perdite finanziarie significative, danni alla reputazione e non conformità normative. Gli attacchi ransomware rappresentano un'altra minaccia notevole, nei quali i cyber criminali criptano i dati di vitale importanza e chiedono un riscatto in cambio del loro ripristino. Questi attacchi possono causare interruzioni operative, perdite finanziarie e danni alla business continuity. Inoltre, i cyber criminali che prendono di mira fornitori chiave o partner logistici possono interrompere l'intera supply chain, causando ritardi, carenze e insoddisfazione dei clienti.

La natura interconnessa delle supply chain le rende particolarmente suscettibili alla diffusione dei rischi cyber. Un soggetto compromesso può essere un gateway per consentire agli aggressori di spostarsi lateralmente attraverso la rete della supply chain, con conseguenti reazioni a catena. Ciò amplifica l'impatto degli incidenti informatici e può potenzialmente interessare più organizzazioni all'interno della supply chain.

Sfide della Supply Chain

Garantire la sicurezza della supply chain è una priorità essenziale per le organizzazioni. Tuttavia, presenta le sue sfide.

Una sfida principale è quando si fa affidamento su più partner di terze parti, ciascuno con le proprie pratiche di sicurezza informatica. Ciò può rendere difficile il mantenimento di standard di sicurezza coerenti lungo tutta la supply chain, portando a potenziali vulnerabilità.

La condivisione delle informazioni è stata una sfida nel nostro settore per anni e deve ancora essere concordata tra il settore pubblico e privato e gli stessi Stati membri.

Un'altra sfida è la visibilità limitata che le organizzazioni hanno sulle pratiche di sicurezza informatica dei loro fornitori o provider di servizi logistici. Con una visione chiara di queste pratiche, può essere facile valutare accuratamente i potenziali rischi e adottare misure proattive per mitigarli.

Inoltre, le supply chain sono ecosistemi complessi con molti stakeholder, tecnologie e processi. Questa complessità porta a un panorama di cybersicurezza dinamico e in continua evoluzione che richiede monitoraggio e adattamento continui.

La terminologia relativa alle varie definizioni e il significato in termini di portata e approcci di implementazione possono creare incoerenze.

I rischi a livello degli Stati membri potrebbero essere più difficili da gestire per un'organizzazione piccola. Ad esempio, sarebbe difficile rispondere ad attacchi sponsorizzati da uno Stato aventi più risorse a disposizione, un'elevata motivazione e il coinvolgimento dei servizi di intelligence.

Per affrontare queste sfide in modo efficace, le organizzazioni devono lavorare a stretto contatto con i propri partner per garantire standard di sicurezza coerenti lungo tutta la supply chain. Devono inoltre implementare solidi processi di monitoraggio e valutazione per identificare potenziali rischi e vulnerabilità e adottare misure proattive per mitigarli. Gli Stati membri dovrebbero prendere in considerazione l'esecuzione di alcune delle valutazioni del rischio ICT/OT al loro livello, compresa la creazione di politiche nazionali generali e la comprensione comune nell'ambito della gestione della catena di approvvigionamento ICT/OT.

Cosa possono fare le organizzazioni?

Garantire la sicurezza delle informazioni sensibili è della massima importanza per qualsiasi organizzazione. Per raggiungere questo obiettivo, ci sono varie misure che le organizzazioni possono adottare:

1 Per mantenere un'elevata protezione contro le minacce digitali, tutte le organizzazioni dovrebbero disporre di politiche di sicurezza delle informazioni ben sviluppate e solide. Ciò comporta la conduzione di valutazioni del rischio complete e continue e l'esecuzione di adeguate verifiche su fornitori e collaboratori di terze parti per rilevare e mitigare potenziali vulnerabilità. Adottando queste misure proattive, le aziende possono salvaguardare i propri dati sensibili e impedire che gli attacchi informatici compromettano le loro operazioni.

2 Per migliorare la resilienza complessiva della cybersecurity di un'organizzazione, è fondamentale implementare un approccio globale e stratificato alla sicurezza. Questo approccio comprende una serie di misure, come robusti protocolli di crittografia, controlli di accesso adeguati, gestione meticolosa delle risorse, patch regolari del software, severi controlli di sicurezza fisica e un ambiente di sviluppo sicuro. Implementando queste misure di sicurezza essenziali, le organizzazioni possono ridurre significativamente il rischio di attacchi informatici e proteggere i propri dati sensibili da accessi e sfruttamento non autorizzati.

3 Avere una strategia ben fatta per gestire gli incidenti informatici è importante. Non basta creare e dimenticarsene; test regolari sono fondamentali per garantire che il piano sia efficace e possa essere eseguito senza indugio. Educare i dipendenti a identificare e rispondere alle e-mail di phishing è una componente fondamentale di questo piano. Inoltre, solide procedure di backup e ripristino possono aiutare a ridurre al minimo i danni causati da un incidente informatico. Le organizzazioni possono gestire meglio le potenziali violazioni della sicurezza adottando questi passaggi fondamentali.

4 Le aziende e le società devono prestare attenzione ai servizi di rete che espongono su Internet. Solo quei servizi che sono stati rigorosamente autorizzati e ritenuti sicuri dovrebbero essere messi a disposizione del pubblico. Ciò è essenziale per mantenere l'integrità della rete dell'organizzazione e proteggerla da potenziali minacce alla sicurezza.

5 La collaborazione tra i partner della supply chain è fondamentale per garantire la sicurezza e la protezione delle operazioni aziendali. Lo scambio di informazioni preziose, come informazioni sulle minacce, best practice e lezioni apprese, svolge un ruolo fondamentale nel mitigare i rischi associati agli attacchi ransomware. È essenziale riconoscere che la minaccia ransomware persiste e le aziende devono adottare una strategia a lungo termine per contrastarla in modo efficace. Lavorando insieme e condividendo le conoscenze, i partner della supply chain possono rafforzare le proprie difese e ridurre al minimo l'impatto di potenziali minacce informatiche.

6 Considerare che alcuni studi hanno dimostrato che è prassi per le aziende migliorare le proprie difese di cybersecurity solo un anno dopo essere state prese di mira dal ransomware. Pertanto, è importante non dare per scontato che le organizzazioni recentemente vittime di tali attacchi abbiano già adottato misure adeguate per proteggersi da minacce future.

Pratiche di Gestione delle Relazioni con i Fornitori

Quando un fornitore e un'organizzazione concordano determinati termini e condizioni, è imperativo redigere un contratto che funge da documento base che delinea i termini e le condizioni del rapporto. Mi piace chiamarla una "Bibbia" perché espone dettagli cruciali che richiedono un accordo reciproco. Il contratto dovrebbe contenere diversi elementi essenziali, come la conformità ai requisiti legali e regolamentari, una comprensione condivisa della condivisione dei dati, norme che disciplinano il subappalto e le condizioni a catena, ruoli e responsabilità chiaramente definiti, un piano per la gestione degli incidenti e l'adempimento degli obblighi di notifica, il diritto di audit, monitoraggio delle prestazioni del servizio, un piano di gestione del cambiamento, procedure di ripristino di emergenza, requisiti di sicurezza per prodotti e servizi ICT/OT, garanzie dei fornitori e dei provider di servizi in merito ai controlli di sicurezza, procedure per la risoluzione del contratto e la gestione dei prodotti a fine ciclo formazione per entrambe le parti sulle regole di assunzione e comportamento, classificazione dei beni condivisi e dei beni informativi accessibili a fornitori e provider di servizi e obblighi di entrambe le parti in materia di protezione e accesso alle risorse informative.

Conclusione

Per salvaguardare la supply chain globale dalle minacce cyber, le aziende devono lavorare insieme in uno sforzo congiunto. Ciò comporta una comprensione approfondita dei vari tipi di rischi cyber esistenti, delle loro modalità di trasmissione lungo la supply chain e delle sfide coinvolte nella loro mitigazione. Le misure efficaci per affrontare questi rischi includono la collaborazione, la valutazione dei rischi, solidi controlli e policy di sicurezza e lo sviluppo di piani di risposta agli incidenti. Inoltre, con l'introduzione di nuove normative come NIS2, spetta alle organizzazioni garantire che le proprie terzi parti rispettino standard di sicurezza informatica più elevati, rafforzando così la cybersecurity complessiva della supply chain.

Le supply chain, infatti, sono in continuo cambiamento ed evoluzione, interagendo con numerosi servizi esterni. Per un utente malintenzionato, questa complessa rete di sistemi interconnessi rappresenta un obiettivo interessante e vulnerabile. Pertanto, quando si valuta la supply chain, è comune prendere in considerazione vari scenari di minaccia, inclusa una panoramica completa che specifici modelli di minaccia che si concentrano su elementi e componenti critici.

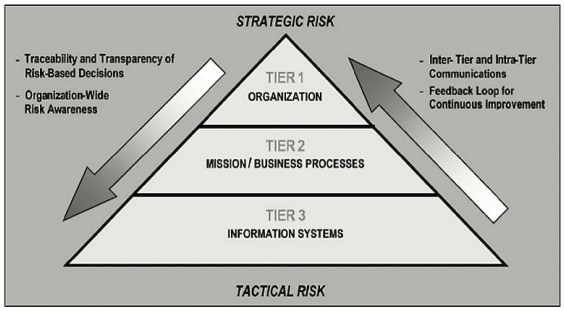
Un approccio proattivo e cooperativo che coinvolga tutte le parti interessate è essenziale per gestire con successo i rischi cyber nella supply chain. ■

Cybersecurity Supply Chain Risk Management (C-SCRM): un approccio dinamico.

Autore: Francesco Corona

Il NIST (National Institute of Standard Technology) nella pubblicazione SP 800-161r1[B001] offre una chiara ed efficace metodologia integrata globale di gestione del rischio cyber di una tipica Suply Chain operante nel settore della sicurezza informatica attraverso un modello organizzativo multilivello. La metodologia comprende le linee guida sullo sviluppo di piani di implementazione della strategia C-SCRM, le politiche, i piani e le valutazioni del rischio sui prodotti e servizi della Supply Chain.

La gestione dei rischi dinamici della sicurezza informatica lungo tutta la catena di fornitura è un'impresa complessa che richiede una necessaria trasformazione culturale e un approccio coordinato e multidisciplinare all'interno di un'impresa, nonché tecnologie avanzate di monitoraggio e controllo basate su ambienti di Cyber Threat Intelligence preferibilmente integrate con motori A.I. adattabili ai modelli C-SCRM. Un'efficace gestione del rischio

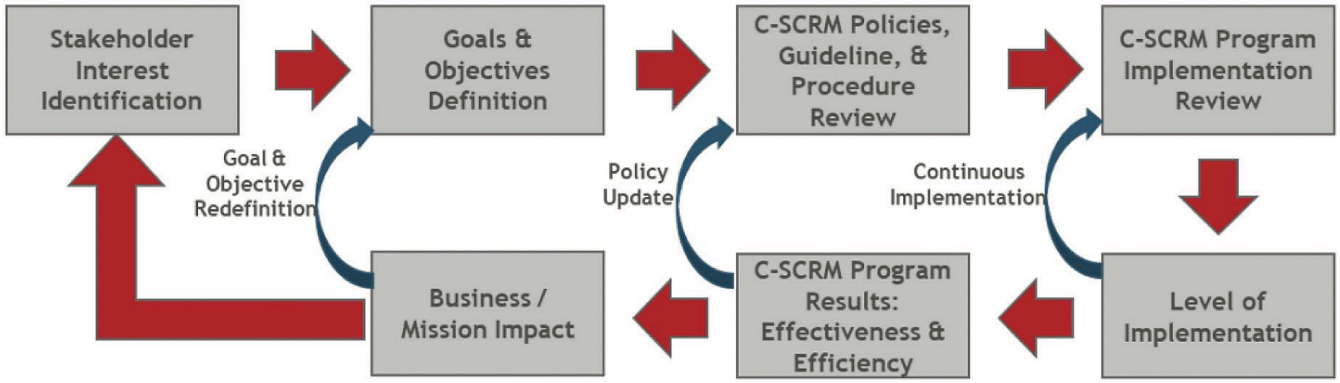


della catena di approvvigionamento della sicurezza informatica richiede precise metriche con l'impegno di stakeholder all'interno dell'azienda (reparti, processi) e all'esterno dell'azienda (fornitori, sviluppatori, integratori di sistema, fornitori di servizi di sistema esterni e altri fornitori di servizi relativi a ICT/OT) con cui collaborare attivamente, comunicare, condividere e intraprendere azioni che garantiscono risultati favorevoli agli obiettivi della mitigazione dei rischi. Le imprese dovrebbero mirare a infondere comportamenti provenienti da più discipline e processi (ad esempio, sicurezza delle informazioni, approvvigionamento, gestione del rischio aziendale, ingegneria del software, ufficio legale, sistemi informativi, risorse umane, ecc.) nei loro approcci alla gestione dei rischi di sicurezza informatica, tutta la filiera di approvvigionamento deve essere coinvolta. Le imprese possono definire ruoli espliciti per collegarli ed integrarli nei processi come parte delle più ampie attività di gestione del rischio di un'impresa.

Questo orchestrare è parte integrante dello sforzo sostenuto per identificare e mitigare i rischi portandoli sotto la soglia dell'accettabilità. Stabilire e sostenere una capacità C-SCRM crea una serie di vantaggi significativi. Un programma C-SCRM consolidato, strutturato su tre livelli (strategico, tattico, operativo) consentirà alle aziende di comprendere quali risorse sono più

BIO

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



C-SCRM Metrics Development Process

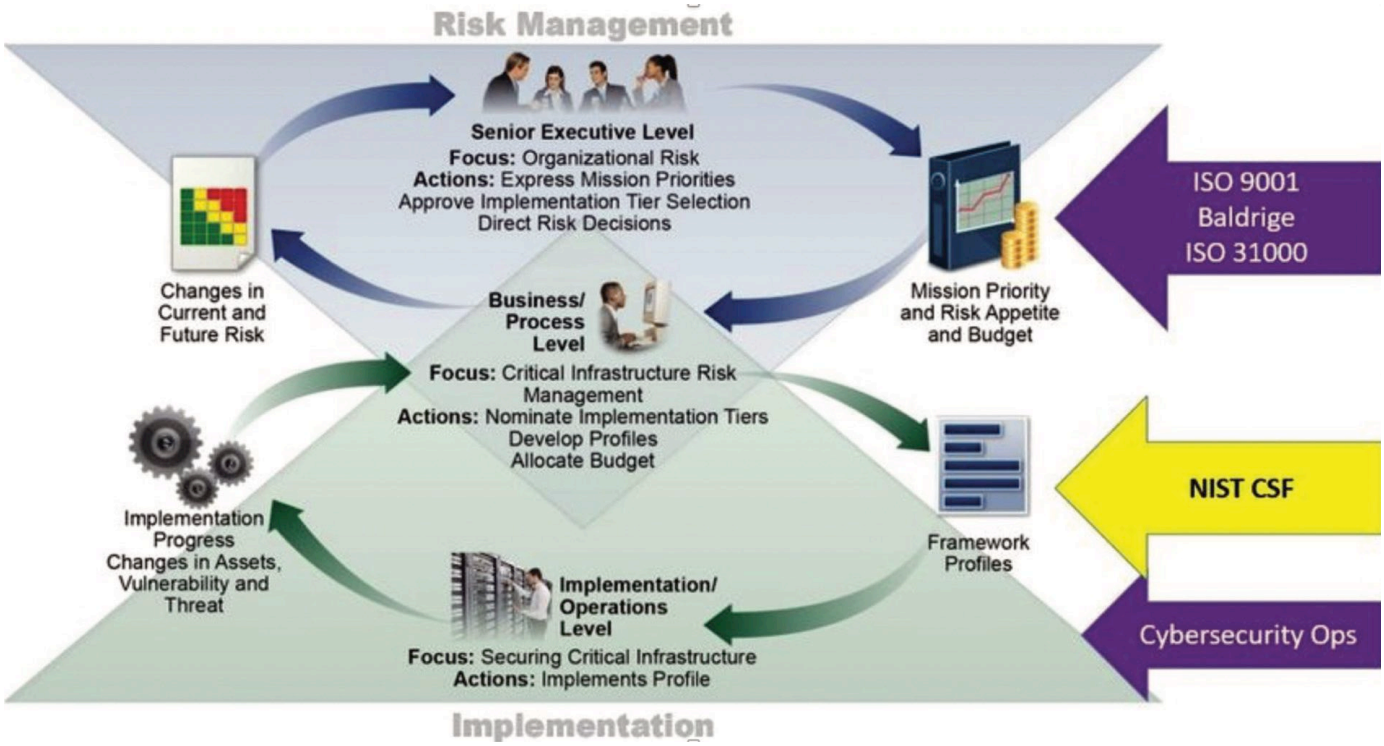
suscettibili alle debolezze e alle vulnerabilità della catena di approvvigionamento, riduce inoltre la probabilità che la supply chain venga compromessa da una minaccia alla sicurezza informatica migliorandone la capacità di rilevare, rispondere e recuperare in modo efficace eventi che comportano interruzioni significative delle attività. Quindi le organizzazioni dovrebbero garantire che i piani C-SCRM siano progettati per:

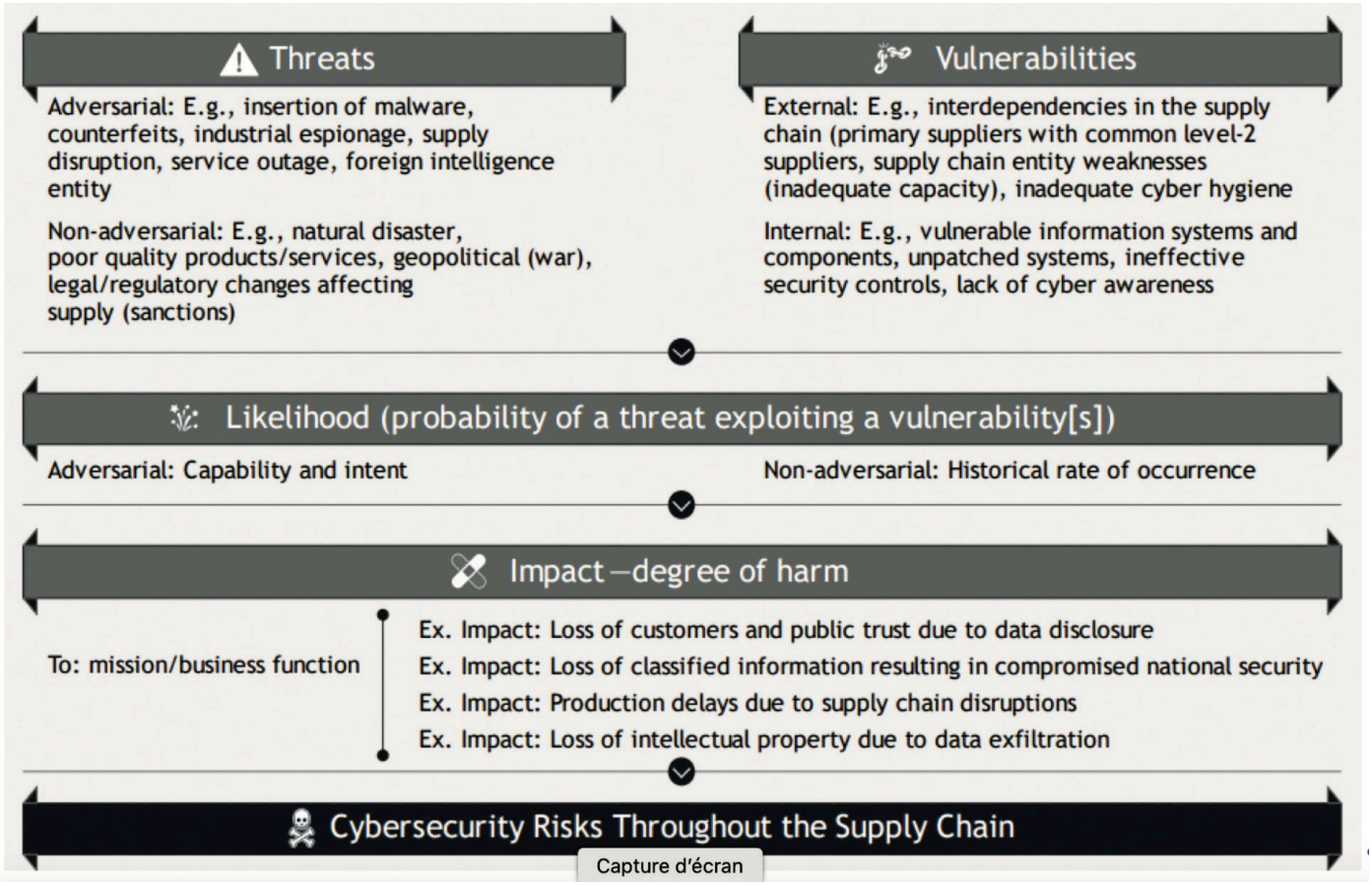
- Gestire piuttosto che eliminare il rischio poiché il rischio è parte integrante della ricerca del valore;
- Garantire che le operazioni siano in grado di adattarsi alle minacce costantemente emergenti o in evoluzione;
- Essere reattivi ai cambiamenti all'interno della propria organizzazione, dei programmi e del supporto ai sistemi informativi;
- Adeguarsi alle pratiche in rapida evoluzione dell'offerta globale.

L'efficienza operativa viene raggiunta attraverso una struttura, uno scopo e un sistema chiari allineati con le funzionalità e con l'assegnazione di priorità. il consolidamento e razionalizzazione dei processi C-SCRM esistenti, dipende da una maggiore garanzia che i prodotti e servizi acquistati siano di alta qualità, autentici, affidabili, resilienti, manutenibili, sicuri. In altri termini i fornitori di servizi e prodotti tecnologici devono essere entità su cui si può fare affidamento per soddisfare gli obiettivi aziendali.

Rischi per la sicurezza informatica lungo la catena di approvvigionamento (Supply Chain)

Si riferiscono al potenziale danno o compromissione che deriva dai rischi di sicurezza informatica posti in essere dai fornitori, dalle loro catene di approvvigionamento e dai loro prodotti o servizi. Le vulnerabilità cyber della Supply Chain, possono portare a impatti negativi e persistenti rispetto





alla mission aziendale. Essi possono rappresentare un ampio spettro di casistiche che vanno dalla riduzione dei livelli di servizio al furto di proprietà intellettuale o al degrado dei processi di business.

Potrebbero essere necessari alcuni mesi prima che tali vulnerabilità vengano sfruttate o scoperte. Può anche essere difficile determinare se un evento sia la risultante diretta di vulnerabilità appartenenti alla Supply Chain. Le vulnerabilità sono spesso interconnesse e possono esporre le imprese a rischi di sicurezza informatica a cascata. Ad esempio, un'interruzione del servizio su larga scala a un importante fornitore di servizi cloud può causare interruzioni del servizio o della produzione per più entità all'interno della catena di approvvigionamento di un'impresa e portare a effetti negativi all'interno di molteplici processi di business.

