Cybersecurity Trends

Edizione italiana, N. 3 / 2021

INTERVISTE VIP:

FRANCO AMICUCCI
ALESSANDRO CURIONI

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder Centrale: Cyber Exposure

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

Misurare il nostro tempo.

Autore: Nicola Sotira

Vaccini, Green Pass, riaperture delle attività, prove di un rientro alla normalità dopo avere vissuto uno scenario catastrofico, in cui tutte le attività sociali sono state bloccate. Ci siamo abituati alle riunioni virtuali ed abbiamo assistito alla rapida ascesa dello shopping on-line di ogni genere dal cibo all'abbigliamento, molto di quello che prima veniva acquistato in luoghi fisici è migrato rapidamente nel digitale che continua a crescere in ogni settore. Anche la didattica sta avviando programmi che sfruttano sempre di più le modalità digitali che, adesso, affiancano le lezioni in presenza. Ovviamente la criminalità organizzata segue i soldi e, non solo, trova nuove occasioni nelle transizioni drammatiche, e sposta sempre di più la sua attività sul lucroso e meno rischioso settore digitale. Sappiamo bene che le applicazioni con i dati a loro associati sono la linfa di tutte le organizzazioni digitali, come sappiamo che le architetture di sicurezza tradizionale forniscono una visibilità limitata sull'ambiente applicativo. Infine, il confine classico è completamente saltato, basti pensare alle architetture multi-cloud, i lavoratori remoti e la mobilità che sta cambiando il paradigma classico. Tutto questo crea un'ampia superficie di attacco esposta a potenziali exploit aumentando, così, il rischio per il business. Diventa quindi rilevante gestire la misura della postura cyber che si basa sulla telemetria in tempo reale del comportamento e iterazione sulle componenti esposte in modo da valutare continuamente la conformità ed il rischio nell'ambiente applicativo. Questa gestione tipicamente include anche un punteggio che, generalmente, viene utilizzato come una delle dimensioni della valutazione del rischio, del reporting e della prioritizzazione degli interventi operativi. La gestione della postura cyber può essere utilizzata dalla squadra di sicurezza con i seguenti benefici:

- **Coordinamento dei team SOC, CERT e sistemi informativi**, ovviamente nonostante l'obiettivo condiviso di protezione dell'infrastruttura aziendale, queste squadre possono essere isolate nella loro visione d'insieme. L'utilizzo di questo approccio permette di avere una visibilità olistica e la condivisione delle informazioni tra i gruppi di sviluppo, sicurezza e caccia alle minacce.
- **Inventario aggiornato delle applicazioni:** avere unna visione aggiornata in tempo reale degli ambienti applicativi. La telemetria in tempo reale e gli approfondimenti della gestione della postura cyber consentono alle squadre di sicurezza di mantenere uno scenario aggiornato di ciò che è presente oltre a monitorane le prestazioni.
- **Misurare i progressi:** uno dei principali vantaggi forniti da questo tipo di approccio è la capacità di misurare i risultati nel tempo. I CISO spesso hanno il problema del rappresentare la loro efficacia, la misura della postura Cyber permette di mantenere la visibilità su tutte le attività della squadra di sicurezza in un ambiente applicativo complesso e per monitorare, misurare e comunicare i propri progressi. ■

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e 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.

Virtual Event | 26-27 October | Secure Your Free Pass with Code: CYBERSECTRENDS

ItaliaSec Summit 2021

The ItaliaSec IT Security Conference returns virtually for the 5th successive year on 26th-27th October, as part of a European series dedicated to tackling regional cyber security challenges.

ItaliaSec is a CPE certified summit which brings together 100s of IT security experts from a range of industries across Italy, such as Banking & Finance, Food & Beverage, Oil & Gas, Government, Utilities, Manufacturing and Retail.

Network with senior security experts and benchmark your digital maturity with industry leaders from the likes of Sky Italia, Banco de Poupanca e Credito, GE Medical Systems Italia, European Space Agency, Deloitte, Versace, BNP Paribas, and ABB. Learn from a range of interactive sessions like panel discussions, real-life case studies and thought-led keynotes, as well as enjoying dedicated networking time.

For the full agenda, speaker list and to learn more about the event, visit: italy.cyberseries.io.

Members of Cybersecurity Trends can secure their FREE pass with code CYBERSECTRENDS here: italy.cyberseries.io/register

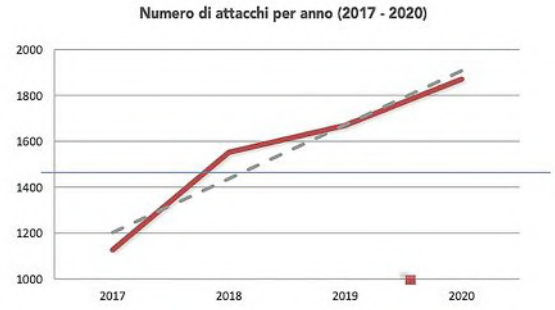
*** Offer is for end-users only. Individuals who work for cyber security companies and/or consultancies do not qualify for a free pass, but can get 10% off their ticket with code: SECURE10**

L'assessment di sicurezza con il Framework Nazionale per la Cybersecurity e la Data Protection.

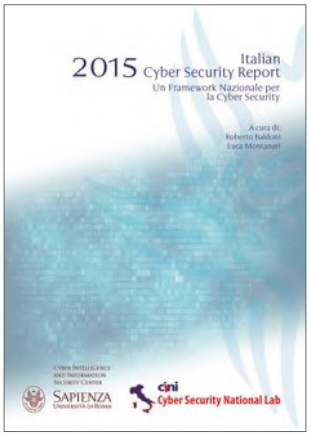
Autori: **Marco Angelini, Leonardo Querzoni**

Il rischio legato al verificarsi di attacchi informatici che possano compromettere la sicurezza di informazioni o operazioni è una realtà con cui tutte le organizzazioni, sia pubbliche che private ed operanti nei più diversi settori produttivi, si confrontano ormai giornalmente. Il forte impulso allo spostamento *online* delle attività di business, causato da maggiori opportunità di sviluppo piuttosto che da fattori contingenti come il perdurare dell'emergenza sanitaria provocata dal COVID, ha causato, indirettamente, anche un aumento del numero e della magnitudo degli attacchi informatici.

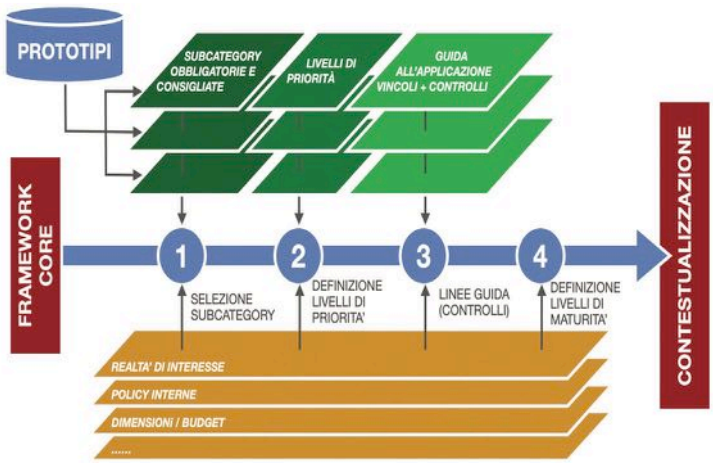
Nel suo rapporto 2021 il Clusit ha stimato un incremento degli attacchi cyber a livello globale nel 2020 pari al 12% rispetto all'anno precedente, con un trend in costante crescita nei precedenti tre anni. Qualunque organizzazione oggi, indipendentemente dalla sua missione, dalla natura del suo business, e dalla sua dimensione, non può ignorare questo fenomeno.



Negli ultimi anni si sono affermati, a livello globale, numerosi framework che permettono di guidare l'adozione di misure di sicurezza atte a prevenire e mitigare il rischio attraverso un opportuno meccanismo di governance. Alcuni di questi framework hanno una natura generalista e sono quindi adattabili ad ogni contesto, mentre altri sono stati pensati e sviluppati nell'alveo di determinati settori produttivi, cogliendone le specifiche caratteristiche. In generale, i framework per la cybersecurity permettono a chi li adotta di identificare un livello di sicurezza target e quindi definire un programma di interventi per il raggiungimento di tale obiettivo. Il Framework Nazionale per la Cybersecurity e la Data Protection (anche "Framework Nazionale" di seguito) rappresenta uno strumento di misura della postura di sicurezza di un'organizzazione in termini di maturità e completamento di attività volte a ridurre il rischio cibernetico. Pubblicato nel 2015 e aggiornato nel 2019 alla versione 2.0 al fine di cogliere gli aspetti legati alla Data Protection espressi nel GDPR, il Framework Nazionale consente di approfondire diverse dimensioni inerenti alla cybersecurity.



Il Framework Nazionale nasce sulla base del NIST Cybersecurity Framework, ampiamente riconosciuto a livello internazionale, del quale eredita sia l'approccio basato sul rischio, che la struttura tecnica. All'interno del Framework Nazionale sono definite 117 attività abilitanti per la sicurezza, organizzate in cinque principali *function*: identify, protect, detect, respond, recover. Le *function* coprono uno spettro ampio ed eterogeneo di attività che spaziano dai processi di gestione dei dati sensibili, alla protezione della supply chain. Per questo motivo, per essere applicato in modo efficace, il Framework Nazionale deve essere inizialmente contestualizzato al dominio in cui lo si vuole utilizzare. Questa operazione di "contestualizzazione" (Figura 1) richiede di tenere in considerazione gli eventuali ulteriori vincoli che il dominio impone nella selezione delle singole attività abilitanti (dette *subcategory*) che nello stesso hanno senso. Tra i vincoli più importanti che è necessario tenere in considerazione durante la fase di contestualizzazione del Framework Nazionale ci sono quelli legati alla *compliance* rispetto a regolamenti di settore, nazionali e no. Per semplificare questo aspetto, il Framework Nazionale mette a disposizione uno strumento di supporto chiamato "prototipo di contestualizzazione". Un prototipo rappresenta una selezione ragionata di attività abilitanti legata ad uno specifico regolamento o standard. In fase di contestualizzazione, diversi prototipi possono essere applicati al framework per identificare in modo semplice quali attività non dovranno essere escluse dalla contestualizzazione per supportare successivamente la *compliance* rispetto ai regolamenti di interesse. Il corretto uso dei prototipi semplifica fortemente l'attività di contestualizzazione del framework e fornisce la possibilità di definire un processo di contestualizzazione comune a tutte le realtà appartenenti a specifici settori regolamentati.



Contestualizzazione del Framework Nazionale per la Cybersecurity e la Data protection.

Sin dal momento della sua introduzione, il Framework Nazionale ha rappresentato un punto di riferimento in Italia per realtà fortemente eterogenee (dalla grande P.A. alla piccola impresa) che lo hanno adottato come strumento per l'organizzazione della propria strategia di difesa rispetto alle minacce cibernetiche. Le recenti evoluzioni normative, che in diversi settori hanno imposto vincoli legati alla gestione della sicurezza dei sistemi ICT, hanno ulteriormente messo al centro dell'attenzione il Framework Nazionale; si consideri ad esempio l'implementazione della NIS, con le relative linee guida basate sui contenuti del framework; più recentemente il DL n.105 del 21 Settembre 2019 ha istituito il cosiddetto *perimetro di sicurezza nazionale cibernetica,* indicando nel successivo DPCM n.81 del 14 Aprile 2021 le misure di sicurezza che le organizzazione coinvolte devono adottare, riprendendo le stesse direttamente dal Framework Nazionale.

Il Framework Nazionale per la Cybersecurity e la Data Protection è il frutto di una libera collaborazione tra organizzazioni private, pubblica amministrazione e centri

BIO

Marco Angelini è ricercatore in Ingegneria Informatica presso la Sapienza Università di Roma. I suoi interessi di ricerca includono la Cybersecurity, specificamente focalizzato sulla difesa delle infrastrutture critiche, la modellazione della governance della sicurezza e la valutazione del rischio cyber. È autore di più di 50 pubblicazioni su journal e in conferenze scientifiche internazionali. È co-autore del Framework Nazionale di Cyber Security, prodotto dal centro di ricerca in Cyber Intelligence and Information Security della Sapienza (CIS), di cui è membro.

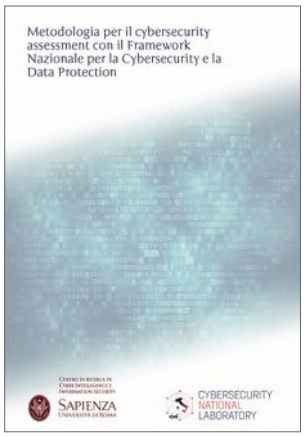
BIO

Leonardo Querzoni è professore associato presso la Sapienza Università di Roma. I suoi interessi di ricerca spaziano dalla sicurezza informatica ai sistemi distribuiti con un particolare focus sull'affidabilità e la sicurezza dei sistemi complessi. È autore di più di 100 pubblicazioni su journal e in conferenze scientifiche internazionali. È inoltre co-autore del Framework Nazionale di Cyber Security, prodotto dal centro di ricerca in Cyber Intelligence and Information Security della Sapienza (CIS), di cui è membro, in collaborazione con il Consorzio Interuniversitario Nazionale per l'Informatica (CINI).

di ricerca, con il supporto del Dipartimento Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri. Il mantenimento e l'evoluzione dello stesso sono curati dal Centro di Ricerca in Cyber Intelligence e Information Security (CIS) dell'Università degli Studi di Roma La Sapienza, in collaborazione con il Laboratorio Nazionale di Cyber security del CINI. Il Framework Nazionale e le risorse ad esso connesse sono liberamente disponibili alla pagina https://www.cybersecurityframework.it.

L'assessment di sicurezza

Qualunque sia la natura del framework di cybersecurity che un'organizzazione adotta, la stessa si confronterà inevitabilmente con la necessità di valutare quanto le misure di sicurezza attualmente implementate le permettano di soddisfare i requisiti stabiliti dall'obiettivo finale. Questa pratica è nota con il nome di *cybersecurity assessment*, e permette di valutare periodicamente il progresso nell'implementazione di un programma volto all'incremento del livello di sicurezza. Anche in questo ambito sono state proposte nel tempo più metodologie, con diversi livelli di dettaglio, che fanno riferimento ad alcuni dei framework più noti (es. NIST CSF, ISO 27001, etc.).



In generale, si distinguono due macro-approcci all'assessment:

ASSESSMENT QUALITATIVO - le metodologie riconducibili a tale approccio si basano sul presupposto che le pratiche e le soluzioni oggetto della valutazione non permettono una quantificazione oggettiva della loro qualità. Preferiscono quindi andare a valorizzare elementi soggettivi e aspetti che sono difficilmente misurabili.

ASSESSMENT QUANTITATIVO - Tale approccio presume che l'oggetto di valutazione sia misurabile attraverso una serie di metriche opportunamente definite. Tale misurazione deve essere svolta nel modo più oggettivo possibile, cercando di limitare eventuali contaminazioni del dato misurato derivanti da considerazioni di carattere soggettivo.

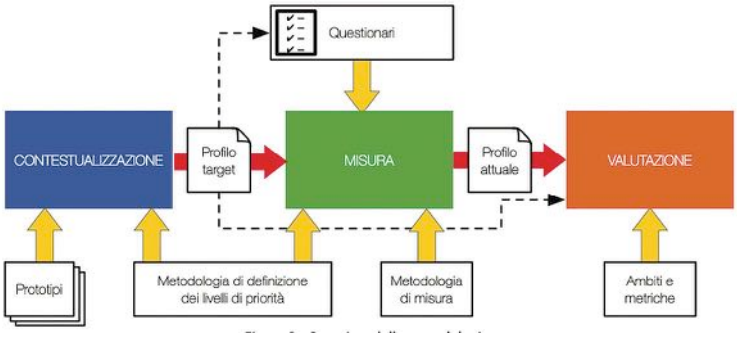
Le metodologie di assessment qualitativo vengono spesso adottate laddove sia preferibile un approccio alla valutazione più "snello" o dove i processi di valutazione debbano essere svolti in tempi ridotti o con costi limitati. Di converso, le metodologie quantitative sono più adatte laddove sia necessario un monitoraggio periodico delle performance di un processo di cybersecurity governance o nel caso in cui si debba procedere a una misurazione del ritorno di un investimento nell'ambito della sicurezza cyber. Pertanto, i due approcci non sono esclusivi, ma anzi costituiscono le basi per condurre un cybersecurity assessment in maniera integrata.

Diverse metodologie per il cybersecurity assessment sono oggi disponibili, seppur con alcuni limiti. Infatti, la maggior parte di esse si configurano come soluzioni chiuse, offerte esclusivamente dai vendor che hanno curato il loro sviluppo, e caratterizzate da forte eterogeneità. Tali elementi potrebbero rendere complessa la loro interoperabilità con conseguenze rilevanti sul processo di gestione della cybersecurity. In questo senso, la comparabilità dei risultati ottenuti applicando metodologie concorrenti potrebbe essere limitata o non applicabile (in particolare per gli assessment quantitativi), favorendo un meccanismo di lock-in che spingerebbe le organizzazioni a continuare a rivolgersi allo stesso vendor per garantire la corretta interpretabilità degli assessment sul lungo periodo. Come conseguenza, organizzazioni diverse non avrebbero modo di comparare reciprocamente l'efficacia delle diverse azioni implementate nei rispettivi piani di cybersecurity, rendendo il processo di assessment una pratica circoscritta ai confini della singola organizzazione.

Per superare queste limitazioni, è stata recentemente pubblicata sul web, una nuova metodologia di assessment, completamente aperta e incentrata sull'uso del Framework Nazionale.

Metodologia di assessment della sicurezza basata sul Framework Nazionale

La metodologia di assessment della sicurezza basata sul Framework Nazionale per la Cybersecurity e la Data Protection segue un approccio quantitativo, e prevede tre principali fasi operative, come visibile in Figura 2:



Fasi della metodologia e loro relazioni

FASE 1 - Contestualizzazione. Questa prima fase ha l'obiettivo di contestualizzare il Framework alla realtà di interesse. Tale fase, come riportato nel documento originale del Framework, ha come input specifici strumenti di supporto denominati prototipi di contestualizzazione (mapping di specifici elementi normativi/standard tecnici/best practices con il Framework), già pubblicati o definiti ad hoc dall'organizzazione, unita ad una metodologia di definizione del livello di priorità per ogni subcategory del Framework (ricordiamo che con la priorità si intende valutare il contributo all'abbattimento del rischio cyber fornito da ogni

subcategory). Il prodotto di questa fase è il *profilo target*, ovvero lo stato di sicurezza informatica desiderato per l'organizzazione, al quale tendere e sul quale viene realizzato l'assessment. La sua corretta definizione è quindi funzionale allo svolgimento delle successive due fasi.

FASE 2 - Misura. Nella fase di misura si procede a individuare l'attuale postura di sicurezza cyber dell'organizzazione (il *profilo attuale*) rispetto a quanto definito nel profilo target. Tale processo ha quindi come input il profilo target e un questionario creato su di esso che mira ad analizzare lo stato di sicurezza informatica per ciascuno dei controlli definiti all'interno del profilo target. L'assessment avviene attraverso interviste a soggetti competenti per le specifiche esigenze di analisi e raccolta di evidenze per dispositivi e processi all'interno dell'organizzazione tramite l'erogazione assistita del questionario. Il risultato delle interviste viene espresso in termini di *copertura* e *maturità*, rappresentanti la metodologia di misura per ogni controllo individuato. La copertura misura quanto dello specifico controllo di sicurezza è attualmente implementato all'interno dell'organizzazione, mentre la maturità ne definisce il grado di sofisticazione implementativa.

FASE 3 – Valutazione. Nella terza fase i risultati della fase di misura vengono valutati secondo diversi possibili ambiti. Questa fase conferisce ai risultati di assessment un alto grado di riutilizzo e versatilità, permettendo la loro proiezione, lettura e interpretazione su ambiti differenti, che assolvono compiti differenti all'interno del processo di gestione della sicurezza dell'organizzazione. Di conseguenza, questa fase ha come input il profilo attuale e l'insieme di ambiti su cui proiettare i risultati dell'assessment, ciascuno coadiuvato delle rispettive misure di interesse. In questo modo è possibile calcolare, a partire dai valori di copertura e maturità di ogni subcategory, delle metriche di interesse per l'ambito stesso. Gli ambiti applicabili possono essere diversi: a titolo di esempio riportiamo l'ambito di compliance, che permette di valutare la postura cyber dell'organizzazione rispetto a specifici standard e/o regolamenti, oppure l'ambito della gestione del rischio, in cui si mira invece a comprendere l'attuale stato di esposizione rispetto alle minacce cyber. Tali misure possono considerare in modo opportunamente pesato i contributi delle varie subcategory al raggiungimento di determinati obiettivi per l'ambito stesso, permettendo quindi di analizzare i risultati dell'assessment da differenti punti di vista.

Vantaggi e prospettive nell'uso della Metodologia

La struttura della metodologia di assessment della sicurezza abilita una serie di vantaggi che la distinguono da altre metodologie e framework esistenti e la rendono non solo integrabile con esse, ma anche punto centrale dell'assessment da cui poi si potranno proiettare i risultati sugli altri framework.

Un primo vantaggio fondamentale dell'approccio proposto è la capacità di effettuare una sola volta la fase di misura, e successivamente poter interpretare i risultati ottenuti secondo diversi punti di vista (ambiti) e framework alternativi. Ad esempio, il settore di un'organizzazione che si occupa di risk management darà particolare rilevanza agli aspetti inerenti alla gestione del rischio e relative metriche annesse (es: rischio potenziale, rischio residuo), mentre il settore legale porrà particolare attenzione agli aspetti di compliance (es: copertura GDPR). Ciascun settore assegnerà differenti pesi ai controlli di maggiore interesse, comportando una modifica dei punteggi risultanti ed evidenziando i controlli specifici del proprio ambito di competenza. Questa attività abilita una visione unificata, declinabile opportunamente su determinati ambiti, che non necessita di assessment ripetuti e specifici per l'ambito, rendendo quindi più efficiente il processo di assessment, riutilizzabile il suo risultato, e diminuendo la difficoltà di interpretazione derivante da molteplici assessment eseguiti tramite framework differenti.

Un secondo vantaggio della metodologia presentata è l'abilitazione del concetto di confrontabilità tra assessment, cioè la capacità di confrontare la propria postura di sicurezza rispetto a quella di altre organizzazioni, per via dell'utilizzo del Framework Nazionale come elemento unificante. La confrontabilità sarà totale qualora entrambe le organizzazioni utilizzino la stessa definizione di contestualizzazione (es: organizzazioni appartenenti allo stesso settore e di dimensioni simili). La confrontabilità sarà parziale, ma ancora presente, qualora le contestualizzazioni utilizzate non siano uguali, in termini di differenza tra le contestualizzazioni (es: quali subcategory o controlli di sicurezza non risultino utilizzati), differenza tra i profili attuali sull'intersezione delle contestualizzazioni. Ulteriore caratteristica, soggetto di ricerca attiva, è la capacità di rivalutare un assessment condotto da una organizzazione A con profilo target A sul profilo target B di un'altra organizzazione: questo elemento abilita, ad esempio, un'organizzazione alla valutazione della postura cyber di un fornitore rispetto ai propri standard di sicurezza, eventualmente differenti in tutto o in parte da quelli del fornitore.