Kill Chain e intelligenza artificiale

Risulta altresì possibile raggiungere un'ottima gestione dinamica del rischio cyber, con capacità operative di gran lunga migliorative in termini di costi e tempi di risoluzione, se in affiancamento all'implementazione della metodologia C-SCRM del NIST come da riferimenti bibliografici[B001], sia possibile per l'impresa attivare metodi dinamici di rilevazione e mitigazione del rischio cyber che lavorano come sensori paralleli nei punti chiave della catena di approvvigionamento generando segnalazioni di eventi critici secondo una tipica Kill Chain. Potremo a tal fine coniare l'acronimo SC-KC per individuare una relazione proficua ai fini di gestione operativa dei rischi tra Supply Chain e Kill Chain. Sotto questa prospettiva, i cosiddetti Ambienti Federati con specifici protocolli SLA siglati tra azienda e fornitori, possono rappresentare una soluzione affidabile[B003]. Monitorate e analizzare in modo correlato, dinamico e centralizzato gran moli di dati provenienti dai sistemi distribuiti di Cyber Intelligence lungo tutta la Supply Chain, utilizzando poi in ADD-ON moduli di Intelligenza Artificiale in affiancamento a piattaforme di analisi che arricchiscono e che correlano i dati operando attraverso analisi delle TTP (Technics, Tactics and Procedures del modello Kill Chain) in riferimento alle CVE (Common Vulnerabilities and Exposures) rilevate, potrebbe rappresentare una postura aziendale avanzata e lungimirante contro tutti i rischi cyber provenienti dalle terze parti operanti in una tipica catena di approvvigionamento.

Bibliografia utile

[B001] Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (nist.gov)

[B002] https://www.researchgate.net/publication/344611063_Artificial_intelligence_and_machine_learning_in_dynamic_cyber_risk_analytics_at_the_edge

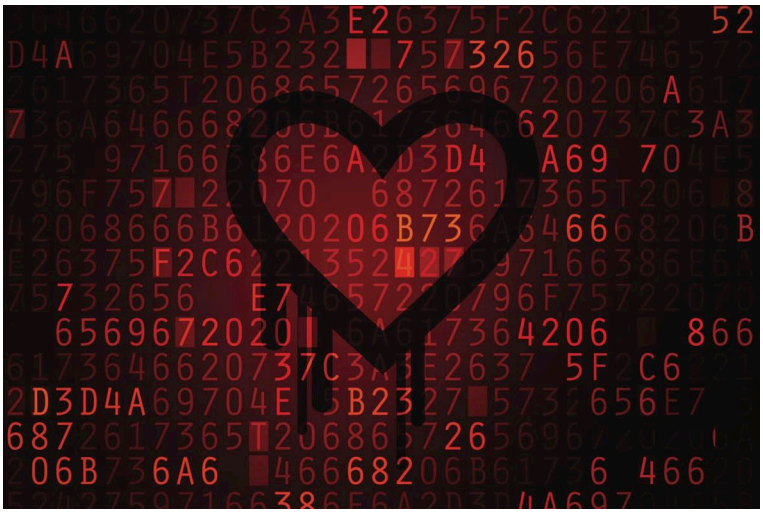
[B003] https://documents.trendmicro.com/assets/white_papers/wp-supply-chain-as-kill-chain-security-in-the-era-of-zero-trust.pdf ■

Rischi della Supply Chain nel Ciclo di Vita dello Sviluppo del Software: un Decennio dopo Heartbleed.

Autore: Viktor Polic

Introduzione

La vulnerabilità "Heartbleed" di OpenSSL del 2014 è servita da campanello d'allarme per l'industria del software, richiamando l'attenzione sui rischi significativi inerenti la supply chain. Un semplice messaggio heartbeat ha esposto a un grave bug che ha messo a rischio i dati degli utenti, un evento che è servito come reminder urgente dell'importanza cruciale di testare le librerie di terze parti. Dopo un decennio, continuiamo a confrontarci con vulnerabilità simili. Nel nostro mondo sempre più connesso, dove i confini tra il mondo fisico e quello digitale si confondono, i rischi della supply chain nel ciclo di vita dello Secure Software Development Life Cycle (SSDLC) hanno conseguenze di vasta portata in un ampio spettro di settori. Questo articolo approfondisce il panorama dei rischi, esplorando i principi fondamentali dell'SSDLC, le tecniche per l'analisi del codice, i devastanti failure alla supply chain e l'importanza critica dell'SSDLC per l'Internet of Things (IoT) e la Operational Technology (OT).



Un ritorno a Heartbleed: l'Importanza di Testare Librerie di Terze Parti

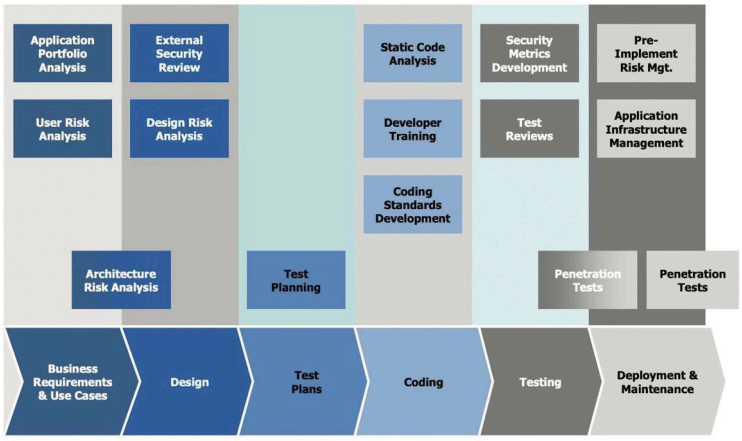
All'indomani della vulnerabilità Heartbleed, l'industria del software ha iniziato a capire che trascurare di testare rigorosamente le librerie di terze parti era una svista fatale. OpenSSL, un software open source ampiamente utilizzato per comunicazioni sicure, conteneva un bug che consentiva l'accesso non autorizzato a informazioni sensibili. Anche se OpenSSL non è stato sviluppato dalle organizzazioni che hanno risentito da Heartbleed, esse hanno dovuto sostenere l'impatto maggiore poiché avevano incorporato questa libreria di terze parti con vulnerabilità nei loro sistemi.

Rischi della Supply Chain del Software e Principi SSDLC

L'incidente Heartbleed ha rafforzato l'importanza dei solidi principi SSDLC, un approccio che integra le pratiche di sicurezza direttamente nel

ciclo di vita dello sviluppo del software. I componenti fondamentali di SSDLC includono l'analisi dei requisiti, la progettazione, la codifica, i test e la manutenzione, il tutto con particolare attenzione alla sicurezza fin dall'inizio. In particolare, l'approccio "shift-left" sottolinea la necessità di considerare i problemi di sicurezza il prima possibile nel ciclo di vita, piuttosto che applicare successivamente patch e correzioni al software sviluppato.

Security in the SDLC



Eoin Keary & Jim Manico

Analisi Statica e Dinamica del Codice

Le analisi statiche e dinamiche del codice fungono da strumenti preziosi in un approccio SSDLC. L'analisi statica del codice consiste nell'analisi del codice sorgente senza eseguire il programma, consentendo il rilevamento delle vulnerabilità nelle fasi iniziali. D'altra parte, l'analisi dinamica del codice prevede l'esame del software mentre è in esecuzione, consentendo l'identificazione di errori di runtime che l'analisi statica potrebbe non rilevare. La combinazione di questi approcci fornisce una visione completa delle potenziali vulnerabilità sia nel codice sviluppato che nelle librerie di terze parti.

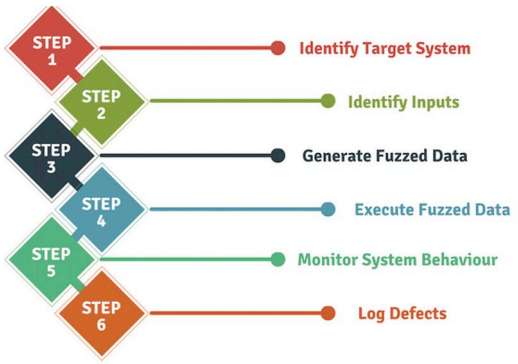
Il fuzzing, noto anche come fuzz testing, è una tecnica molto efficace impiegata durante l'analisi statica del codice. Fondamentalmente, il fuzzing prevede l'iniezione deliberata di dati non validi o inaspettati in un sistema software al fine di scoprire vulnerabilità come arresti anomali, perdite di memoria o comportamenti imprevisti. Alimentando un sistema con un'ampia gamma di input irregolari, gli sviluppatori possono identificare problemi che potrebbero passare inosservati durante i test regolari ma che potrebbero essere potenzialmente sfruttati in scenari reali.

BIO

Il Dr. Viktor Polic ha 30 anni di esperienza professionale interfunzionale nella gestione e governance delle informazioni, con particolare attenzione alla sicurezza delle informazioni, alla gestione dei rischi e assurance per grandi organizzazioni del settore pubblico con presenza globale nei settori tecnologico, finanziario, umanitario e dello sviluppo. Contribuisce attivamente a gruppi di lavoro interorganizzativi per stabilire politiche, standard e linee guida nell'area della sicurezza delle informazioni, protezione dei dati personali, programmi di sensibilizzazione, analisi dei rischi e metriche.Conduce ricerche in crittografia, regolamentazione della protezione dei dati, garanzia delle informazioni e gestione del rischio. Docente da 20 anni in corsi universitari e post-laurea sui temi dell'informatica, gestione delle telecomunicazioni, sistemi di supporto alle decisioni aziendali e corsi di sicurezza informatica come docente a contratto presso la Webster University di Ginevra, un centro nazionale certificato di eccellenza accademica nella difesa informatica (CAE-CD). È anche membro del comitato scientifico per gli studi avanzati sulla sicurezza delle informazioni presso il dipartimento di studi gestionali della facoltà di scienze economiche e sociali dell'Università di Ginevra.Sostiene il progresso nella sicurezza delle informazioni come autore in riviste professionali come CSO e ISACA journal e come relatore a conferenze professionali internazionali come il congresso della Cloud Security Alliance, i vertici dei Chief Information Security Officer internazionali, GITEX Global, GISEC e altri. Viktor è membro di (ISC)2, ISACA e IACR, e titolare di certificati CISSP, CISA e CRISC attivi.

Un vantaggio significativo del fuzzing sta nella sua capacità di automatizzare la scoperta di nuove vulnerabilità precedentemente sconosciute. Gli strumenti di analisi statica convenzionali fanno molto affidamento sul rilevamento di modelli noti di codice non sicuro. Sebbene tali strumenti siano efficaci per rilevare problematiche comuni e ben comprese, potrebbero non scoprire vulnerabilità nuove o complesse. Il fuzz testing, d'altra parte, non si basa su modelli di vulnerabilità note, ma piuttosto sul comportamento del sistema di fronte a input irregolari. Ciò rende il fuzzing un potente strumento per portare alla luce vulnerabilità precedentemente inesplorate.

Detto ciò, l'implementazione efficace del fuzzing nell'analisi statica del codice richiede un'attenta pianificazione ed esecuzione. Per cominciare, gli sviluppatori devono decidere i tipi di input da utilizzare per i test. Questi potrebbero variare da dati totalmente casuali a input che sono versioni leggermente modificate di quelli normali. Quest'ultimo, spesso noto come "mutational fuzzing", può essere particolarmente utile per scoprire problemi di casi limite. Inoltre, l'interpretazione dei risultati del fuzzing può essere complessa, poiché non tutti i comportamenti irregolari indicano una vulnerabilità della sicurezza. Pertanto, è fondamentale incorporare il fuzz testing come parte di un SSDLC completo, insieme ad altre tecniche di analisi statica e dinamica, per una comprensione completa della postura di sicurezza di un sistema software.



Gli analisti di sicurezza della Deutsche Telekom, utilizzando diverse tecniche per causare comportamenti imprevisti nelle applicazioni (code coverage-guided fuzzers - AFL e libFuzzer), hanno recentemente scoperto una vulnerabilità nella libreria MatrixSSL (AFL e libFuzzer) e AddressSanitizer, un tool per rilevare errori di memoria. CVE-2022-43974 è una vulnerabilità bufer overflow che potrebbe consentire la divulgazione di informazioni e l'esecuzione di codice in modalità remota. La libreria del software è stata patchata.

MatrixSSL è una libreria open source integrata Secure Sockets Layer (SSL) e Transport Layer Security (TLS). MatrixSSL è scritto in C e fornisce un'opzione minimalista e ad alte prestazioni per l'aggiunta di funzionalità SSL/TLS ad applicazioni, dispositivi e sistemi integrati o con risorse limitate.

Uno dei vantaggi più significativi di MatrixSSL è il suo poco spazio in memoria che la rende una scelta popolare per l'uso nei dispositivi IoT, sistemi in tempo reale e altri ambienti in cui le risorse di sistema sono preziose.

MatrixSSL supporta una gamma di algoritmi crittografici ed è conforme ai principali standard del settore. Ciò lo rende flessibile e adattabile a diversi requisiti di sicurezza e ambienti normativi. MatrixSSL include anche funzionalità per analizzare e convalidare i certificati X.509, comunemente utilizzati nei protocolli SSL/TLS.

I ricercatori di sicurezza del software di Loria, INRIA in Francia, hanno scoperto una vulnerabilità buffer over-read nella libreria wolfSSL utilizzando un nuovo protocollo fuzzer chiamato tlspuffin. CVE-2022-42905 descrive questa vulnerabilità per questa libreria critica. WolfSSL, precedentemente noto come CyaSSL, è un'implementazione leggera, portatile e open source dei protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS). È progettato pensando ai sistemi integrati e agli ambienti con risorse limitate, offrendo un minimo spazio, altamente desiderabile in tali ambienti.

Un aspetto importante di wolfSSL è il suo focus su una solida sicurezza, con test completi e peer review per garantire la robustezza. Inoltre, offre supporto per crittografia hardware e accelerazione hardware per velocizzare le operazioni nei sistemi che includono hardware specifico per questo scopo.

In termini di utilizzo, wolfSSL può essere trovato in un'ampia gamma di applicazioni, inclusi dispositivi IoT, router, stampanti e persino sistemi aeronautici, rendendolo uno strumento importante nello sviluppo di sistemi software sicuri.

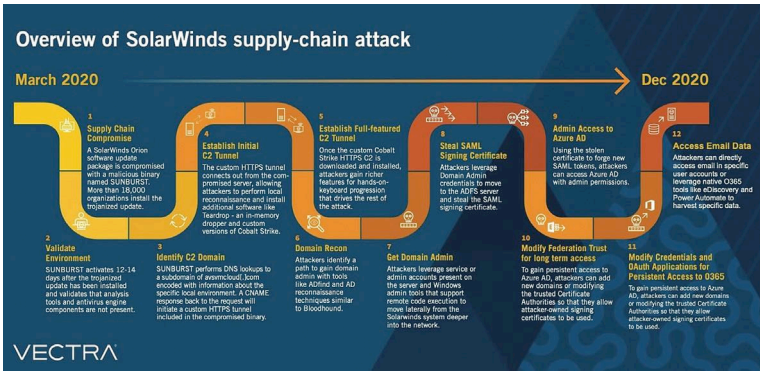
Esempi di devastanti failure della Supply Chain del Software

Forse nessun incidente sottolinea le terribili conseguenze delle interruzioni della supply chain meglio dell'hack di SolarWinds Orion. Nel 2020, gli attori delle minacce hanno manipolato il processo di sviluppo della piattaforma software Orion, incorporando codice dannoso negli aggiornamenti software. L'uso diffuso del software SolarWinds Orion ha fatto sì che la vulnerabilità abbia raggiunto molte organizzazioni, comprese le agenzie governative.

L'impatto diretto dell'attacco è stato notevole. Ha colpito fino a 18.000 clienti SolarWinds, inclusi diversi dipartimenti del governo degli Stati Uniti e aziende Fortune 500. La violazione dei dati ha compromesso informazioni sensibili, portando potenzialmente a minacce alla sicurezza nazionale e perdite finanziarie significative. Inoltre, il costo della riparazione, che include l'identificazione e la rimozione della minaccia, l'indagine sull'intera portata della violazione e il rafforzamento delle misure di sicurezza, è stato monumentale.

Oltre all'impatto diretto, l'hacking di SolarWinds Orion ha avuto anche conseguenze indirette di vasta portata. Ha accresciuto la consapevolezza delle potenziali vulnerabilità nelle supply chain dello sviluppo del software,

portando a un maggiore controllo e attenzione normativa al ciclo di vita dello sviluppo del software e alle pratiche di cybersecurity. Ha spinto le organizzazioni di tutto il mondo a rivalutare le proprie strategie di sicurezza informatica, in particolare in relazione ai rischi del software di terze parti e della supply chain. L'hack ha sottolineato l'importanza fondamentale di rigorose misure di sicurezza informatica, monitoraggio continuo e capacità di risposta rapida per mantenere la sicurezza e l'integrità dei sistemi digitali.



Infine, l'hack di SolarWinds Orion ha avuto un impatto significativo sulla fiducia - fiducia nei fornitori di software, nei sistemi digitali e anche nell'infrastruttura di Internet. Ricostruire questa fiducia è un compito complesso, che richiede maggiore trasparenza, pratiche di sicurezza migliorate e, potenzialmente, regolamentazione e supervisione più rigorose. L'hack ha ricordato in maniera molto forte che nel nostro mondo digitale interconnesso, la sicurezza dei singoli componenti ha un impatto sulla sicurezza dell'intero ecosistema.

SSDLC in IoT e OT: Settore manifatturiero, automobilistico e sanitario

Le implicazioni dei principi SSDLC si estendono oltre il software tradizionale e nei campi in espansione di IoT e OT. Con queste tecnologie, i difetti del software possono tradursi in minacce alla sicurezza e alla protezione del mondo reale. Nel settore manifatturiero, le vulnerabilità possono interrompere le linee di produzione, portando a costosi tempi di inattività. Nell'industria automobilistica, le violazioni possono compromettere le prestazioni del veicolo e la sicurezza dei passeggeri. Nel frattempo, nel settore sanitario, i guasti del sistema e le violazioni dei dati potrebbero mettere a rischio la vita dei pazienti e la privacy. Un solido SSDLC che incorpori test rigorosi e misure di sicurezza è essenziale per mitigare questi rischi.

Analizziamo il seguente esempio. I Rockwell Automation PanelView sono una serie di pannelli utilizzati nei sistemi di controllo industriale. Questi dispositivi forniscono un'interfaccia grafica che consente agli operatori di interagire con il sistema di controllo di una macchina o di un processo. I terminali PanelView sono utilizzati per applicazioni come il monitoraggio, il controllo e la visualizzazione grafica delle informazioni, consentendo agli operatori di comprendere lo stato dell'operazione e prendere decisioni consapevoli sulla base dei dati presentati.

I terminali PanelView sono disponibili in diverse forme, dimensioni e complessità, che vanno dai modelli base push-button ai modelli full-featured con touchscreen. Sono utilizzati in vari ambienti industriali tra cui la produzione, l'imballaggio e le industrie di trasformazione.

Le capacità di questi dispositivi possono variare notevolmente, ma in generale consentono agli utenti di:

1. Monitorare lo stato e le prestazioni della macchina o del processo in tempo reale.
2. Controllare le operation come l'avvio o l'arresto di un processo, la regolazione delle impostazioni o il comando manuale.
3. Visualizzare e analizzare i dati storici per il monitoraggio delle prestazioni o la risoluzione dei problemi.
4. Avvisare gli operatori di potenziali problemi o malfunzionamenti tramite allarmi o messaggi.

I dispositivi Rockwell Automation's PanelView HMI possono essere utilizzati in vari ambienti sanitari per migliorare l'efficienza, mantenere il controllo della qualità e facilitare operazioni affidabili. Alcuni dei casi d'uso nel settore sanitario includono:

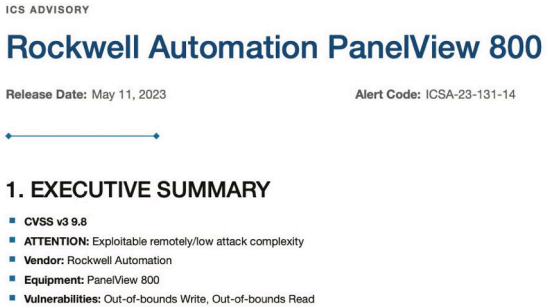
- **Industria Farmaceutica:** Nei processi di produzione farmaceutica, PanelView può aiutare a monitorare e controllare i processi di produzione. Ciò potrebbe includere la supervisione di aspetti come la miscelazione degli ingredienti, il controllo della temperatura e della pressione o i processi di sterilizzazione. Può anche aiutare a garantire una rigorosa conformità alle normative mantenendo meticolose registrazioni in tempo reale dei parametri di processo e dei dati di controllo della qualità.
- **Apparecchiature Mediche:** le interfacce PanelView possono essere integrate in varie apparecchiature mediche come macchine per dialisi, sistemi di ventilazione o macchinari di laboratorio automatizzati. Consentono agli operatori sanitari di controllare l'apparecchiatura, monitorare lo stato del paziente e regolare i parametri secondo necessità.
- **Infrastrutture Ospedaliere:** gli ospedali spesso si affidano a sistemi complessi per il riscaldamento, la ventilazione e l'aria condizionata (HVAC), l'illuminazione e la sicurezza. PanelView può fornire un'interfaccia per la gestione di questi sistemi, semplificando il monitoraggio

e la regolazione secondo necessità per un funzionamento ottimale e un'efficienza energetica.

- **Biotecnologie e Scienze Della vita:** nei laboratori di biotecnologie e scienze della vita, PanelView può aiutare a gestire e monitorare processi come il sequenziamento del DNA, la sintesi proteica o i sistemi automatizzati di coltura cellulare. Può aiutare a garantire il mantenimento delle condizioni corrette e avvisare gli operatori di eventuali anomalie che potrebbero compromettere la validità degli esperimenti o della produzione.
- **Medical Supply Chain e Inventory Management:** i sistemi automatizzati di archiviazione e recupero nel settore sanitario possono utilizzare le interfacce PanelView per gestire e monitorare le operazioni. Ciò include il monitoraggio dei livelli di inventario, l'automazione del processo di recupero e la supervisione delle attività di manutenzione.

In questi modi e altro ancora, PanelView di Rockwell Automation aiuta a semplificare i processi, mantenere gli standard di qualità e garantire operazioni affidabili ed efficienti nel settore sanitario. Poiché la trasformazione digitale continua a rimodellare l'assistenza sanitaria, è probabile che tali strumenti diventino sempre più essenziali.

Questi dispositivi costituiscono una parte essenziale della tecnologia operativa in molti ambienti industriali, colmando il divario tra gli esseri umani e i processi automatizzati. Nel contesto di un mondo industriale sempre più digitale, contribuiscono all'efficacia e all'efficienza delle operazioni, aiutando le aziende a raggiungere una maggiore produttività e ridurre i tempi di inattività.


ICS ADVISORY

Rockwell Automation PanelView 800

Release Date: May 11, 2023 Alert Code: ICSA-23-131-14

1. EXECUTIVE SUMMARY

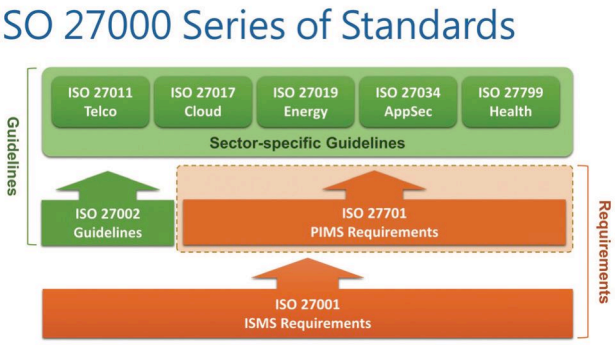
- CVSS v3 9.8
- ATTENTION: Exploitable remotely/low attack complexity
- Vendor: Rockwell Automation
- Equipment: PanelView 800
- Vulnerabilities: Out-of-bounds Write, Out-of-bounds Read

L'11 maggio 2023, la Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti ha pubblicato un avviso sulle vulnerabilità che interessano Rockwell Automation PanelView 800 che potrebbero consentire l'esecuzione di codice in modalità remota. Il punteggio CVSS v3 di 9,8 è quello attribuito a questa CVE. Il prodotto è vulnerabile all'out-of-bounds write che potrebbe consentire a un utente malintenzionato di eseguire un heap buffer overflow se l'utente ha abilitato la funzionalità di posta elettronica nel file di progetto utilizzato da WolfSSL. Quella funzione è disabilitata per impostazione predefinita. Per gli utenti che richiedono la funzione, è disponibile una patch. CISA raccomanda le seguenti misure difensive:

- Ridurre al minimo l'esposizione della rete per tutti i dispositivi del sistema di controllo e assicurarsi che non siano accessibili da Internet.
- Individuare le reti del sistema di controllo e i dispositivi remoti dietro i firewall e isolarli dalle reti aziendali.
- Quando è richiesto l'accesso remoto, utilizzare reti private virtuali (VPN), riconoscendo che le VPN potrebbero presentare vulnerabilità e dovrebbero essere aggiornate alla versione più recente disponibile. Una VPN è sicura solo quanto i suoi dispositivi connessi.

Framework Normativi che Impongono Controlli SSDLC

Man mano che il panorama del rischio si evolve, stanno emergendo quadri normativi che prescrivono controlli obbligatori in SSDLC. Questi includono standard come ISO/IEC 27034, che fornisce linee guida per la sicurezza delle applicazioni, e il NIST Cybersecurity Framework, che offre un approccio basato sul rischio per la gestione del rischio di sicurezza informatica. Questi framework mirano a garantire che le organizzazioni di tutti i settori integrino la sicurezza nei loro processi di sviluppo software.

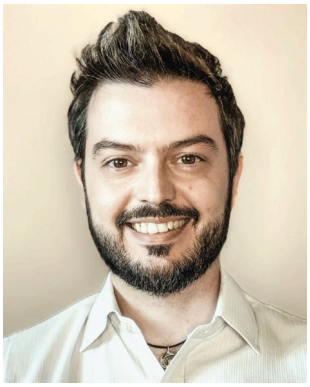


Negli Stati Uniti, sulla base dell'ordine esecutivo presidenziale sul miglioramento della sicurezza informatica della nazione, l'Office of Management and Budget ha emesso una guida per garantire che le agenzie federali utilizzino software che è stato creato seguendo pratiche di sicurezza comuni. L'obiettivo è utilizzare solo software che segua standard di sviluppo software sicuri, crei un modulo di autocertificazione per i produttori e le agenzie di software e consenta al governo federale di identificare rapidamente i bug di sicurezza quando vengono scoperte nuove vulnerabilità.

Conclusioni

La vulnerabilità Heartbleed in OpenSSL ha messo in evidenza i rischi inerenti alla supply chain del software. Dieci anni dopo, continuiamo ad affrontare queste sfide, come dimostrato da incidenti come l'hacking di SolarWinds Orion. Poiché i confini tra il mondo digitale e quello fisico hanno i contorni sempre più sfumati e poiché ci affidiamo sempre più a IoT e OT in tutti i settori, la necessità di un solido SSDLC diventa più urgente che mai. L'adesione ai framework normativi che impongono i controlli SSDLC non è semplicemente un problema di compliance; è una necessità per la sicurezza e la resilienza del nostro mondo interconnesso. Guardando al futuro, il principio è chiaro: la sicurezza non può essere un dettaglio; deve essere incorporata in ogni fase del ciclo di vita dello sviluppo del software. ■

Rischi e priorità nella gestione della Cybersecurity delle Terze Parti.



Autore: Matteo Herin

Sono passati oltre 20 anni dall'ormai leggendario *Bezos' API Mandate* che ha formalizzato il paradigma alla base dell'ecosistema digitale di oggi per il quale *tutto è integrabile con tutto, basta che esponga delle API.*

Jeff Bezos' Big Mandate

(circa 2002 — paraphrased)

1. All teams will henceforth expose their data and functionality through service interfaces.
2. Teams must communicate with each other through these service interfaces.
3. No other communication is allowed other than service interfaces over the network.
4. It doesn't matter what technology they use.
5. All service interfaces must be designed to be **externalizable**.
6. Anyone who doesn't do this will be fired.

https://plus.google.com/+RipRowan/posts/eVeouesvaVt

È naturale quindi intuire come aziende estremamente diverse tra loro per dimensioni, maturità tecnologica, velocità di crescita e "livello" di cybersecurity siano incoraggiate a interagire in virtù della facilità con cui è possibile farlo rapidamente, in modo standard e *cost effective* grazie a questo paradigma. In altre parole, oggi è davvero semplice, per un'azienda sufficientemente digitale, integrarsi con altre realtà digitali per creare valore subito, sperimentando e migliorando tramite iterazioni secondo il paradigma Agile. Un esempio significativo del settore retail, che sottolinea quanto un'integrazione tecnologica e di processo a basso costo e bassa complessità, possa aprire opportunità di business con revenue di ordini di grandezza superiori al costo dell'operazione, è il servizio di spesa a domicilio tramite piattaforme di delivery.

Se dal punto di vista operativo, quindi, tutto appare più semplice e agile, dal punto di vista della cybersecurity i toni sono - apparentemente - molto più tendenti al grigio. Le motivazioni sono diverse, ma proviamo a metterle in ordine per macro aree:

1 Il paradigma di controllo: se anni fa lo "shadow IT" era nemico giurato di ogni CISO e relativo team, oggi lo "Shadow Digital" porta il problema a un nuovo livello; proprio in virtù della semplicità con cui uno strato di

API porta il sistema A della mia azienda a comunicare con sistema B del fornitore o partner, com'è possibile garantire che questa interconnessione sia censita, valutata e governata da un punto di vista della cybersecurity? Com'è possibile avere una panoramica ragionevolmente affidabile dello stato dell'arte dei sistemi e delle integrazioni presenti in azienda?

2 Fail Fast e approccio ciclico: se test e iterazioni hanno una frequenza elevata grazie a costi-opportunità contenuti, appare evidente come il

BIO

CISO & head of network di Carrefour Italia, Matteo è un appassionato di cybersecurity fin dai primi anni 2000 e ha fatto della sua passione il suo lavoro. In qualità di responsabile della Cybersecurity (CISO) e della Rete di Carrefour Italia, si occupa della costante evoluzione e del miglioramento di entrambi i mondi, cercando di costruire un mondo retail in cui cybersecurity, infrastrutture, servizi digitali e persone interagiscano in modo fluido ed efficiente. Amante assoluto dei gatti, Matteo ha trascorso gli ultimi 7 anni nel settore retail e i precedenti 10 anni come consulente di cybersecurity in diversi settori, tra cui energia, editoria e automotive.

modello di governance e gestione della cybersecurity debba trovare il modo di essere efficace anche a questa velocità. Se nel contesto dello sviluppo del codice le best practice sono note, e si spera diffuse, la cybersecurity supply chain ha trovato spazio sotto i riflettori solo recentemente. Secondo una ricerca condotta da Gatepoint Research nel 2023, sebbene l'84% del campione consideri l'argomento una priorità alta, solo il 13% è in grado di implementare monitoraggi continui sulle proprie terze parti.

3 Lo standard è che non ci sono standard: il modo in cui ogni azienda concepisce, implementa e mantiene un sistema di gestione della cybersecurity è diverso; in più, in molti settori, non sono presenti framework o regolamentazioni obbligatori che rendano la valutazione di un partner immediata o quantomeno direttamente interoperabile con il proprio ISMS. Se in questo momento stai pensando a NIST o ISO27001, immagina di vederli implementarli in una start-up che ha appena ottenuto il Round A, ma sta attivamente collaborando col nostro dipartimento Marketing da qualche settimana…

4 Le minacce sono in costante evoluzione: la conseguenza più diretta di questo (abusato) assioma è che mantenere un sistema di cyber operation efficiente ed efficace costa; in ultima istanza, quando qualcosa andrà terribilmente storto, non saranno le policy o le certificazioni che permetteranno all'azienda di alzare le serrande la mattina dopo, ma la preparazione delle persone, le procedure e gli strumenti di gestione degli incidenti e la capacità di recovery. E se questo vale per la propria azienda, **deve** valere anche per le terze parti più rilevanti. Secondo Verizon (Data Breach Report 2022) i breach causati da una terza parte valgono in media il 62% del totale delle intrusioni, un dato difficile da ignorare.

Ora che abbiamo provato a identificare alcune delle principali criticità, vediamo come provare a gestirle.

La prima fase nel processo di gestione della cybersecurity delle terze parti è l'identificazione dei rischi potenziali. Le aziende devono valutare attentamente le terze parti coinvolte nelle loro operazioni e capire come queste possano influenzare il proprio livello di rischio cyber. Questo può includere la valutazione delle politiche di sicurezza, la revisione delle misure di protezione dei dati, la verifica delle prassi di gestione delle vulnerabilità, ecc. Niente di straordinario, insomma, dov'è quindi il problema? L'affidabilità della valutazione e il livello di automazione del processo.

Una volta identificati i rischi, è importante condurre una valutazione della sicurezza delle terze parti. Ciò implica l'analisi approfondita delle politiche, dei processi e delle tecnologie di sicurezza adottate. È fondamentale verificare se le terze parti dispongono di un sistema di gestione della sicurezza dell'informazione robusto, che includa politiche di accesso, autenticazione, crittografia e monitoraggio adeguati, oltre a una capacità operativa

sufficiente. Sviluppare dei KPI e KRI che siano pragmatici, significativi e implementabili è forse l'obiettivo più importante di questa fase perché qui si gettano le fondamenta del modello di controllo continuo, la fase successiva. Raccogliere i dati e calcolare i KPI e KRI rappresenta il principale costo, e dunque ostacolo, alla velocità che ci serve per essere efficaci nel completare cicli di audit con frequenze ragionevoli e - perché no - rapportate al rischio. Prototipare e pensare all'automazione sono i nostri driver, in questa fase.

La fase successiva è spesso sottovalutata o - a volte convenientemente - dimenticata: fare di tutto per adeguare contratti, accordi e allegati tecnici affinché includano requisiti specifici in termini di cybersecurity. Le parti dovranno definire chiaramente le aspettative e le responsabilità in termini di gestione dei dati, misure tecniche di protezione, risposta agli incidenti e miglioramento continuo. È essenziale stabilire un meccanismo di monitoraggio continuo per garantire il rispetto di questi accordi contrattuali. Se naturalmente è possibile partire dall'implementazione di audit manuali, la richiesta di report dettagliati sulla sicurezza, eccetera, è l'adozione di soluzioni di monitoraggio automatizzato che nel lungo periodo farà la differenza. Se non si è in grado di misurare con costanza i propri partner digitali per verificare che "ciò che è sulla carta, è anche nei fatti" si allargherà la discrepanza tra rischio stimato e il reale rischio in capo all'organizzazione.

Nonostante tutte le misure preventive, gli incidenti di sicurezza prima o poi avvengono. Non è un caso che Detect, Respond e Recover Identificate dal NIST siano fasi *"right of the BOOM!"* ovvero quando l'incidente è in corso. Per questo, è fondamentale avere un piano di gestione degli incidenti ben definito che coinvolga anche le terze parti. Le organizzazioni devono stabilire un processo chiaro per segnalare e rispondere agli incidenti, garantendo la collaborazione delle terze parti coinvolte, oltre che testarlo periodicamente. Da best practice, inoltre, è indispensabile condurre analisi post-mortem per identificare le *root cause* e apportare le modifiche necessarie. Questa *lesson learned* è il volano della ciclicità iterativa del sistema che porterà al miglioramento continuo: un obiettivo sano e remunerativo, considerando che per IBM e Ponemon (Data Breach 2022) un data breach rappresenta, in media, un costo di 4.35 M$ per l'organizzazione che lo subisce.

A questo punto appare molto chiara la necessità di stabilire una relazione trasparente con i propri partner chiave sia dal lato contrattuale che operativo. Particolare attenzione va posta a tutti gli elementi di interazione, partendo dal diritto di auditabilità, passando per la misurazione dei KPI, fino alle regole d'ingaggio in fase di *incident response*. Un lavoro consistente, che, in ottica di efficientamento, può essere automatizzato almeno in parte con l'adozione di piattaforme SaaS proposte sul mercato da vendor specializzati.

Non va sottovalutata quindi l'importanza di costruire una comunità di partner aperta, affidabile e resiliente attraverso la formazione e lo scambio di informazioni sulle pratiche di sicurezza, la condivisione di intelligence e indicatori tecnici (IoC in primis) con le terze parti coinvolte. I benefici di accedere a questa comunità e, attraverso i legami di secondo livello, a un ecosistema di organizzazioni che, condividendo attori e tecnologie a volte comuni, punteranno a raggiungere lo stesso obiettivo: migliorare il proprio livello di maturità cyber ed essere più efficaci contro le minacce vecchie e nuove.

È chiaro come ad oggi la gestione della cybersecurity delle terze parti sia diventata un imperativo per le aziende che operano nella società digitale. La protezione dei dati e la prevenzione degli attacchi richiedono un approccio olistico che coinvolga una valutazione accurata dei rischi, accordi chiari, monitoraggio continuo, gestione degli incidenti e un programma di interscambio di formazione e informazioni. Solo attraverso una gestione consapevole della cybersecurity delle terze parti, le aziende possono proteggere sé stesse e i loro clienti da minacce sempre più sofisticate in un contesto dall'evoluzione così rapida. ■

Analisi della Darknet Exposure dei principali fornitori di tecnologia.

Autore: Richard Hancock

Negli ultimi anni, è stato registrato un aumento degli attacchi informatici a livello globale. I report indicano che gli attacchi complessivi sono aumentati del 38% nel 2022 rispetto agli anni precedenti, con il 68% delle organizzazioni che ha riferito di aver subito un attacco informatico noto nell'ultimo anno. [1,2] Inoltre, il costo medio di un data breach ha raggiunto il record massimo di $ 4,35 milioni. [1] Il costo medio di un attacco ransomware è di $ 4,54 milioni, escluso il costo del pagamento del riscatto.[1] Con l'aumento degli attacchi informatici, è più importante che mai unire la threat intelligence e i dati del darknet in ogni aspetto della postura di sicurezza, indipendentemente dalle dimensioni di un'organizzazione.

BIO

Richard Hancock ha lavorato in DarkOwl per quasi 2 anni e mezzo come nostro specialista di Darknet Intelligence e responsabile del team di ingegneria delle vendite. Richard ha un background come linguista arabo e investigatore OSINT (Open-Source Intelligence) con oltre sette anni di esperienza nel supportare organizzazioni del settore pubblico e privato all'interno e all'esterno degli Stati Uniti su argomenti come antiterrorismo, darknet intelligence, social engineering e criminalità informatica. Richard ha precedentemente sostenuto contratti governativi mentre viveva in Medio Oriente per cinque anni sia ad Amman, in Giordania, sia ad Abu Dhabi, negli Emirati Arabi Uniti.
Connettiti con Rich su LinkedIn: https://www.linkedin.com/in/richardhancock1/

Cybersecurity Risk

In termini semplici, il rischio cyber è la quantità di rischio potenziale che la tua organizzazione deve affrontare contro un attacco informatico. Nel calcolare il rischio organizzativo, una minaccia include tutto ciò che può causare danni a un'organizzazione che provoca un'interruzione dei servizi o della produzione. [3] Una delle maggiori minacce poste da un attacco informatico è la perdita o l'esposizione pubblica dei dati, che presenta un rischio significativo per il brand e la reputation dell'azienda.

I dati rubati presentano vari rischi per un'organizzazione che vanno dalla fuga di proprietà intellettuale o informazioni riservate che hanno un impatto diretto sulle entrate di un'azienda o dati sfruttati dai criminali informatici per frodi e tecniche di social engineering, che possono minacciare direttamente i dirigenti e i leadership importanti [4]. Inoltre, esiste anche un rischio indiretto attraverso i vendor e i fornitori di terze parti. Le conseguenze di un attacco contro una società potrebbero includere [3]:

- Accesso non autorizzato a una rete aziendale
- Uso improprio delle informazioni da parte di un utente autorizzato
- Perdita di accesso ai dati aziendali (tramite cancellazione o crittografia)
- Interruzione del servizio o della produttività
- Perdita di reputazione e danno al brand e all'immagine aziendale

Darknet 101

I dati della Darknet sono una fonte principale di informazioni sulle attività criminali e illecite. La darknet, o dark web, è uno strato di Internet a cui

non è possibile accedere dai browser tradizionali. È stata specificamente progettata per l'anonimato ed è accessibile solo tramite strumenti e software speciali. Informazioni aziendali sensibili vengono regolarmente trapelate o vendute sulla darknet. Questi insiemi di dati diffusi nella darknet possono essere utilizzati per identificare le minacce alla sicurezza informatica e calcolare il rischio di un'organizzazione. Esistono altre reti che sono anche strumenti preziosi per valutare il rischio cyber per le aziende, quali ad esempio le piattaforme di messaggistica istantanea come Telegram, il deep web e alcuni siti high-risk surface. La consapevolezza del rischio consente a un'organizzazione di essere meglio preparata ad affrontare le potenziali minacce.

Rischio di Terze Parti e Attacchi alla Supply Chain

Gli attacchi informatici legati ad attacchi a terze parti e alla supply chain sono in aumento, infatti il 60% di tutte le violazioni dei dati avviene tramite una terza parte. [5] I data breache di terze parti sono in aumento man mano che le supply chain diventano più complesse e le aziende di tutto il mondo diventano sempre più interconnesse. I fornitori di terze parti rappresentano un rischio significativo per le aziende di tutte le dimensioni perché la maggior parte delle organizzazioni non dispone di una visione adeguata delle misure implementate da un'azienda di terze parti per proteggere i dati dei clienti. [4]

Le terze parti includono, a titolo esemplificativo ma non esaustivo, vendor, come fornitori e produttori, partner, affiliati, distributori, servizi di provider, rivenditori e agenti. [3] Le terze parti possono avere accesso a informazioni quali: dati aziendali sensibili, dati finanziari, termini contrattuali e prezzi, dati di pianificazione strategica, proprietà intellettuale, dati delle credenziali, informazioni di identificazione personale (PII) di clienti e dipendenti e informazioni sanitarie protette (PHI) e possono inconsapevolmente contribuire a far sì che un aggressore ottenga l'accesso non autorizzato a una rete aziendale. [3] Il rischio rispetto al vantaggio devono essere esaminati attentamente prima di impegnarsi con terze parti, in particolare nella tecnologia e nella sicurezza informatica.

Infatti, il 48% delle organizzazioni considera la complessità delle relazioni con terze parti il problema principale e il 54% delle aziende non controlla adeguatamente i fornitori di terze parti e non dispone di un elenco completo di tutte le terze parti che hanno accesso alla propria rete. [5,6] Attualmente, il rischio più importante della supply chain deriva da moduli nella comunità open source che non sono adeguatamente controllati o sono mal gestiti. [7]

Una full immersion in Esempi di Darknet Exposure

Uno dei casi d'uso per approfondire i dati di DarkOwl è il monitoraggio dell'attività degli attori ransomware. La maggior parte degli attori ransomware, come Lockbit e AlphaV, ha una presenza attiva sui forum darknet (XSS o Exploit) oltre ai loro dedicated leak sites (DLS), che di solito sono ospitati su TOR ("The Onion Router"). Si prevede che la dimensione globale del mercato dell'intelligence darknet aumenterà a un tasso CAGR del 22,3% entro il 2028, per un totale di 1,3 miliardi di dollari. [8]

Utilizzando il principale prodotto di dati darknet di DarkOwl, Vision UI, gli analisti di DarkOwl sono stati in grado di effettuare ricerche nella darknet e altre piattaforme per scoprire ed esaminare l'esposizione alla darknet dei cinque principali fornitori della supply chain. Gli attacchi alla supply chain, noti anche come attacchi alla catena del valore o di terze parti, sono attacchi di sicurezza informatica, indipendenti dal settore, che causano danni e distruzione a un'organizzazione. L'interfaccia utente di Vision fornisce la più grande fonte di dati darknet disponibile in commercio, consentendo potenti funzionalità di interrogazione per cercare, monitorare e creare alert per infrastrutture critiche. Di seguito sono riportati i risultati di questa ricerca.

Cisco Systems

Gli analisti di DarkOwl hanno scoperto un database trapelato sul forum di hacking del deep web, Exploit, contenente un indirizzo e-mail Cisco insieme a due numeri di telefono, un indirizzo IP, un indirizzo dell'ufficio e un nome/cognome. Questo database conteneva informazioni sensibili relative a una società immobiliare negli UAE (Emirati Arabi Uniti) per oltre 700.000 persone. Il forum, Exploit, è un popolare forum di hacking che ha i cui principali utenti sono quelli di lingua russa.

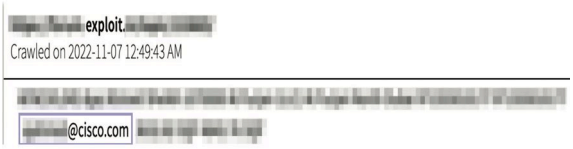


Figura 1: *Cisco System email mention on Exploit; Source: DarkOwl Vision*

In un'altra ricerca, un indirizzo e-mail Cisco e una password in chiaro sono trapelati su un popolare sito Web russo di frodi carding, il Carding Store. Questo indirizzo Cisco era una delle numerose e-mail trapelate con password in chiaro utilizzate per registrare account Fortnite e acquistare skin (outfit che i personaggi indossano nel videogioco).