Un terzo vantaggio della metodologia risiede nel suo utilizzo come base del Framework Nazionale, in relazione ai suoi utilizzi in attività di regolamentazione nazionale e internazionale quali l'applicazione della direttiva NIS ed il Perimetro di sicurezza nazionale cibernetica. In questi ambiti la metodologia proposta permette di quantificare lo stato di copertura e maturità implementativa delle misure di sicurezza adottate rispetto allo strumento scelto, abilitando al contempo la proiezione verso framework già utilizzati in modo trasparente (fase 3 della metodologia). Di conseguenza, la quantificabilità e la portabilità dell'assessment prodotto lo rendono già consistente, nella forma, con quanto atteso dalle organizzazioni soggette a queste due regolamentazioni.

Infine, un ultimo vantaggio concerne l'utilizzo della metodologia e dei suoi prodotti come strumento di comunicazione tra le aree che, all'interno di un'organizzazione, si occupano di sicurezza informatica e non solo. I tre livelli di un'organizzazione su cui agisce in modo principale la metodologia sono riportati in Figura 3:

Relazione tra la metodologia di assessment della sicurezza e i livelli organizzativi

- *Livello tecnico*. A livello tecnico, la metodologia fornisce la capacità di organizzare e tracciare lo stato dei singoli controlli operativi e la loro semantica in relazione alla tipologia di requisito collegato (regolamenti tecnici, normativa, best practices)
- *Livello esecutivo*. A livello esecutivo, la metodologia permette di ottenere una visione dello stato di sicurezza di un'organizzazione interpretabile rispetto ai diversi ambiti che trattano la sicurezza informatica, come ad esempio la compliance oppure la gestione dei rischi, permettendo a diversi attori di ragionare sull'assessment rispetto al loro ambito di competenza in modo unificato rispetto ai controlli effettuati.
- *Livello dirigenziale*. A livello dirigenziale, la metodologia permette di ottenere una visione generale, non legata ai singoli aspetti tecnici, dello stato di sicurezza dell'organizzazione, tramite l'utilizzo del Framework Nazionale per la Cybersecurity e la Data Protection. La comparabilità che la metodologia fornisce permette di informare processi di decision making con opportune valutazioni sullo stato di operatività sia rispetto al proprio settore di afferenza che rispetto ad attori similari.

La metodologia è aperta e adottabile da chiunque: dalla singola organizzazione che decide di sviluppare internamente un processo di assessment, al vendor che offre la sua applicazione come servizio verso terzi. La metodologia abilita ulteriormente la condivisione, lo scambio e il confronto dei risultati, anche tra attori differenti. Tale confronto potrà in futuro supportare la creazione di benchmark di valutazione tra aziende operanti nello stesso settore, e una condivisione di best practice di cybersecurity. Maggiori dettagli tecnici inerenti alla sua implementazione sono disponibili sul sito del Framework Nazionale per la Cybersecurity e la Data protection https://www.cybersecurityframework.it. ■

Verso la creazione di un polo Cyber per la tutela della sicurezza nazionale.

Intervista VIP a Marco Castaldo.

Autore: Massimiliano Cannata

Il cyber spazio è la nuova frontiera da proteggere. I maggiori pericoli per la sicurezza degli stati arrivano da minacce globali, sempre più sofisticate, difficili da prevenire, come dimostrano tanti casi eclatanti, quello della Regione Lazio è solo uno degli ultimi esempi. Alle nostre latitudini le ripercussioni di una tale decisione hanno generato un dibattito che ha portato alla istituzione di un'agenzia per la Cyber sicurezza nazionale. Il tema, particolarmente caldo, ha bisogno di una strategia di sistema. Marco Castaldo, consigliere delegato di Yoroi sta lavorando su questo delicato terreno.

Dott. Castaldo, Yoroi è diventata parte importante di un Polo nazionale della cyber security. Dobbiamo pensare che il privato arriva sempre prima del pubblico?

Questo è quello che succede abitualmente nei paesi capitalistici. Il privato ha processi decisionali più immediati, è disponibile a rischiare per anticipare un potenziale trend, è alla ricerca di aree ancora "vergini" dove occupare spazi significativi e ha una velocità superiore di adattamento rispetto alle mutate condizioni di mercato. Ragionando più in generale credo che quello che un paese moderno deve fare è creare le condizioni ottimali, di "sistema", per favorire e agevolare la libera iniziativa. Unico accorgimento che va seguito è relativo al controllo degli "animal spirits", perché non agiscano in contrasto con l'interesse pubblico, in quel caso bisognerà intervenire con regolamentazioni adeguate.

Per tornare alla sua domanda, posso dire che il mio impegno da quando sono entrato nel settore della cyber security è stato polarizzato dal desiderio di favorire la costruzione di un polo nazionale, attraverso la co-fondazione

BIO

Marco Castaldo è Consigliere Delegato di Yoroi. Napoletano, vive da tre decenni a Roma; si è laureato con lode in Economia e Commercio e ha conseguito un MBA. Ha una solida esperienza internazionale, ha lavorato nel mondo della finanza, prima in TPL S.p.A. (oggi Technip S.p.A), poi in Azimut e Credit Suisse. Da 20 anni è partner di Falcon Capital, una società con sede legale a Londra e attiva sui mercati internazionali in operazioni di venture capital. Ha co-fondato nel 2018 il Gruppo Cybaze che deteneva Mediaservice e Yoroi e che recentemente si è societariamente concentrato tutto in Yoroi, semplificando e ottimizzando la catena societaria. Oggi è Amministratore Unico di Fort Cyber (ex Cybaze S.p.A), che detiene il 35% di Yoroi e Consigliere Delegato di Yoroi, oltre ad essere sempre un Partner di Falcon Capital. Yoroi è una brillante società verticale in cyber security ed è la risultante di un processo di concentrazione dentro di se di altre due società, Cybaze - a sua volta la risultante della fusione tra Emaze e Cybsec - e Mediaservice.

del gruppo Cybaze che comprendeva Mediaservice e Yoroi e che è stato recentemente riorganizzato in un'unica società, Yoroi. Con l'arrivo di Tinexta, che ad inizio anno ha acquisito la maggioranza azionaria di Yoroi ma anche di Corvallis e di Swascan mettendo le tre società "a sistema", la costruzione del polo nazionale è diventata una solida realtà.

L'operazione societaria è sicuramente importante e complessa. Quello che più interessa CyberSecurity Trends sono le strategie di intervento sul fronte della sicurezza informatica. Cosa può dirci in proposito?

Nella cyber security si gioca un pezzo della sicurezza del paese; favorire lo sviluppo di campioni nazionali è a nostro avviso di primaria importanza per l'Italia. Detto questo, va precisato che i nostri sforzi sono orientati alla creazione di un polo cyber con tecnologie proprietarie in grado di misurarsi con le grandi società internazionali, capace di difendere e mantenere i dati sensibili che appartengono alle maggiori aziende e alle grandi organizzazioni sul territorio italiano. Il polo di cui sto parlando per dimensioni di fatturato e di persone è già tra i leader assoluti del mercato, e presenta obiettivi di ulteriore crescita molto importanti.


NETWORK DIGITAL 360

CYBERSECURITY360

L'ACQUISIZIONE

Ecco il maggiore polo della cyber security in Italia, Colajanni: "Nostre PMI saranno più sicure"

Home > News analysis

Condividi questo articolo

L'acquisizione da parte di Tinexta di Yoroi, Swascan e della divisione progetti e soluzioni e R&D di Corvallis, per un investimento iniziale di 47,8 milioni, è una buona notizia per il mercato cyber italiano. Ma anche per la sicurezza informatica delle nostre PMI. Ecco perché

Vi sono delle best practices cui avete fatto riferimento nel percorso di crescita?

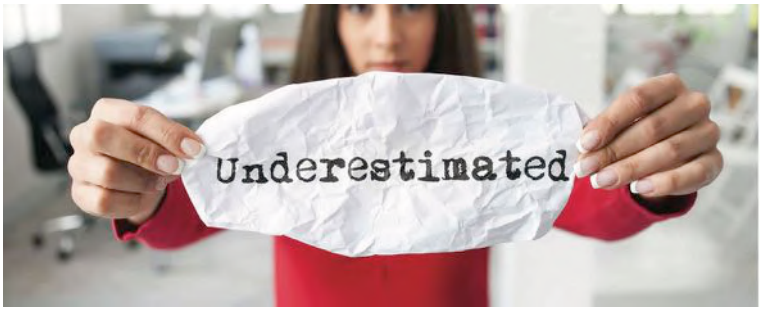
Come è noto, Israele è il paese più avanzato nell'ambito della cyber security. Il modello israeliano insegna che la creazione di un ecosistema che veda la collaborazione di aziende private, università e organismi governativi,

in presenza di risorse finanziarie significative pubbliche e private e con l'obiettivo di finalizzare la ricerca scientifica verso applicazioni concrete, produce innovazione, favorisce l'emergere di talenti e assicura anche ritorni importanti sugli investimenti. Noi abbiamo cercato di costruire, nel nostro piccolo, un ecosistema che somigliava a quella tipologia, allacciando rapporti strategici con Università eccellenti e attirando capitali di rischio di investitori sofisticati. Oggi, con un socio di maggioranza come Tinexta, una

società quotata che possiede azionisti istituzionali, la nostra vocazione di campione nazionale è pienamente espressa.

Stime ufficiali della Polizia Postale ci dicono che nell'ultimo anno gli attacchi contro le infrastrutture critiche, quali danneggiamento, interruzione del servizio, furto dei dati a scopo eversivo sono aumentati in Italia del 246%, dato che corrisponde a un incremento del 78% delle persone indagate. Il quadro è reso ancora più fosco dalla "mafia digitale", fenomeno emergente e sempre più pervasivo, capace di rubare dati e di richiedere il "pizzo" di nuova generazione, che consiste nella richiesta di un riscatto da soddisfare in cripto valuta. Questa escalation che riguarda realtà geografiche a tutte le latitudini, vede in particolare il nostro paese al 14esimo posto nella classifica delle nazioni europee più esposte al rischio, che cosa deve portarci a pensare?

Il tema dei rischi cibernetici in Italia è stato a lungo largamente sottovaluto, sia dal settore pubblico che da quello privato, con il risultato che siamo in ritardo rispetto ai paesi più avanzati. Dal punto di vista della domanda la necessità di gestire i rischi cyber è stata concepita fino a poco fa esclusivamente come un costo e come un dovuto adeguamento formale alle normative, in particolare la GDPR; da un punto di vista dell'offerta è stata considerata all'inizio sostanzialmente come occasione di business e di monetizzazione – penso alle Big Four, ad Accenture ed ai grandi system integrator – del proprio portafoglio clienti.



Oggi la situazione è radicalmente cambiata. C'è stata negli ultimi tre anni una crescita tumultuosa delle società che dichiarano di fare cyber security e l'attualità dimostra quotidianamente che il tema è sempre più strettamente connesso con la competitività sia della singola organizzazione – pubblica o privata che sia – che del sistema paese. Competitività che va letta in relazione allo sviluppo della digitalizzazione, sempre più integrata – IOT, Industria 4.0, 5G etc. – con i vantaggi che comporta in termini di aumento della produttività, ma anche di rischi cyber sempre maggiori. Per questo va ricordato che anche la competitività si gioca sulla sicurezza e difesa dei dati sensibili e strategici personali e delle organizzazioni. Le grandi partite internazionali di business e di geo-politica ruotano attorno a questi concetti. E comincia ad essere sempre più chiaro che la sicurezza del singolo – sia esso un privato o un'organizzazione – non può prescindere dalla crescita complessiva della sicurezza del proprio universo di riferimento – pensiamo ad esempio al tema della security della supply chain – in mancanza della quale gli sforzi e gli investimenti individuali potrebbero essere vanificati.

Di fronte abbiamo una grande alleanza di criminali informatici che si scambiano giornalmente nel dark web strumenti, tecnologie, strategie, suggerimenti operativi allo scopo di massimizzare i ritorni delle attività criminose. È indispensabile dunque che tutti – ed in particolare chi come noi è sul campo ogni giorno – siano proattivamente concentrati nell'organizzare "la difesa collettiva" contro il cyber crime.

Sicurezza e democrazia

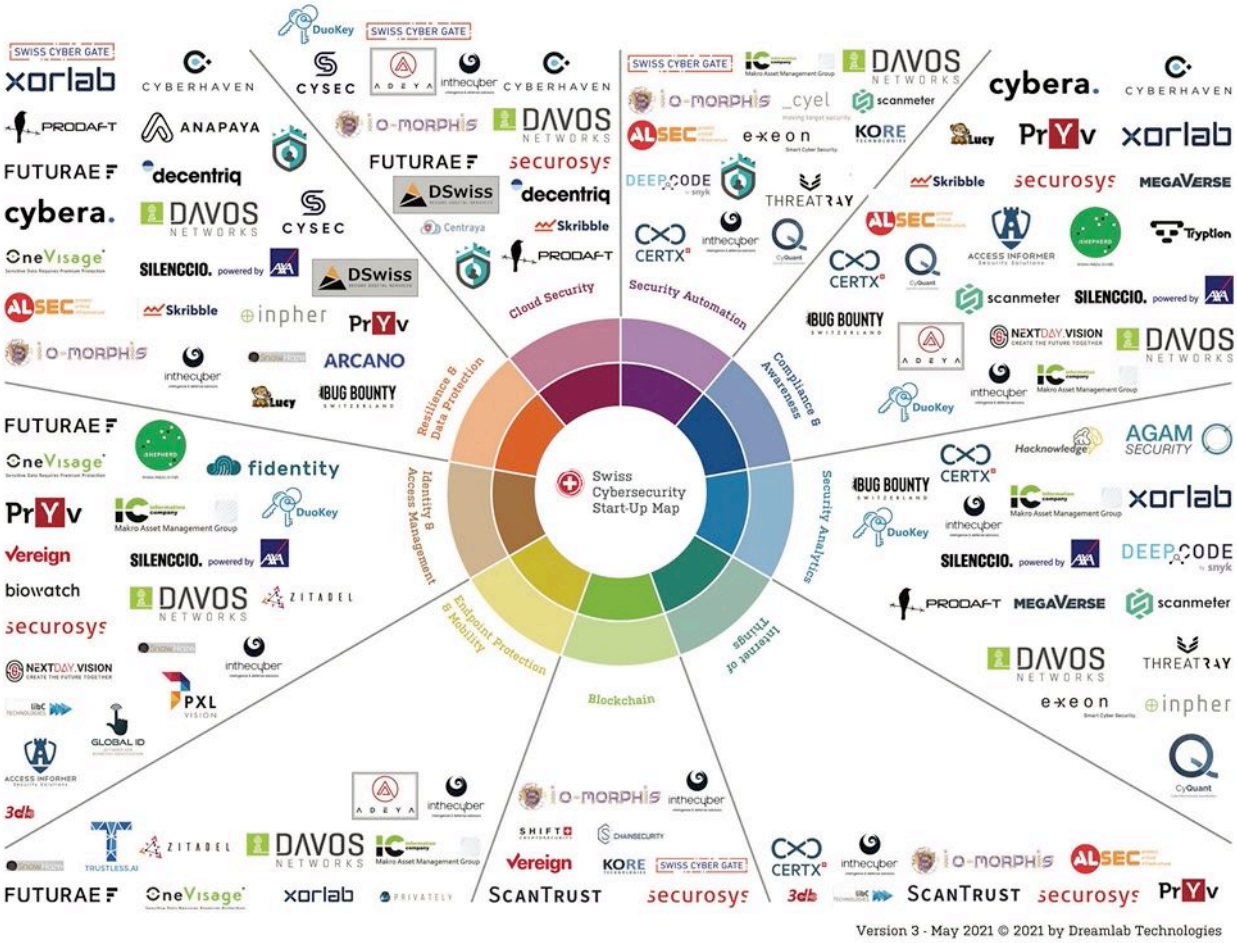
Non crede che quello di cui Lei parla ha delle ripercussioni sullo stato di salute e sugli equilibri della democrazia?

Il nesso esiste certamente, anche perché i temi fondamentali della difesa delle libertà democratiche passano attraverso la necessità di difendere la libera formazione del consenso politico e quindi attraverso

l'urgenza di contrastare l'uso di notizie false che inducono percezioni distorte della realtà, il cui effetto è enormemente amplificato dai social network e dalle tecniche di *profiling* sempre più sofisticate. Chi si occupa di cyber security non può non sentire una forte responsabilità in relazione a queste tematiche.

La vicenda della pandemia ha dimostrato quanto significativamente può influenzare la sicurezza delle nostre comunità e del nostro vivere civile e quali danni immani può portare un'informazione manipolata dalle fake news.

Lei ha un'esperienza consolidata riguardo all'utilizzazione dei capitali di rischio per la creazione



L'esempio delle start-up della Svizzera

di imprese innovative. Come si posiziona l'Italia in questo delicato ambito?

Mi dispiace doverlo dire ma è molto indietro rispetto ai paesi, in particolare di matrice anglosassone e non solo…, anche se si intravedono i primi segnali di svolta. L'Italia è un paese dove storicamente i capitali privati hanno preferito usare la leva finanziaria per fare investimenti, ponendosi nelle condizioni di dover poi subire gli inevitabili e conseguenti condizionamenti del sistema bancario e finendo col perdere capacità e velocità di reazione ai cambiamenti e agli sviluppi di mercato. D'altra parte, va detto che il risparmio privato è stato per decenni assorbito quasi interamente dai titoli di stato, la cultura finanziaria è rimasta molto bassa così come la propensione al rischio, che cresce in misura direttamente proporzionale al rafforzamento delle competenze finanziarie. Il risultato è che oggi è probabilmente più rischioso investire su titoli di stato di lunga durata che su una società tecnologica attiva in settori a crescita elevata. Il ragionamento che stiamo facendo è valido, non scordiamocelo, se si è capaci di valutare il modello di business e la qualità del management.

Vi sono molte resistenze, insite nel nostro DNA, che ostacolano la diffusione di quella cultura del rischio che è il "sale" di ogni attività di business?

Non nego che negli ultimi 20 anni le abitudini di investimento degli italiani si siano avvicinate a quelle dei paesi più sviluppati, almeno in termini di utilizzo di strumenti quali, ad esempio, i fondi di investimento. Va anche detto, però, che la propensione verso il mercato azionario, che

per decenni è stato visto come puro azzardo (il detto "giocare in borsa" è molto esplicativo in proposito) si presenta ancora troppo bassa. Quello che avviene sul terreno del *private equity* e del *venture capital*, con volumi di investimento storicamente insignificanti rispetto ai paesi più sviluppati, ha confermato questo trend. Il problema è che un mercato dei capitali che non alloca efficientemente le risorse disponibili rappresenta un enorme freno per la crescita della nostra economia. E l'allocazione efficiente passa per la capacità di saper valutare e saper "prezzare" correttamente il rischio di ogni investimento. Vorrei insistere sul concetto di rischio - che di solito alle nostre latitudini è visto come una pessima parola – che è un elemento positivo nel contesto delle attività di investimento. Non dimentichiamo che è la *governance* del rischio che rende disponibile una corretta remunerazione del capitale investito.

Rafforzare la cultura delle start up

Non si può dire che il nostro Paese sia la patria delle start up. Quali debolezze vanno superate per colmare un gap che appare evidente rispetto ad altre nazioni che sono molto più avanti anche nella promozione dei talenti innovativi?

Oltre ad un aumento della cultura finanziaria su cui mi sono appena soffermato, occorrono modifiche strutturali del "sistema Italia" con riferimento, ad esempio, al funzionamento della giustizia civile e alla rigidezza e ai costi del mercato del lavoro, oltre ad una radicale riforma della burocrazia, vera palla al piede del paese. Gli italiani hanno dimostrato da sempre di non essere secondi a nessuno in termini di capacità professionali,

di attitudine all'innovazione, di capacità di pensare - come dicono nei luoghi iconici dell'innovazione - "out of the box"; ma di fatto hanno caratterialmente e storicamente mostrato difficoltà a sentirsi parte di una squadra. Questa natura individualistica è anche la principale causa del "nanismo" di cui la massa delle imprese italiane è affetta, senza contare che nelle dinamiche del mercato globalizzato, partire con l'idea di restare piccoli è già una "quasi condanna" al fallimento.

Non crede che al di là degli aspetti economici, vi sia un "gap" culturale che non consente al nostro capitalismo di compiere un salto di visione?

L'aspetto "culturale" cui lei si riferisce riguarda molto spesso l'innamoramento per la propria azienda; il vero startupper ha una naturale propensione all'exit ed è spesso un imprenditore seriale in settori diversi. Quello che conta è la capacità di innovare. Pensiamo a Elon Musk e alla sua poliedricità di interessi. Da noi c'è ancora spesso l'idea che un'azienda debba restare nostra per la vita e passare ai nostri figli... A dispetto di questa impostazione dura a morire, va detto però che si intravedono segnali positivi da qualche anno a questa parte, con una accelerazione nell'ultimo anno. L'interesse del mercato per operazioni di private equity comincia ad essere di una certa consistenza. Anche sul fronte degli eco-sistemi, che favoriscono la crescita delle start up, c'è fermento. Mi piace ricordare, ad esempio, il successo della Developer Apple Academy fondata a Napoli e di tutto il polo tecnologico della Federico II di cui fa parte, grazie al grande lavoro di Giorgio Ventre, amico caro della mia infanzia. Si tratta di un modello che ricorda gli ecosistemi israeliani di cui facevo cenno. Probabilmente, è questa la spiegazione che mi do e che offro a Cybersecurity Trends, le nuove generazioni digitali stanno cambiando pelle e sono sempre più simili a quelle di altri paesi del mondo con economie più sviluppate. Rimane, comunque, compito primario della classe dirigente di questo paese agevolare un processo di trasformazione che non può tardare ancora a compiersi.

Essere attrattivi è importante. I luoghi dell'innovazione, dalla Silicon Valley, alla Bengalore Valley, (lei ricordava Israele) hanno saputo creare un ecosistema adatto a generare quella cultura del rischio che da sempre è il motore dell'impresa. In Italia risulta più difficile creare condizioni capaci di stimolare il pensiero innovativo. Quali sono le ragioni?

Al di là degli aspetti su cu ci siamo già soffermati, la difficoltà di fare impresa in Italia è in larga parte generata dalla burocrazia soffocante, che impedisce la traduzione

immediata di idee innovative in start up e la difficoltà, come dicevo, di trovare capitali di ventura disponibili a prendere rischi significativi, nonostante la liquidità sul mercato non sia mai stata così elevata.

Per sviluppare un'adeguata cultura del venture capital, quali competenze occorre sviluppare?

Un buon *venture capitalist* ha una elevata predisposizione al rischio; ma oltre a questa deve

avere la capacità di valutare sia il valore potenziale dell'innovazione che l'efficacia dei modelli di business su cui porrà l'attenzione, ma anche la qualità umana, prima ancora che professionale, dello startupper e del suo team. Carenze manageriali sono più facili da colmare, ed in questo i business angels possono essere fondamentali, ma talento ed intuizione sono merce molto, molto rara.

Tempo della burocrazia e tempo dell'innovazione mal si conciliano. Tra le riforme di sistema che potrebbero aiutare il rilancio dell'economia va sicuramente collocata la riforma della giustizia e un adeguamento dell'apparato normativo, che presenta ancora troppe vischiosità rispetto alla rapidità del cambiamento che connota la digital economy. Qual è la sua riflessione in merito?