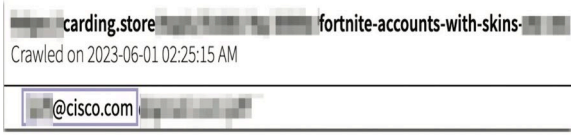


Figura 2: *Cisco System email mention on Carding Store, with Fortnite account skins; Source: DarkOwl Vision*

Schneider Electric

Il dominio se.com, che appartiene a Schneider Electric, è stato recentemente menzionato nel sito di

perdite dedicato .onion (DLS) di Lockbit. Il dominio menzionato rappresenta Schneider Electric che è stato recentemente preso di mira dal ransomware Lockbit il 25 maggio 2023.

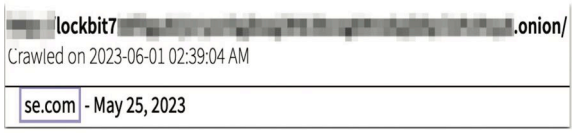


Figura 3: *Schneider Electric mentioned on LockBit in a leaked database; Source: DarkOwl Vision*

Lo screenshot qui sotto illustra come il database se.com appare direttamente sul DLS di Lockbit.

Figura 4: *Schneider Electric mentioned on LockBit; Source: Tor Anonymous Browser*

GitHub

Gli screenshot seguenti ritraggono un utente di lingua russa che condivide un collegamento a un repository GitHub contenente il codice sorgente di un attacco brute force per dispositivi Android sul noto forum darknet in lingua russa, XSS. La seconda immagine ritrae le stesse informazioni nel formato originale direttamente sul forum XSS. Un attacco brute force è un attacco che implica il tentativo di identificare tutte le combinazioni (solitamente password) per trovare una corrispondenza delle credenziali tramite tentativi ed errori fino a ottenere l'accesso. [9]

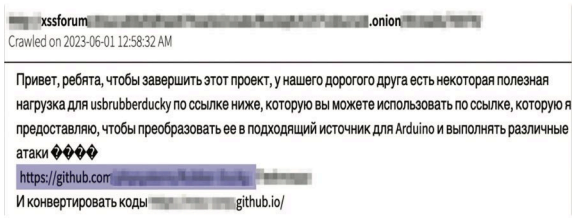


Figura 5: *XSS mention of Russian threat actor sharing link to brute force attack source code for Android devices on GitHub; Source: DarkOwl Vision*

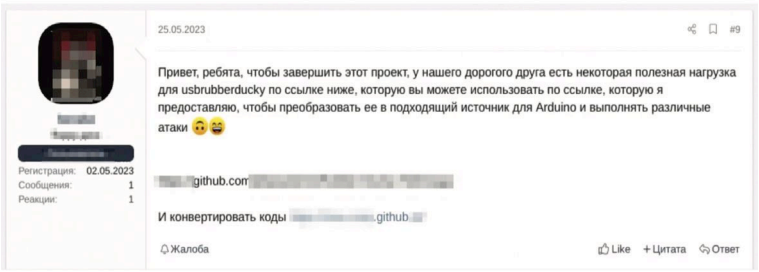


Figure 6: *Brute force attack source code on GitHub; Source: Tor Anonymous Browser*

Okta

Gli analisti di DarkOwl hanno trovato un annuncio per un database trapelato da Okta.com dal sito TOR Dark Leak Market. Okta fornisce software basato su cloud utilizzato per l'autenticazione sicura degli utenti e il controllo dell'identità. [10] Questo database conteneva l'accesso all'infrastruttura IT amministrativa globale. Dark Leak Market è un popolare mercato darknet che aggrega tutti i database trapelati pubblicamente disponibili. I cyber criminali possono condividere, scambiare o vendere apertamente database trapelati su questo sito.

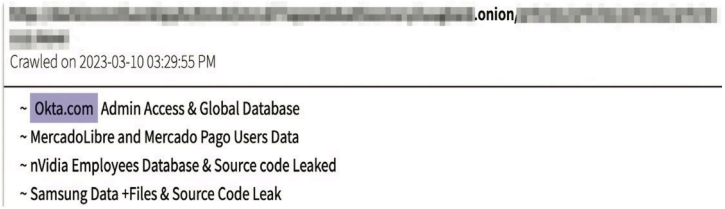


Figura 7: *Admin access database on Dark Leak Market; Source: DarkOwl Vision*

Nord

Gli analisti di DarkOwl hanno anche trovato un utente di Breach Forums che vendeva un tutorial per insegnare ad altri i principi della sicurezza operativa (OPSEC) sulla darknet, che menziona come utilizzare efficacemente una VPN Nord per rendere anonima la propria attività su Internet. Breach Forums era un popolare forum di hacking ospitato sia sul deep che sul dark web che è stato recentemente sequestrato in un'operazione delle forze dell'ordine.

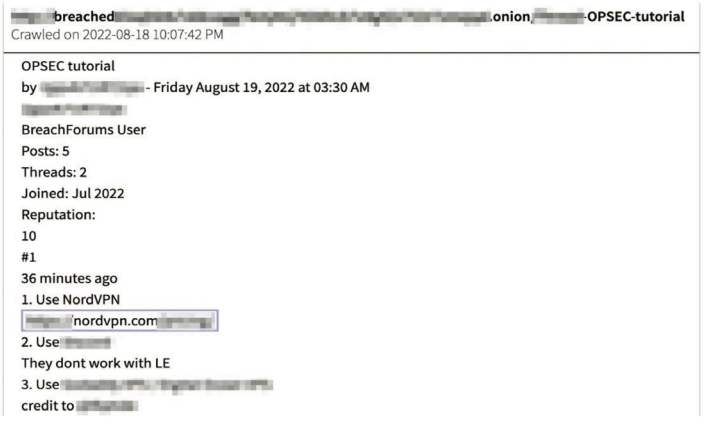


Figura 8: *OPSEC Tutorial with Nord VPN on Breached; Source: DarkOwl Vision*

Conclusioni

I dati della darknet migliorano la capacità di un'organizzazione di comprendere le minacce a cui è esposta la propria organizzazione, gestire i rischi di terze parti e arricchire il contesto per comprendere il panorama generale delle minacce. L'intelligence Darknet consente a un'organizzazione di comprendere i propri punti deboli e di intraprendere azioni per proteggere la propria organizzazione dalla perdita di dati, profitti e reputazione.

Il 65% delle organizzazioni non ha identificato quali terze parti hanno accesso ai loro dati più sensibili. [5] L'utilizzo dei dati darknet per valutare il rischio aziendale e di terze parti è il primo passo per prevenire le violazioni dei dati dei fornitori di terze parti.

Informazioni su DarkOwl

DarkOwl utilizza il machine learning e gli analisti per raccogliere automaticamente, continuamente e in modo anonimo, indicizzare e classificare i dati del darknet, del deep web e della rete di superficie ad alto rischio che consentono la semplicità nella ricerca.

La nostra piattaforma raccoglie e archivia i dati quasi in tempo reale, consentendo di interrogare i siti darknet che cambiano frequentemente posizione e disponibilità, in modo sicuro e protetto senza dover accedere alla darknet stessa.

DarkOwl è unico non solo per la profondità e l'ampiezza dei suoi dati darknet, ma anche per la pertinenza e la reperibilità dei suoi dati, i suoi strumenti di indagine e la professionalità del servizio clienti. Come aspetto importante, i dati di DarkOwl vengono raccolti in modo etico e sicuro dalla darknet, consentendo agli utenti un accesso sicuro e anonimo alle informazioni e alle minacce rilevanti per la loro missione. La nostra passione, il nostro focus e la nostra competenza è il darknet.

Sources

1 https://pages.checkpoint.com/cyber-attack-2022-trends.html

2 https://www.netwrix.com/68_of_organizations_experienced_a_cyberattack_within_the_last_12_months.html

3 https://www.darkowl.com/blog-content/understanding-darknet-risk/

4 https://www.darkowl.com/blog-content/cyber-risk-modeling-introducing-darksonar/

5 https://reciprocity.com/blog/how-to-prevent-third-party-vendor-data-breaches/

6 https://www.getastra.com/blog/security-audit/third-party-data-breach-statistics/

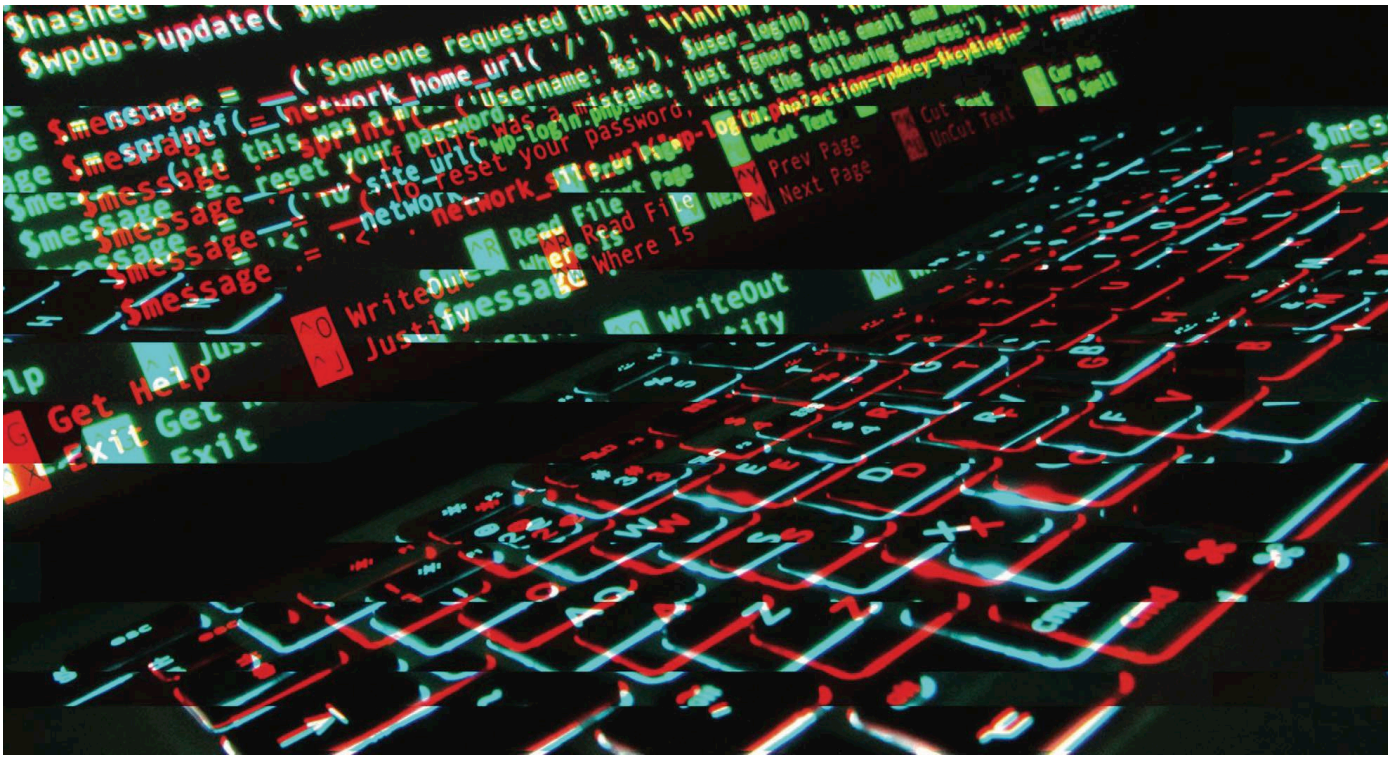
7 https://thenewstack.io/the-challenges-of-securing-the-open-source-supply-chain/

8 https://www.msspalert.com/cybersecurity-research/global-dark-web-intelligence-market-could-be-worth-1-3-billion-by-2028/

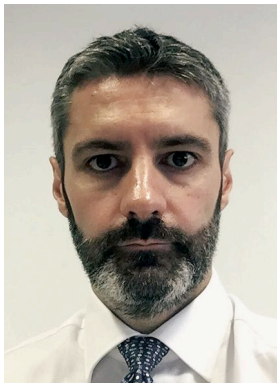
9 https://www.darkowl.com/resources/darkowl-glossary-of-darknet-terms/

10 https://support.okta.com/help/s/article/what-is-okta?language=en_US

Per ulteriori informazioni, visitare www.darkowl.com. ■



Un approccio dinamico del rischio richiede informazioni e automazioni.



Autore: Massimo Cappelli

La funzione del rischio si basa su tre fattori: minaccia, vulnerabilità e impatto. Implicito ma decisamente importante è l'oggetto della vulnerabilità su cui la minaccia si può abbattere per provocare poi un impatto.

Un semplice esempio potrebbe essere un ladro (attore della minaccia) che utilizza un piede di porco (strumento della minaccia) per aprire una porta di un magazzino (oggetto), per rubare un attrezzo (impatto). In questo caso, non viene esplicitata la vulnerabilità che è intrinseca all'oggetto. Se la porta fosse blindata e chiusa a mandate, probabilmente sarebbe meno vulnerabile al piede di porco, utilizzato dal ladro. Se la porta fosse chiusa con un semplice chiavistello, sarebbe molto più vulnerabile.

Traslato nel mondo cyber potremmo vederla così: un gruppo criminale (attore della minaccia) utilizza un exploit (strumento) per entrare in un server (oggetto) e rubare delle informazioni (impatto). La vulnerabilità è intrinseca al server. Se sul server e sugli applicativi in esso contenuti, fosse stato attuato un processo di patching aggiornato, sarebbe meno vulnerabile a potenziali exploit.

Consideriamo tutti i fattori singolarmente:

- Minaccia che potremmo vedere composta dall'attore e dagli strumenti da esso utilizzato e le tecniche, tattiche e procedure;
- Vulnerabilità comprensiva anche dell'informazione sull'oggetto interessato dalla vulnerabilità stessa;
- Impatto che è il danno subito e si esplicita in una interruzione di servizio, in un furto di informazioni e conseguenti perdite economiche.

Questi tre fattori, costituiti a loro volta da più sotto-fattori, sono fondamentali per il calcolo del rischio. Il calcolo del rischio fino a qualche anno fa, ma ancora oggi in qualche azienda, è un processo il cui risultato è una fotografia.

Si calcola il rischio una volta all'anno, se va bene, e si fotografa il livello per poi definire i piani di rientro. I meno fortunati si ritrovano in mano un risultato qualitativo (alto, medio, basso), mentre i più fortunati con un valore quantitativo. Il processo del rischio fa partire dei piani di rientro per mitigare e ridurre quanto più possibile il rischio stesso.

Questo poteva andare bene in un mondo in cui la velocità e il cambiamento dei fattori concomitanti alla valutazione del rischio erano relativamente bassi. Nel 2022, sono uscite in media più di 60 vulnerabilità al giorno, per non parlare dei malware che possono annoverare decine di migliaia di varianti giornaliere e gli stessi asset tecnologici (e non) a supporto dei servizi sono in continuo cambiamento.

Pertanto, è necessario strutturarsi in modo tale da poter monitorare costantemente l'evoluzione del rischio ed essere in grado di mitigare per quanto sia possibile lo stesso, attraverso un approccio real-time.

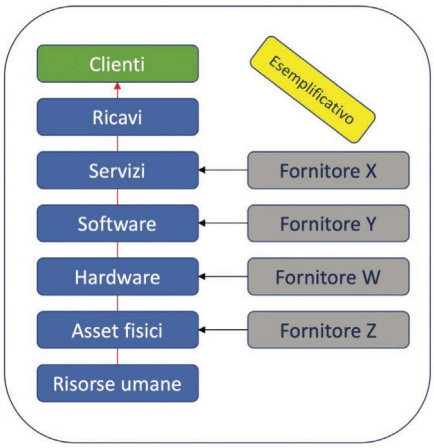
Da cosa partire? Sicuramente dal comprendere cosa si deve difendere. Il mio punto di partenza, nel caso si parli di un'azienda privata, sarebbe il bilancio aziendale d'esercizio. Questo documento, spesso sottovalutato,

BIO

Massimo Cappelli è Responsabile delle attività di Early Warning, Brand Protection, Information Sharing e Cyber Threat Intelligence nella struttura CERT di Poste Italiane. Nella sua passata esperienza ha lavorato come consulente in Booz Allen Hamilton e Booz & Company nella practice Risk, Relisience and Assurance.

presenta una serie di informazioni utili a comprendere cosa si deve difendere. All'interno del bilancio d'esercizio ci sono informazioni sui ricavi, da quali linee produttive o di servizi questi vengono prodotti, quanto personale c'è in azienda, quali aree geografiche interessano il business dell'azienda, l'organizzazione e così via.

Supponiamo di concentrarci solo sui servizi che generano ricavi. Isolando solo le informazioni sulla produzione dei ricavi, l'attività successiva è scendere quanto più possibile nelle informazioni a supporto: marginalità, canali di vendita del prodotto o del servizio e da qui poi procedere con l'approfondimento all'interno dell'azienda su quali siano gli asset propedeutici alla produzione dei ricavi.



I ricavi sono generati da servizi/prodotti, erogati attraverso canali, supportati da asset informatici (hardware e software) e asset fisici (data center, uffici, stabilimenti) attraverso il lavoro del personale aziendale e il supporto di fornitori e del loro personale.

L'ideale sarebbe tracciare i ricavi in base al servizio erogato near real time sui sistemi per comprendere il flusso e le eventuali interruzioni e di conseguenza le perdite dirette a livello economico (operazioni effettuate sui canali digitali; consumi energetici e relativo valore economico; acquisti online; …). Se non fosse possibile, anche l'analisi dello storico potrebbe aiutare per dare un'idea dei flussi. In alcuni casi, se si considera canoni mensili fissi, le perdite potrebbero essere stimate in base al tasso di churn dei clienti associabili ai disservizi e l'impatto anche in ricavi mancati per cattiva pubblicità. Sono solo esempi.

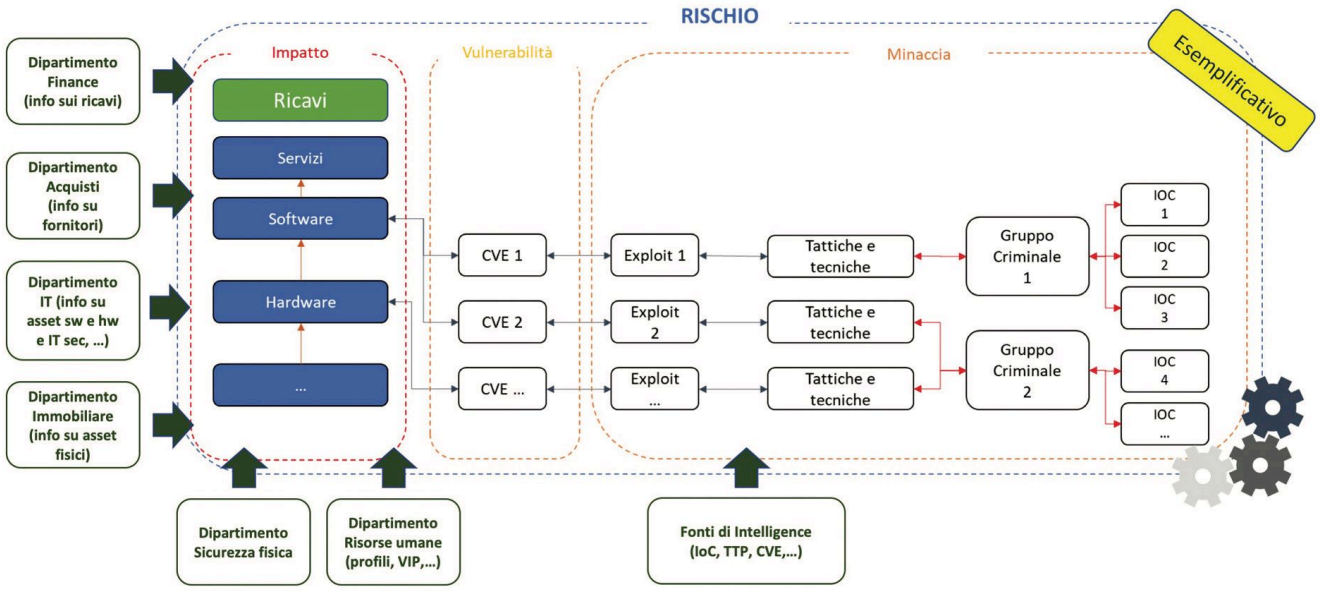
Stabilito il **perimetro** del servizio (catene tecnologiche, asset fisici, personale e fornitori, …) si passa a verificare quali minacce e vulnerabilità possano impattare sullo stesso. L'identificazione del perimetro è forse la parte più dispendiosa delle attività in termini temporali e relazionali. Questo processo può essere supportato da precedenti analisi del rischio, controlli audit, che possono costituire una base di partenza dell'analisi. È un lavoro che richiede un approccio multidisciplinare.

Il perimetro è il fulcro del sistema di valutazione del rischio.

La funzione del rischio rimane sempre la stessa, sono le tempistiche della sua applicabilità che cambiano e il perimetro informativo che si ampia. Invece di essere una fotografia statica annuale, mensile, o periodica la funzione del rischio dinamico viene popolata continuamente da informazioni che ne cambiano, eventualmente, il risultato. Il popolamento avviene attraverso flussi costanti di informazioni che devono poi essere verificati, normalizzati, contestualizzati per poi fornire degli input allo scenario del rischio. In questo modo, lo scenario del rischio viene ricalcolato in base all'input fornito.

Il sistema richiede, innanzitutto, la capacità di immagazzinare e trattare una grande mole di dati e capacità computazionali per elaborarle. I dati, almeno in questa prima fase, devono essere normalizzati e strutturati per permetterne la continua correlazione.

Una volta stabilite le correlazioni da effettuare, è necessario anche inserire degli algoritmi in grado di pesare l'informazione. Ad esempio, pesare di più gli asset propedeutici all'erogazione di servizi che generano maggiori ricavi o margini più alti. Attenzionare maggiormente le CVE che hanno un'alta probabilità di sfruttabilità, attraverso la creazione di algoritmi probabilistici, e prioritizzarle maggiormente



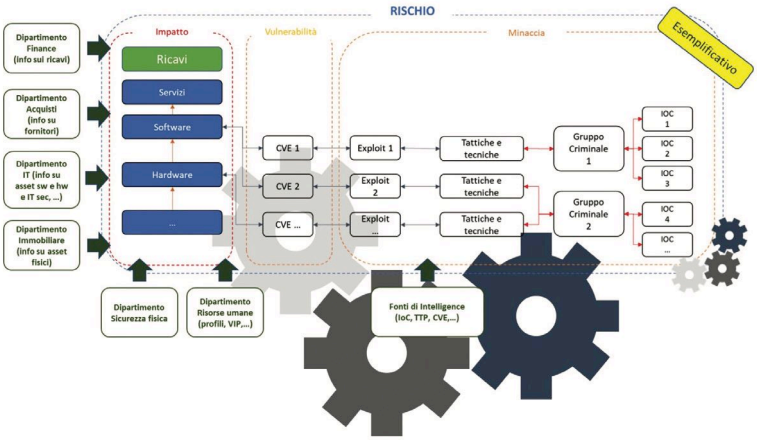
nel momento in cui le fonti di intelligence annoverano l'utilizzo delle stesse da particolari gruppi criminali. La cosa più vicina e associabile al perimetro, è la vulnerabilità, sfruttabile da una minaccia, come rappresentato nella figura sopra.

Stessa cosa per le tattiche e tecniche di attacco, andando a prioritizzarne il monitoraggio in base al maggior utilizzo da parte dei criminali. Se più criminali utilizzano le stesse TTP, allora sarebbe una buona pratica quella di identificare le tecniche maggiormente utilizzate e verificare se ci sono gli strumenti idonei per monitorare l'infrastruttura interna alla ricerca di riscontri.

Allargando il perimetro di monitoraggio, si devono creare dei sistemi di monitoraggio dei fornitori, sia attraverso l'utilizzo di sistemi di valutazione sia grazie al monitoraggio delle fonti di intelligence che possono rilevare potenziali compromissioni, sia attraverso sistemi propri o di terze parti che ne valutano la postura di sicurezza online in real time. Un collegamento con il database preposto alla registrazione dei fornitori e dei relativi contratti permetterebbe di ricevere i dati delle aziende fornitrici e trovare correlazioni con altre fonti di intelligence (in caso di attacchi che le riguardino), ma anche permetterebbe poi di verificare se vi siano utenze personali o collegamenti LAN to LAN fra le due aziende confrontando i dati con i DB di reti e dell'Active Directory. Inoltre, permetterebbe di monitorare anche eventuali flussi email provenienti dai domini delle aziende colpite dall'attacco (dove questo fosse possibile in termini normativi e tecnici).

Un esempio di scenario di alto livello: Supponiamo di ricevere una informativa relativa ad un gruppo criminale specifico che mira a colpire aziende nel nostro settore e nella nostra area geografica. Inserendo questo nuovo input nel nostro sistema di calcolo dinamico del rischio, mi aspetterei:

- Ricezione da parte delle fonti informative delle informazioni collegate al gruppo criminale: IoC, CVE sfruttate, TTP;
- Dal sistema di asset verificherei se le CVE, sfruttate dal gruppo criminale, sono presenti sui miei asset e quale servizio vi è associato. Se le CVE sono già in un piano di patching, se ci sono contromisure specifiche in essere e così via;
- Riuscirei a determinare il valore economico delle perdite in caso quell'asset venisse attaccato in base a un potenziale blocco del servizio oppure in base alle informazioni in esso contenute;
- Dai sistemi perimetrali verificherei se gli IoC collegati al gruppo criminale sono riconosciuti oppure no;
- Verificherei se ci sono informazioni relative alle TTP, soprattutto per identificare quali tecniche solitamente



usano per i movimenti trasversali e se ho la possibilità di identificare eventuali eventi che mi possano allertare al riguardo;

- Verificherei quali sono gli Amministratori di Sistema che possono accedere a quegli asset e se ci siano stati tentativi di contatto, via email, verso di loro da attori malevoli o se risultano delle anomalie comportamentali di accesso degli stessi;
- Verificherei se fra gli annunci o le informative degli attacchi, effettuati dal gruppo criminale, compaiono anche nostri fornitori.

Queste serie di verifiche mi dovrebbero portare ad un livello di rischio e permettere anche di identificare quali azioni mettere in essere per ridurlo. Ad esempio, prioritizzare un patching, bloccare degli IoC non ancora identificati dai sistemi, chiudere delle utenze di fornitori o delle LAN to LAN fino a incidente rientrato e così via. Il valore del rischio rimarrebbe uguale fintanto che un ulteriore input lo vada a modificare: una CVE associata a un gruppo; una nuova CVE pubblicata; ulteriori IoC aggiornati e attribuiti ad un gruppo; un asset cambiato o la postura di sicurezza di un nostro fornitore peggiorata.

L'esempio non è esaustivo e probabilmente approssimativo. Il concetto che si vuole esprimere è quello di continuità di elaborazione in modo da rendere dinamico anche il calcolo del rischio. Ogni input deve essere recepito automaticamente dal sistema e deve rielaborare immediatamente il calcolo del rischio.

Per questo è necessario un lavoro pesante a monte per strutturare le informazioni e creare i canali di approvvigionamento. L'interpretazione del dato stesso ha un ruolo rilevante. In alcuni casi è necessario individuare anche i giusti partner, soprattutto per quanto riguarda le fonti di intelligence. Le fonti di intelligence sono preziose per tutte le informazioni che riguardano minaccia e vulnerabilità ma spesso richiedono un lavoro di normalizzazione elevatissimo in quanto il dato non è strutturato e quindi poco usufruibile in maniera automatizzata nei propri sistemi.

La creazione di un sistema Big Data Analytics in grado di contenere numerose informazioni è un'attività dispendiosa. Identificare i database; trovare il modo in cui agganciarli, verificare la consistenza delle informazioni, creare le giuste query, automatizzarle e definire gli alert, non è semplice. Pertanto, è necessario avere le idee chiare e gli obiettivi di analisi che si vuole raggiungere in modo da portare a casa dei risultati a fasi successive.

Quindi è necessario dotarsi di pazienza e tanto spirito di sacrificio. ■

La convergenza degli investimenti assicura lo sviluppo della digital economy.

Intervista VIP a Gabriele Faggioli.

Autore: Massimiliano Cannata

"Ritengo che siamo ormai entrati in un circolo vizioso su cui occorre ragionare molto attentamente. La digitalizzazione non è una gara che prima o poi finisce. Non ci sarà mai un punto di arrivo. È interesse dei vendor continuare a mettere sul mercato tecnologie, è interesse dei clienti essere competitivi e quindi dotarsene. È nella natura dell'uomo evolvere. Il problema è che la tecnologia costa e costa ancora di più difenderla. Ci dobbiamo chiedere se il modello di informatica distribuita dove ogni azienda e pubblica amministrazione fanno sostanzialmente quello che vogliono sia sostenibile o meno. Secondo me non è così. Pensare che le aziende siano in grado di avere competenze, tecnologie, capacità di investimento è semplicemente miope, direi addirittura impossibile. Soprattutto pensando alle PMI e alle piccole e medie pubbliche amministrazioni". Gabriele Faggioli, come ci ha già dimostrato nelle altre occasioni in cui CST lo ha sollecitato ha le idee molto chiare, sulla rete dei fenomeni che sta caratterizzando lo sviluppo tecnologico.

Prof, la digitalizzazione è un percorso ad ostacoli che sta comunque avanzando. Il rischio nella dimensione della complessità caratterizzato dal continuo divenire di reti , strumenti e sistemi ha assunto un profilo dinamico. Che cosa comporta tutto questo in concreto per aziende, cittadini e istituzioni?

Da 25 anni che nei convegni sento sempre le stesse frasi: "la sicurezza non è un costo e un investimento", "la sicurezza non è un prodotto o un servizio ma un processo", "l'anello debole è il fattore umano", "l'anello debole sono i fornitori", "l'anello debole sono le PMI, "non è un problema se, ma di quando ti attaccheranno" e potrei andare avanti. Evidentemente qualcosa è andato male visto che non solo non si vede un rallentamento del fenomeno ma addirittura stanno esplodendo. Se si continua a pensare allo stesso modo, avremo sempre gli stessi risultati. L'unica via è quella di concentrare le tecnologie, fare economie di scala, in un certo senso togliere le tecnologie alle imprese e alle pubbliche amministrazioni in una logica di convergenza che permetta investimenti congiunti. Ogni paragone con la sicurezza sul lavoro, che sento fare spesso, è fuorviante e profondamente sbagliato. Nel campo della sicurezza sul lavoro noi difendiamo noi stessi e i lavoratori da incidenti che possono capitare per i rischi intrinsechi e per comportamenti errati. Nella cyber ci difendiamo da continue minacce esterne. Nella sicurezza fisica non c'è qualcuno che spara sui lavoratori o che ci lancia bombe incendiarie o che cerca di entrare negli uffici per portare via i server. Se continuiamo a pensare che ogni azienda grande o piccola che sia debba avere un suo esercito, non ne usciremo mai.

Come si stanno evolvendo le minacce e cosa devono maggiormente temere le organizzazioni produttive sempre più bersaglio di attacchi cyber che si presentano molto strutturati ed evoluti?

Dai dati che abbiamo la minaccia più evidente e incombente continua a essere il ransomware.

La doppia estorsione è ancora la strategia più perseguita ed è naturale visti i pochi rischi che comporta e i grandi guadagni che permette di fare. I dati che raccogliamo come Clusit raccontano una situazione sconfortante in Italia, dove gli attacchi gravi riusciti sono aumentati di oltre il 160% fra il

BIO

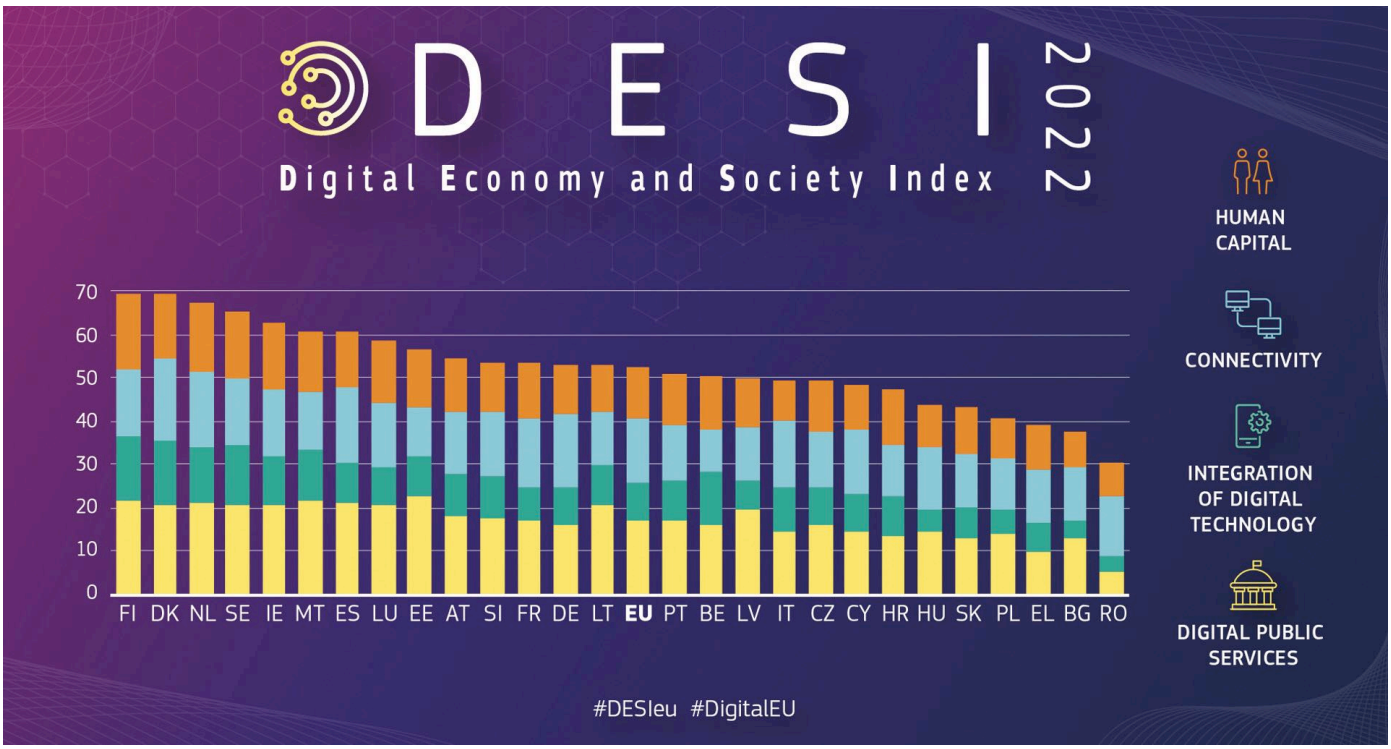
Gabriele Faggioli è Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica), Responsabile Scientifico dell'Osservatorio Cybersecurity & Data Protection del Politecnico di Milano e senior advisor degli Osservatori della Digital Innovation del Politecnico di Milano (dove è Adjunct Professor). È CEO di Digital360 S.p.A. e di Partners4innovation S.r.l. (società controllata da Digital360 S.p.A.). È stato membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. Specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amminstrativa degli enti e nel diritto dell'editoria e del markerting, Gabriele ha pubblicato diversi libri fra cui, da ultimo, "I contratti di cloud computing" (Franco Angeli), "I contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

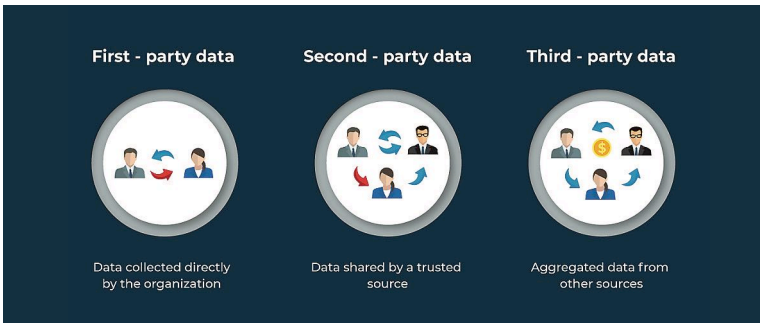
2021 e il 2022 ma, d'altronde, perché non dovrebbe essere così visto che spendiamo in sicurezza informatica lo 0,1% del PIL dove la percentuale è fra un terzo e un mezzo rispetto ai paesi a noi confrontabili? E se parliamo di percentuale, figuriamoci in valore assoluto visto che loro hanno PIL molto più grandi del nostro. Se mettiamo insieme i dati dell'indice DESI dove l'Italia è agli ultimi posti per competenze digitali con i dati degli investimenti, abbiamo chiara la situazione.

La catena del valore digitalizzata crea un contagio delle vulnerabilità. Parafrasando Pier Lévy dovremmo parlare di responsabilità collettiva NKN solo di intelligenza collettiva. Entrano in gioco le terze parti in questa dinamica. Quali strategie vanno seguite per innalzare il livello di sicurezza?

Le terze parti sono un elemento chiave. Penso che le normative dovrebbero insistere molto di più sulla loro responsabilizzazione. Insisto sulla necessità di comprendere il senso di fondo, quando la mia azienda mi manda in treno o in aereo non deve studiare se i sistemi frenanti o i sistemi di volo sono sicuri o meno. Diamo per scontato che lo siano e non è richiesto di analizzarlo. E allora perché dovremmo tutti studiare se un cloud provider, un fornitore di servizi di outsourcing, un soggetto a cui esternalizzo un processo o un servizio è sicuro o meno?

Si tratta di replicare all'infinito le stesse analisi per poi arrivare (quasi) tutti a dire che quel gestore di posta elettronica in cloud è sicuro. Certo, non ci sono anche i grandi fornitori mondiali ma andiamo alla sostanza: è sostenibile questo modello di catena unita alla evoluzione rapidissima digitale e all'impostazione normativa attuale? No credo e i fatti lo dimostrano. Penso da tempo che servono azioni anche legislative che mirino a spostare il baricentro della responsabilità dai clienti ai fornitori perché li stanno le competenze e le tecnologie.





Quali sono le filiere maggiormente esposte al rischio cyber?

In Italia sicuramente il manufatturiero. Ma penso sia normale considerando come è fatto il mercato, tanti piccoli imprenditori che fanno tanti micro investimenti che danno che risultato tanta grande insicurezza. Anche il settore sanitario è perennemente sotto pressione ma, comunque, dai dati emerge in tutta evidenza che siccome il ransomware non ha preferenze, alla fine se sono poco protetto sarò attaccato qualunque sia il mio settore di mercato.

Il Garante della Privacy ha ricordato recentemente i 5 anni dalla approvazione del GDPR. Quale deve essere il giusto bilanciamento tra tecnica è libertà?

A me piace pensare che l'unico limite dovrebbe essere quello di non far danno ingiusto agli altri. Ma ovviamente è principio troppo generico per poterlo applicare. È molto difficile pensare a una impostazione normativa, per ovvi motivi, rigida, che possa accompagnare l'evoluzione tecnologica. Preferirei un approccio basato su normative che diano indicazioni di principio e generali, rispetto a tantissimi obblighi e divieti puntuali. Di sicuro il rischio di una contrapposizione esiste ma il nostro Garante ha dimostrato una grande sensibilità e la vicenda ChatGpt lo dimostra. È possibile evolvere senza venire meno ai principi chiave fissati in Europa.

In occasione della due giorni alla Sapienza organizzata da CRS 4 è emersa la carenza di figure professionali adeguate in un mercato come quello della cyber security che ha assunto un valore strategico nella società dell'informazione. Qual è la sua opinione in merito?

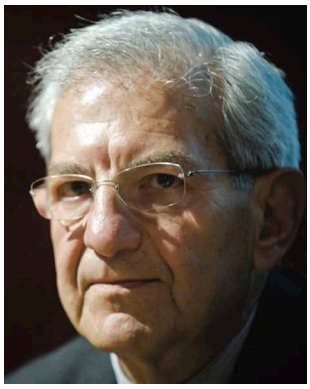
Non ci sono dubbi. L'indice DESI della Commissione Europea racconta di una Italia gravemente in ritardo nelle competenze digitali, non solo di sicurezza informatica. Ritengo che sia una vergogna nazionale e che bisognerebbe intervenire immediatamente fin dalle scuole primarie. Da un altro punto di vista è una grandissima occasione per chi invece sta investendo in questo settore e, comunque, vuol dire che nei prossimi anni le giovani e i giovani avranno una grandissima opportunità lavorativa. Cerchiamo di vedere, dove possibile, il bicchiere mezzo pieno.

Il grande sviluppo dell'intelligenza generativa come ha cambiato, se le ha cambiate, le "carte" in tavola per chi si occupa di cyber security?

Sicuramente la capacità di analisi, predittiva e reattiva ha già avuto e sempre più avrà dei grandi vantaggi dall'IA. Il problema secondo me sarà capire chi si avvantaggerà di più fra attaccanti e difensori. Consideriamo che gli attaccanti possono giocare senza regole e a budget potenzialmente illimitato, contrariamente a quello che possono fare i difensori che da una parte devono rispettare le normative e dall'altra hanno molti limiti rispetto a una potenziale reazione e contrattacco. Quindi ci troviamo di fronte a un campo da gioco che non è piano e regolare, nel quale una squadra gioca senza arbitro e può fare tutti i falli che vuole. In conclusione la mia risposta è sì. L'IA può cambiare le carte in tavola ma bisogna vedere chi dopo avrà le carte migliori da giocare. ■

Il potere delle piattaforme nella grande agorà del "metaverso".

Intervista VIP a Luciano Violante.



Autore: Massimiliano Cannata

"È ancora presto per dire quali scenari si aprono con lo sviluppo del metaverso. McKinsey valuta in due/tre trilioni di dollari gli investimenti entro questo decennio. Gli avatar tra poco avranno anche il tatto e il gusto. È difficile fare valutazioni attendibili il nostro sforzo deve tendere alla costruzione di una civiltà digitale, caratterizzata dall'autonomia e dal dominio della persona sull'algoritmo, senza di cui non può esserci futuro". Luciano Violante, giurista e magistrato, presidente della Fondazione Leonardo, colosso della difesa, aereo spazio e sicurezza impegnata nella definizione dello statuto etico e giuridico di questa che è l'ultima tappa della rivoluzione digitale, invita in questa intervista alla cautela, quando si affronta un tema dalle mille sfaccettature come è appunto il metaverso.

Presidente, i grandi player pubblici e privati stanno cercando di migliorare la* governance *della rete, nel tentativo di garantire la sicurezza delle comunicazioni e delle transazioni, il rispetto della Privacy e dei diritti inviolabili persona, la trasparenza. Come va affrontata questa sfida?

Lo sviluppo tecnologico non si può certo arrestare, così come non si può fermare la creatività umana. Ma si può pensare di indirizzare e costruire una governance delle tecnologie insieme ai tecnologi, nella consapevolezza che gli ambiti economici e sociali che risentiranno maggiormente di questa nuova rivoluzione sono gli stessi del web 2.0: relazioni umane, marketing, comunicazione, finanza ed economia, educazione, salute, con una differenza importante: la potenza della mutazione in questo caso sarà incommensurabilmente superiore, rispetto ad altri "salti" di paradigma che abbiamo sperimentato. Un aspetto ci tengo subito a puntualizzare: la costruzione dell'autonomia e del dominio della persona sull'algoritmo è l'obiettivo da porsi nel presente, per poter essere liberi nel futuro. Sta alla nostra responsabilità poterla realizzare.

Nel suo intervento ufficiale presso il Garante in occasione della giornata europea per la protezione dei dati personali si è soffermato su un neologismo: "figitale". Possiamo spiegare il significato?

Nel linguaggio ordinario il termine indica un nuovo paradigma che interessa ogni aspetto del vivere, dell'abitare, dell'apprendere, del fare, dall'ambiente alla città, dal gaming alla didattica, dall'etica al lavoro, dai fondali marini allo spazio. Un solo esempio: la catena cinese Kentucky Fried Chicken ha installato nei propri fast-food degli schermi intelligenti capaci di sfruttare il riconoscimento facciale e l'intelligenza artificiale per proporre offerte speciali ai clienti.

Dall' "homo videns" tematizzato da Giovanni Sartori all' "homo distans", che si sostanzia in una dimensione dell'io che si "allontana dal proprio corpo". Dobbiamo avere paura di questa condizione dell'essere che ancora poco conosciamo?

Parlerei di *homo distans*, con riferimento alla possibilità di socializzare tra persone che sono distanti e dialogano attraverso i propri avatar. Esiste il rischio, che va affrontato e temperato, di un ulteriore allentamento dei legami sociali e interpersonali. Rischio che non possiamo sottovalutare e di cui dobbiamo occuparci, con il massimo della responsabilità.

I rischi della reintermediazione

L'oligopolio delle piattaforme mette a rischio le libertà democratiche. Esistono delle contromisure efficaci?

Nella nostra società l'inganno più pericoloso è la disintermediazione. Non è in corso la cancellazione dei mediatori: è in corso la loro sostituzione. I vecchi mediatori – partito, associazione, chiesa, famiglia, sindacato – si presentavano come tali sulla scena pubblica, erano scalabili, avevano statuti conoscibili. I nuovi mediatori non si presentano come tali, non sono scalabili, non hanno visibili statuti. Microsoft, Amazon, Google ci danno a costi accettabili e con efficienza i servizi che ci sono indispensabili. In cambio consegniamo loro gratuitamente e liberamente tutti i nostri dati. Se gli stessi dati ci venissero chiesti dallo Stato, partirebbero cortei e campagne di stampa. In realtà quello che è in corso è un processo di reintermediazione, che va studiato con molta attenzione.

A cosa si riferisce in particolare?