La digital economy ha come campo da gioco il mondo; non esistono barriere per definizione se non – almeno per quanto riguarda l'Italia - barriere di tipo linguistico, per l'ancora troppo poco diffusa conoscenza dell'inglese; una criticità per la quale il nostro sistema scolastico porta una grande responsabilità. In una competizione globale va ricordato che i sistemi nazionali diventano fattori di competitività; se il nostro non si affretta a colmare i gap con i paesi più avanzati, la partita per il nostro tessuto imprenditoriale rischia di essere persa in partenza o, quantomeno, siamo in un campionato dove partiamo con molti punti di penalizzazione. Per questo non possiamo sprecare un'occasione come l'ingente quantità di fondi in arrivo per il PNRR che potranno – se spesi bene – dare una radicale spinta al sistema paese per fargli prendere finalmente la velocità dei paesi tecnologicamente ed infrastrutturalmente più avanzati del nostro. ■

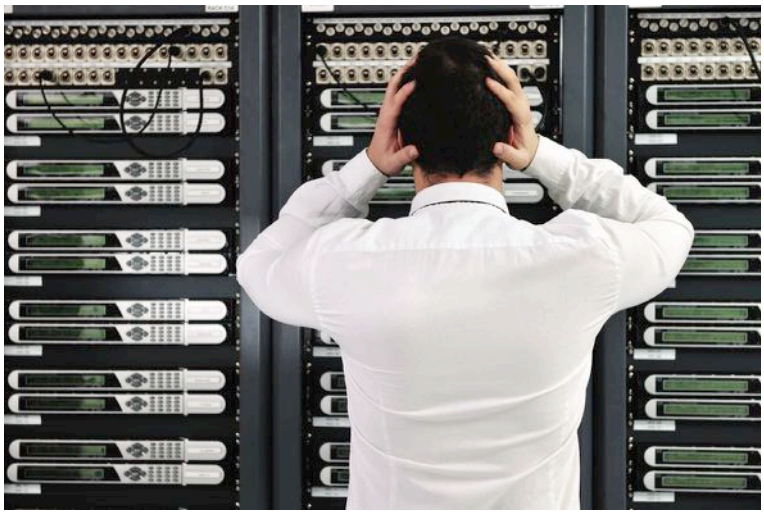
La gestione della superficie di attacco esterna (EASM), un approccio necessario per fronteggiare le nuove minacce.

Autore: Yaron Tal

Digital Trasformation, il passaggio alle infrastrutture Cloud, la convergenza IT e OT e il lavoro a distanza sono alcune aree chiave in cui stanno emergendo nuovi requisiti di sicurezza.

Quando esce una nuova vulnerabilità di sicurezza inizia una corsa frenetica tra gli aggressori che scansionano Internet per identificare i sistemi vulnerabili e i difensori che devono implementare patch e altre mitigazioni per proteggere le loro reti e con una visione più attuale del fenomeno: il business dell'azienda.

Non appena vengono annunciate nuove vulnerabilità, gli aggressori si precipitano a trarne vantaggio, le scansioni iniziano entro 15 minuti dal rilascio degli annunci CVE (Common Vulnerabilities and Exposures).



Le organizzazioni criminali che negli ultimi mesi hanno messo a soqquadro i sistemi di mezzo mondo sono diventate milionarie grazie agli ultimi cyber attacchi posti in atto. E sono proprio i "ricavi" di questi gruppi il dato più preoccupante, considerando poi che 8 volte su 10 chi ha pagato viene nuovamente colpito nell'arco di 6-12 mesi, significa che il mercato di questo tipo di crimine può vantare già una base di "clienti" solida e purtroppo "fidelizzata".

All'interno di questo scenario sono nati nuovi strumenti che Gartner ha identificato come External Attack Surface Management (EASM),

BIO

Yaron Tal, Founder & CTO di Reposify, è un affermato imprenditore tecnologico ed esperto di sicurezza informatica con quasi due decenni di esperienza nello sviluppo di soluzioni software per la sicurezza informatica. Prima di fondare Reposify, Yaron ha ricoperto vari ruoli manageriali in startup dove ha acquisito una vasta esperienza nella guida di team di ricerca e nello sviluppo di soluzioni di successo. Yaron è un ex-studente dell'Israel Cybersecurity Center, dove ha lavorato per oltre quattro anni come sviluppatore di sistemi embedded, ricercatore e team leader.

External Attack Surface Management Ecosystem

Source: Gartner
737807_C

Gartner

prodotti innovativi che supportano le organizzazioni nell'identificazione dei rischi derivanti da risorse e sistemi connessi a Intenet - che le organizzazioni potrebbero ignorare - e che aiutano i professionisti della sicurezza a identificare le vulnerabilità esposte da risorse aziendali note e sconosciute e a dare la priorità ai problemi più critici tra quelli da affrontare.

Le esposizioni e le vulnerabilità sconosciute nell'ecosistema IT delle organizzazioni sono in continuo aumento. Un'analisi delle recenti violazioni della sicurezza ha indicato che circa il 35% delle violazioni e degli incidenti di sicurezza è derivato da esposizioni Internet sconosciute e dalla mancanza di visibilità adeguata.

La maggior parte delle organizzazioni dispone di Shadow IT e di risorse esposte che sono sconosciute e quindi gestite. Anche le risorse note ai team della sicurezza potrebbero essere inconsapevolmente esposte a Internet, a causa di una configurazione errata o una semplice dimenticanza. Con nuove istanze Cloud attive ogni secondo, ambienti di sviluppo che aumentano e diminuiscono, la superficie di attacco delle organizzazioni è in costante mutamento.

Secondo Reposify, uno dei principali fornitori di soluzioni di gestione della superficie di attacco esterna, il 64% in media delle risorse Internet di un'organizzazione fa parte del suo perimetro di rete non ufficiale ed è probabile che non sia gestito e quindi a rischio.

Man mano che le reti continuano a espandersi, l'individuazione e la risoluzione dell'esposizione dovrebbero evolversi. La scoperta dovrebbe andare oltre il perimetro visibile e dovrebbe essere eseguita dall'esterno verso l'interno a una velocità e una scala senza precedenti.

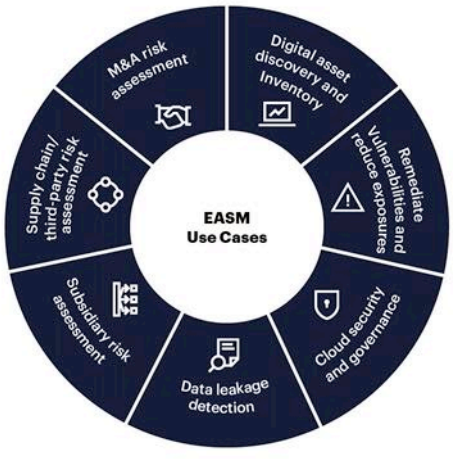
Mentre gli aggressori scansionano continuamente Internet alla ricerca di risorse esposte da prendere di mira. Le tradizionali soluzioni di valutazione del rischio sono costruite per reti note e tralasciano i principali punti ciechi negli ecosistemi IT delle organizzazioni.

Nel tentativo di scoprire le loro risorse esposte, i team di sicurezza utilizzano in genere gli stessi scanner Internet utilizzati dagli aggressori. Se gli attaccanti e le organizzazioni utilizzano gli stessi strumenti, automaticamente gli aggressori che dedicano il loro tempo solo a pedinare, elaborare strategie e attaccare, hanno un enorme vantaggio competitivo rispetto ai team di sicurezza che hanno molto di più da gestire.

EASM diventerà una soluzione standard per ogni team di sicurezza?

Nel marzo 2021, Gartner ha riconosciuto la gestione della superficie di attacco esterna (EASM) come una tecnologia emergente che integra la gestione delle vulnerabilità e altre soluzioni. Come mai? Gartner afferma che EASM supporta i leader della sicurezza nell'identificare i rischi critici da risorse Internet, conosciute e non, che potrebbero essere sfruttate dagli avversari. Comprendere veramente l'intera portata dell'azienda e dei suoi rischi è una sfida enorme, i team di sicurezza devono reagire rapidamente e evolvere continuamente.

Common Use Cases for External Attack Surface Management



Source: Gartner
737807_C

Gartner

Le organizzazioni leader stanno ora riconoscendo la necessità di un nuovo modo per scoprire, monitorare e gestire le proprie risorse Internet ed è in aumento l'adozione di soluzioni di gestione della superficie di attacco esterno.

Le soluzioni EASM dovrebbero includere questi 5 componenti chiave:

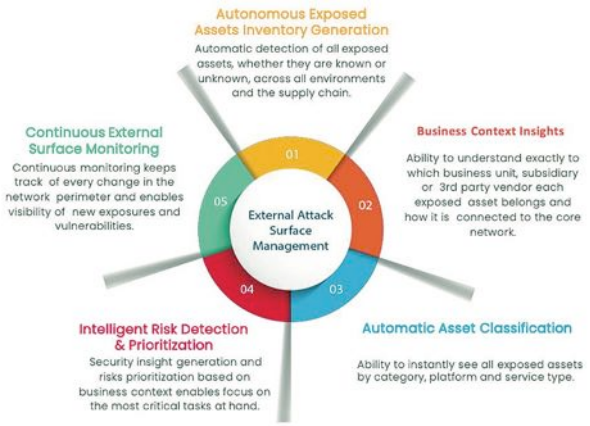
1 Asset discovery: rilevamento automatico di tutte le risorse esposte, note o sconosciute, in tutti gli ambienti e nella catena di approvvigionamento. La soluzione dovrebbe anche generare un inventario delle risorse esposte senza richiedere alcun input da parte del cliente.

2 Analisi degli asset e security issue: classifica automaticamente tutte le risorse esposte per categoria, piattaforma e tipo di servizio e analizza le risorse per un'ampia gamma di problemi di sicurezza, tra cui vulnerabilità, problemi di controllo degli accessi, problemi di configurazione, problemi di crittografia e rischi di phishing tra altri.

3 Prioritizzazione dei rischi: la priorità dovrebbe essere basata sul contesto aziendale e consentire ai team di concentrarsi sulle attività più critiche. La soluzione dovrebbe anche fornire una chiara visibilità dell'ecosistema aziendale e attribuire i rischi alla relativa unità aziendale o al fornitore di terze parti.

4 Remediation: la soluzione dovrebbe fornire una guida alla risoluzione, strumenti integrati e integrazioni di supporto per semplificare il processo di riparazione in modo che i team possano risolvere più problemi in meno tempo possibile.

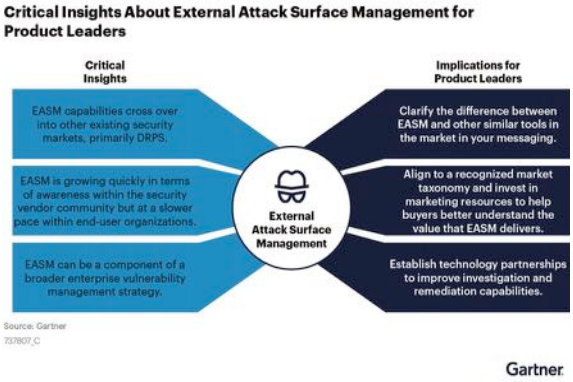
5 Continuous External Attack Surface Monitoring: monitoraggio continuo che terrà traccia di ogni cambiamento nel perimetro della rete e consente la visibilità di nuove esposizioni e vulnerabilità quasi in tempo reale.



Come valutare una soluzione EASM?

Ecco 6 criteri che ti aiuteranno a valutare efficacemente la qualità di una soluzione di External Attack Surface Management:

1 **Data Coverage and Association Robustness** - La capacità di trovare risorse esposte che si trovano al di fuori della rete ufficiale è fondamentale. Questi punti ciechi rappresentano spesso il rischio maggiore per la tua postura di sicurezza. Le analisi non si limiteranno ai certificati e ai banner. Includono l'arricchimento autonomo di identificatori univoci estratti dai tuoi ambienti e dallo stack tecnologico esistente per offrire una visibilità completa del tuo inventario di risorse connesse a Internet.



2 **Data Freshness -** Non tutti i beni sono uguali. Alcune risorse, come le istanze cloud, cambiano proprietà molto frequentemente. Per tali risorse, devi capire cosa possiedi in questo momento, non cosa possedevi un giorno o anche un'ora fa. La soluzione dovrebbe supportare una visualizzazione in tempo reale della tua superficie di attacco e regolare automaticamente la frequenza di scansione in modo che corrisponda al tuo inventario.

3 **Accuratezza e trasparenza dei dati -** Con così tanti dati che il tuo team sta già elaborando, aggiungere più rumore al sistema sotto forma di falsi positivi è l'ultima cosa di cui hai bisogno. La soluzione dovrebbe avere algoritmi di associazione robusti che indichino anche il livello di confidenza dell'associazione e il percorso di scoperta

4 **Data Actionability -** Un'analisi completa della sicurezza, che va oltre i CVE standard, un piano d'azione intelligente per la definizione delle priorità e la correzione sono fondamentali per migliorare la tua posizione di sicurezza in tempo reale. Inoltre, dovrebbe essere considerata anche la facilità di integrazione con il tuo stack tecnologico.

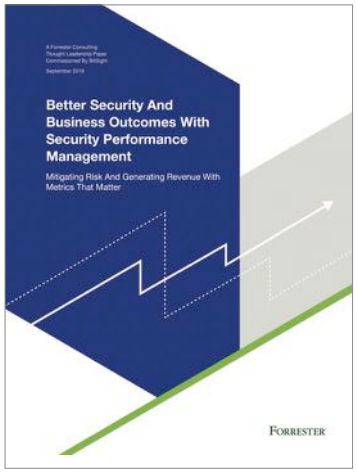
5 **Monitoraggio della supply chain -** I tuoi fornitori di terze parti e la catena di approvvigionamento sono una parte inestricabile della tua superficie di attacco. La soluzione dovrebbe scoprire automaticamente tutte le tue risorse esposte che sono gestite dai tuoi fornitori e permetterti di vedere quali esposizioni hanno i tuoi fornitori che potrebbero metterti a rischio.

6 **Facilità nelle operazioni quotidiane -** La soluzione dovrebbe offrire una scoperta continua e autonoma senza necessità di configurazione o intervento da parte dell'organizzazione. L'interfaccia utente dovrebbe aiutare a comprendere rapidamente i rischi e semplificare il processo di riparazione. Le soluzioni principali includeranno il flusso di lavoro integrato, il raggruppamento di risorse e problemi per varie categorie. ■

Una misurazione efficace del rischio informatico favorisce il miglioramento continuo.

Autore: Jacob Olcott

Va da sé che la cybersecurity ha assunto maggiore importanza negli ultimi anni. L'adozione dell'infrastruttura come servizio (IaaS) e del software come servizio (SaaS), l'aumento del BYOD (Bring Your Own Device) e la forza lavoro remota a causa del COVID-19 e l'Internet delle cose (IoT) hanno notevolmente ampliato le superfici di attacco delle organizzazioni. Gli attori delle minacce ne hanno approfittato per lanciare ransomware sofisticati e altri tipi di attacchi informatici con successo ben pubblicizzato.



È fondamentale proteggere questa superficie di attacco in continua crescita: in caso contrario, potrebbero verificarsi danni finanziari e reputazionali devastanti. Un rapporto di Forrester commissionato da BitSight nel 2019 ha rilevato che più di un terzo delle aziende ha subito delle perdite finanziarie a causa di una mancanza reale o percepita di rigore in materia di sicurezza.

Di conseguenza, la cybersecurity, un tempo di competenza esclusiva dei team IT, sta diventando un effort a livello di organizzazione con una maggiore richiesta di responsabilità. In questo clima, i leader della sicurezza hanno bisogno di un modo efficace per misurare e segnalare il rischio informatico utilizzando metriche basate su dati, indipendenti e oggettivi.

Misurazione efficace del rischio informatico

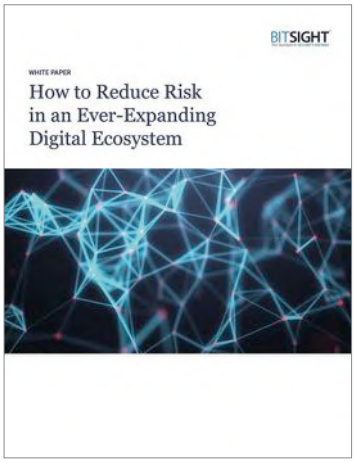
Una misurazione efficace del rischio informatico può avere significati diversi a seconda dell'organizzazione. Tuttavia, ci sono una serie di fattori chiave che dovresti considerare quando sviluppi o migliori la tua capacità di misurare il rischio informatico. Diamo un'occhiata.

Capire la tua superficie di attacco

La superficie di attacco di un'organizzazione è definita come la somma delle risorse digitali che possono essere sfruttate dagli hacker, comprese le reti locali e le vulnerabilità delle infrastrutture cloud. È essenziale comprendere la superficie di attacco della tua organizzazione e il modo in cui i controlli di sicurezza affrontano il rischio.

BIO

Jacob Olcott è Vice President of Communications and Government Affairs in BitSight. In precedenza, è stato consulente legale e politico in materia di sicurezza informatica presso la U.S. Senate Commerce Committee e U.S. House of Representatives Homeland Security Committee. Prima di BitSight, è stato advisor di Fortune 1000 in merito alla governance della sicurezza informatica e ai problemi tecnologici. Ha anche lavorato come professore a contratto sulla sicurezza informatica presso la School of Foreign Service della Georgetown University. Ha conseguito lauree presso l'Università del Texas ad Austin e la University of Virginia School of Law.



Questo presenta diverse sfide. Molti team di sicurezza si affidano a una varietà di strumenti con un approccio frammentario che richiede l'utilizzo di più strumenti, molti dei quali hanno funzionalità ridondanti. Tutto ciò è inefficiente e, peggio ancora, non garantisce una visione completa dell'intera superficie di attacco.

Pertanto, l'implementazione di una soluzione che offra visibilità sull'intero ambiente dovrebbe essere considerata essenziale. Questo tipo di visibilità è l'unico modo per comprendere appieno la superficie di attacco, misurare il rischio informatico e migliorare continuamente il tuo programma di sicurezza.

Benchmarking

Il benchmarking ti aiuta a comprendere e valutare lo stato di sicurezza informatica della tua organizzazione confrontandolo con concorrenti del settore. Fornisce risposte chiare a domande chiave, come ad esempio:

- Quanto è sicura la mia organizzazione?
- Quanto dovrebbe essere sicura?
- Sono presenti gap nel programma di sicurezza della mia organizzazione e come possono essere affrontati?
- Per il mio programma di sicurezza sto spendendo più o meno risorse di quanto dovrei?

Il benchmarking può identificare eventuali gap presenti nel tuo programma di sicurezza informatica in base a un confronto dei vettori di rischio all'interno di organizzazioni simili. Ti consente, inoltre, di confrontare il tuo programma con organizzazioni più grandi e consolidate, per ottenere informazioni su come dare priorità agli sforzi di sicurezza informatica per raggiungere la maturità del programma target.

Per comprendere l'impatto dei programmi di sicurezza e comunicare le modifiche ai decision maker è necessaria una soluzione che fornisca una visione quantitativa e comparativa delle prestazioni della sicurezza informatica nel tempo. È necessario trovare strumenti che forniscano una misurazione continua data-driven basata sui dati delle prestazioni di sicurezza, che ti consentano di valutare e monitorare lo stato di sicurezza informatica della tua organizzazione e misurare l'impatto degli sforzi di mitigazione del rischio.

Reporting

Che si tratti di un attacco ransomware che interrompe le normali operazioni o di una violazione che danneggia la reputazione, gli incidenti di sicurezza possono avere

un impatto finanziario significativo. Quindi, hai bisogno di una comprensione accurata della postura di sicurezza della tua organizzazione per i processi decisionali. È essenziale sviluppare una strategia per comunicare il rischio alla leadership.

Il reporting sulla sicurezza informatica basato sul rischio, al contrario del reporting basato sulla conformità o sugli incidenti, è un modo estremamente efficace per comunicare il rischio agli stakeholder aziendali. Il reporting basato sul rischio considera:

- **Past performance:** come erano gli stessi numeri del mese scorso o dell'ultimo trimestre? Stiamo migliorando o peggiorando nel tempo?
- **Risk concentration:** come si comportano le diverse unità aziendali e filiali nella nostra organizzazione?
- **Industry benchmarks:** come si confrontano le prestazioni con i nostri colleghi e concorrenti?
- **Financial quantification:** qual è la posta in gioco finanziaria con la nostra attuale posizione di rischio?
- **Cybersecurity frameworks:** in che modo i nostri risultati si allineano ai framework di sicurezza informatica per il nostro settore?

Uno strumento di reporting efficace dovrebbe rendere le prestazioni di sicurezza comprensibili alla leadership e favorire conversazioni produttive sul rischio informatico. È necessario identificare una soluzione in grado di generare report a livello granulare con dettagli su sistemi compromessi e vulnerabilità, protocolli di sicurezza, rischi relativi al comportamento degli utenti, l'infrastruttura di rete e di dominio. Con un linguaggio comune e una serie di KPI indipendenti e obiettivi, puoi comunicare meglio con la leadership.

Come BitSight può aiutarti

BitSight Security Ratings ti consente di misurare le prestazioni del tuo programma di sicurezza nel tempo e di aumentare la responsabilità.

Aggiornate quotidianamente, le valutazioni di sicurezza BitSight ti consentono di identificare e classificare le aree di rischio per la sicurezza informatica critiche o sproporzionate nell'ambito della tua impronta tecnologica. Forniamo una misurazione indipendente, basata sui dati e dinamica della posizione di sicurezza informatica della tua organizzazione, che è correlata alle prestazioni finanziarie. Questo contesto e visibilità ti consentono di affrontare i problemi più urgenti e ottenere risultati positivi.

BitSight aiuta le organizzazioni a misurare i rischi, a proteggersi da perdite di entrate e danni alla reputazione e a comunicare efficacemente le aree di miglioramento. In breve, forniamo le informazioni necessarie per apportare miglioramenti continui al tuo programma di sicurezza informatica. ■

Conosci davvero il tuo perimetro? Un efficace approccio alla Cyber Exposure.

Autore: **Andrea Rossini e Daniele Nicita**

Sempre più insistentemente si parla di Cyber Exposure e di Attack Surface Management, come se fossero concetti nuovi, mai affrontati in precedenza.

In realtà, i responsabili di sicurezza hanno ben chiaro in mente il loro significato e l'importanza di questi concetti per la Security Posture. Quello che si nota negli ultimi mesi, però, è un aumento della difficoltà di gestione di queste problematiche, anche da parte di chi è già abituato da tempo a doverle fronteggiare. Questo trend

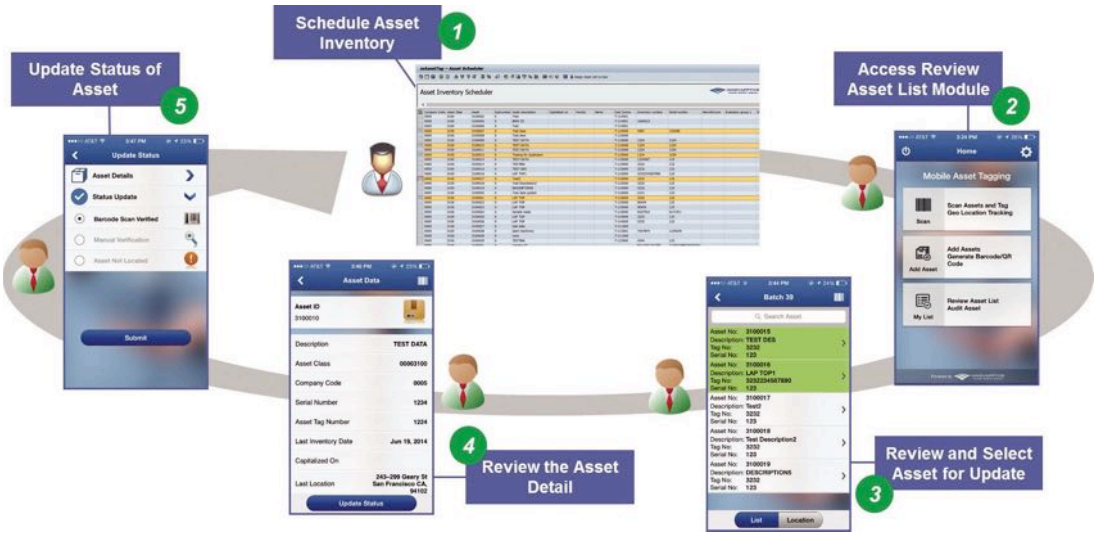
era, dunque, presente anche nel recente passato, ma i cambiamenti delle abitudini lavorative degli ultimi mesi hanno determinato un notevole mutamento dei loro contenuti e delle attività correlate.

Satya Nadela, il CEO di Microsoft scrisse nell'ormai "lontanissimo" Aprile del 2020 di aver vissuto "2 years of digital transformation in 2 months"[1]. Oggi, a un anno e mezzo di distanza, il vecchio concetto di Attack Surface Management risulta, quindi, ormai definitivamente obsoleto.

Shilpi Handa, nell'articolo "The Essential Elements of Effective Vulnerability Management"[2] pubblicato da Gartner nell'ottobre 2020, spiega bene cosa sia cambiato per le varie organizzazioni: la maggior parte delle aziende dispone ormai di complesse interconnessioni tra server, istanze cloud, desktop, laptop, dispositivi mobili, Internet of Things (IoT) e altro ancora, cioè di una rete di difficile monitoraggio di risorse dinamiche, in continuo movimento, e spesso delocalizzate. Tutto ciò, ovviamente, ha determinato un aumento del rischio di esposizione a minacce esterne all'organizzazione. Mantenere un inventario accurato delle risorse è quindi fondamentale per qualsiasi solido programma di sicurezza informatica. Altrettanto fondamentale la necessità di estendere il Vulnerability Management anche a questo inventario.

Digital transformation e Asset Inventory sono, quindi, le tematiche da cui partire per comprendere le nuove problematiche in ambito di Cyber Exposure. La Digital Transformation ha cambiato profondamente e molto velocemente il modo in cui le organizzazioni si espongono all'esterno (Cyber Exposure) e i meccanismi finora utilizzati per la gestione di questo rischio, tra cui i processi e le soluzioni di Inventory Management e di Vulnerability Management, non sempre sono riusciti ad adattarsi con la stessa velocità.

Cyber Exposure - Cybersecurity Trends



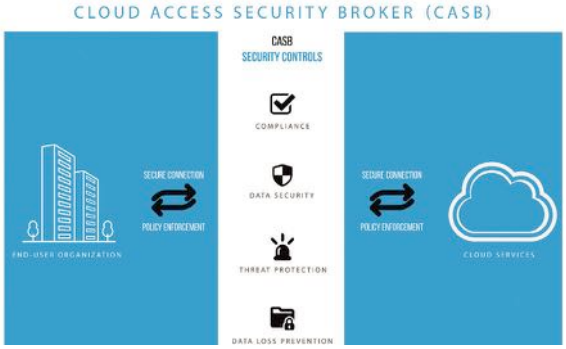
Cosa è cambiato all'interno e all'esterno delle organizzazioni?

Come ben sappiamo le organizzazioni sono state costrette ad accelerare i propri progetti di Digital Transformation e il movimento verso il cloud ha senz'altro guidato questo trend. Ciò ha comportato nuove problematiche per la Cyber Security:

- Come mantenere aggiornato in tempo reale il proprio inventario delle istanze cloud.
- Come applicare i controlli e le policy di sicurezza in queste istanze.
- Come rilevare nuovi asset, non solo nel cloud, creati al di fuori degli account preposti.

Per fronteggiare tali problematiche sono emerse diverse soluzioni di cloud security suddivise da Gartner in 3 grandi macro-soluzioni:

- CASB (Cloud Access Security Broker), la cui implementazione è strettamente correlata all'istituzione di policy di governance e rappresenta un buon



primo passo, ma che non risolvono il problema delle implementazioni cloud non autorizzate.

- CWPP (Cloud Workload Protection Platform), efficaci per proteggere i dati all'interno di strumenti SaaS basati su cloud, ma non sufficienti ad identificare le infrastrutture IT nascoste (es. istanze cloud di sviluppo e collaudo).

- CPSM (Cloud Security Posture Management) in grado di monitorare se i dipendenti aderiscono alle policy, ma solo per le istanze cloud note.

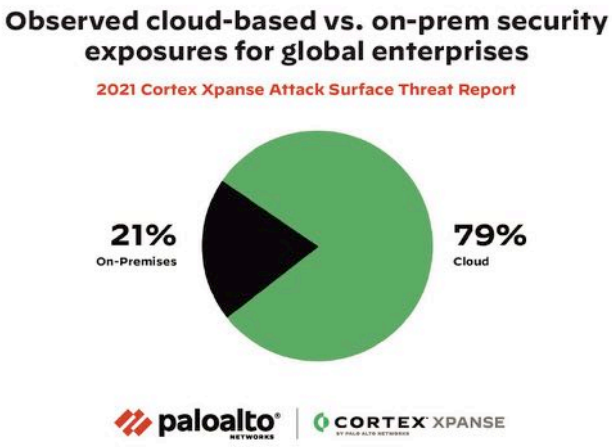
Queste soluzioni hanno come limite di agire esclusivamente su quanto è noto a priori.

Il processo di Cloudification, tuttavia, non è l'unico trend a impattare sulla Cyber Exposure, anche se è da solo responsabile del 79% dei problemi più critici riscontrati.

Bisogna infatti considerare anche che, con la massiva e improvvisa adozione dello Smart Working, molte risorse aziendali, pensate per lavorare in reti interne, sono entrate nel perimetro della Cyber Exposure.

A livello aziendale si assiste inoltre a un proliferare di servizi esternalizzati, o comunque non gestiti direttamente dalla IT, distribuiti su diversi provider di hosting. La Cybersecurity deve esserne a conoscenza, in modo da gestirli e soprattutto adeguarli agli standard di conformità e sicurezza. Governare la propria Supply Chain è quindi un altro aspetto da considerare, e poco importa che si tratti di asset gestiti da terze parti o meno, le aziende devono ora tenerne obbligatoriamente conto.

Nell'immaginario collettivo, tutte le organizzazioni hanno piena conoscenza della propria struttura IT, ma a causa di questi trend ciò non corrisponde necessariamente al vero.



I team di sicurezza devono applicare standard e policy di governance anche a risorse che non vedono e non sanno di possedere. In termini di sicurezza, questo si traduce nel peggior incubo di un CISO: una superficie di attacco effimera che in caso di violazione costringe ad ammettere davanti al consiglio di amministrazione che non si era a conoscenza delle risorse compromesse. Secondo le nostre analisi, anche le organizzazioni con programmi di vulnerability management estremamente maturi sono in grado di identificare solo l'80% circa della propria superficie di attacco.

Se da un lato il contesto in cui ci troviamo ad operare ha reso sempre più complesso e difficile per le aziende tenere sotto controllo il proprio perimetro, dall'altro ha reso più semplice ed economico per gli hacker ricercare e sfruttare le vulnerabilità.

Le risorse computazionali sono diventate così poco costose che oggi basta spendere circa $10 per affittare la potenza del cloud computing necessaria per effettuare una scansione dell'intero Internet alla ricerca di sistemi vulnerabili. Da analisi e rilevazioni effettuate dal team Cortex Xpanse di Palo Alto Networks, si osserva che in una giornata tipo gli hacker effettuano scansioni una volta ogni ora, mentre le aziende più organizzate possono impiegare anche settimane. L'assioma per cui la sicurezza di un'infrastruttura equivale a quella del suo anello più debole è sempre valido e gli attaccanti sono alla costante ricerca di questo anello.

Un esempio eloquente è quanto visto accadere subito dopo la pubblicazione della vulnerabilità Zero-day relativa a Microsoft Exchange annunciata il 2 Marzo 2021 da Microsoft: in quel caso gli attaccanti hanno avviato delle scansioni entro cinque minuti dall'annuncio.

Situazioni analoghe si presentano mediamente ogni 12 ore, non necessariamente legate a zero-day ma anche a problemi di configurazione, ad accessi remoti non sicuri (RDP, Telnet, SNMP, VNC, ecc.) o a servizi che non dovrebbero essere esposti (Database, SNMP, interfacce di amministrazione, IoT, ambienti di sviluppo, ecc.). Vivere con un nuovo problema ogni 12 ore evidenzia la natura effimera dell'IT di oggi.

BIO

Andrea Rossini ricopre il ruolo di System Engineer Specialist per le soluzioni Cortex di Palo Alto Networks. Con oltre 20 anni di esperienza nel mondo della Cyber Security ha ricoperto diversi ruoli come Consultant, Business Unit Manager, System Engineer e Solutions Architect in società di consulting e multinazionali del settore. Grazie a questo esteso background di esperienze si è altamente specializzato nell'analisi e progettazione di soluzioni di Cyber Security, comprendendo come fornire soluzioni di sicurezza e coniugare le esigenze del business. Nel corso degli ultimi anni si è fortemente specializzato in tematiche di Cyber Resilience ed Incident Response. Andrea si è laureato in Informatica presso l'Università Statale di Milano dove ha successivamente conseguito il Master in ICT Security e possiede inoltre le certificazioni ISC2 CCSP, ITIL e CompTIA Security+.

BIO

Daniele Nicita è Cortex Systems Engineer Specialist per Italia, Malta e Grecia. Nell'agosto 2019 entra a far parte della divisione Cortex di Palo Alto Networks con il compito di sviluppare e supportare i Team locali. Daniele inizia la sua esperienza nel mondo della Cyber Security oltre 20 anni fa ricoprendo diversi ruoli in diverse multinazionali, sia a livello italiano sia internazionale, sempre focalizzate sul mondo della Sicurezza Informatica e soprattutto sulla gestione degli Incidenti e sulla Threat Intelligence.

Quanto conta essere proattivi?

Diventa quindi fondamentale introdurre un nuovo KPI denominato MTTI - Mean Time to Inventory. MTTI misura il tempo necessario alle organizzazioni per eseguire un inventario completo delle risorse, esterne e interne, e assegnare ad esse una classificazione basata sulla criticità. MTTI diventa particolarmente critico quando viene annunciato un nuovo CVE.

Le organizzazioni utilizzano già metriche simili per misurare l'efficacia della propria sicurezza informatica come, per esempio, il tempo di permanenza (Dwell Time), il tempo medio di rilevamento (MTTD) o tempo medio di risposta (MTTR). Tuttavia, queste misurazioni sono di natura intrinsecamente reattiva e concentrate di conseguenza solo su asset già conosciuti e oggetto di un incidente informatico.

La domanda da cui partire diventa quindi: come facciamo a proteggere qualcosa che non sappiamo di avere?

La questione non è puramente teorica ma reale, visto i diversi casi accaduti in cui si evidenzia che la velocità di identificazione sarebbe stata un'efficace garanzia di protezione dalle minacce.

Tra Dicembre 2020 e Febbraio 2021 Accelion ha pubblicato diversi CVE e relative patch per rispondere a una serie di vulnerabilità emerse nella propria soluzione Accelion File Transfer Appliance (FTA). A partire da Febbraio 2021 sono stati resi noti molteplici data breach che hanno sfruttato queste vulnerabilità principalmente da parte del threat actor Clop/FIN11[3]. Nonostante la soluzione Accellion FTA fosse dichiarata legacy dal produttore, era ancora utilizzata attivamente dal 25% dei loro clienti come repository pubblico di dati critici e sensibili. Anche oggi, dopo diversi mesi, data breach legati a questo problema continuano a emergere. La pubblicazione di sistemi vulnerabili non opportunamente patchati o in EOL è considerato uno dei primi 3 problemi elencati nella ASM Top 10 Exposures[4].

A Marzo 2021 Microsoft ha annunciato di aver identificato diverse vulnerabilità presenti sulle versioni di Microsoft Exchange Servers on-premises e di aver riscontrato il loro sfruttamento attraverso exploit di tipo zero-day da parte del threat actor Hafnium[5]. Identificare e mettere in sicurezza tutte le istanze pubbliche di Microsoft Exchange Server è diventata la priorità per tutte le aziende e organizzazioni.

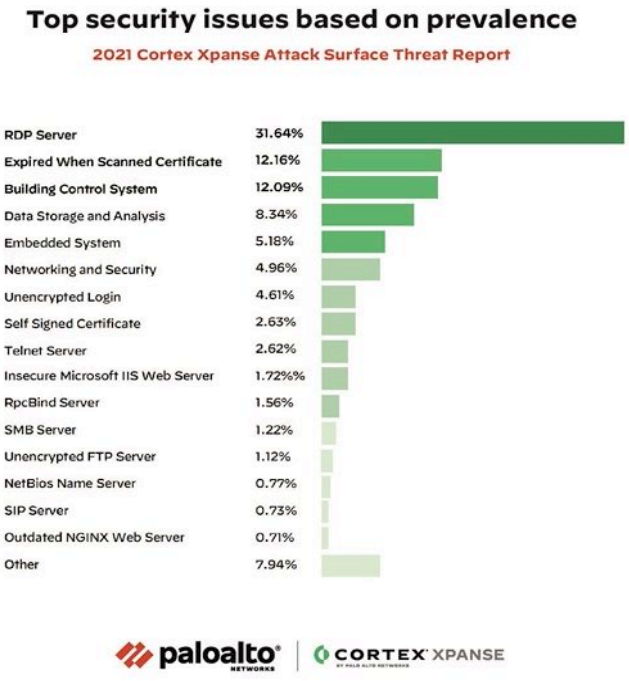
Infine a Luglio 2021 Kaseya ha comunicato ai propri clienti che la propria soluzione di remote monitoring e management Kaseya VSA esponeva una vulnerabilita zero day che era stata utilizzata per veicolare ransomware dal famoso gruppo hacker REvil[6]. In questo caso gli attaccanti hanno sfruttato una vulnerabilità zero-day per bypassare l'interfaccia di autenticazione ed eseguire codice arbitrario sul server Kaseya VSA, di fatto distribuendo agli

endpoint il ransomware grazie alle funzionalità di software distribution offerte nativamente dal prodotto. Anche in questo caso, poter avere un immediato riscontro sui propri sistemi Kaseya esposti e quindi sfruttabili per attacchi avrebbe dovuto essere la base per un adeguato piano di protezione.

Da questi esempi si evince che la corsa ad aggiornare tutti i propri sistemi risulta essere una gara persa in partenza, se non si è adeguatamente preparati e organizzati.

Oltre al tema noto delle vulnerabilità, bisogna considerare anche la problematica relativa alla pubblicazione di strumenti di accesso remoto non sicuri o adeguatamente protetti, considerati al primo posto nella classifica pubblicata da ASM Top 10 Exposures[7].

A tal proposito, il protocollo RDP (Remote Desktop Protocol) è considerato il vettore iniziale di attacco ransomware più popolare ed è stato utilizzato per anni. La divisione Unit 42 di Palo Alto Networks ha studiato i dati di oltre 1.000 incidenti e ha scoperto che nel 50% dei casi di distribuzione di ransomware, RDP era il vettore di attacco iniziale[8]. Se a ciò aggiungiamo il fatto che l'RDP rappresenta il 30% delle esposizioni totali[9] e che, dal primo trimestre 2020 (pre-COVID-19) al secondo trimestre 2020 (post-COVID-19), le esposizioni RDP sono aumentate del 59% tra tutti i fornitori di servizi cloud[10], è facile comprendere le motivazioni per cui viene ritenuto così critico.



È estremamente facile, infatti, esporre RDP involontariamente, lasciandolo su un sistema dimenticato, su un istanza cloud, su un dispositivo precedentemente protetto dai firewall aziendali, o collegando il proprio device direttamente a Internet. Lasciare RDP aperto equivale, quindi, a permettere a chiunque di accedere al proprio sistema come se fosse fisicamente di fronte alla tastiera.

Essendo tecnicamente possibile scansionare l'intero Internet in soli 45 minuti, se RDP fosse esposto, questo verrebbe tempestivamente trovato da malintenzionati e sottoposto ad attacchi di tipo Credential Theft, Brute Force o Man-in-the-middle.

Per questi motivi RDP viene oggi anche simpaticamente chiamato Ransomware Deployment Protocol.

Come affrontare queste nuove sfide?

Oggi più che mai, la maggior parte dei principali obblighi di compliance richiede un requisito fondamentale: mantenere e aggiornare continuamente il proprio inventario delle risorse.

Dato il presupposto che, nella migliore delle ipotesi, quelle conosciute rappresentano solo l'80% di ciò che si possiede effettivamente e dato il contesto descritto in continua rapida evoluzione, risulta necessario oggi occuparsi anche e soprattutto delle proprie risorse esposte esternamente.

Innanzitutto si deve partire dall'individuazione di ciò che si ha esposto esternamente, creando e tenendo sempre aggiornato un inventario completo che includa:

- Dispositivi IoT e sistemi utilizzati per il remote working, asset che spesso mancano di una protezione di sicurezza sufficiente.
- Infrastrutture cloud, che vengono attivate e disattivate con un ritmo molto rapido.
- Sistemi in gestione a terze parti, di cui è difficile monitorare la compliance.
- Certificati, indirizzi IP, servizi e protocolli di comunicazioni, classificati dagli standard come rischiosi.

Parafrasando il noto detto «Non puoi migliorare ciò che non puoi misurare», e portandolo in un contesto più attinente alla cyber security, si potrebbe dire "Non puoi proteggere ciò che non sai di possedere": mantenere questo inventario in una moderna infrastruttura tecnologica in continuo cambiamento ed evoluzione è un compito impossibile per un essere umano. Richiede, quindi, un sistema ed un approccio automatizzato, sia per scoprire risorse sconosciute sia per garantire la sicurezza.

Tradizionalmente, la mappatura delle risorse sulla rete di un'organizzazione è sempre stata un'attività fortemente manuale, soggetta a inevitabili errori, soprattutto se gestita tramite un foglio di calcolo in carico ad IT. D'altra parte, in passato, per scansionare Internet per determinare la struttura e la topologia delle proprie risorse erano necessari mesi. Tutto è cambiato nel 2013: i nuovi algoritmi hanno consentito la scansione globale di Internet a una velocità 1.500 volte più alta rispetto al passato. Oggi, sono necessari meno di 45 minuti per comunicare con ogni singolo IP pubblico

nello spazio IPv4 (4,3 miliardi di IP) su una singola coppia porta-protocollo. Per metterlo in prospettiva, il tempo necessario per guardare un episodio della tua serie preferita.

Le moderne soluzioni di Attack Surface Management (ASM) tengono conto di tutto ciò per fornire un inventario completo di tutte le risorse (indirizzi IP, domini, certificati, risorse cloud e on-prem) e mappare la responsabilità interna all'organizzazione per ciascuna risorsa.

Dato che gli hacker possono scansionare l'intera Internet alla ricerca di sistemi vulnerabili in meno di un'ora, i difensori devono tenere il passo e garantire che il loro tempo medio di inventario (MTTI) sia più veloce di quello degli aggressori.

Non sapendo a priori dove sono gli asset di una azienda, le soluzioni di ASM devono scansionare e analizzare la totalità di internet. La difficoltà e, quindi, il valore della soluzione, diventa la capacità di attribuire una risorsa, magari esposta dietro a un indirizzamento di una adsl domestica, di un fornitore esterno oppure di un cloud provider pubblico, a una specifica organizzazione.

Per ottenere questo processo di attribuzione è necessario creare un link tra ogni asset identificato e il relativo proprietario. Per fare ciò non è sufficiente basarsi sulla proprietà di uno specifico range di indirizzi IP, ma è necessario analizzare certificati, informazioni, comunicazioni di questi asset e molto altro.

Vista l'enormità dei dati da analizzare e le tempistiche strette richieste, si rende quindi necessario l'utilizzo di algoritmi di machine learning e artificial intelligence a supporto di una corretta e pronta attribuzione.

Piu in generale, una soluzione di ASM dovrebbe anche supportare il processo di riduzione della superficie di attacco di un'organizzazione, in modo che le risorse possano essere aggiornate, disattivate o segregate da Internet così da non essere più bersaglio degli aggressori.

Un corretto processo di ASM dovrebbe iniziare dunque con la scansione dell'intero spazio IPv4 per individuare tutte le risorse connesse alla rete internet e procedere poi con la successiva attribuzione automatica in real time alla specifica azienda. In caso di individuazione di risorse precedentemente sconosciute, il processo dovrebbe proseguire associando correttamente la risorsa e inviando apposita notifica all'azienda, al team o alla persona individuata come responsabile della protezione di tale risorsa.

Lo step successivo e altrettanto fondamentale consiste nel verificare la conformità dell'inventario fin qui rilevato alle policy specifiche di ogni singola azienda e alle best practice di mercato, così da trasformare un semplice elenco di asset in una lista actionable di rischi da gestire.

Una volta avuta la corretta visibilità sui rischi rilevati si potrà passare al processo di mitigation degli stessi, sfruttando l'integrazione con soluzioni di SOAR, patch management, vulnerability management, cloud security posture management e quant'altro.

È evidente che avere un corretto processo per la gestione della Cyber Exposure è essenziale, ma è altrettanto essenziale avere gli strumenti adeguati a supporto di tale processo.

Un servizio che sia di reale supporto al processo di ASM dovrebbe fornire:

- Un unico repository di informazioni automatizzato e continuamente aggiornato per tutte le risorse connesse a Internet.
- La corretta associazione degli owner a tutte le risorse precedentemente individuate, conosciute e sconosciute.
- Tutte le esposizioni e i relativi rischi.
- L'integrazione con i processi di Incident Response aziendali, automatizzando la risoluzione dei rischi e il reporting degli stessi.
- Il monitoraggio continuo della rete internet per scoprire, valutare e mitigare i rischi man mano che la superficie di attacco cambia.

Palo Alto Networks ha vissuto in prima persona i cambiamenti imposti dalla Digital Transformation e dal Flex Working e si è subito attivata per gestire la propria Cyber Exposure.

All'interno del Security Operation Center questa problematica è dunque ben conosciuta da tempo ed è stata gestita sfruttando l'integrazione tra le soluzioni Cortex XSOAR e Cortex XDR insieme alla soluzione Cortex Xpanse (ex Expanse).

CORTEX XPANSE BY PALO ALTO NETWORKS

Per illustrare il proprio approccio alla problematica, Palo Alto Networks organizza appositi incontri dove è possibile confrontarsi con le funzioni CISO e SOC interne per discutere insieme delle scelte effettuate e delle soluzioni adottate. ■

1 https://www.microsoft.com/en-us/microsoft-365/blog/2020/04/30/2-years-digital-transformation-2-months/
2 https://www.gartner.com/en/documents/3991384/the-essential-elements-of-effective-vulnerability-manage
3 https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident
4 https://attacksurfacetop10.com/top-ten-exposures
5 https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
6 https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details
7 https://attacksurfacetop10.com/top-ten-exposures
8 https://www.paloaltonetworks.com/resources/research/2020-unit42-incident-response-and-data-breach-report
9 https://start.paloaltonetworks.com/asm-report
10 https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-1h21

Cyber exposure: dalle vulnerabilità alla valutazione dei rischi.[1]

Autore: **Giancarlo Butti**

Non è sufficiente individuare quale sia il proprio perimetro di esposizione e le relative vulnerabilità. È anche fondamentale individuare quali siano i reali rischi ai quali è esposta una organizzazione.