Alle piattaforme, cui si faceva prima riferimento, che orientano la nostra vita quotidiana in misura maggiore rispetto ai mediatori tradizionali. In passato si conosceva l'indirizzo, il numero di telefono, i dirigenti e gli addetti del proprio partito o sindacato, della propria parrocchia. Si poteva mettere in discussione la leadership del partito e del sindacato e candidarsi al loro posto. Al contrario oggi non abbiamo l'indirizzo e il numero di telefono di Amazon, né tanto meno possiamo pensare di scalarla. I rischi sono evidenti. Per i mediatori occulti non ci sono né regole né contropoteri; senza idonee contromisure sono destinati a esercitare sulle nostre vite un potere infinito. I flussi di pensiero pilotati attraverso i social media contano più della intelligenza individuale. Chi governa l'ambiente digitale ha la possibilità di decidere non solo cosa compriamo, ma cosa pensiamo e come ci orientiamo nel mondo.

BIO

Presidente della Fondazione Leonardo, Luciano Violante è docente di Diritto pubblico presso l'Università "La Sapienza" di Roma e l'Ateneo della Valle d'Aosta. Giurista e Magistrato, negli "anni di piombo" ha ricoperto il delicato incarico di giudice istruttore a Torino dove si è subito distinto per l'impegno sistematico e l'azione di contrasto del fenomeno del terrorismo. Parlamentare di lunga militanza nelle file del Pci, del Pds e dei Ds, è stato presidente della Commissione parlamentare antimafia (1992-1994) e della Camera dei deputati (1996-2001) ed ha fatto parte della commissione di "10" saggi, nominati dal Presidente emerito della Repubblica Giorgio Napolitano, con la finalità di definire le riforme istituzionali e economico-sociali necessarie per lo sviluppo del Paese. Attualmente è al vertice di "Italiadecide" (cfr. www.italiadecideit) l'associazione *bipartisan* che può vantare tra i soci fondatori personalità del calibro di Carlo Azeglio Ciampi, Giuliano Amato, Gianni Letta, Pier Carlo Padoan, Giulio Tremonti. Lo scopo di questa realtà associativa è quello di contribuire al miglioramento della qualità delle politiche pubbliche e di valorizzare i diversi livelli di *governance* territoriale attraverso un'applicazione puntuale e rigorosa della logica della sussidiarietà. Alcune delle sue pubblicazioni per Einaudi: *Non è la piovra, Un Mondo asimmetrico, Magistrati, Politica e Menzogna, Il dovere di avere doveri*. Ha inoltre curato i volumi degli Annali della Storia d'Italia su: *La criminalità, Legge, dirito, giustizia, Il Parlamento.*

Da dove proviene, a suo avviso, questo immenso potere?

Microsoft, Google, Amazon, le più grandi piattaforme, controllano il 64% del mercato cloud infrastrutturale. Microsoft ha circa il 90% dei sistemi operativi per server e PC e gestisce Office che è il pacchetto software più diffuso al mondo. Il 92% delle nostre caselle di posta elettronica è gestito da Microsoft, Apple, Google. Sempre per definire il peso delle compagnie del digitale, ricordo che nel 1990 le prime cinque imprese USA in termini di capitalizzazione erano IBM, Exxon, General Electric, AT&T, Philip Morris. Nel 2020 erano Apple, Microsoft, Amazon, Alphabet, Facebook. Nello stesso anno, inoltre, ciascuna delle cinque maggiori compagnie tecnologiche valeva più delle 76 maggiori società energetiche messe insieme. Viviamo in un oligopolio. Gli oligopolisti hanno nelle loro mani persone, imprese, Stati. Se girassero l'interruttore, il mondo si fermerebbe. Questa è la loro forza con cui dovremo imparare a misurarci. ■

La partita della rivoluzione digitale, si vince se mettiamo al centro l'uomo.

Intervista VIP a Michele Petrocelli.

Autore: Massimiliano Cannata

"Quando il 10 febbraio 1996 a Philadelphia il computer Deep Blue sconfiggeva Kasparov nel gioco allora ritenuto più umano e razionale di tutti, gli scacchi, è probabilmente iniziata una nuova era, in cui le macchine entravano nella sfera del pensiero e dell'apprendimento umano. Ma la partita a scacchi esistenziale che abbiamo adesso davanti a noi, faccia a faccia con il nostro futuro, è quasi una versione moderna della scena del "Settimo Sigillo", in cui di fronte a noi c'è un avversario imbattibile, ineluttabile ed imperscrutabile. Ma questo non deve lasciarci impauriti o rassegnati. La partita a scacchi è inesorabilmente persa solo se riteniamo che le regole del gioco non possano essere cambiate. Eppure, proprio l'innovazione tecnologica ci insegna che la partita che giochiamo tutti i giorni si basa su pezzi sempre diversi e regole nuove, tanto che è il cambiamento, piuttosto, a preoccuparci. Ma è proprio per questo che la riscoperta dell'essere umano e la sua collaborazione con la macchina è il valore più profondo di questa rivoluzione. Perché le macchine sono e saranno sempre più brave, veloci ed efficienti nelle risposte, ma sono gli esseri umani chiamati a cercare e porre nuove domande, capaci di mutare scenari e riscrivere il senso dell'agire, della coscienza, della giustizia e della vita. Ritrovare l'umanità oltre la razionalità è la vera mossa con cui va iniziata ogni giorno, la partita".

Michele Petrocelli, docente di Economia politica, Economia monetaria e Strategia dell'innovazione presso l'università Guglielmo Marconi di Roma, nel saggio (In)Coscienza Digitale (ed. Lastarìa) tratteggia un affresco straordinariamente lucido ed equilibrato della rivoluzione digitale entro cui siamo immersi, senza avere la giusta consapevolezza che tutto è cambiato. Per dirla con Baricco è cambiata la scacchiera non solo il gioco degli scacchi. Una metafora da cui parte Petrocelli per una disamina che coglie tutte le contraddizioni ma anche la grande opportunità di un mondo nuovo che dobbiamo imparare ad "abitare".

Prof Petrocelli siamo immersi nella rivoluzione digitale, tarda però a farsi strada una esatta consapevolezza della nuova condizione che ha generato un mutamento del sistema economico e della posizione dell'uomo nell'universo. Quali sono le ragioni di questa lentezza?

La rivoluzione digitale che viviamo è profonda e riguarda tutti gli aspetti della nostra vita. Digitalizzare significa trasformare la realtà in numeri, e come tali elaborarli anche grazie ad una capacità di calcolo impressionante e sempre crescente. E in questa realtà c'è anche ciascuno di noi, i nostri

BIO

Michele Petrocelli conseguito la laurea con lode in Economia e il Dottorato di Ricerca (PhD) in "Economia e Finanza nel governo dell'impresa", entrambi presso l'Università La Sapienza di Roma. Dal 2001 è al Ministero dell'Economia e delle F. Attualmente è Dirigente del Dipartimento del Tesoro. Dal 2004 è docente all'Università degli studi Guglielmo Marconi di Roma, dove attualmente insegna Economia politica, Economia e organizzazione aziendale e Strategie dell'Innovazione ed è Direttore del Master in "Marketing Management". Ha ricoperto diversi incarichi accademici e ha preso parte a diversi progetti internazionali di ricerca in materie economiche.

comportamenti, le preferenze, le scelte. Davanti a questo scenario l'adeguamento è difficile perché, rispetto al passato, la frequenza del cambiamento conseguente all'innovazione è elevatissima, e non siamo abituati a questa velocità. La vita di ognuno di noi è completamente immersa in un ambiente dominato dalle tecnologie digitali, strumento prezioso, in grado di aprire possibilità straordinarie e allo stesso tempo generare rischi importanti. Per cogliere le opportunità e per contenere i rischi, il passaggio chiave non è tecnologico, è culturale. Nel viaggio intrapreso con la scrittura di "(In)Coscienza Digitale" ho provato a riflettere proprio su questo, pensando a come l'impatto di questa rivoluzione tecnologica sia sistemico e come la soluzione, in fondo, non sia che nella maggiore consapevolezza delle nostre qualità umane.

La dicotomia uomo - macchina ha radici antiche. Per avere un'idea che risale al "repertorio" degli studi umanistici, basti pensare alle macchine di Leonardo, specchio della grande capacità umana di creare e innovare. Oggi appare tutto più difficile, stentiamo infatti a governare quella che Severino definiva "cieca volontà di potenza della tecnica". Qual è il suo giudizio in merito?

La tecnica è diventata la componente dominante della vita sociale. La tecnologia, in sé stessa, ha una portata liberatoria fortissima: ci libera dalla fatica, aumenta la produttività, ci concede tempo libero per il pensiero e la creatività, ci permette di conoscere i fenomeni come mai in passato. Ma per fare questo, deve essere compresa e governata da chi la utilizza, aiutando le persone a valorizzare chi sono e ciò che vogliono fare. Per superare il dilemma posto da Severino, dobbiamo cercare concepire il nostro rapporto con le macchine non come "dicotomia" ma come collaborazione, complementarità. Gli esseri umani aiutano le macchine ad apprendere, le macchine amplificano le capacità degli esseri umani di comprendere ed agire nel mondo. Il rischio si presenta quando deleghiamo alle macchine le nostre scelte, senza esserne completamente consapevoli, perdendo il controllo dei processi decisionali, produttivi e sociali che ci riguardano. L'importante è acquisire coscienza e conoscenza di questi processi e governarli, indirizzarli, sfruttando la "potenza" della tecnologia, condizionata alla "nostra" volontà.

Innovazione, sorveglianza, post democrazia, tre termini complessi costituiscono il sottotitolo del suo interessante saggio. Possiamo spiegare come si coniugano questi concetti in quella che Floridi ha definito infosfera, caratterizzata da una "ontologia ibrida" in cui reale e virtuale si mescolano?

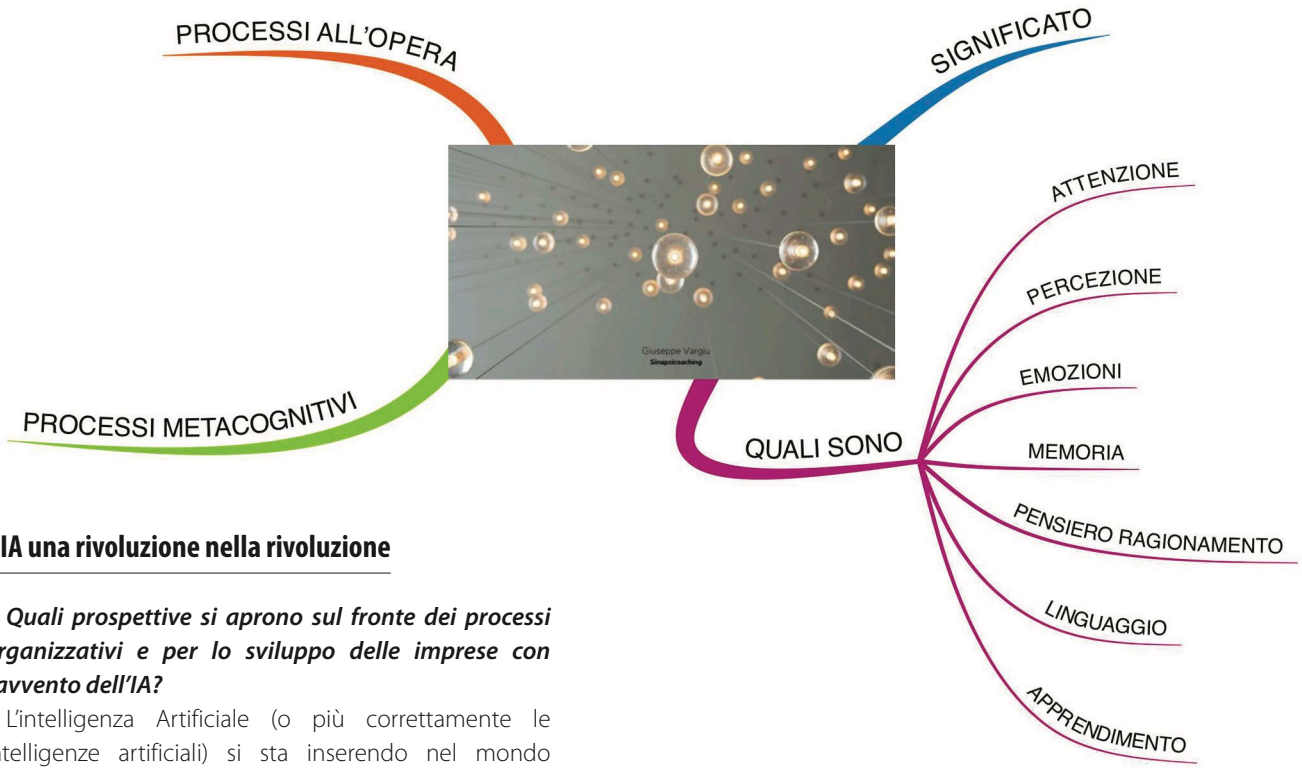
Sono concetti che fanno parte inevitabilmente dell'*Onlife*, dove i confini tra la vita online e quella offline tendono a sparire. Oggi siamo ormai connessi gli uni con gli altri, diventando progressivamente parte integrante di un'"infosfera" globale. Questo però nasconde un paradosso. L'accesso ipoteticamente infinito, continuo e completo all'informazione finisce per limitare la capacità delle persone di formarsi dei giudizi autonomi, di "essere informate". La facilità della tecnologia di fornire con continuità informazioni riduce il tempo di elaborarle, comprenderle e formarsi un giudizio autonomo.

Contemporaneamente, lo sviluppo degli algoritmi di ricerca e selezione delle informazioni favorisce la

polarizzazione delle posizioni. È un fenomeno noto, si chiama "camera dell'eco", ed esiste da sempre: poiché tendiamo a cercare conferme alle nostre tesi, più che smentite, siamo, per natura, più inclini a riconoscere e processare le informazioni che rafforzano le nostre idee e le nostre convinzioni rispetto a quelle che le confutano. Tendiamo dunque a circondarci di persone e contenuti che sono d'accordo con noi. Gli algoritmi dei social media amplificano questo processo perché ci espongono, automaticamente, i contenuti più affini ai nostri pensieri, ai nostri gusti, ai nostri ideali. Il risultato di queste due tendenze è che non abbiamo più la disponibilità di tempo e spazio per il confronto, la riflessione, l'elaborazione, elementi distintivi di un sistema democratico. Succede così che il consenso si polarizza e si perde di vista la mediazione e la ricerca del dialogo.

Possiamo fare qualche esempio per capire meglio il fenomeno di cui stiamo parlando?

Gli scandali connessi con le campagne elettorali social di Cambridge Analytics che hanno acceso una luce su come il contagio emotivo trasmesso sui social possa sfruttare questa debolezza della nostra capacità cognitiva per indirizzare voti in maniera arbitraria. Quello che appare più evidente è il pericolo a cui sono esposte le nostre libertà davanti alla forza dirompente della rivoluzione digitale. L'unica risposta possibile è la conoscenza, dei propri processi cognitivi, della capacità della tecnologia di influenzarli e di indirizzare le nostre scelte. Un processo conoscitivo che possa "vaccinarci" e renderci immuni da questi pericoli.



L'IA una rivoluzione nella rivoluzione

Quali prospettive si aprono sul fronte dei processi organizzativi e per lo sviluppo delle imprese con l'avvento dell'IA?

L'intelligenza Artificiale (o più correttamente le intelligenze artificiali) si sta inserendo nel mondo produttivo dal basso e dall'alto. Dal basso, proseguendo il processo tipico delle rivoluzioni industriali, in cui le macchine si sostituiscono alle persone nei processi routinari e "robotizzabili", che la tecnologia può compiere in modo più veloce, efficiente, efficace, sicuro, produttivo. Ma questo processo di sostituzione avviene anche dall'alto. La tecnologia può, infatti, gestire i processi elaborativi e decisionali, applicati a molti dati. L'IA generativa sta, inoltre, divenendo in grado di produrre contenuti, immagini, codice, in modo sempre più simile a quello che produrrebbe un essere umano. La rivoluzione che avremo quando l'IA generativa entrerà nei software di produttività individuale sarà dirompente, forse simile a quando i computer sono comparsi sulle scrivanie delle persone, ma con una velocità di inserimento nei processi lavorativi molto più alta.

È proprio la "sostituzione" della forza lavoro che preoccupa, non crede?

I timori sarebbero comprensibili se considerassimo solo il fenomeno della "sostituzione" di lavoro con capitale, ma così facendo rischieremmo di non cogliere la vera opportunità della grande trasformazione in atto. Il processo produttivo si innova profondamente solo nella misura in cui le macchine collaborano con l'essere umano. È in questa collaborazione, infatti, il valore aggiunto dei nuovi processi di trasformazione, in quell'area in cui il lavoro è ibrido, le persone guidano l'apprendimento delle macchine e la tecnologia aumenta la capacità delle persone di analizzare e comprendere i fenomeni, memorizzare informazioni, studiare scenari. L'intelligenza artificiale generativa produce contenuti in modo veloce, contenuti che in prospettiva risponderanno a criteri qualitativi sempre più alti. Il valore decisivo in questa nuova dinamica espressiva e produttiva si innesca quando l'individuo può applicare su quei contenuti la propria valutazione critica.

Secondo una recente inchiesta de La Repubblica l'intelligenza artificiale aumenta la produttività. Come va affrontata questa evoluzione che modifica il modo di fare e concepire l'impresa?

Vi sono dei lavori che verranno svolti dalle macchine. Altri che verranno sostituiti molto più tardi. Altri ancora, probabilmente, resteranno a pieno appannaggio dell'essere umano. Tra questi ultimi sicuramente i temi che riguardano l'arte, la creatività (che è cosa diversa dalla capacità generativa dell'intelligenza artificiale), l'etica, la giustizia, il pensiero laterale

Intelligenza artificiale, una rivoluzione che fa scattare la produttività nelle aziende italiane

di Beniamino Pagliaro

Per le realtà lavorative un enorme guadagno di efficienza. Ma dovranno ripensare i processi produttivi e raccogliere i propri dati. Chi non lo fa rischia di restare fuori gioco

e l'empatia. Competenze tipiche delle persone, che vanno sviluppate in modo completamente diverso da come abbiamo fatto in passato. Sono competenze che si sviluppano esaltando l'autonomia, l'apprendimento, la curiosità. Sviluppando la motivazione intrinseca (quella che ci spinge ad agire per il piacere di quello che facciamo), riconoscendo il valore del contributo umano. Significa creare spazi in cui sviluppare il proprio potenziale, in cui esiste il tempo per l'innovazione e la creatività.

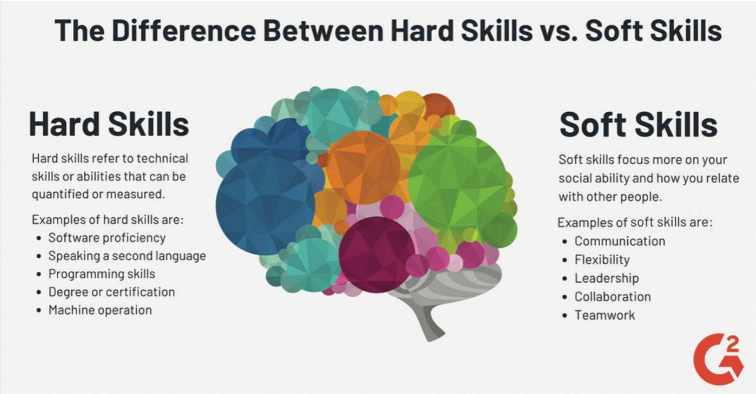
Essere digitale: cosa ci aspetta

Il futuro non è dunque così nero, come alcuni osservatori si ostinano a dipingerlo?

Se acquisiamo coscienza critica e capacità interpretativa, sicuramente no. Lo spazio ed il tempo liberato dalla tecnologia nelle vite delle persone possono lasciare il posto a questa capacità innovativa, sviluppata collaborando con le macchine. Significa ripensare il modo di lavorare, la fiducia nelle persone, nella loro qualità individuale. Se poniamo in essere processi lavorativi che, invece di amplificare la collaborazione, mettono le persone in competizione con le macchine, finiremo col perderci tutti.

Cruciale il rafforzamento delle competenze. Una recente assise sulla rivoluzione digitale organizzata Presso La Sapienza di Roma da Cyber 4.0 e dal Ministero dello Sviluppo Economico ha sottolineato come la criticità di questa fase sia determinata dalla necessità di costruire profili adeguati a un mercato del lavoro profondamente modificato dalla rivoluzione digitale. Come si può rispondere alla domanda delle imprese?

Investendo in formazione, non vedo altra soluzione. Le professioni e le competenze vedono il loro tasso di obsolescenza aumentare e accelerare a causa dell'aumentata frequenza dell'innovazione. Dare alle persone la curiosità, il tempo e l'opportunità per adeguare le proprie conoscenze al cambiamento è un investimento per le imprese come per le persone. In questo mutato contesto il sistema universitario per primo, deve giocare una nuova partita, meno autoreferente e più efficace nell'anticipare il cambiamento e nell'affiancare le imprese che stanno affrontando la transizione tecnologica verso il digitale. Soft e hard skills devono essere costruite insieme per cambiare passo.



Guardiamo alla più stretta attualità. Che idea si è fatto della polemica generata dalle misure adottate dal Garante sul fronte della privacy in relazione alla utilizzazione di ChatGPT. Sono atteggiamenti draconiani, come hanno stigmatizzato molti osservatori, o si tratta di una giusta attenzione per la privacy e i principi etici?

Parlando di regolamentazione della tecnologia e dell'IA in questo caso, possiamo riconoscere tre approcci. Uno, di stampo statunitense (modello Silicon Valley n.d.r) che crede ciecamente nel valore della tecnologia che, per la sua capacità di liberare l'uomo, deve essere assecondata, utilizzata, stimolata. Una sorta di filosofia del *laissez-faire* in campo tecnologico. Per questo modello fermare l'innovazione non solo è impossibile, ma costoso e deleterio. C'è poi l'approccio europeo, che potremmo definire di stampo neoumanista, in cui al centro c'è la persona e la sua individualità, i suoi diritti, la sua personalità. Per questo modello la regolamentazione deve avere l'obiettivo di mettere la tecnologia al servizio dell'individuo e dei suoi bisogni individuali e sociali. Il terzo approccio, più dirigista, prevede che lo sviluppo della tecnologia debba essere diretto ed indirizzato dai governi centrali per i fini che questi ritengono più opportuni (il modello cinese può fare da esempio n.d.r). Stiamo parlando di tre modelli di regolamentazione, che sono il riflesso di filosofie e visioni del mondo molto diverse.

A quale bisognerebbe dare più spazio e credito?

Ritengo che l'approccio dell'Unione Europea sia quello più corretto e che quindi non si debba in sé temere o frenare lo sviluppo tecnologico (che va anzi incoraggiato ed incentivato), ma comunque vigilare perché i suoi effetti, le sue potenzialità ed i suoi limiti siano compresi dalle persone. Proteggere la libertà del singolo, mantenendo un approccio aperto, etico e pienamente informato sull'utilizzo degli strumenti high tech è essenziale se vogliamo dare qualità al processo di sviluppo della tecno scienza. Se guardiamo all'enorme patrimonio di dati che circolano sulle reti, probabilmente si è cominciati con ritardo a far scattare delle policy efficaci di tutela e di protezione, "la nave era salpata", recuperare era forse impossibile. Sull'IA generativa siamo ancora in tempo, perché le persone prima di utilizzarla la comprendano, siano informate dei limiti e delle potenzialità, cosicché la possano applicare coscientemente, per realizzare i progetti, che legittimamente coltivano. ■

Cybersecurity vuol dire responsabilità condivisa.