Quali sono le regole che consentono, una volta definito il perimetro da analizzare, di individuare quelli che sono i rischi ai quali un'organizzazione è esposta?

Il percorso è lungo e in questo articolo ci soffermeremo ad analizzarne solo una parte, al fine di dare evidenza della complessità dello stesso e di come, di conseguenza, sia sempre fondamentale nella fase di analisi e ancor più nella fase di esposizione dei risultati, documentare dettagliatamente tutte le scelte effettuate, le regole applicate, i modelli e le semplificazioni utilizzate.

Purtroppo quest'ultimo aspetto è decisamente poco curato e nella maggior parte dei casi ci si trova di fronte a delle analisi dei rischi nelle quali vengono esposti solo dei risultati, senza essere in grado di individuare quale sia stato il processo che ha portato a tali valutazioni e per quale motivo siano state effettuate le scelte che le hanno determinate.

Sia la ISO 31010, sia il NIST 800 30 R1 elencano una serie di elementi che determinano il livello più o meno elevato di incertezza[2] che caratterizza un'analisi dei rischi ed è quindi importante avere coscienza dei limiti che caratterizzano qualunque tipo di analisi al fine di dare il giusto peso ai risultati ottenuti.

Il livello di incertezza è ancora maggiore se il processo viene svolto automaticamente, ad esempio mediante strumenti di intelligenza artificiale che, nella maggior parte dei casi, operano come delle black box, non consentendo nemmeno a chi ha sviluppato il sistema, di comprendere realmente come si comporta l'algoritmo individuato dalla rete neurale.

Tutto ciò è vero tranne se al posto dei tradizionali sistemi di machine learning non si utilizzino, ad esempio, sistemi neuro fuzzy[3]. Questi sistemi combinano le tecniche delle reti neurali con quelle della logica fuzzy, permettendo di sviluppare sistemi trasparenti che non solo consentono di visionare l'algoritmo elaborato, ma anche di intervenire sul medesimo per ottimizzarlo, sia tramite un intervento diretto dell'analista, sia ad esempio mediante algoritmi genetici.

Documentare il percorso che ha portato a una valutazione del rischio è fondamentale. Ciò permette di effettuare una corretta valutazione di quali siano gli effetti delle eventuali contromisure messe in atto per fronteggiare i rischi che sono stati individuati o per valutare l'evoluzione della situazione nel tempo, in conseguenza di eventi esterni (nuove minacce, nuove

BIO

Giancarlo Butti ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano.
Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, whitepaper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN, Università degli studi di Milano.
Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali e una decina on line. Ha pubblicato 21 fra libri e whitepaper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT…
È socio e proboviro di AIEA, socio del CLUSIT e di BCI. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico e GDPR di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti, SOC, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR.
È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/ IEC27001, CRISC, ISM, DPO, CBCI, AMCBI.

vulnerabilità…) o interni di un'organizzazione (nuovi apparati del sistema informativo, variazioni nelle configurazioni, variazioni di versioni…).

Sarebbe, infatti, necessario per una corretta valutazione, procedere con un'analisi del tutto simile a quella eseguita in precedenza per quanto attiene alle scelte e ai modelli utilizzati; ma se questi elementi non sono documentati, o se l'analisi viene svolta in automatico senza possibilità di decodifica dell'algoritmo utilizzato, sarà difficile effettuare un reale confronto fra i risultati…

Ma veniamo all'oggetto principale di questo articolo.

Qual è il ruolo delle vulnerabilità nell'ambito di un'analisi dei rischi?

Il rischio è legato alla possibilità che una minaccia, sfruttando una vulnerabilità, produca un danno. Ogni asset è soggetto a specifiche minacce, che possono in genere attuarsi sfruttando vulnerabilità intrinseche nell'asset stesso. Spesso le vulnerabilità sono identificabili con l'assenza di qualcosa.

Consideriamo un esempio di minaccia molto intuitivo, anche se non riguarda il mondo cyber, quale può essere un terremoto:

- un edificio costruito senza criteri antisismici presenta una specifica vulnerabilità verso quella minaccia
- se l'edificio è costruito in una zona dove la minaccia di un terremoto è nulla anche il rischio sarà nullo.

La valutazione delle vulnerabilità è quindi strettamente connessa alle minacce. L'identificazione delle vulnerabilità può prendere in considerazione la reale situazione dell'asset (con eventuali misure di sicurezza già in essere) oppure può essere effettuata senza considerare la presenza di alcuna misura di sicurezza (rischio inerente o intrinseco).

Secondo il **NIST SP 800 30** una minaccia è qualsiasi circostanza o evento che potrebbe avere un impatto negativo su operazioni e beni di un'organizzazione e sulle persone, attraverso un sistema informativo (accesso non autorizzato, distruzione, divulgazione o modifica delle informazioni e / o negazione del servizio).

Gli eventi di minaccia sono causati da fonti di minaccia.

Le fonti di minaccia sono caratterizzate da:

- una volontà e una modalità con cui sfruttare una vulnerabilità (nel caso di attacchi volontari)
- una situazione e un metodo che possono sfruttare accidentalmente una vulnerabilità negli altri casi.

La minaccia è quindi un'azione volontaria, involontaria o un evento accidentale che, sfruttando una vulnerabilità, provoca un danno.

La valutazione della probabilità che un evento di minaccia possa avere delle conseguenze può essere effettuata con varie modalità.

La più semplice è quella di demandare tale valutazione direttamente all'analista, che in base alla propria esperienza e alla eventuale presenza di dati storici[4], valuta qual è la probabilità che una determinata minaccia abbia effetti sull'oggetto di analisi (un asset, un servizio, un processo… in funzione del modello utilizzato).

Altre metodologie introducono elementi di valutazioni più strutturati, che distinguono il tipo di minaccia (volontaria, accidentale…) e introducono ulteriori parametri per la valutazione che permettono di ottenere un risultato più preciso e ripetibile.

Ad esempio il **NIST Special Publication 800-30 Rev 1** propone una valutazione organizzata in 3 fasi:

- in primo luogo, viene valutata:
  - nel caso di minaccia di tipo deliberato, la probabilità che eventi di minaccia siano messi in atto da parte di un attaccante
  - nel caso di minacce accidentali, la probabilità che eventi di minaccia si verifichino
- in secondo luogo, viene valutata la probabilità che gli eventi di minaccia, una volta messi in atto o verificatisi, comportino effettivamente degli impatti negativi sugli asset/processi dell'organizzazione
- infine, viene valutata la probabilità complessiva come una combinazione delle due precedenti secondo lo schema qui riportato.

Più dettagliatamente per quanto attiene gli atti deliberati, una valutazione della probabilità di accadimento si basa sulle caratteristiche di chi porta avanti l'attacco:

- le sue capacità e competenze
- le sue intenzioni
- i suoi obiettivi.

Al riguardo, il **NIST (800 30 RV1)** propone le tabelle D3, D4, D5, G2 qui riportate.

Per eventi diversi dagli atti deliberati (G3), la probabilità che l'evento si verifichi si stima utilizzando:

- dati storici
- dati empirici o
- altri fattori.

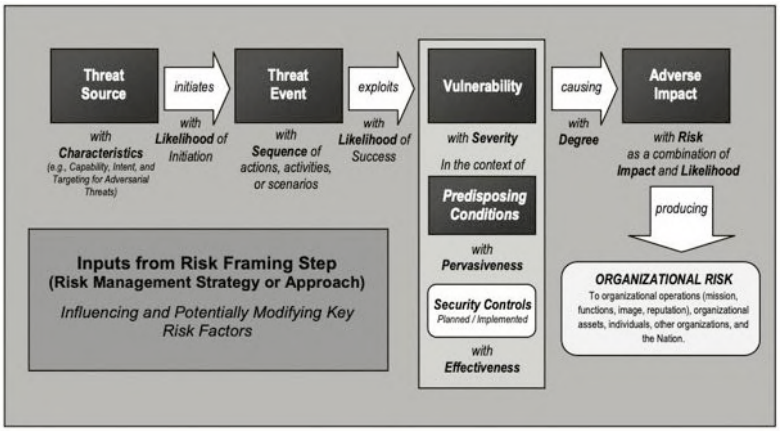


TABLE D-3: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year.**
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year.**
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year.**
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years.**
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years.**

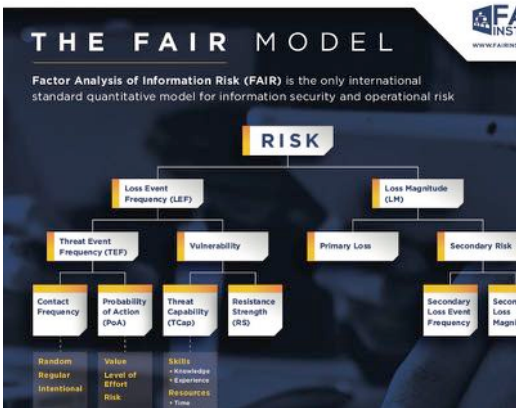
TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

La tabella G4 indica la probabilità che un evento, una volta avviato, possa provocare effettivamente un danno e la tabella G5 indica la probabilità complessiva[5].



Di analogo tenore è la metodologia proposta dal **FAIR (Factor Analysis of Information Risk),** che pur subendo una evoluzione nel tempo ha mantenuto un approccio analogo.

Nella versione del 2005, ad esempio, la metodologia FAIR valutava la probabilità di un evento come dipendente da un lato dalla Threat event frequency (a sua volta dipendente da Contact ed Action) e dall'altro dalla Vulnerability (a sua volta dipendente da Control Strenght e da Threat Capability).

Nella versione del 2015 la terminologia è leggermente cambiata per cui la Frequenza di minaccia è una funzione di Frequenza di contatto e Probabilità di attacco, mentre la Vulnerabilità è una funzione di Capacità di attacco e Azione di contrasto.

I parametri presi in considerazione dal NIST e da FAIR sono quindi leggermente diversi, ma entrambe le metodologie amplificano la possibilità di stimare in modo più oggettivo i parametri che entrano nella valutazione.

La metodologia proposta dal NIST è essenzialmente di tipo qualitativo o semiquantitativo, mentre FAIR è caratterizzato da un approccio quantitativo e quindi sta riscuotendo sempre più estimatori.

Un altro aspetto particolarmente importante da prendere in considerazione, nella costruzione della propria metodologia di analisi dei rischi, riguarda la complessità (o all'opposto le semplificazioni introdotte) nel modello che rappresenta la realtà della organizzazione che si sta analizzando.

È evidente che ogni asset ha le sue vulnerabilità ed è caratterizzato da una specifica criticità legata al suo ruolo nel contesto aziendale; ne deriva che un server che eroga un servizio in produzione è molto più critico di un server utilizzato per lo sviluppo o test.

Ma in entrambi i casi questi componenti non sono elementi isolati, ma fanno parte di una struttura complessa e soprattutto con interazioni molto articolate fra loro.

La corretta rappresentazione della correlazione fra asset e fra servizi/processi da essi supportati non è affatto semplice ed è, oltretutto, molto dinamica.

La complessità della relazione fra gli asset è ben illustrata ad esempio dalla **metodologia Magerit (Methodology for Information Systems Risk Analysis and Management),** di cui esponiamo alcuni paragrafi specificatamente dedicati a tale argomento.

MAGERIT V.2
The dependency between assets

The only concern is whether asset A depends, significantly, on another asset B. In other words, dependency between assets is a Boolean value: yes or no.

$A \rightarrow B$

The dependency can be transitive:

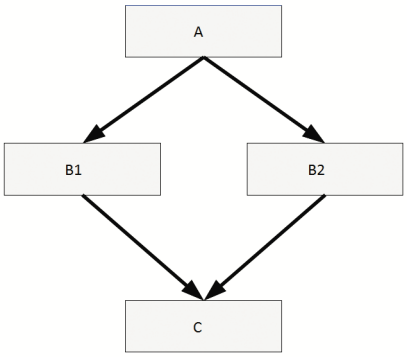
$(A \rightarrow B) \wedge (B \rightarrow C)$

A depends on B; B depends on C.

It can even be represented as a diamond shape:

$(A \rightarrow B_1) \wedge (A \rightarrow B_2)$ $(B_1 \rightarrow C)$ $(B_2 \rightarrow C)$

A depends on B1 and B2; B1 and B2 depends on C.



The transitive closure of direct dependencies between assets is of interest.

A C B, (A B) (B C)

A depends (indirectly) on C if and only if there is an asset B, so that A depends directly or indirectly on B and B depends directly on C.

The following does not differentiate between direct and indirect dependencies.

It must be established whether asset A depends on asset B, and to what extent. The concepts of direct or indirect dependency stated in the qualitative model are applied, but now the dependency is rated by a coefficient between 0.0 (independent assets) and 1.0 (assets with absolute dependency). This coefficient is called the degree of dependency.

As the dependency can be direct or indirect, it is calculated on the basis of the transitive closure of the direct dependencies between assets.

A C B, (A B) (B → C)

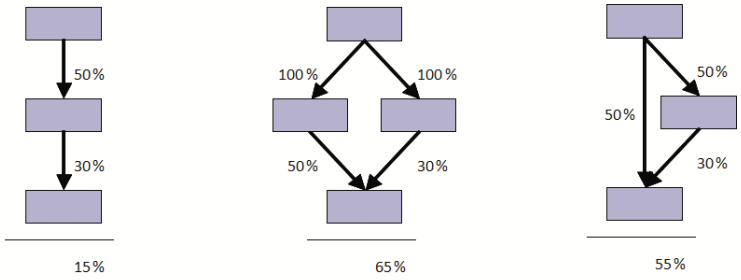
A depends (indirectly) on C if, and only if, there exists an asset B so that A depends directly or indirectly on B, and B depends directly on C.

By calculating the degree of dependency as:

Degree (A C) = Σi { degree (A Bi) × degree (Bi → C) } Where the sums are carried out following this formula:

a + b = 1 − (1 − a) × (1 − b)

Examples



Consideriamo ad esempio il fatto che, sfruttando una determinata vulnerabilità, un server che supporta un processo considerato non critico sia reso indisponibile.

Le conseguenze a prima vista potrebbero essere considerate di lieve entità.

Consideriamo ora il caso in cui il processo alimenti realmente un processo critico. È evidente che l'indisponibilità di tale server, se prolungata, farà sentire i suoi effetti anche sul processo critico che dipende indirettamente dal suo funzionamento.

Quindi mappare correttamente i processi, i sottostanti assest e le correlazioni fra tutti gli elementi è fondamentale per dare il giusto peso ai vari componenti del sistema informativo e calibrare, di conseguenza, le priorità degli interventi in un'ottica di ottimizzazione costi/benefici.

Un modello semplificato della propria organizzazione, che non prenda in adeguata considerazione le correlazioni esistenti, perde quindi molto della sua effettiva capacità di rappresentazione del rischio e di conseguenza, operando con budget e risorse limitate, aumenta la possibilità di effettuare scelte sbagliate.

CONCLUSIONI

La corretta valutazione dei rischi è fondamentale per indirizzare correttamente le priorità nelle azioni correttive da intraprendere, ma requisito fondamentale affinché questo avvenga è che siano adeguatamente documentate in fase di analisi dei rischi:

- le scelte effettuate
- la metodologia scelta
- il perimetro di indagine
- la completezza
- l'accuratezza con cui si è svolta l'analisi dei rischi
- il dettaglio del modello con cui sono descritti gli asset da analizzare e le loro correlazioni. ■

1 Parte del testo è tratto e adattato dal libro: G. Butti – A. Piamonte - **Governance del rischio Dall'analisi al reporting e la sintesi per la Direzione**
https://www.iter.it/prodotto/governance-del-rischio-dallanalisi-al-reporting-e-la-sintesi-per-la-direzione/

2 Si veda in proposito: G. Butti - **I rischi nell'analisi dei rischi: gli errori da evitare per rendere fruibile e ripetibile l'analisi effettuata**
https://www.cybersecurity360.it/legal/privacy-dati-personali/i-rischi-nellanalisi-dei-rischi-gli-errori-da-evitare-per-rendere-fruibile-e-ripetibile-lanalisi-effettuata/

3 Si vedano in proposito: G. Butti - **Intelligenza artificiale e soft computing nella lotta al terrorismo**
https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/intelligenza-artificiale-e-soft-computing-nella-lotta-al-terrorismo.html
G. Butti – Lorenzo Schiavina - **INTELLIGENZA ARTIFICIALE E SOFT COMPUTING. APPLICAZIONI PRATICHE PER AZIENDE E PROFESSIONISTI**
https://www.francoangeli.it/Ricerca/scheda_libro.aspx?id=24187

4 L'utilizzo di dati storici, in particolare per la valutazione della probabilità di accadimento di un evento, nasconde delle insidie e pertanto è necessario valutare attentamente quale sia la profondità storica con cui utilizzare tali dati.
Questa non è assoluta, ma va determinata per ogni singola tipologia di evento, considerando il contesto di riferimento.
Ad esempio, una serie di incidenti di sicurezza derivanti dal malfunzionamento di un apparato o dalla mancanza di contromisure, non possono essere presi in considerazione se nel frattempo l'apparato è stato sostituito ovvero se sono state implementate delle contromisure.
Non ha quindi senso definire a priori di prendere in considerazione tutti gli eventi anomali ed incidenti registrati, né che si prendono in considerazione solo quelli degli ultimi 6 mesi.
Deve essere, infatti, presa in considerazione la serie storica di eventi che ha ancora valore, cioè che è applicabile ad una situazione (ad esempio un componente del sistema informativo) che non è stata cambiata nel tempo.

5 Si rinvia al documento originale del NIST per una trattazione completa.

Futures Literacy: conoscenze e tecnologie ecco il binomio del futuro.

Intervista VIP a Franco Amicucci.

Autore: Massimiliano Cannata

Viviamo nell' "infosfera" una dimensione, per usare una definizione di Luciano Floridi in cui tutti siamo immersi. On life è uno stato, una condizione ibrida che ci vede perennemente connessi. Cambia il modo di essere nel mondo per dirla con Heidegger, ma anche e soprattutto il modo di apprendere. Dott. Amicucci, lei ha una grande esperienza sul terreno della docenza e della formazione, come ci si deve orientare in questa società complessa e altamente tecnologizzata?

Il tema del sapersi orientare coinvolge ogni persona e ogni organizzazione, perché viviamo un'epoca caratterizzata da continue ondate di cambiamento che ci proiettano, di volta in volta, in territori nuovi e inediti per l'esperienza umana. Territori nuovi che necessitano nuovi alfabeti, nuove chiavi di lettura e interpretazione, un apprendimento continuo, come ci sta richiedendo, ad esempio, l'onda della rivoluzione digitale. Orientarsi, quando si è pienamente immersi nelle trasformazioni in atto, non è facile. Abbiamo bisogno di aver chiaro il proprio posizionamento

e possedere un sistema con alcuni punti di riferimento. Non siamo più quelli che eravamo, i cittadini dell'epoca industriale, e non abbiamo ancora acquisito una chiara identità di cittadini dell'infosfera, che sanno muoversi agilmente nella dimensione ibrida fisica e digitale.

Tra il non essere più e il non essere ancora, dove ci collochiamo dunque?

In una terra di mezzo, tipica dell'adolescenza, oscilliamo tra entusiasmi,

BIO

Franco Amicucci è sociologo, formatore, docente. Autore di diverse pubblicazioni, tra le quali "La formazione fa Spettacolo" – Il Sole24ore e "Boundaryless Learning", a cura di Franco Amicucci e Gabriele Gabrielli (Franco Angeli). Nel 2017 è stato eletto CEO della Formazione (premiazione LeFonti Awards). Tra le varie esperienze, Amicucci ha insegnato Sociologia della Comunicazione all'Università di Macerata e collaborato con Luiss Business School e docente del Consorzio Universitario Nettuno, con lezioni televisive su RAI2 nei 2000 e 2001. Ha fondato skilla.com, prima eLearning company italiana. Con oltre 40 anni di esperienza nella formazione in Italia, ha operato nelle principali organizzazioni e multinazionali italiane, da Confindustria a FCA, Rai, Leonardo, Sisal, Cisl, Telethon e centinaia di organizzazioni.

quando scopriamo l'apparente onnipotenza della rete, e la paura di non farcela, di non essere all'altezza del nuovo mondo. Edgar Morin, uno dei giganti del pensiero contemporaneo, ci è venuto in aiuto con la metafora dell'arcipelago, il nuovo vissuto dei moderni navigatori della conoscenza, che non hanno più la certezza della terra ferma, ma possono fare riferimento a tante isole di certezza, quelle che troviamo durante la navigazione a mare aperto. Tra le isole di certezza utili oggi alle persone e alle organizzazioni, mi piace mettere il tema delle nuove competenze necessarie per vivere nella società digitale, come la competenza dell'apprendere per tutto l'arco della vita, la cultura e la competenza digitale, il pensiero critico, l'adattabilità e la flessibilità cognitiva. Queste sono solo alcune delle competenze che scuole e aziende dovranno mettere al centro dei programmi.

La pandemia, scrive nel suo interessante saggio "Apprendere nell'infosfera" (ed. Franco Angeli), ha accelerato molti processi. Cosa ci ha insegnato questa esperienza e quali sono le sfide che le imprese devono affrontare nell'era post covid?

La pandemia ha accelerato tutti i processi di innovazione che erano già in atto e ora abbiamo una consapevolezza collettiva su alcuni di questi, come lo smart working e le nuove forme di apprendimento in modalità digitale. Per le imprese le sfide sono molte e il rischio che sta emergendo è quello di vivere le nuove sfide in modo difensivo con la cultura del "c'è un cambiamento che ci coinvolge, vediamo come affrontarlo per ridurne i danni e sopravvivere". Questa è la cultura di chi vive il cambiamento come un incidente di percorso, che passerà per poi ritornare alle abitudini consolidate, atteggiamento che alcune organizzazioni stanno assumendo per lo smart working e la didattica digitale. La maggior parte delle organizzazioni, per fortuna, sta cogliendo gli impulsi di innovazione vissuti per pensare al futuro, ai nuovi modelli organizzativi che dovranno essere sempre più agili, dimostrando di possedere un DNA aperto e flessibile, capace di assorbire il continuo divenire che segna la contemporaneità.

Come apprendere nell'infosfera

Sta mutando il lavoro e soprattutto le competenze aziendali. Quale mission dovrà avere la formazione manageriale e di quali strumenti dovrà dotarsi per rafforzare l'efficacia dei messaggi educativi e la stessa qualità dei contenuti?

L'Unesco indica come prioritaria una nuova competenza, definita *futures literacy*, che richiama ogni ruolo di responsabilità a operare per un futuro sostenibile per le organizzazioni e la società ed essere protagonisti attivi dei cambiamenti costanti, veloci ed esponenziali che ci circondano. Per questo è fondamentale riuscire a comprendere come sarà il futuro che ci aspetta e quale potrà essere il ruolo da giocare in esso.