Intervista VIP a Davide Giribaldi.

Autore: Massimiliano Cannata

A caccia di rischi cyber per allevare talenti. In maniera non ufficiale Davide Giribaldi si definisce così, fotografando molto bene il suo modo di intendere e praticare la sicurezza. Giribaldi è uno studioso senza frontiere conosce le organizzazioni, ha girato e continua a girare mezzo mondo. "La sicurezza è prima di tutto cultura" questo il vero leitmotiv della nostra conversazione, "è responsabilità condivisa, è attenzione a tutti gli attori nessuno escluso. Le terze parti sono dentro l'orizzonte di una governance illuminata del rischio Cyber, che non deve erigere muri ma affinare competenze e linguaggi per vincere una partita che sa di civiltà".

Dott. Giribaldi, il rischio dinamico si inquadra nell'orizzonte mutante della complessità. Che cosa comporta questa condizione che connota non solo l'economia, ma in senso più ampio la società in tutte le sue articolazioni?

Il primo livello di analisi da prendere in esame riguarda la digitalizzazione tecnologica, un processo rapidissimo, che corre a una velocità esponenziale. Questo è l' *"oikos"*, per dirla in termini classici l'ambiente cui dobbiamo riferirci per sviluppare qualsiasi riflessione. Aziende istituzioni, cittadini che si muovono nella contemporaneità avvertono una potente spinta all'innovazione, sono i tempi e i linguaggi a fare la differenza, perché il problema di fondo è culturale. Le

imprese, soprattutto quelle meno strutturate, hanno evidenti difficoltà organizzative a stare al passo dei ritmi evolutivi, stesso ragionamento va fatto per la PA, rallentata da tradizionali "ossificazioni burocratiche". L'ostacolo più forte è rappresentato dal deficit di competenze e viene prima degli aspetti finanziari e di sostenibilità economica, che pur preoccupano e che prendono le prime pagine dei giornali. C'è insomma un alfabeto del digitale da costruire e far conoscere, per far comprendere quali sono i reali benefici della "quarta rivoluzione".

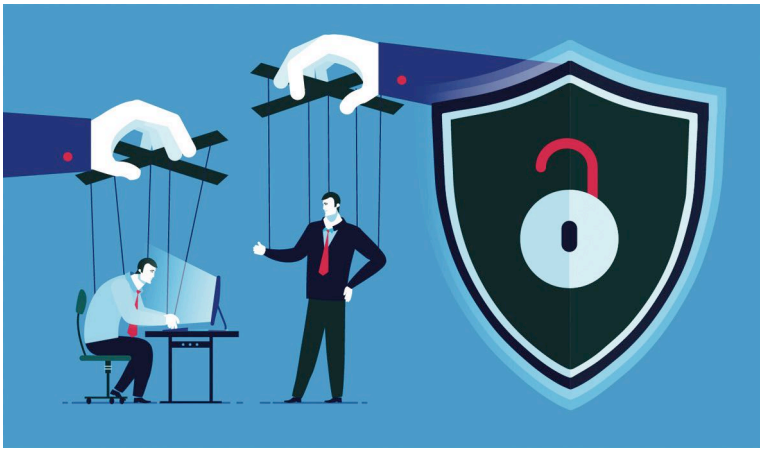
Da che cosa dipende questa "fragilità" strutturale, da lei presa in esame, che esercita degli inevitabili riflessi sulla carenza di figure professionali richieste dal mercato della cyber security?

Un certo retaggio "crociano" e la generale impostazione del nostro sistema formativo che non ha, come sappiamo, riconosciuto il giusto valore agli istituti tecnici e alle scuole di avviamento professionale hanno avuto e hanno il loro peso. Non si tratta di alimentare nessun dualismo, non esistono due culture, piuttosto bisogna operare per facilitare il giusto mix tra il corredo di competenze umanistiche, molto importanti nelle organizzazioni, e le competenze tecniche ingegneristiche, informatiche che non possono mancare. Sul campo mi accorgo in particolare che quando

si parla di digitalizzazione molti manager e dirigenti tendono a dire: se abbiamo sempre fatto così perché dovremmo cambiare. Se ci soffermiamo nell'ambito della cybersecurity che più ci interessa, il commento generale diventa: deve capitare proprio a me di subire un attacco? Questo fa capire la distanza che esiste tra l'esigenza reale di innovazione e il percepito diffuso in larga parte del mondo produttivo e dell'opinione pubblica.

Gli attacchi alle reti informatiche stanno diventando sempre più frequenti. Cosa dobbiamo maggiormente temere?

Lo scenario geopolitico che si è creato con il conflitto in Ucraina ha determinato uno scatto in avanti delle strategie di attacco cyber. Vi sono molti gruppi che approfittando della situazione e studiando il teatro di guerra operano una sorta di "pesca a strascico", affinando azioni, interventi, percorsi di attacco. Cosa può succedere? I tentativi più significativi per operare delle truffe e per violare i sistemi, soprattutto nell'universo delle PMI, vengono messi in atto utilizzando tecniche *ransomware* e *phishing*. Queste modalità hanno alla base una cosa molto importante: la conoscenza dell'ingegneria sociale, che come ci ha insegnato Kevin Mitnick, ammantano l'inganno



di motivazioni che trovano la loro radici in bisogni essenziali dell'uomo. Mettere fretta, chiedere aiuto, sono situazioni che fanno leva sui nostri sentimenti, sul senso di scarsità che ci attanaglia, e che ci rende deboli.

I linguaggi e le metodologie del cyber criminali si stanno indubbiamente affinando. La nostra capacità di risposta a che punto è?

Alle organizzazioni viene richiesta efficacia e rapidità, fattori che impongono una riflessione. Oggi soprattutto in determinati settori che

BIO

Davide Giribaldi è GRC & Information Security Advisor. Dal 1994 nel settore dell'information security, è specializzato nella Governance dei rischi cyber in contesti critici e si occupa di processi e contromisure in ambito sicurezza delle informazioni, continuità operativa e gestione delle crisi presso Società Multinazionali e Pubbliche Amministrazioni europee. Ha una laurea in Scienze Economiche e un master in Intelligenza Artificiale ed etica delle tecnologie emergenti. È Certified Data Privacy Solutions Engineer (ISACA) nonché Auditor/Lead per gli standard ISO 27001:2017 - 27701:2019 - 37001:2016 - 22301:2019. Fa parte del Consiglio Direttivo di Assintel, l'Associazione italiana delle imprese ICT di Confcommercio Milano, è membro del Gruppo di Lavoro Cyber & Data di European Digital SME Alliance e partecipa in qualità di esperto al Gruppo di lavoro 5 ISO/IEC JTC 1/SC 27/ - Identity management and privacy Technologies - per conto di SBS (Small Business Standards, l'associazione europea che rappresenta gli interessi delle PMI nel processo di standardizzazione a livello europeo e internazionale).

non "vivono" solo di tecnologie, la risposta che viene messa in campo presenta connotati di tipo difensivo. Sappiamo in realtà che una cybersecurity che vuole attuare una vera *governance* del rischio deve crescere su tre *"p": prevenzione, predittività e proattività*. Reagire quando una minaccia è già diventata evento comporta costi e guai peggiori. Per attivare azioni di contenimento bisogna partire dalla cultura, ritorno su questo aspetto, poi si innestano i processi, in ultimo arrivano gli apparati tecnologici. Spesso tendiamo prima ad alzare il "muro" della strumentazione, in seguito si pensa alle strategie. Un approccio siffatto non può essere vincente. Non serve erigere "muri", pareti trasparenti e vetri blindati possono essere più utili per vedere cosa c'è oltre, per

non perdere quello sguardo di insieme che un security manager deve avere. Senza visione prospettica non si fa, insomma, molta strada.

Testare le terze parti diviene un'attività strategica

Quali strategie vanno seguite per innalzare il livello di sicurezza delle cosiddette "terze parti" che nella catena del valore digitalizzata?

Il rischio si propaga anche per contagio dal piccolo al grande con conseguenze spesso drammatiche come la

stretta attualità ci fa vedere ogni giorno. I fattori di sistema sono decisivi. La responsabilità va distribuita e condivisa da tutti gli attori della filiera. Cybersecurity significa responsabilità condivisa che deve partire dall'alto. La cyber security è una cultura che deve innestarsi in qualsiasi tipo di processo che riguarda l'azienda. Le terze parti sono un perno essenziale della catena. La normativa "NIS2" che entrerà in vigore entro ottobre del 2024 prevede una valutazione puntuale degli standard di qualità e di sicurezza dei fornitori.

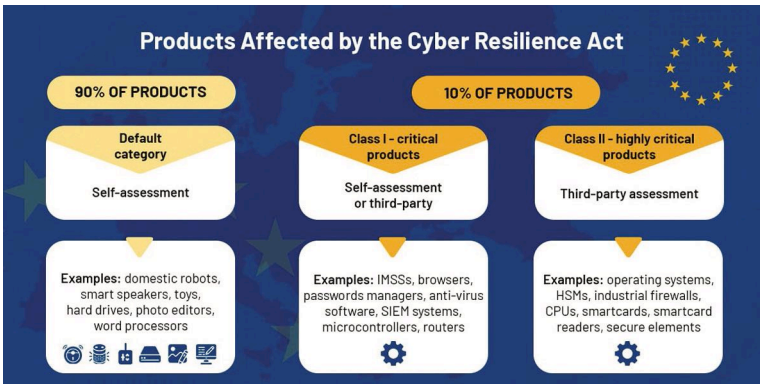
"Testare" le terze parti diventa dunque di capitale importanza per il business?

Assolutamente sì. Lo vediamo in concreto. Quando ci influenziamo, la responsabilità del contagio è quasi sempre di qualcuno che incautamente ci ha avvicinato. Trovare un linguaggio comune nelle aziende sarebbe

molto importante per innalzare il livello di protezione. Le diverse BUSINESS UNIT praticano linguaggi e stili comunicativi spesso molto distanti. Anche in questo caso un approccio culturale adeguato, capace di informare processi e comportamenti aiuterebbe. Quello che serve è un interprete, capace di semplificare i messaggi per aprire la strada della condivisione della responsabilità. La cybersecurity non è un vincolo è un'opportunità perché rappresenta la chiave di ogni successo futuro per manager e imprenditori. Le aziende che investono in sicurezza potranno dare fiducia ai clienti, acquisendo importanti quote di mercato.

Serve una regolazione illuminata per indirizzare i ritmi tumultuosi dello sviluppo tecnologico al servizio della collettività. Italia ed Europa stanno facendo bene su questo delicato terreno?

Se guardiamo lo scenario europeo dal punto di vista normativo possiamo dire che si sta facendo un buon lavoro. Il GDPR ha da poco "compiuto" 5 anni, non sarà una norma perfetta perché andrà aggiornata, ma non ce ne sono di migliori nel mondo, poste a tutela dei dati personali e delle persone fisiche. L'Europa sta, inoltre, cercando di creare in termini strategici un'infrastruttura giuridica, penso al regolamento sull'intelligenza artificiale, al *Cyber Resilience*



Act, alla stessa NIS2 cui facevo riferimento prima, al regolamento *Dora*, strumenti che devono guidare lo sviluppo. Se poi guardiamo alle istituzioni, non possiamo non considerare il lavoro di ENISA, l'apporto del nuovo centro della cyber security nato in Romania e la recente creazione dell'ACN, l'agenzia italiana di settore.

Essere "pronti" ad affrontare il rischio dinamico

Sembra che ci siano le condizioni per guardare con fiducia al futuro. Lei si definisce un ottimista?

Non si tratta di assumere etichette ma di guardare la realtà in divenire con equilibrio. Ricordiamoci che il motore dello sviluppo tecnologico sono gli

Stati Uniti e la Cina, l'Europa avrà la capacità di contrastare questo dominio? Pongo l'interrogativo perché credo ci sia molto da fare per far sì che le forze in campo trovino un equilibrio. Le diseguaglianze sono un vulnus della contemporaneità, difficile sanarle. Neanche l'etica, giustamente chiamata in causa quando si parla di redistribuire potere e ricchezza, può metterci d'accordo.

Questioni "delicate" difficili da affrontare in una intervista, non crede?

Non possiamo tacere aspetti delicati che riguardano non solo la sicurezza ma la vita di tutti. Pensiamo alla guida autonoma, che porrà tanti dilemmi. Sono ambiti della riflessione che hanno appassionato l'uomo fin dall'antichità, per fortuna non esiste un pensiero unico. Non c'è più solo l'etica classica, agganciata al trascendente, cristallizzata, immodificabile. L'impegno che tutti dobbiamo mettere, come manager, ma più in generale come classe dirigente, è quello di tornare a pensare come far crescere l'individuo in una società che muta continuamente, che si nutre di differenze in un mondo senza centro. Cose impensabili ieri sono possibili oggi, senza flettere sui principi non possiamo affrontare il futuro con regole obsolete.

Quali sono le filiere maggiormente esposte al rischio cyber?

Se pensiamo all'Italia tutto quello che sta attorno alla PA possiamo ritenere che sia a rischio. La sanità per la sovrapposizione di tecnologie vecchie e nuove è un altro ambito da seguire con attenzione. Non sottovaluterei la tutela del patrimonio informativo, marchi e brevetti. Difficile rendere sicuri questi asset strategici. Torna prepotente il tema rischio dinamico e terze parti su questo delicatissimo versante. La proprietà intellettuale la digitalizziamo certo, ma dove mettiamo questi dati? Se un brevetto sottratto finisce all'asta nel dark web, la vita dell'impresa è finita. Si parla poco di questi aspetti, a mio giudizio determinanti nell'immediato futuro.

Cyber Security Readiness ***è un progetto che oltre a coinvolgere molti player istituzionali, guarda alle PMI che sono state al centro della nostra discussione. Essere pronti di fronte al rischio dinamico, non è una pura utopia?***

Non credo, se si acquisisce la giusta consapevolezza. Il progetto cui lei si riferisce è stato presentato a La Sapienza in occasione della due giorni organizzata da Cyber 4.0 *(Cybersecurity Competence Center)* in collaborazione con il Ministero delle Imprese e del Made in Italy. L'iniziativa è molto interessante e potrà avere un importante sviluppo a patto di entrare in una logica europea. Bisogna aderire alle associazioni che sostengono valori e principi comuni.

Faccio l'esempio della *European Digital SME Alliance*, che mi vede direttamente impegnato, ma sono tante le realtà che operano in questa logica. Dobbiamo fare sistema, questo il punto. Nei tavoli internazionali bisogna avere alle spalle la forza della rappresentanza associativa, per farsi sentire. C'è molto da fare, ma sono ottimista anche su questo, perché credo che il valore dell'associazionismo sia molto importante. Ho iniziato con un termine greco, e chiuderei la nostra conversazione alla stessa maniera, richiamando la "koinè", il senso di comunità che la polis ha insegnato all'Occidente. Facciamo tesoro di questo patrimonio di civiltà, per creare un "blocco sociale" aperto all'innovazione e alle esigenze di sicurezza e di libertà che da sempre scandiscono le tappe del progresso dell'uomo. ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

L'importanza dell'educazione continua per le persone all'interno delle Aziende

La rapida evoluzione delle tecnologie ha portato ad un aumento esponenziale delle minacce cyber, che mettono a rischio sia le Aziende che le persone.

È diventato sempre più importante per le organizzazioni oltre che implementare solide misure di sicurezza informatica, anche porre l'attenzione sull'adozione di una formazione continua delle persone. Questo articolo esplorerà l'importanza dell'educazione costante per le Aziende e per le persone nel contesto della Cybersecurity, mettendo in luce anche l'aspetto psicologico, che svolge un ruolo chiave nella protezione dai pericoli informatici.

Includere il fattore umano nella formazione

La psicologia dell'utente è un elemento importante da considerare nella progettazione di un processo di formazione. Ad esempio, le persone tendono ad utilizzare password deboli o a cadere nella trappola di messaggi di phishing a causa di fattori psicologici; le password semplici sono più facili da ricordare oppure un'e-mail che richiede un'azione immediata per evitare di perdere un'occasione imperdibile, ci porta ad agire d'impulso. Pertanto, è essenziale formare le persone anche su aspetti psicologici che influenzano i nostri comportamenti e che vengono usati dai cyber criminali per compiere le loro illecite azioni.

I vantaggi della formazione continua:

SVILUPPO DI NUOVE ABITUDINI
Attraverso la ripetizione costante di comportamenti sicuri, le persone interiorizzano le nozioni apprese in modo efficace, creando delle nuove abitudini di sicurezza che diventano parte integrante del modo di agire.

CONSOLIDAMENTO DELLE CONOSCENZE APPRESE
Per consolidare nuove conoscenze è indispensabile avere dei piani di formazione continui che consentono di consolidare le informazioni nel tempo, permettendo all'individuo di apprendere in modo più approfondito e duraturo.

EVOLUZIONE DELLE MINACCE
Le minacce informatiche sono in continua evoluzione, di conseguenza i contenuti della formazione devono essere aggiornati sulle ultime minacce e sulle contromisure da adottare per proteggersi in modo efficace.

APPRENDIMENTO GRADUALE
Sono consigliati piani di formazione continui che prevedono un approfondimento graduale e approfondito di un argomento complesso come può essere la Cybersecurity, permettendo alle persone di acquisire una migliore comprensione di questo argomeno.

La nostra Missone è passare dall' Informazione alla Trasformazione

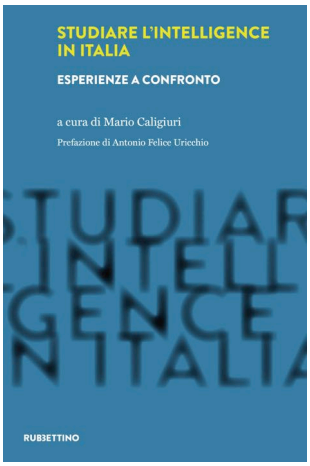
www.securitymind.cloud.cloud

Bibliografia

Mario Caligiuri (a cura di)
Studiare l'intelligence in Italia
Esperienze a confronto
Ed. Rubbettino

Autore: Massimiliano Cannata

Intelligence, sicurezza e poteri dello stato



Mario Caligiuri, professore ordinario di pedagogia presso l'Università della Calabria, dove dirige il master di Intelligence, promosso nel 2007 con Francesco Cossiga, oltre ad aver curato per la Treccani la voce intelligence è considerato uno dei massi esperti di cyber security. La raccolta curata da Rubbettino costituisce una pregevole testimonianza perché fa luce su un ambito per troppo tempo ammantato da una scarsa conoscenza e da false interpretazioni. "Negli ultimi decenni – spiega lo studioso - nel nostro Paese, c'è stata una marcata trasformazione della percezione dell'Intelligence. A questo fenomeno hanno concorso diversi fattori: la ridefinizione dell'attività dei Servizi dopo la fine della Guerra fredda, la diversità dei tempi decisionali richiesti dalla globalizzazione, l'egemonia delle multinazionali finanziarie, l'invadenza della criminalità, la sovrabbondanza informativa e la sorveglianza di massa, le conseguenze degli attentati dell'11 settembre, le severe ricadute della crisi economica mondiale del 2007, l'immigrazione di massa, il fondamentalismo islamico che dal 2014 al 2017 ha sconvolto l'Europa. Da qui una triplice trasformazione dell'Intelligence: da luogo oscuro dello Stato ad arma segreta delle democrazie, da sistema di previsione del futuro a strumento di interpretazione del presente, da metodo esoterico per pochi a processo di comprensione delle informazioni per tutti. In tale quadro si colloca la legge di riforma del settore del 2007. Quattro anni prima, nell'ambito di una riflessione sullo stato dell'arte degli studi accademici sull'Intelligence in Italia, avevo constatato una serie di ritardi nello sviluppo della cultura della sicurezza, sul piano scientifico, editoriale e culturale. Da allora, i settori di studio sull'Intelligence si sono ampliati: oggi, in Italia, sono quattro le aree di approfondimento in ambito accademico, per lo più master in Cyber Security, Criminologia, Intelligence economica e Big Data Analytics". Lo studio racconta questa trasformazione, che ha determinato un cambio di passo anche sul terreno delicato della formazione. L'Università della Calabria ha saputo fare da apripista coinvolgendo una molteplicità di figure professionali. Tappa importante, ricordata dallo stesso Caligiuri il 2018, è l'anno in cui ha preso il via la Laurea Magistrale ed è stata istituita la Società Italiana di Intelligence (Socint), la cui priorità è fare di questa disciplina una materia di studio negli atenei del nostro Paese. Nel 2020 Socint è diventata anche casa editrice: da allora le sue pubblicazioni sono cresciute in quantità e qualità. Nel 2021 la Laurea Magistrale in Intelligence e analisi del rischio è stata trasformata in Laurea Magistrale in Intelligence per la legalità e la tutela del patrimonio culturale e archeologico. Per la prima volta in Italia, inoltre, l'Intelligence è divenuta corso di specializzazione in un Istituto Tecnico Superiore. Aspetto non secondario se si considera la guerra dei talenti e dei saperi che si sta combattendo sul fronte della transizione digitale. Importante il nesso tra l'intelligence, definita "sapere sociale" e la Sicurezza, anche su questo aspetto Caligiuri mostra di avere le idee molto chiare: "la prima regolamentazione legislativa dei nostri Servizi fu stimolata dalla sentenza della Corte Costituzionale secondo cui la sicurezza è un diritto preminente, che precede e consente l'esercizio di tutti gli altri. Dice bene Giorgio Galli secondo cui l'Intelligence non è uno Stato nello Stato, una "quinta colonna", ma è quella parte dello Stato che stabilizza il sistema democratico, a prescindere dall'alternanza al potere delle maggioranze parlamentari. Se riflettiamo su questi temi l'Intelligence è sostanza stessa della democrazia e la preserva dalle fisiologiche degenerazioni. Oggi siamo di fronte a uno spill-over, un salto di specie, una frattura epocale, una metamorfosi irreversibile. Per esemplificare il concetto potremmo riferirci al bruco nell'atto di trasformarsi in farfalla. Non sappiamo se le categorie culturali, finora sperimentate, ci aiuteranno a comprendere il nuovo che avanza e che ancora abbiamo difficoltà a cogliere. Sappiamo però che serviranno visioni del futuro per capire quello che sta realmente accadendo. Ha ragione Moisés Naím quando afferma che la trasformazione in atto più potente è quella del potere. Il potere è uno strumento organizzativo necessario nella società e risulta efficiente quando rappresenta una garanzia, non certo quando degenera in arbitrio. Sarà bene riflettere su questo passaggio se ci sta a cuore la salute e la qualità della democrazia". ■

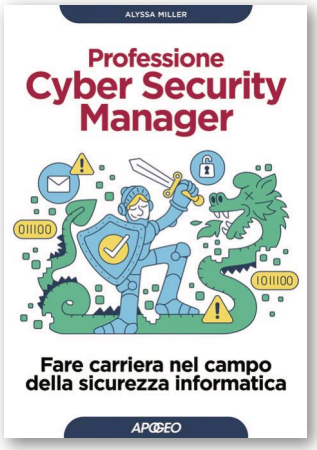
Alyssa Miller
Professione Cyber Security Manager
Apogeo 2022

Alyssa Miller
Professione Cyber Security Manager
Fare carriera nel campo della sicurezza informatica
Apogeo Editore

Autore: Roberto Tiozzo*

Una guida utile per capire il nuovo orizzonte di una professione in divenire

Professione Cyber Security Manager "è una guida preziosa per coloro che aspirano a entrare nel campo entusiasmante



e in continua crescita della cybersecurity. Scritto da Alyssa Miller, CISO dell'americana Epiq Global, lo studio offre un approccio completo alla cyber security che enfatizza sia le competenze tecniche che quelle non tecniche necessarie per avere successo nel settore. Una qualità del lavoro è data dalla presentazione chiara e molto ben strutturata. L'autrice comincia fornendo una solida base per i neofiti, offrendo una comprensione dei fondamenti delle reti informatiche, dei sistemi operativi e della sicurezza delle informazioni. Questa base è essenziale, poiché garantisce che i lettori provenienti da diverse esperienze professionali possano seguire il percorso e comprendere i concetti fondamentali.