Per ogni manager la *futures literacy* consiste nella capacità di saper combinare le conoscenze e le tecnologie che ci aiutano a comprendere il presente e a indirizzare ogni scelta, alimentati da immaginazione "e visioning", che deve essere orientata ad adattare, attrezzare, potenziare le organizzazioni alla sfide del futuro. Utilizzare il futuro per innovare il presente, sfruttare al meglio le infinite possibilità della nostra epoca, che è la più ricca della storia non scordiamocelo, per opportunità di apprendimento.

La formazione manageriale, in questo scenario evolutivo, è quella che più di ogni altra, ha le potenzialità di cavalcare le opportunità di apprendimento presenti nell'infosfera, grazie alla possibilità di praticare un apprendimento prevalentemente esperienziale, continuo, tra formale e non formale.

La tecnologia rende ancora più impegnativo il compito della formazione manageriale?

L'apprendimento manageriale si sta basando sempre più sulla capacità di elaborare dati, costruire reti di relazioni arricchenti, riflettere sui trend e gli scenari evolutivi, fare benchmark sulle migliori pratiche organizzative e manageriali presenti a livello nazionale e internazionale. A fronte di questo scenario credo che l'innovazione più importante sarà quella di acquisire, da parte del management di ogni organizzazione, un diverso *learning mindset,*

che comporta la consapevolezza che l'apprendimento continuo e pervasivo è uno dei fattori strategici per il successo della propria organizzazione.

Il primo formatore è il manager stesso, che forma con il suo stile di leadership, la sua comunicazione, la sua modalità di coinvolgimento ogni presa di decisione.

Il tempo, diceva Sant'Agostino se non mi chiedono cosa sia conosco la definizione, se mi chiedono che cosa è rimango spiazzato. Lei parla di modalità sincrona e asincrona riferendosi all'apprendimento in modalità virtuale. Può spiegare di che si tratta?

Per modalità sincrona intendiamo la classica modalità d'aula, dove docente e allievo sono in relazione nello stesso momento. Quella che comunemente viene chiamata Dad, Didattica a Distanza erogata con la modalità del webinar, attraverso piattaforme ormai comuni nel linguaggio delle aziende e delle scuole, come Teams, Webex, GoogleMeet e altre è sempre una modalità sincrona, un'aula a distanza, con docente e allievi distanziati fisicamente.

La modalità asincrona è invece lo studio di corsi online in autonomia, senza la presenza del docente, con lo studente o lavoratore che si collega, quando ne ha la possibilità, durante l'orario di lavoro o fuori orario, a un sito web speciale, chiamato piattaforma e-Learning o LMS – Learning Management System e accede con username e password personale. La piattaforma terrà traccia del suo studio, degli orari di fruizione, dei test superati quando previsti, come un vero e proprio registro digitale. Ma il

concetto di tempo ci richiama a un altro cambiamento in atto, molto importante.

Quale, può essere più esplicito?

Nella nostra epoca l'apprendimento non è più un processo lineare, cumulativo, misurato in anni di studio e ore di formazione, che potremmo identificare come una forma di "Chrónos formativo", ma sta evolvendo verso un processo basato su rotture e salti di paradigmi, dove il saper disapprendere, creare dei vuoti, è sempre più necessario per acquisire rapidamente nuove abilità, culture, modelli di riferimento, che in questo caso potremmo definire come il "Kairós dell'apprendimento", dove la persona apprende dalle esperienze più significative che possono essere anche attimi che aprono nuove finestre sul mondo, da successi ed errori, dalla capacità di fare domande alla sua rete di relazioni, alla grande biblioteca ipertesto che è il web e di saper filtrare, riorganizzare, dare valore alla conoscenza per poi rimetterla in circolazione.

La rivoluzione intelligente

Lo Smart working è in questo momento al centro di molte attenzioni e di molte polemiche. A questa modalità si affianca lo Smart e-learning, può dirci qualche cosa in più in proposito?

La pandemia ha fatto esplodere lo smart working per tutta quella parte del mondo del lavoro svincolata dai processi operativi che richiedono presenza, che in Italia, secondo di dati del World Economic Forum, rappresenta circa il 38% della popolazione lavorativa. Ricordiamoci sempre che la maggioranza dei lavoratori non ha avuto questa possibilità.

Il dibattito attuale è tra chi considera lo smart working come una pratica emergenziale, per poi tornare a lavorare come prima, e tra chi la considera come nuova modalità che trasformerà per sempre le relazioni e la cultura del lavoro. Personalmente propendo su questa seconda posizione. Va poi detto che insieme allo smart working le organizzazioni hanno visto l'accelerazione della digitalizzazione dei processi lavorativi, come i digital tool e i sistemi di video conferencing, insieme ad una forte accelerazione della modalità di apprendimento in ambienti virtuali, che possiamo definire in smart learning. Durante il periodo di utilizzo massivo della smart working, le stesse persone hanno sperimentato nuove modalità di apprendimento, che erano già familiari per le aziende ad alta intensità di lavoro intellettuale, mentre altri settori erano molto lontani da questo orizzonte, per motivi facilmente comprensibili.

Adesso l'onda prevalente porta alla "restaurazione". Dopo l'emergenza torneremo in ufficio riportando indietro le lancette della storia?

Sono emersi tanti problemi in questa fase, inutile negarlo. Per un paese come l'Italia, invecchiato e a bassa cultura digitale, il tema delle infrastrutture e delle competenze digitali sono importanti e decisive per il futuro del lavoro, perché, tra le principali criticità che hanno ostacolato e ostacolano il pieno utilizzo dello smart working, la carenza di cultura e competenze digitali e di infrastrutture tecnologiche adeguate sono risultate evidenti e da superare rapidamente. Ma sono emersi anche tanti vantaggi, come quelli di un maggior equilibrio vita familiare e lavoro, flessibilità, maggior autonomia, minori costi in tempo e costi di trasporto. La preoccupazione per la perdita di socialità è comune alle persone e alle imprese ed è questo uno dei punti di maggior attenzione in questa fase. Forti delle lezioni apprese e delle competenze acquisite, si stanno introducendo nuove pratiche organizzative e percorsi formativi finalizzati al mantenimento della socialità, al miglior uso del tempo e della programmazione del lavoro che permettano al tempo stesso il diritto alla disconnessione delle persone per un miglior equilibrio vita lavorativa e vita privata oltre a una migliore produttività. Infine, appare urgente non solo dalla prospettiva delle aziende, una nuova attenzione al benessere psicologico e alla resilienza delle persone per attraversare questo periodo, che si prospetta lungo e difficile.

Intelligenza artificiale, big data, blockchain che impatto hanno sull'apprendimento?

Siamo solo agli inizi, ma già si intravede, dalle prime esperienze in atto, un nuovo mondo che presto sarà familiare. Quando navighiamo in internet o facciamo ricerca su Google, le nostre attività vengono tracciate, veniamo profilati in forme sempre più raffinate, i nostri dati vanno ad alimentare un enorme mole di dati e così riceviamo pubblicità, comunicazioni, notizie sulla base dei nostri interessi e gusti. Dietro questi processi c'è il mondo dell'intelligenza artificiale, il mondo dei big data. Proviamo ora ad immaginare di utilizzare questi ambienti, ormai familiari, per l'apprendimento, sfruttando a nostro vantaggio quello che ora viviamo in negativo, come invasione della nostra privacy e condizionamento occulto. Ma, come tutte le energie, la responsabilità delle conseguenze non è dell'energia, ma dall'uso che se ne fa. Immaginiamoci allora di offrire a ogni bambino, a ogni

giovane, a ogni lavoratore, una formazione sempre più personalizzata, che segua i suoi interessi, i suoi gusti, le sue attitudini, quando serve, dove serve e che questa modalità lo accompagni per tutta la vita, dove al posto della pubblicità, la persona riceverà consigli, informazioni, messa in contatto con il miglior esperto della sua squadra, del mentor più adatto per i suoi bisogni, suggerimenti di community con interessi comuni, guide e tutorial a disposizione ogni volta che si affronta un nuovo problema o un nuovo lavoro. Poi, man mano che la persona acquisisce competenze, nuove abilità, nuove conoscenze, queste verranno riconosciute, certificate e validate in blochchain. Si tratta di "pesare" una diversa moneta, la moneta intellettuale che rappresenterà il bene più prezioso per la persona, non svalutabile!

La "frontiera mobile" della sicurezza informatica

La nostra rivista è focalizzata sulla cyber security. La formazione di questo delicato ambito quali linguaggi e strumenti deve utilizzare per essere al passo con i tempi di una trasformazione scientifica e tecnologica rapida e per molti versi sconvolgente?

La formazione sulla cyber security, come tutti i saperi che richiedono non solo la conoscenza, ma anche l'attivazione di comportamenti coerenti,

generalizzati nell'insieme dell'organizzazione, richiede un apprendimento profondo, una memoria corporea che porti a comportamenti automatici, che garantiscano la sicurezza del comportamento in ogni condizione psico-fisica e ambientale. Per arrivare a questo non sono sufficienti i classici corsi in aula o in e-learning, ma bisogna attraversare e riattraversare il dominio disciplinare della cyber security con una molteplicità di linguaggi, attività, prove, esperienze, ripetizioni, test per arrivare all'acquisizione di saperi che garantiscano comportamenti con elevati standard di sicurezza. È inoltre fondamentale la continuità degli apprendimenti nel tempo, non basta aver superato dei test una volta, ma la formazione con queste modalità che si definiscono "immersive" deve essere ricorrente.

Una parte del suo saggio è dedicata a un territorio di applicazione poco noto, il micro-learning. Di che cosa si tratta?

Quando su YouTube ricerchiamo una nuova ricetta o informazioni su un paese che vogliamo visitare e consultiamo il tutorial di 5 minuti, stiamo utilizzando un oggetto di apprendimento in *micro-learning,* un trend che si impone sempre di più sulla scena dell'apprendimento. Possiamo definirlo come una metodologia che fa riferimento a un processo di granularizzazione dell'apprendimento per mettere a disposizione unità di contenuto piccole e autoconsistenti, componibili in percorsi personalizzati. Dal punto di vista didattico è più facile apprendere un contenuto breve alla volta, che tanti contenuti erogati di seguito, come avviene nella classica giornata formativa di 8 ore in aula. Nell'infosfera il micro-learning emerge come uno dei linguaggi emergenti, una modalità che va di pari passo con l'affermarsi delle APP di apprendimento e dello smartphone come strumento utilizzato sempre più anche nella formazione. Ad esempio, la nuova generazione che ora sta gestendo Skilla, la società che fondai nel 2000, ha creato una APP, Digital Journey, per formare le competenze digitali delle persone delle grandi organizzazioni, compresa la competenze della cyber security, basata sul *micro-learning,* con un impegno richiesto di 3 – 4 minuti al giorno di formazione, tutti i giorni dell'anno. Stiamo parlando di "App" che si avvalgono di sistemi di intelligenza artificiale per formare con un'alta personalizzazione del percorso formativo processi di *gamification* e partecipazione delle persone nel creare esperienze sempre più coinvolgenti.

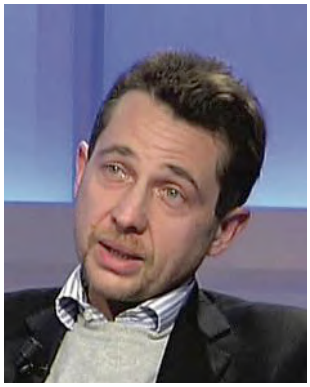
La sua ricerca si conclude aprendo il sipario sulle "sfide aperte". Può tratteggiarne qualcuna anche ai nostri lettori?

Per la scrittura del libro ho coinvolto e intervistato quattordici persone, provenienti da mondi diversi, manager d'azienda, imprenditori, studenti, startupper, insegnanti, agricoltori, un monaco benedettino, per farmi

raccontare come si aggiornano nella quotidianità, quali mondi stanno scoprendo e quali difficoltà incontrano. Da questi racconti emerge che stiamo vivendo, nell'infosfera, tante nuove opportunità e tante nuove problematiche, tensioni da vivere, se ben gestite, come generative. Ad esempio, è comune oscillare tra entusiasmo e preoccupazione, dove da una parte abbiamo l'entusiasmo quasi adolescenziale per le tante esperienze possibili, dall'altra la preoccupazione di non farcela, di essere emarginati se si rimane indietro con l'aggiornamento. Un'altra sfida è quella data dal rischio di chiudersi in cerchie chiuse, omogenee, rassicuranti, ma tendenti all'isolamento, spesso vicine alla cultura delle sette. Una tensione comune è data dalla connessione continua, che apre il tema della ricerca di un nuovo stile di comportamento, che sappia mettere in equilibrio vita lavorativa e vita privata, connessione e distacco. La tensione tra fiducia e controllo è presente in ogni ambito dell'esistenza, e va ben gestita anche nei due mondi di cui abbiamo parlato, quello dello smart working e quello dell'auto-apprendimento in smart learning, perché se si lavora senza la presenza del capo e si studia senza la presenza dell'insegnante, nuovi valori dovranno regolare i rapporti. La fiducia è uno di questi. Credo, infine che dobbiamo dare un senso a queste sfide e per questo ho concluso il testo con una frase che si trova all'ingresso di una scuola in un villaggio sperduto della Nigeria: "il sapere è, e deve essere visto, come una forma di felicità. Una delle poche felicità a cui può aspirare il genere umano". ■

La "grande convergenza" sarà il tema dei prossimi anni.

Intervista VIP a Alessandro Curioni.



Autore: Massimiliano Cannata

In questa delicata fase di trasformazione sociale ed economica che sta cambiando il volto delle nostre città la sicurezza è sempre più al centro dell'attenzione. Quello che colpisce è la rapidità crescente e la sofisticazione con cui gli attacchi cyber mettono a rischio le organizzazioni complesse. Lei ha recentemente pubblicato il giallo "Il giorno del bianconiglio" (ed. Chiarelettere), si tratta di un progetto che presenta più facce (probabilmente diventerà una serie Tv). Da quale molla è stato spinto?

Questo romanzo nasce da un'idea improvvisa legata a un fatto di cronaca che risale alla fine del 2015, quando circa 80 mila abitanti di Kiev restarono al buio a causa di un attacco informatico alla rete elettrica. Al momento pensai che qualcuno avrebbe potuto scriverci un libro, poi alcuni amici mi convinsero che l'autore potevo essere io. Detto questo è innegabile che rientra nella mia idea di divulgazione quella di stimolare la riflessione sul tema da parte di un pubblico sempre più vasto e, se parliamo di libri, la narrativa è di gran lunga il genere che vanta il maggior numero di lettori.

Guardiamo all'attualità. Il recente attacco alla Regione Lazio è solo l'ultimo di una catena di eventi che ha riguardato partiti politici, infrastrutture critiche, strutture sanitarie. Cosa dobbiamo apprendere da questi fenomeni, destinati a ripetersi in quella che definiamo società del rischio?

La prima e più importante lezione che ci offre un caso come quello della Regione Lazio deve essere la consapevolezza di come un incidente che si verifica nel mondo digitale sia in grado di produrre effetti devastanti anche in quello reale. La seconda si può sintetizzare in una semplice affermazione: "nessuno è al sicuro". Da un lato accanto ai casi mediaticamente rilevanti se ne verificano decine di cui non si ha notizia, dall'altro il più oscuro fornitore di una grande organizzazione può essere la testa di ponte ideale per colpire il "pesce grosso".

La cyber security, come dimostra la recente creazione di un'agenzia nazionale, ha assunto un valore strategico. Quali iniziative vanno messe in campo per rafforzare le capacità di difesa degli stati, particolarmente esposti all'azione di criminali ben organizzati e senza scrupoli?

Mi permetta una provocazione: a questo punto sarebbe opportuno passare dalla strategia all'azione. Continuare a dire che è indispensabile un'azione a livello internazionale o fare dichiarazioni di principio sulla cooperazione tra questo e quel paese non basta più. La cosa più importante

è stata probabilmente l'iniziativa normativa riguardante le infrastrutture critiche, un passaggio importante che tuttavia richiede ulteriori affinamenti. In primo luogo, la creazione di un meccanismo di *information sharing* tra gli attori coinvolti, che non può dipendere dalla buona volontà dei singoli o dai rapporti di amicizia che legano diversi security manager. Altro aspetto decisivo, evitare di avere una situazione a due velocità che porterebbe inevitabilmente lasciare indietro le PMI e le piccole pubbliche amministrazioni trasformandole in vittime designate. Questo vale non solo per l'Italia, ma anche per qualsiasi altro paese.

Il Cloud di stato

Il ministro Colao ha proposto la creazione di un "Cloud di stato" per aggregare competenze e azioni strategiche di cyber security. Cosa pensa di questa iniziativa?

Potrebbe avere il vantaggio di standardizzare il livello di protezione di tutte le realtà che usufruiranno dei suoi servizi, ma per contro potrebbe

BIO

Alessandro Curioni (1967). Dopo 15 anni di attività giornalistica, alla fine degli anni Novanta, inizia a occuparsi di nuove tecnologie e nel 2001 si dedica a tempo pieno alle tematiche della sicurezza informatica. Nel 2003, dopo due anni di studio, pubblica per Jackson Libri il volume "Hacker@ tack - Guida alla sicurezza informatica". Da questa esperienza nasce, in collaborazione con il Gruppi I. Net (in seguito British Telecom) un programma di corsi di formazione dedicati a quelle tematiche. All'attività di formatore affianca quella di consulente per i clienti del gruppo I.Net, attività che si protrae fino al 2008, anno in cui fonda DI.GI. Academy, azienda specializzata nella formazione e nella consulenza nell'ambito della sicurezza informatica, della quale è azionista e presidente. Negli ultimi quindici anni è stato consulente per primarie aziende nazionali e multinazionali tra le quali Edison S.p.A., Cardif Assicurazioni del Gruppo BNP Paribas, Vittoria Assicurazioni, Pepsico Italia, attività che alterna con quella di formatore (ENI, Poste Italiane, A2A, etc.) e conferenziere. Nel 2015 riprende la sua attività pubblicistica per diverse testate cartacee - tra cui «Il Sole 24 ore» (compresi gli allegati sul tema) - e on line e nel 2016 pubblica, con la casa editrice universitaria Mimesis, il libro "Come pesci nella rete – Guida per non essere le sardine di Internet" dedicato a problemi della sicurezza informatica personale, a cui seguono diversi altri pamphlet di successo («La privacy vi salverà la vita», «Questa casa non è un hashtag», "CyberWar" etc) mentre con Chiarelettere ha pubblicato nel 2021 il suo primo giallo intitolato «Il giorno del Bianconiglio». Dal 2018 Curioni è anche docente a contratto nel corso di sicurezza dell›informazione per la Cattolica di Milano.

diventare un pericolosissimo *"single point of failure"*: un attacco che avesse successo potrebbe azzerare la capacità operativa dell'intero apparato statale. Come sempre a fare la differenza sarà l'esecuzione del progetto.

Prevenire, come è noto, dovrebbe essere molto meglio che curare. Vi sono best practice e metodiche cui i manager della sicurezza possono fare utilmente riferimento?

La corretta valutazione del rischio cyber è il vero "Sacro Graal" del settore. Riuscire nell'impresa permetterebbe di aumentare di ordini di grandezza la capacità di prevenzione e di allocare in modo efficace ed efficiente le risorse. La difficoltà che al momento sembra

insormontabile non è tanto nel metodo o nelle modalità con cui il rischio viene analizzato, valutato e gestito perché esistono framework e best practices anche molto raffinate, ma in quello che si trova a monte. Mi riferisco alla raccolta delle informazioni necessarie e alla qualità del dato. In buona sostanza il problema è l'input. Facciamo un confronto con un'altra attività di valutazione del rischio: la polizza furto in ambito automobilistico. Nel definire il premio le assicurazioni partono da basi dati molto precise, articolate che permettono di stabilire un dato soggetto, che utilizza una certa vettura in una specifica località a quale livello di rischio è soggetto. Questo per la semplice ragione che tutti i furti di auto vengono denunciati in modo circostanziato. Quelle stesse informazioni viceversa non esistono rispetto ai furti di dati. Pochi denunciano e spesso quelli che lo fanno non sono in grado di fornire anche i dettagli più elementari come il quando e il dove. Alcuni pensano che la soluzione sarà in qualche algoritmo intelligente, ma resta il fatto che senza il supporto di database sufficienti è impossibile perseguire i responsabili.

Strutture come i Cert e i Data Center sono gli asset di difesa utilizzati da molte aziende. Come debbono attrezzarsi per disinnescare tutto quello che avviene nella parte "oscura della rete"?

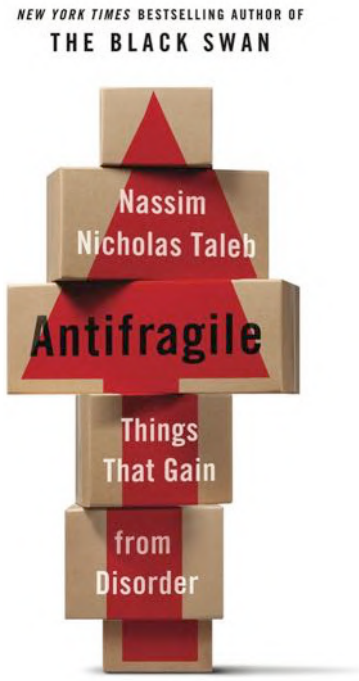
Il problema non è tecnologico, ma riguarda le competenze. Dobbiamo prendere atto che tutte le diverse categorie di professionisti che rientrano nel dominio della cybersecurity sono numericamente inadeguate a fare fronte alle richieste di mercato. Mi limito a citare il caso dello scorso agosto, quando le principali società di cyber security olandesi hanno chiesto un intervento del governo perché non più in grado di gestire tutte le richieste di intervento che arrivavano. Alla fine per disinnescare una bomba ci vuole un artificiere e per il momento non può essere altro che un essere umano, a patto di avere a disposizione gli strumenti adatti, le buone tecnologie, infatti, non mancano.

La fragilità è nel DNA della rete

La debolezza di Internet, ha detto in una recente interessante intervista apparsa sul Corsera, dipende dall'interconnessione di web ed elettricità, mix che rende questa infrastruttura potente ma fragile. Lo sviluppo dell'IOT e dei BIG Data rende ancora più complesso il quadro. I manager della sicurezza quali saperi debbono mettere in campo a fronte di uno scenario in continua evoluzione?

La cosiddetta grande convergenza sarà il tema dei prossimi dieci anni accanto all'utilizzo delle grandi basi e delle intelligenze artificiali. Impossibile

conoscere e tanto meno padroneggiare tutte le tecnologie sottostanti. Credo che un buon manager più che competenze dovrà mettere in campo una particolare "sensibilità" che deve spingerlo a farsi continuamente delle domande. Per esempio: la nuova macchina smart per il vending del caffè che l'azienda ha deciso di installare può essere una minaccia? Ovviamente sì. Ricordiamoci che quando si parla di tecnologia conta "quanto ne sai", se parliamo di sicurezza conta "chi sei".



Il capitale umano rimane l'anello debole della catena. Quali investimenti vanno programmati e quali strumenti utilizzati per rafforzare know how e competenze su questo importante e imprescindibile ambito?

Si tratta di un tema di educazione che non si risolve con un corso aziendale, ma attraverso programmi pluriennali. Non serve infatti addestrare qualcuno all'utilizzo di un software, occorre cambiare il suo modo di pensare e di conseguenza agire. In questo senso serve con estrema urgenza un intervento deciso sul mondo della scuola, la principale agenzia educativa. Introdurre come obbligatoria l'educazione digitale sarebbe un primo passo per creare quella consapevolezza di base sulla

quale poi costruire le capacità critiche necessarie per affrontare la società dell'informazione. Non dimentichiamoci che i ragazzi oggi alle elementari e alle medie saranno quelli che domani gestiranno i centri di controllo delle smart city, dei trasporti automatizzati e via dicendo.

La resilienza è un termine "vigliacco", la definizione provocatoria è di Nicholas Taleb autore di un interessante saggio "Antifragile" in cui sostiene che non bisogna rimuovere le fragilità ma lavorare su di esse per superare ogni atteggiamento difensivo e sfidare la complessità e i processi non lineari. Sul piano non solo e non tanto teorico, quanto squisitamente pratico, il consiglio di Taleb la convince?

La teoria è una grande cosa, ma il passaggio alla pratica è spesso più complesso del previsto. Diciamo che oggi il temine resilienza più che

vigliacco è abusato e spesso utilizzato impropriamente o almeno in modo un po' troppo estensivo. Credo che il tema di Taleb offra qualche importante spunto su riflessioni che poi portano a decisioni e conseguenze molto pratiche. Personalmente, in senso un po' più esteso, faccio spesso riferimento a una pratica che ho chiamato *"problem unsolving"*. Cerco di chiarire con un esempio. Una delle ossessioni che affligge chi si occupa di cyber security è la vulnerabilità. Poche cose ci mettono ansia come la scoperta di un bug in un software o di una lacuna di un protocollo a cui per somma sfortuna corrisponde un exploit. Proviamo a immaginare che la nostra vulnerabilità venga resa inoffensiva modificando la configurazione di un nostro sistema di sicurezza. Il problema non è risolto, ma non è più un rischio. Dopo sei mesi, appare la patch che rimuove il bug. In quel momento si deve prendere una decisione: installarla con il rischio, legato a qualsiasi cambiamento, di introdurre una nuova vulnerabilità della quale non sapremmo nulla, oppure lasciare le cose come stanno? In buona sostanza esiste la possibilità che non tutti i problemi debbano essere risolti e, di conseguenza è possibile che non tutte le fragilità debbano essere rimosse. Rimane piuttosto di importanza fondamentale continuare sempre a farsi domande, non cessando mai di esercitare il dubbio. Per nessuna ragione al mondo, le dico in conclusione, dobbiamo smettere di riflettere. ■

Identificare e rispondere agli attacchi ransomware: 5 domande a cui rispondere.

Autore: Antonio Forzieri

splunk>

Il 2021 è stato un anno particolarmente ricco di notizie e di innovazione da parte dei cyber criminali, soprattutto sul fronte ransomware che ha vissuto un anno particolarmente fertile per gli attaccanti. Uno degli attacchi più dirompenti, da questo punto di vista è stato quello di Kaseya, ancor peggiore di quello di Wannacry, definito giustamente il più grande attacco ransomware della storia, fino al prossimo ovviamente.

Anche in Italia le notizie inerenti attacchi ransomware si sono guadagnate il proprio spazio nel telegiornale in prima serata con l'attacco a Regione Lazio, segno che si tratta di un fenomeno ormai capillare e pervasivo.

Molti sono nuovi e vecchi attaccanti che si alternano sulla scena. Recentemente il gruppo che opera il servizio RaaS (Ransomware as a Service) REvil è tornato operativo dopo una "meritata" pausa di ben due mesi. Forse il tempo necessario per godersi gli incassi e aggiornare la piattaforma o forse solo l'handover da un gruppo a un altro per la gestione della piattaforma RaaS.

Il modello RaaS ha, di sicuro, riscosso molto successo. In tale modello infatti, gli attori operanti la piattaforma e quelli che compiono l'attacco vero e proprio, condividono il profitto dovuto al pagamento del riscatto in caso di attacco andato a buon fine. Lo scenario poi è molto più ampio e articolato: ci sono attaccanti che si "limitano" a compromettere organizzazioni rivendendo poi gli accessi ai gruppi che effettivamente diffondono il payload ransomware, ci sono attaccanti che invece ricercano la collaborazione di un insider dietro, così come ci sono attaccanti che effettuano l'intera operazione in autonomia.

Per coloro che sono interessati a un approfondimento tecnico sull'attacco vi consiglio di dare un occhiata a "REvil Ransomware Threat Research Update and Detections", un blog post del Splunk Threat Research Team.

Negli ultimi due anni, l'84% delle organizzazioni ha subito un grave incidente di sicurezza. Secondo i risultati del rapporto sullo stato della sicurezza di Splunk, più del 30% di questi incidenti erano attacchi ransomware.

Quindi, quali domande dovrebbero porsi le organizzazioni e quali misure dovrebbero intraprendere per prevenire o mitigare la prossima minaccia ransomware?

1. Possiamo difenderci da un attacco ransomware?

Forse. Ma almeno dovremmo provarci.

Molto spesso si è portati a credere che un attacco ransomware avvenga nell'arco di pochissime ore: non c'è nulla di più sbagliato.

Gli attaccanti prima di effettuare la cifratura dei dati hanno bisogno di ottenere accesso all'organizzazione (che abbiamo detto possono

eventualmente acquistare), ottenere un livello di privilegi elevato, avere visibilità della rete, di fare una mappa dell'organizzazione, comprendere il ruolo dei diversi server all'interno dell'organizzazione, trovare i dati rilevanti, i server di backup, capire come il processo di backup funzioni all'interno dell'organizzazione, installare il payload di cifratura sui diversi server che si vogliono colpire e solo alla fine, una volta compreso a fondo l'ambiente in cui si è, effettuare la cifratura dei dati.

Queste attività richiedono settimane, spesso mesi, fino a un anno in alcuni scenari, ed è qui che abbiamo l'opportunità (il dovere direbbero alcuni colleghi) di capire che le cose non stanno andando come dovrebbero.

È capitato che alcuni clienti abbiano rilevato e fermato l'attacco grazie al monitoraggio degli accessi anomali, piuttosto che attraverso il monitoraggio delle anomalie sull'endpoint o sul proprio domain controller, che poi gli ha permesso di intervenire prontamente, evitando impatti decisamente più importanti.

In questo scenario anche gli attacchi alla supply chain giocano un ruolo importante, e nel corso del 2021 abbiamo visto diversi esempi: Codcov e Kaseya, solo per citare di due attacchi con maggiore impatto.

Il nostro report State of Security ha rilevato che il 78% delle aziende si aspetta un altro attacco alla supply chain in stile SolarWinds, ma solo il 23% delle organizzazioni ha rivalutato o modificato le proprie politiche in merito alla gestione del rischio dei fornitori.

2. Abbiamo un piano per rilevare e contenere un attacco ransomware?

Il passo successivo per affrontare la minaccia di un attacco ransomware è definire il piano non solo per rilevare e rispondere al ransomware, ma anche per confermare la resilienza contro gli attacchi ransomware che hanno fatto notizia o sono stati condivisi dai tuoi partner di intelligence.

La creazione del tuo piano di risposta inizia con la comprensione della realtà della tua rete e delle tue risorse. Per effettuare un piano di monitoraggio accurato possiamo utilizzare diversi strumenti, il framework MITRE ATT&CK risulta essere estremamente utile nella definizione di un piano di copertura di use case con conseguente riduzione del rischio: utilizziamolo per definire la nostra strategia e valutare il nostro livello di maturità.

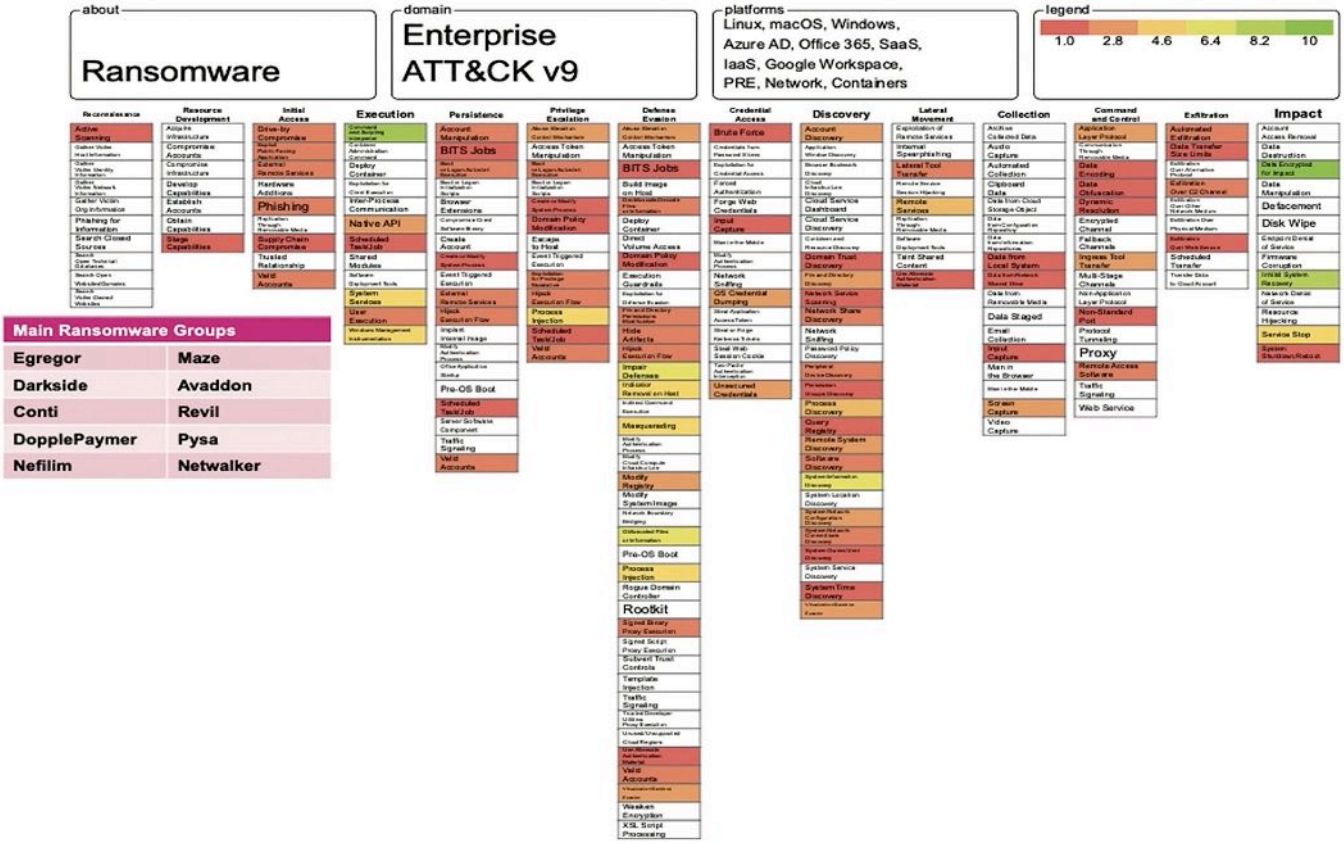
Stiamo monitorando tutto quello che ci serve o abbiamo dei punti ciechi? Abbiamo un processo più o meno automatizzato che verifichi se siamo stati coinvolti da una compromissione di una terze parti?

BIO

In Splunk, Antonio Forzieri (Cyber Security Specialization and Advisory, EMEA) ricopre il ruolo di leader per l'offerta Cyber Security. In precedenza, Antonio ha lavorato per Symantec dove ha ricoperto il ruolo di leader per l'offerta Cyber Security a livello EMEA inizialmente e a livello Global successivamente supportando clienti nella realizzazione di complesse iniziative in ambito Cyber Security che vanno dalla costruzione/evoluzione di Cyber Defense Center fino all'implementazione di Programmi di Cyber Intelligence per clienti pubblici e privati. Prima dell'esperienza in Symantec Forzieri ha lavorato per altre aziende italiane con incarichi svolti in tutta EMEA dove si è occupato di diverse tematiche tra le quali Compliance, Endpoint Security, Data Loss Prevention, Encryption, Ethical Hacking, Analisi Frodi, oltre ad attività di formazione in ambito Security. Tra le attività svolte, Forzieri supporta organizzazioni pubbliche e private in caso di attacchi informatici e frodi.
Antonio Forzieri è laureato in Ingegneria delle Telecomunicazioni al Politecnico di Milano, dove è docente nel corso "Mobilità e Sicurezza delle reti".

Il piano di risposta deve anche considerare quello che va oltre il contenimento tecnico. La risposta al ransomware interessa più processi, livelli di gestione e funzioni all'interno dell'organizzazione, come il ripristino delle operazioni, le comunicazioni interne ed esterne, le decisioni sul pagamento del riscatto, le società di servizi professionali specializzate e altro ancora. Infine, il piano deve essere testato attraverso esercizi tabletop interfunzionali che simulano un attacco ransomware prima che se ne verifichi uno reale.

Per quanto riguarda il rilevamento di ransomware nella tua rete, rilevarlo quando i dati sono cifrati è troppo tardi. Serve un piano di rilevamento che ci permetta di identificare le tecniche utilizzate dai gruppi ransomware PRIMA che i nostri dati vengano cifrati. Per farlo possiamo usare il framework ATT&CK, qui di seguito trovare



un esercizio fatto per i principali gruppi ransomware osservati nel biennio 2019-2021: siamo in grado di rilevare le tecniche utilizzate da questi gruppi? Abbiamo le corrette sorgenti di dati?

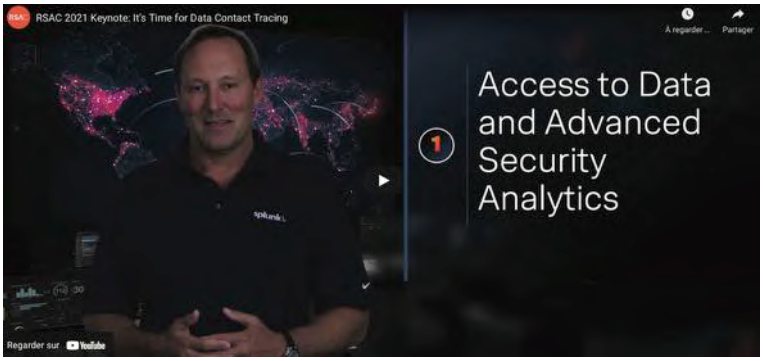
3. Abbiamo accesso ai dati di cui abbiamo bisogno per comprendere l'impatto di un attacco ransomware?

Nel caso che un attacco ransomware vada a buon fine, diventa di vitale importanza comprenderne l'impatto. La risorsa chiave, anche in questo caso, è costituita dalla disponibilità dei dati corretti.

Tutte le tracce di un attacco sono rintracciabili nei dati che collezioniamo col nostro SIEM, come ha giustamente evidenziato Doug Merritt, CEO di Splunk nel suo keynote all'ultima RSA Conference.

Abbiamo la necessità di monitorare accuratamente la nostra infrastruttura al fine di poter comprendere come e fino a che punto un utente malintenzionato sia penetrato nella nostra infrastruttura e sfruttando quali debolezze. Il processo di sicurezza utilizzato non deve infatti solo essere resiliente in caso di compromissione, ma deve permettere di poter apprendere da eventuali compromissioni, quali punti migliorare e quali gap colmare.

Vista la compartecipazione sempre più frequente delle aziende parte della nostra supply chain è anche di vitale importanza comprendere se il servizio che eroghiamo ai nostri clienti sia stato intaccato durante l'esplorazione della nostra infrastruttura da parte dell'attaccante (movimento laterale) e comunicare prontamente ai nostri clienti fornendo eventuali IoC, perché loro stessi possano attivare eventuali servizi di threat hunting.



(vedi la video su: https://youtu.be/M54sxGtKOMg)

4. Quali processi abbiamo posto in atto per assicurarci di evolvere costantemente il nostro approccio?

Gli attacchi ransomware hanno introdotto importanti cambiamenti nel corso del tempo, nel 2021 sono state osservate moltissime innovazioni ed è stato consolidato il passaggio al modello di business RaaS.

Ma se lo scenario ha visto nuovi attaccanti e nuovi modelli di business, le tattiche, le tecniche e le procedure hanno un tasso di cambiamento decisamente più blando.

Abbiamo un processo per monitorare costantemente l'evoluzione delle TTPs per i nuovi gruppi e delle relative detection necessarie per rilevarle? Anche in questo caso l'adozione del framework MITRE ATT&CK ci viene incontro.

Vale anche la pena notare che alcune compagnie assicurative sono sempre più riluttanti a pagare le richieste di ransomware e ci sono richieste più ampie del settore sia alle vittime che alle compagnie assicurative di non pagare i riscatti.

Tutti questi cambiamenti muteranno inevitabilmente il modo in cui le organizzazioni rispondono alle minacce e agli attacchi ransomware.

5. Ci stiamo muovendo abbastanza velocemente?

Per rispondere in modo efficace al ransomware, le organizzazioni devono agire rapidamente per comprendere l'ambito della compromissione e contenere l'incidente. Il tuo tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR) sono fondamentali. Strumenti come Splunk SOAR consentono di agire più velocemente di quanto un umano possa fare doppio clic. Dall'isolamento delle reti al sinkholing di domini dannosi, è fondamentale disporre del giusto livello di automazione della sicurezza per contrastare efficacemente un attacco ransomware.

Prepararsi per l'inevitabile prossimo attacco

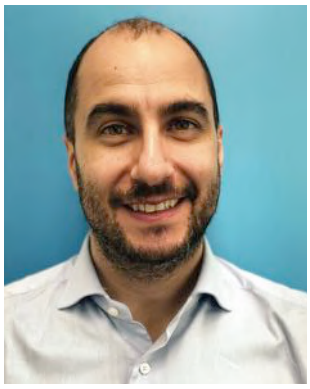
Gli attacchi ransomware non stanno scomparendo. Le organizzazioni devono porre domande difficili su quanto siano preparate a rilevare questo tipo di attacchi e a rispondere. Riconoscere la minaccia rappresentata dai ransomware e costruire un approccio data driven adottando framework di riferimento a livello internazionale è la migliore possibilità che abbiamo per affrontare questa minaccia in continua evoluzione.

Attacchi come Kaseya e Codecov e SolarWinds ci ricordano di assicurarci che le nostre organizzazioni siano preparate per un attacco.

Il team di security researcher di Splunk monitora e valuta continuamente i rischi per la sicurezza che nuove e vecchi breach hanno. Quando arriva la notizia di un attacco, agiamo immediatamente per confermare la sicurezza dei nostri sistemi e del nostro codice. Lo abbiamo fatto dopo gli attacchi di SolarWinds e di nuovo durante l'attacco di Kaseya. Lavoriamo anche per confermare costantemente che tutte le nostre patch e i protocolli di sicurezza siano aggiornati.

Sfortunatamente, i ransomware e gli attacchi alla catena di approvvigionamento sono qui per rimanere, motivo per cui tutti noi di Splunk rimaniamo vigili e impegnati a identificare modi in cui possiamo aiutare meglio i nostri clienti, partner e organizzazioni del settore a prepararsi per loro. ■

Come difendersi dal phishing ora che ci apprestiamo a tornare in ufficio.



Autore: Luca Nilo Livrieri, Manager, Sales Engineering - Southern Europe

Durante lo scorso anno il numero di attacchi di phishing sferrati dai cybercriminali è aumentato in modo significativo e la tendenza è destinata a continuare nel 2021. Gli attaccanti hanno approfittato del caos e della confusione provocati dalla pandemia, e questo clima perfetto ha permesso ai cybercriminali di trasformare le campagne di phishing nella loro arma principale. Le campagne, infatti, sono state progettate in modo da fare leva sull'emotività delle persone e su normali tratti umani quali l'avidità, la curiosità, il timore e il desiderio di aiutare gli altri, particolarmente nel contesto di una pandemia. Ora che le aziende si stanno organizzando per riportare in ufficio la loro forza lavoro distribuita, è probabile che i cybercriminali vorranno cogliere l'opportunità di colpire le imprese in un momento di transizione. Prima di occuparci delle minacce, approfondiamo l'argomento del phishing.

Che cosa si intende per phishing?

Il phishing è un attacco informatico in cui il cybercriminale utilizza e-mail, SMS, app del cellulare o i social media per stabilire un contatto con la vittima e indurla a condividere dati riservati – come password e numeri di conto – o a scaricare inavvertitamente file malevoli che installano virus. Gli attaccanti si spacciano generalmente per un'entità fidata, come una persona o un'azienda con cui la vittima ha contatti frequenti.

Esistono vari tipi di attacchi di phishing, ma i più comuni sono lo spear phishing (mirato a una sola persona), il pharming (dirottamento della vittima su siti fraudolenti), lo smishing (via SMS), il vishing (via cellulare), il dirottamento delle sessioni, il whaling (phishing in ambito finanziario e di grosse aziende), la clonazione e lo spoofing (falsificazione degli ID dei domini). Le campagne di phishing vengono ideate tenendo conto degli interessi delle vittime oppure sfruttando contenuti e argomenti che tendono a suscitare un qualche tipo di reazione. Ora che le imprese si stanno organizzando per riportare in ufficio la forza lavoro remota, è presumibile che i cybercriminali approfitteranno delle vulnerabilità legate a questa transizione per lanciare un'altra ondata di attacchi di phishing.

Il ritorno in ufficio rappresenta un'opportunità per gli hacker

Nel 2020 la maggior parte delle aziende di tutto il modo ha dovuto adattarsi a una nuova normalità in cui i dipendenti lavoravano in smart working. Per gli addetti alla sicurezza aziendale, questa rivoluzione ha

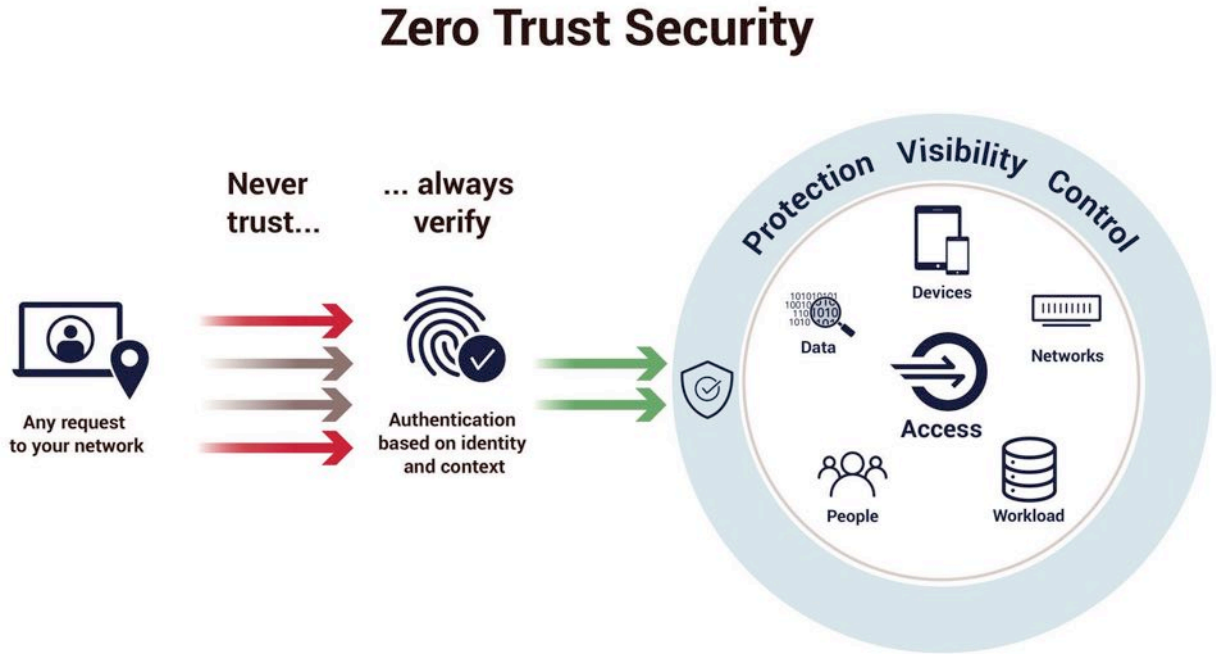
significato elaborare rapidamente nuovi protocolli e procedure per garantire la sicurezza degli endpoint, specialmente perché tanti dipendenti utilizzavano dispositivi personali. Un anno dopo, lavorare con una forza lavoro distribuita geograficamente è diventata la normalità per le aziende, quindi, è probabile che molte di loro continueranno a operare con un modello ibrido, in cui una parte dei dipendenti lavora da remoto in modo permanente o saltuario.