La cybersecurity, come si sta finalmente comprendendo, non riguarda solo chi ha competenze tecniche. A tal proposito, vengono esplorate anche le competenze non tecniche cruciali per un professionista che opera in questo settore come la risoluzione dei problemi, la comunicazione, il pensiero critico, la profilazione psicologica, l'analisi storica e l'etica. Affrontando queste qualità importanti, il libro mira ad aiutare i lettori a comprendere l'importanza di dotarsi di un set di competenze completo e mette in evidenza come queste qualità si integrano con le conoscenze tecniche nel campo della sicurezza informatica.

L'adattamento delle competenze esistenti è un passaggio chiave della trattazione. Molti individui possiedono già abilità preziose acquisite dalle esperienze professionali precedenti. Illustrando come queste competenze possano essere riutilizzate e applicate nel contesto imprenditoriale, il volume offre un approccio pratico ed accessibile per la transizione di carriera. I lettori ne possono ricavare l'ottimistico suggerimento a sfruttare i propri punti di forza esistenti per migliorare il loro percorso in questa delicata professione. L'autrice fornisce, inoltre, numerosi esempi concreti, studi di casi ed esercizi pratici. Questi elementi aiutano a colmare il divario tra teoria e pratica, consentendo di applicare le conoscenze maturate e a sviluppare una comprensione più approfondita della materia. Inoltre, l'inclusione di fonti utili e di riferimenti per approfondire i contenuti fanno di questo saggio una efficace guida per l'autoapprendimento.

La vasta gamma degli argomenti trattati non consente di approcciare in maniera verticale tematiche più squisitamente tecniche. Tuttavia, il testo rappresenta un eccellente punto di partenza per i "neofiti" della cybersecurity che desiderano "transitare" in questo ambito provenendo magari da settori correlati.

Credo si possa dire in conclusione che "Professione Cyber Security Manager" può essere uno strumento eccellente per chiunque desideri entrare nell'industria della cybersecurity. Con il suo approccio olistico, gli esempi pratici e l'accento sul riutilizzo delle competenze esistenti, il libro permette ai lettori di effettuare una transizione di successo e di poter crescere in un settore estremamente dinamico e straordinariamente aperto all'innovazione.

**Roberto Tiozzo è 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.* ■

Terzo Rapporto sul valore della connettività in Italia La nuova fase della digital life in Italia Censis-WindTre

Autore: Massimiliano Cannata

Gli italiani nel "secondo tempo" del digitale

Per 9 italiani su 10 Internet è un diritto di tutti. Ne sono convinti l'84,1% dei giovani, il 90,5% degli adulti e l'88,5% degli anziani. In particolare, per l'80,8% dei cittadini l'accesso alla rete dovrebbe essere gratuito. Per il 46,2% la copertura dei costi dovrebbe avvenire per mezzo di un contributo dei grandi generatori di traffico, come Google e Meta. Dati che fanno riflettere, quelli emersi nel terzo rapporto Censis-WindTre sul valore della connettività. "La rete – commenta Giorgio de Rita, segretario generale dell'istituto di ricerca sociale – durante l'esperienza terribile del lockdown che ha trasformato la vita privata e quella lavorativa è divenuta un diritto fondamentale. In quel momento si è imposto un diverso assetto relazionale, nell'isolamento la possibilità di connettersi ha rappresentato un'ancora di salvezza, che ci ha permesso di non perdere la dimensione dell'altro e di ritrovare un binario per il dialogo. Quella fase è passata, un capitolo nuovo si è aperto, segnato da una domanda diffusa di conoscenza. Non si può parlare di saturazione, gli italiani hanno ancora fiducia che la tecnologia serve al progresso, piuttosto del bisogno diffuso di una *governance* dell'innovazione, di regole, di un maggiore equilibrio". Il fenomeno dirompente dell'intelligenza artificiale, che sta facendo

da grande acceleratore della rivoluzione digitale, è la cartina al tornasole di un paese diviso. Per il 46% è una opportunità, per il 37% una minaccia. Il 60% della popolazione (forse il dato più eclatante) auspica una moratoria delle attività di ricerca su questo delicato ambito, come se si stesse cercando una pausa, una sospensione utile a ridare un senso al divenire. Appare evidente il bisogno di una narrazione meno enfatica delle conquiste, pur indiscutibili, ottenute dalla tecno scienza. È la qualità dell'informazione, che è il respiro della democrazia, a preoccupare una fetta importante dell'opinione pubblica. L'80% del campione interpellato teme il proliferare delle *fake news,* capace di costruire un alone di verità creata che disorienta il percorso esistenziale e lavorativo di ciascuno di noi.

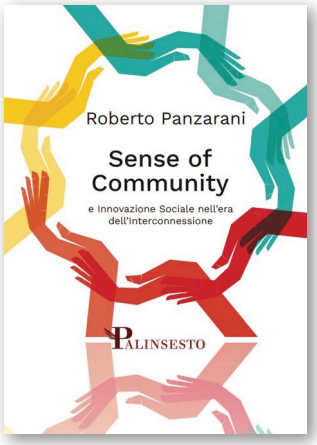
Non lasciare indietro nessuno nella spinta verso il progresso è il secondo aspetto chiave della ricerca che insiste sull'importanza del "welfare digitale" e sulla sostenibilità degli investimenti strutturali, necessari alla transizione tecnologica. Il "diritto di avere diritti" come ci ha insegnato Stefano Rodotà – commenta Mario Morcellini professore emerito di sociologia dei processi culturali e comunicativi de La Sapienza di Roma – è il punto di partenza, a patto di non dimenticare i doveri, a partire dalla formazione continua cui dobbiamo sottoporci tutti. Il gap culturale di fronte ai profondi cambiamenti che hanno una duplice natura socio-tecnologica che stanno modificando il profilo della convivenza intervenendo persino sui tratti della personalità, va colmato con rapidità. Pensiamo che l'istruzione costi? Proviamo con l'ignoranza. Un bambino prima ancora di andare a scuola passa mediamente dalle sei alle sette ore giornaliere sul tablet. Quando si muove tra i banchi, ne sa più del suo maestro. Vuol dire che il paradigma del magister, la sua autorità che ha retto per secoli è crollata, senza che nessuno se ne preoccupi". I giovani "zippati" di tecnologia vogliono insomma risposte all'altezza dalle agenzie educative, per non finire inghiottiti nei pericoli della rete. Stanno cambiando i luoghi del pensiero e i linguaggi del sapere, le tecnologie cognitive suggeriscono codici che non riusciamo ancora a padroneggiare, il futuro dipenderà dal tempo che impiegheremo per mettere ordine alle cose, facendo del digitale un navigatore di conoscenze senza rinunciare mai alla nostra identità. ■

Roberto Panzarani
Sense of Community
e Innovazione Sociale nell'era dell'interconnessione
Ed. Palinsesto

Autore: Massimiliano Cannata

Il Governo del digitale nella business collaboration

"In questa stagione post covid, dominata dalle crisi internazionali, dalla questione sociale che fa ribollire le diseguaglianze e da una



fragilità finanziaria che rischia di mettere sotto scacco il sistema bancario americano ed europeo, i fattori geopolitici condizionano sempre di più l'economia. Bisogna ritrovare il senso di comunità, impegnarsi per la globalizzazione dei diritti dopo aver pensato solo ai mercati, praticando la logica della collaborazione tra la sfera del pubblico e del privato. Altri paesi lo stanno già facendo, è ora che l'Italia impari a guardare oltre…".

Roberto Panzarani, docente di governo dell'innovazione tecnologica dell'Università Cattolica del Sacro Cuore, studia da molti anni i fenomeni di trasformazione del capitalismo che stanno modificando il modo di dare impresa. *Sense of community* (ed. Palinsesto) è il suo ultimo libro, in cui racconta l'esperienza di alcuni centri di eccellenza, che si possono oggi considerare come i "motori della quarta rivoluzione". Il Digital Lab Denmark è uno degli esempi che potrebbe fare scuola. "In quella realtà – spiega lo studioso - Stato e privato hanno trovato una sintesi virtuosa, rendendo attuabile il processo di transizione digitale, prima ancora che venisse approvato il PNRR". Diverso il clima che si respira in Italia, la lentezza nell'istruzione dei progetti rischia, infatti, di far "saltare proprio il banco" del PNRR. Proprio in questa ottica può essere molto utile andare a osservare i luoghi dell'innovazione, (*learning tour* nella letteratura manageriale n.d.r) per apprendere l'importanza del capitale intellettuale, insieme alla valorizzazione del capitale umano, troppo spesso alle nostre latitudini mortificata. Il Nord Est è un punto di osservazione di primario interesse: locomotiva dell'Italia industriale con l'esperienza dei distretti, è stata l'area che per prima ha attuato la logica della *business collaboration*. Scenari interessanti si possono aprire anche in futuro se i distretti sapranno imboccare una linea evolutiva basandosi sullo sviluppo degli asset intangibili e sulla *governance* del fattore tecnologico. Tradizione e innovazione dovranno camminare insieme, sfruttando al meglio il paradigma dell'impresa familiare, che ha fatto grande il made in Italy. Per continuare ad essere competitivi i distretti dovranno aprirsi alla guida di leader che saranno facilitatori del cambiamento. Capacità di ascolto, intelligenza emozionale, flessibilità, caratteristiche presenti soprattutto nel mondo femminile, capacità di attuare quelle che Rifkin definisce attitudine alla *common* collaborativa sono *skill* necessarie per creare aziende più efficienti e soprattutto reattive rispetto alle turbolenze dei mercati. La connettività diffusa, come l'uso intelligente dei *social network*, saranno parte integrante di un modo nuovo di concepire l'organizzazione. L'azienda gerarchica, burocratica e funzionale ha fatto il suo tempo, la stessa logica, in passato dominante, del "comando e controllo" appare inadeguata a gestire i flussi di un'economia fluida. Capirlo in fretta servirà per rimanere protagonisti in questo profondo cambiamento d'epoca. ■

Cyber Hell: indagine su un inferno virtuale (Jin-seong Choi, Corea del Sud, 2022)

Cyber Hell – Indagine su un inferno virtuale è un documentario prodotto da Netflix in Corea del Sud, ispirato a un recente caso di cronaca nera nel mondo del web. Il documentario si basa su un fatto di cronaca svoltosi principalmente su Telegram (app che prevede canali, gruppi e un sistema di messaggistica chat), e malgrado una portata di perversione e morbosità tali da sconvolgere chiunque ne sia venuto a conoscenza (e di solito la curiosità circa casi del genere fa da cassa di risonanza) è stato pressoché ignorato nel resto del mondo.

L'opera del regista sudcoreano è un documentario ma è strutturata come un film, anche perché tutto quello che si è verificato tra il 2018 e il 2020 è talmente clamoroso, a tratti persino quasi irreale, da sembrare la trama di una sceneggiatura: invece si tratta dell'ennesimo caso in cui la realtà ha superato le più cupe fantasie.

In questo lungometraggio, il regista sudcoreano Choi Jin-seong segue le vicende di due studentesse universitarie, di un gruppo di giornalisti e dei poliziotti dell'unità crimini informatici che hanno compiuto indagini sulla cosiddetta "N Room", un network criminale sul web su cui pendono accuse di sfruttamento sessuale. Il fatto di seguire da vicino soprattutto la storia dei poliziotti è indicativo di come Choi abbia voluto rappresentare specialmente il lavoro che attende le forze dell'ordine di oggi e del futuro in tema di cybercrime.

La storia di questa "N Room" (gestita dal nickname GodGod, l'inventore, e riprodotta da Baksa, un copycat) è allucinante, soprattutto perché coinvolge foto e video intimi di ragazze spesso minorenni, comprese in un range che va da "quasi maggiorenne" a "bambina delle elementari". Materiale ripugnante ottenuto da un hacker con metodi fraudolenti e poi utilizzato per tenere sotto ricatto le ragazze stesse.

La caccia alla rete criminale si è fatta ben presto serrata: quando si è arrivati all'ideatore del piano perverso, si è scoperto che era un "semplice" studente universitario, che però col suo piano diabolico aveva già fatto 103 vittime.

Basato su una serie di interviste, immagini di repertorio, filmati di animazione e ricostruzioni virtuali, il documentario si addentra in un mondo oscuro che sembra parallelo al nostro: un mondo di ragazze o bambine sottomesse e costrette a caricare contenuti sessuali espliciti riguardanti loro stesse su gruppi Telegram (e caricarne ripetutamente sempre di nuovi, con la minaccia di diffondere ad amici e parenti quanto già avevano caricato in precedenza o quanto l'hacker si era procurato con altri metodi); mentre dall'altra parte si vedono letteralmente decine di migliaia di utenti che sono disposti a sborsare cifre considerevoli, pagando in criptovalute, versandole sui conti dei gestori dei gruppi Telegram per ottenere l'accesso ai gruppi stessi e al materiale che vi veniva diffuso.

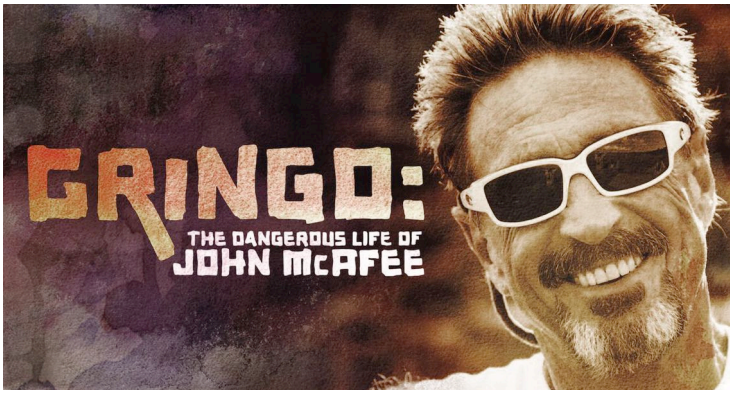
A scoprire per prime il problema delle "N Room", sono state due studentesse di giornalismo che, scegliendo di agire praticamente sotto copertura, si sono infiltrate in un mondo oscuro di uomini che obbligavano minorenni ad umiliarsi e subire ogni sorta di perversione sessuale online. Un primo articolo sul caso non riesce però ad attirare l'attenzione pubblica su quanto stesse succedendo tra i giovani coreani; successivamente, però, quando sulla storia sono piombate le testate più importanti del paese, la polizia si è finalmente occupata del caso.

Risalire alle identità di alcuni degli amministratori delle chat (il già citato "GodGod" e un altro utente che si firmava "il Dottore") è stato però particolarmente difficile e complesso, e ci sono voluti mesi di indagini, intercettazioni e pedinamenti. Mesi in cui è emerso quanto la rete di criminali digitali fosse diffusa, numerosa e strutturata, e in cui sempre più ragazzine sono state adescate e coinvolte loro malgrado. Molte di loro ne ricaveranno traumi permanenti.

La macchina da presa del regista asiatico racconta la storia di uno dei più atroci crimini digitali che abbiano mai sconvolto la Corea del Sud, dei sistemi di anonimato web che hanno fatto sì che il network criminale prosperasse e del coraggio delle vittime che hanno lottato per raccontare al mondo la verità. ■

Gringo: The Dangerous Life of John McAfee (Nanette Burstein, USA 2016)

Probabilmente quasi tutti noi utilizziamo o abbiamo utilizzato su qualche nostro computer una versione del celebre antivirus McAfee, o comunque tutti sappiamo di cosa si tratta. Intuitivamente possiamo desumere che McAfee sia il cognome del programmatore di questo diffusissimo software e infatti è proprio così (John è il nome); è quindi automatico immaginare che il signore in questione sia diventato ricchissimo grazie alla vendita del suo antivirus, e anche stavolta la previsione è azzeccata quanto facile. Quello che proprio non avremmo mai detto, però, è che la vita di un multimilionario,

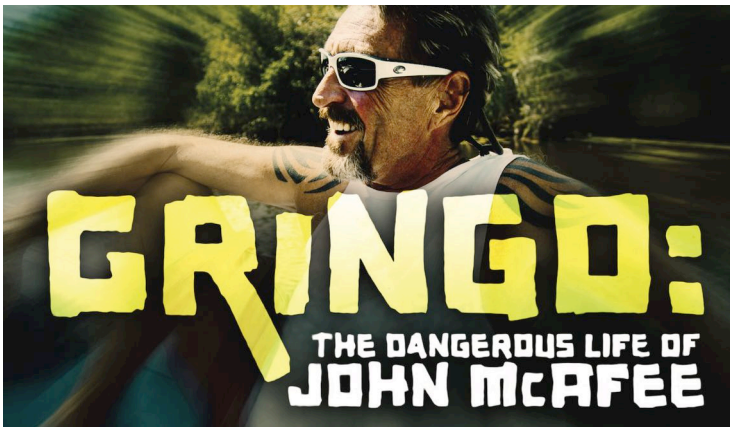


che ipotizziamo essere piena di agi, beni di lusso e magari talvolta persino noiosa (o comunque priva di rischi reali), possa invece essere "turbolenta" come *Gringo: The Dangerous Life of John McAfee*, documentario di Nanette Burstein e prodotto da Parco Chi Young, ci racconta essere quella del nostro famoso creatore di antivirus.

Va detto che lo stesso McAfee smentisce, rappresentando nelle sue interviste l'opera come fiction e non come documentario, e ne ha ben donde, visto che vi si racconta, tra le altre cose, che sarebbe implicato in un omicidio e in traffico internazionale di stupefacenti (ma in Belize, dove ha vissuto e dove si sarebbero consumati i presunti reati, non è mai stato aperto alcun procedimento penale contro di lui).

Il film, che qui non tratteremo quindi né come documentario né come fiction, lasciando che sia la storia a decidere quanto di vero ci sia, mostra dunque la vita di John McAfee, talentuoso programmatore che raggiunge le vette del successo con la sua software house proprio attraverso l'antivirus che porta il suo nome per poi decidere drasticamente di cambiare vita, darsi allo yoga, trasferirsi come detto in Belize e qui trovarsi coinvolto, secondo quanto lascia intendere la ricostruzione di Nanette Burstein (giornalista che riporta anche lo scambio epistolare intrattenuto con McAfee, dal quale emerge una loro relazione controversa), nel misterioso omicidio del suo vicino di casa.

Lo show permette di ascoltare varie testimonianze per farsi un'idea, nonché di immergersi quasi completamente nella non certo noiosa (a questo punto possiamo dirlo) vita del multimilionario, o meglio, in quella che Nanette Burstein ci illustra sarebbe la vita di McAfee secondo il suo punto di vista. La figura del genio del computer, attraverso luci e ombre, emerge impetuosamente, grazie alla sapiente narrazione del film che tiene avvinto lo spettatore ma anche grazie all'indubbio carisma dello stesso McAfee. ■



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

Proteggere i bambini on-line è una sfida globale che richiede un approccio globale. Mentre molti sforzi per migliorare la protezione online dei bambini sono già in corso, la loro portata finora è stata più di carattere nazionale che globale. L'ITU (Unione Internazionale delle Telecomunicazioni) ha avviato l'iniziativa Child Online Protection (COP) per creare una rete di collaborazione internazionale e promuovere la sicurezza online dei bambini in tutto il mondo. COP è stato presentato al Consiglio ITU nel 2008 e approvato dal Segretario generale dell'ONU e da capi di Stato, Ministri e capi di organizzazioni internazionali provenienti da tutto il mondo.

Poste Italiane, insieme alla propria Fondazione GCSEC e alla Polizia Postale e delle Comunicazioni ha prodotto la Versione italiana delle linee guida ITU, guida per la protezione dei bambini nell'uso di Internet e guida per genitori, Tutori ed insegnanti per la protezione dei bambini nell'uso di Internet.

Scaricatele su: www.distrettocybersecurity.it/linee-guida-itu

www.itu.int/cop

DIGITAL CLUB
CYBER

porta a **Cosenza** il

CISO:27001

il 21 settembre 2023 dalle 14:30

in collaborazione con

aipsa
ASSOCIAZIONE ITALIANA PROFESSIONISTI SECURITY AZIENDALE

un progetto

ECHO

Un pomeriggio di networking e formazione con tavoli interattivi di simulazione ristretta agli addetti ai lavori per confrontarsi con i cyber mentor e altri CISO su come affrontare un incidente informatico.

Alcuni dei CYBER MENTOR

NICOLA SOTIRA

ELENA MENA AGRESTI

ALESSANDRO MANFREDINI

ANDREA GUARINO

Il testo e gli intrecci di questo racconto interattivo sono stati creati da Andrea Guarino, Resp. Security Awareness & Training di Acea SpA, nell'ambito delle attività di disseminazione e sensibilizzazione sui temi della sicurezza informatica relative al progetto europeo H2020 "ECHO" (the ECHO project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943).

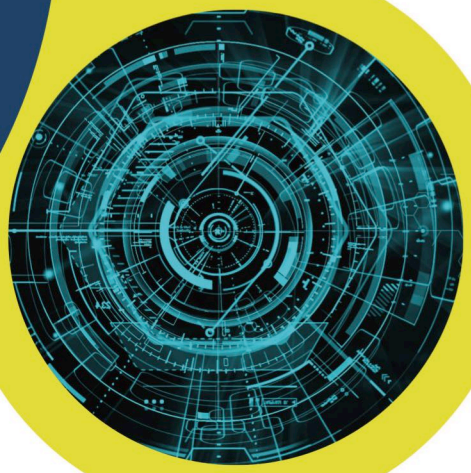
Scrivici per ricevere più informazioni e riservare il tuo posto

cyber@digital-club.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