Dover gestire una forza lavoro distribuita e diversificata rappresenta una sfida per i responsabili della sicurezza perché non consente di avere una visibilità completa su ogni endpoint, specie se personale, che si collega ai sistemi e alle reti aziendali. Il ricorso in massa allo smart working ha accelerato l'adozione di applicazioni per il lavoro diffuso che, tuttavia, in ragione dell'urgenza, non sempre sono state esaminate e valutate per attestarne la sicurezza. Per gestire in sicurezza il ritorno in ufficio o l'adozione di un modello lavorativo ibrido, le aziende devono adottare un approccio Zero Trust, ossia una metodologia che monitora e convalida su base continuativa i privilegi di accesso e i diritti degli utenti e dei relativi dispositivi.

BIO

Luca Nilo Livrieri è l'SE Manager di Crowdstrike per il Sud Europa. L'ingresso in Crowdstrike avviene nel maggio 2021, con la responsabilità di seguire lo sviluppo e la crescita della struttura di prevendita nel Sud Europa. Partecipa ormai da parecchi anni come relatore a diversi eventi nazionali e internazionali su privacy, sicurezza, cloud e digital transformation fra cui Security Summit, ISMS forum, IDC e Cybertech. Prima di Crowdstrike, Livrieri è stato manager per l'Italia, la Spagna e il Portogallo della struttura prevendita di Forcepoint. Ha maturato esperienze come membro dell'"Office of the CSO" e Senior SE per il mercato enterprise, e la formazione e affiancamento del canale di rivendita in Websense e Surfcontrol. Prima di svolgere il ruolo di SE ha lavorato come consulente Gfi-Ois per la programmazione web presso alcune importanti aziende italiane.
Precedentemente ha conseguito la Laurea magistrale in Comunicazione nella Società dell'Informazione, con tesi specialistica presso il dipartimento di informatica dell'Università Degli Studi Di Torino.

Il personale che tornerà a lavorare in sede proverà una certa dose di ansia in merito alla salute, all'igiene, alle nuove misure, alle disposizioni sul distanziamento sociale ecc. e rappresenta un bersaglio ghiotto per nuove



campagne di phishing. Formare il personale sui principi della cybersicurezza e sui comportamenti sicuri che mettono al riparo dalle truffe informatiche – che possono colpire quando si lavora da casa, sui mezzi pubblici o in ufficio – sarà fondamentale perché permette di essere aggiornati sulle nuove minacce e proteggere se stessi e i dispositivi personali e aziendali da attacchi informatici.

Che cosa ci ha insegnato il 2020

L'incertezza generata dalla pandemia ha spaventato le persone e le ha spinte a cercare risposte. I timori legati alla diffusione del virus sono stati abilmente sfruttati per le intrusioni mirate e la tematica COVID-19 è diventata un'esca per le campagne di phishing. Le persone cercavano spasmodicamente informazioni e rassicurazioni da parte della propria azienda, del governo, degli operatori sanitari e di altri specialisti. In un contesto del genere, immaginiamo di ricevere un'e-mail che sembra provenire da una di queste fonti e che annuncia importanti novità sul COVID-19. È verosimile che un'e-mail di questo tenore non venga esaminata attentamente ed è qui che, con un solo clic, la vittima espone il suo dispositivo alla violazione.

Le aziende devono capire in che modo i cybercriminali hanno sfruttato la pandemia nel 2020 e aspettarsi attacchi analoghi anche nel 2021. La fabbricazione e la distribuzione dei vaccini è un argomento caldo in tanti paesi, e ha generato molta curiosità ovunque. È probabile che i cybercriminali prenderanno di mira chi cerca informazioni sui vaccini creando campagne pensate specificamente per dare l'impressione di contenere informazioni sulla tempistica delle campagne vaccinali, su come farsi vaccinare in sicurezza, sull'efficacia dei diversi vaccini, delucidazioni sulle nuove varianti del virus e così via. I programmi di somministrazione dei vaccini saranno l'obiettivo principale delle iniziative di raccolta di dati di intelligence soprattutto se sponsorizzate da attaccanti nation-state alla ricerca di modi per destabilizzare le campagne vaccinali degli stati rivali.

Conclusioni

Il 2021 rappresenta l'anno della speranza, e le aziende devono gestire con cautela la transizione verso la normalità. I cybercriminali faranno tutto quanto in loro potere per spargere il caos e abusare delle insicurezze delle persone tramite le campagne di phishing. I responsabili della sicurezza devono trarre gli opportuni insegnamenti da ciò che è avvenuto nel 2020 ed essere consapevoli che i cybercriminali tenteranno di servirsi di questo momento di transizione per colpire le aziende. Adottare un approccio Zero Trust e fare in modo che il personale sia sempre consapevole dei rischi per la sicurezza sono due misure essenziali per contrastare i rischi informatici, e in particolare quelli derivanti dagli attacchi di phishing.

Riferimenti:

- GTR 2021 - https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf
- https://www.crowdstrike.com/cybersecurity-101/phishing/
- https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/
- https://axaxl.com/fast-fast-forward/articles/cybersecurity-risks-to-consider-when-the-workforce-returns-to-work
- https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html
- https://www.cxotoday.com/corner-office/cybersecurity-post-covid-19-how-to-ensure-safe-return-to-work/ ■

Conseguenze operative della vulnerabilità dei protocolli di rete, un esempio pratico: PetiPotam.

Autore: Michele Fiorilli

Recentemente abbiamo visto come alcune tipologie di Ransomware sfruttino delle vulnerabilità dei protocolli di rete per passare inosservati agli strumenti di sicurezza esistenti all'interno dell'azienda.

Approcciamo la problematica partendo da un caso pratico: la vulnerabilità PetitPotam del protocollo NTML in Windows (o comunque di un abuso di funzionalità legittime del sistema) balzato alle cronache durante questi mesi estivi. In questo tipo di attacco, l'hacker utilizza il protocollo MS-EFSRPC (Encrypting File System Remote Protocol – tipicamente utilizzato per le normali operazioni di maintenance) di Microsoft per connettersi a un server, dirottare la sessione di autenticazione e manipolare i risultati in modo tale che il server ritenga che il cyber criminale abbia un diritto legittimo di accesso IT.

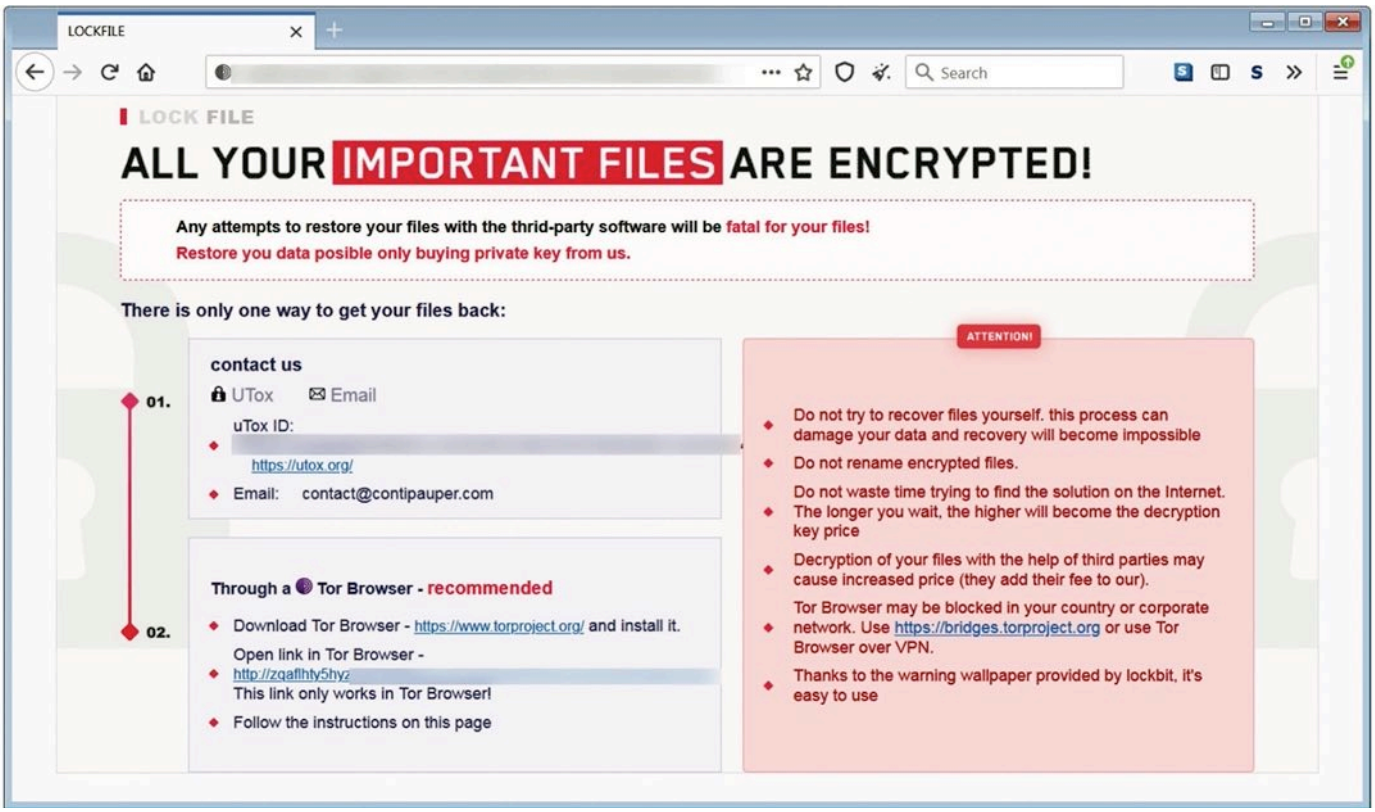
Gli ultimi ransomware, come ad esempio LockFile Ransomware (noti per colpire principalmente i server Exchange e per utilizzare tecniche di crittografia intermittente che possono eludere le tecniche di protezione da ransomware) sfruttano questa vulnerabilità e sono pertanto difficilmente rilevabili da soluzioni tradizionali.

Dalle analisi effettuate LockFile ha uno stile molto simile a quello utilizzato dal LockBit, come si evince dalla figura successiva:

Va comunque sottolineato che le vulnerabilità sono un aspetto "normale" di applicazioni, software e release in generale, e comunque la vulnerabilità

BIO

Michele Fiorilli si è laureato in Ingegneria all'università La Sapienza di Roma, lavorando fin da subito nel settore dell'IT in qualità di Security Engineer. Ha al suo attivo una esperienza pluriennale nei security team di importanti vendor (Cisco, Juniper, Palo Alto, Pulse Secure, VMware) con il compito di seguire i principali clienti del mercato Telco ed Enterprise italiani. A Gennaio 2021 entra a far parte del Team Exabeam entusiasta delle soluzioni e delle innovazioni che l'azienda sta proponendo sul mercato in termini di automazione, ottimizzazione degli investimenti e innovazione sulle componenti di analisi, investigazione e risposta alle nuove cyber minacce.



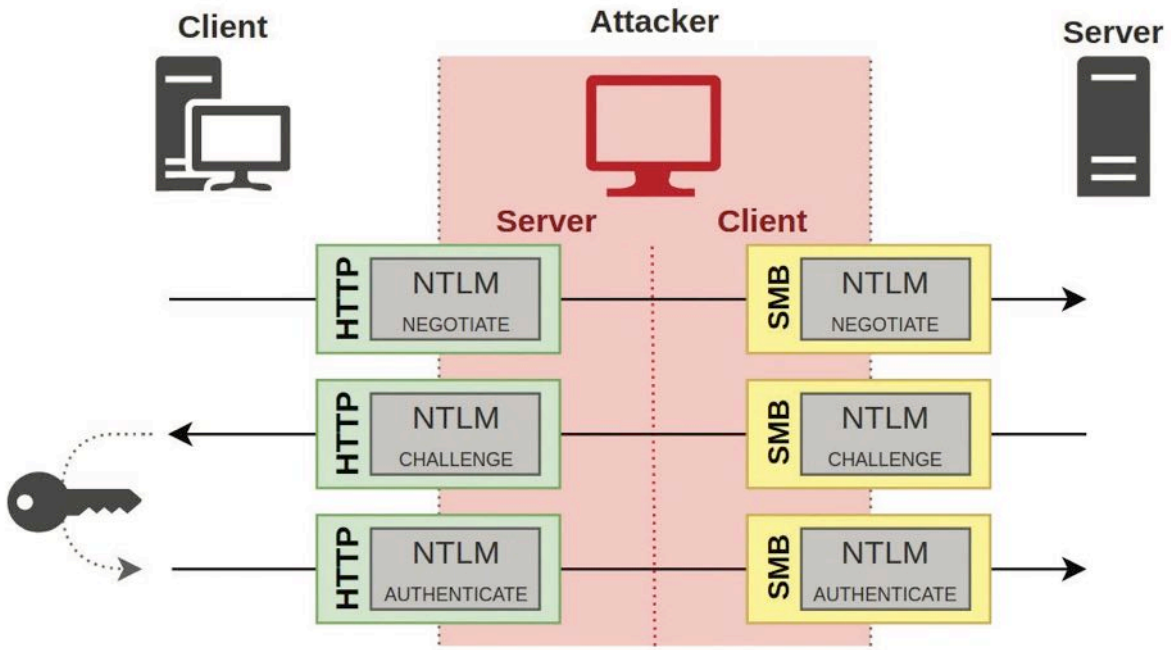
PetitPotam è stata prontamente identificata ed è stato proposto da Microsoft un workaround per risolvere il problema.

Tuttavia, al momento l'unico modo per risolvere il problema in maniera definitiva consiste nel disabilitare il protocollo NTML (operazione non sempre percorribile) oppure, come suggerisce Microsoft, cambiare in parte metodologia di autenticazione utilizzando EPA o delle firme su Kerberos e LDAP. Tutte queste opzioni possono farci pagare un prezzo in termini prestazionali e comunque implicano ulteriori attività operative con le relative tempistiche ed implicazioni pratiche.

Dalle osservazioni precedenti emergono alcune considerazioni importanti:

Anche applicando le best practice in termini di configurazione dei sistemi e di applicazione delle impostazioni consigliate l'attacco va a buon fine

Le operazioni di patching e aggiornamento (che sono assolutamente una pratica da seguire) hanno comunque le loro tempistiche e tempi di attuazione



Ed in particolare oggi ci troviamo a fronteggiare Ransomware che sono in grado di eludere non solo i sistemi tradizionali, basati su signature, policy e pattern statici, ma anche strumenti più moderni.

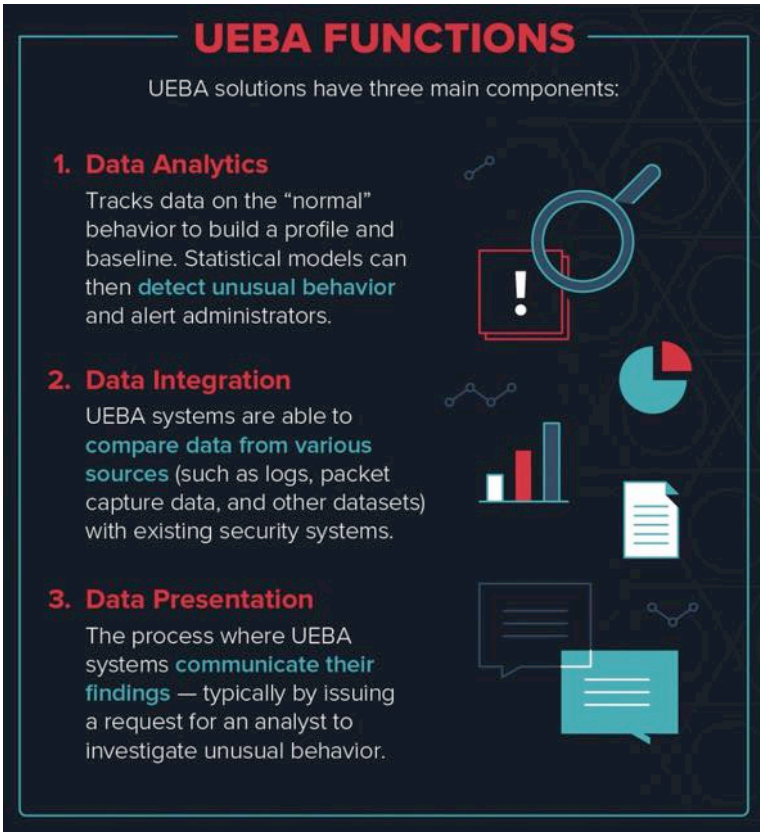
Le organizzazioni possono contrastare questa tipologia di attacchi cambiando approccio, e ragionando sul monitoraggio e il rilevamento precoce di accessi, e in generale di comportamenti insoliti, come ad esempio un utente anonymous o un indirizzo IP inconsueto che accede con diritti di lettura e scrittura ai server di rete.

Le tecniche che sfruttano metodi di analisi comportamentale basati su machine e deep learning possono, infatti, supportarci nel rilevamento di incidenti di sicurezza che tool tradizionali (basati su regole di correlazione o su pattern di attacco) non sono in grado di gestire.

Ad esempio nel caso di utilizzo della vulnerabilità PetitPotam si sarebbero potuti vedere comportamenti anomali, quali la verifica della disponibilità dei diritti di accesso per scrivere e leggere dati da una delle pipe lsarpc/efsrpc/lsass/samr/netlogon nella condivisione IPC$:

- per la prima volta da un indirizzo IP sorgente
- da un utente anonimo
- da un indirizzo IP non consueto

UEBA si può definire come una funzionalità chiave di sicurezza che analizza il comportamento di utenti e device e applica tecniche di analisi avanzate per effettuare la detection di eventuali anomalie comportamentali che possano indicare una potenziale minaccia.



Per capire cosa è UEBA scomponiamo semanticamente l'acronimo:

- USER: per identificare i problemi di sicurezza è fondamentale valutare e analizzare il comportamento degli utenti nei confronti dei device e degli asset aziendali.
- ENTITY: è altresì fondamentale analizzare il comportamento di entità di rete come server, router, applicazioni e device IoT in generale.
- BEHAVIOUR: è la tecnologia utilizzata per identificare il normale comportamento all'interno della propria infrastruttura.
- ANALYTICS: poiché la quantità di dati e log da analizzare è molto grande, è necessario utilizzare motori di Machine Learning e Intelligenza artificiale per fare il match con i dati storici e capire se un'eventuale variazione può essere considerata come un evento di sicurezza.

UEBA permette di mettere insieme attività che possono essere definite "sotto traccia", confrontarle dinamicamente con modelli comportamentali e presentare un evento che nel suo insieme ha una rilevanza in termini di sicurezza assolutamente significativa.

Se da un lato la strada è tracciata, dall'altro la sfida è come realizzare operativamente tutto ciò. In tal senso sono sicuramente due i percorsi da seguire.

Da un lato l'integrazione completa con le informazioni e la telemetria dell'ecosistema esistente (endpoint, device di rete, soluzioni di sicurezza) sia attuale che futuro, nel senso che è necessario stabilire un framework di analisi comportamentale che non imponga limitazione tecnologiche. È necessario essere sempre aperti all'adozione di nuove soluzioni e tool di sicurezza che possano andare a gestire possibili futuri vettori di attacco.

Dall'altro l'automazione come elemento abilitante dell'analisi dei log e delle informazioni di contesto; risulta, infatti, necessario avere strumenti che correlino e presentino in formato facilmente leggibile e orientato alla sicurezza i comportamenti e gli eventi di utenti e device evidenziando in modo immediato eventuali anomalie rispetto alla baseline. L'utilizzo di timeline create automaticamente e arricchite con informazioni di contesto che diano una visione completa di quello che accade (non il semplice alert che costituisce solo la punta visibile dell'iceberg) è fondamentale anche per ridurre i tempi di gestione e di reazione agli incidenti.

In sintesi, di fronte ad attacchi complessi che combinano delle vulnerabilità di protocolli e applicazioni con le metodologie dei ransomware di nuova generazione, l'approccio tradizionale deve necessariamente essere integrato con tecnologie di analisi comportamentale che permettono di prescindere da analisi statiche per concentrarsi su quelle tracce legate al comportamento di utenti e device che sono i primi segnali di un attacco. ■

Per una professionalizzazione della gestione delle denunce di cybercrime dalla Polizia di Stato di Ginevra.

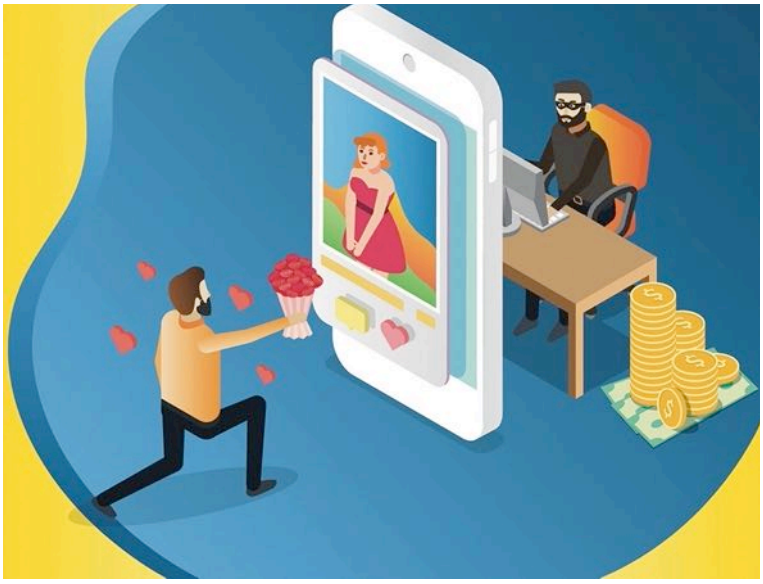
Autore: Patrick Ghion

BIO

Il capitano Patrick Ghion lavora alla Polizia di Stato di Ginevra da oltre 20 anni. Precedentemente responsabile dell'unità di lotta contro i crimini informatici, Patrick Ghion è ora a capo dell'intera sezione forense della polizia giudiziaria dello Stato di Ginevra, forte di 4 brigate tra le quali quella di lotta contro i crimini informatici, ma anche *Cyber Investigations* e *Criminal Intelligence*. Di recente, è stato nominato direttore del Centro regionale di competenza Cyber per la Svizzera occidentale e vicedirettore della rete nazionale per il supporto investigativo nella lotta contro la criminalità informatica.
Prima di entrare nelle forze dell'ordine, Patrick ha lavorato in diverse banche svizzere e ha anche vissuto per un periodo in Asia, come istruttore di sport subacqueo. Padre di due bambini, i suoi principali hobby sono le immersioni subacquee ed il pilotaggio aereo .

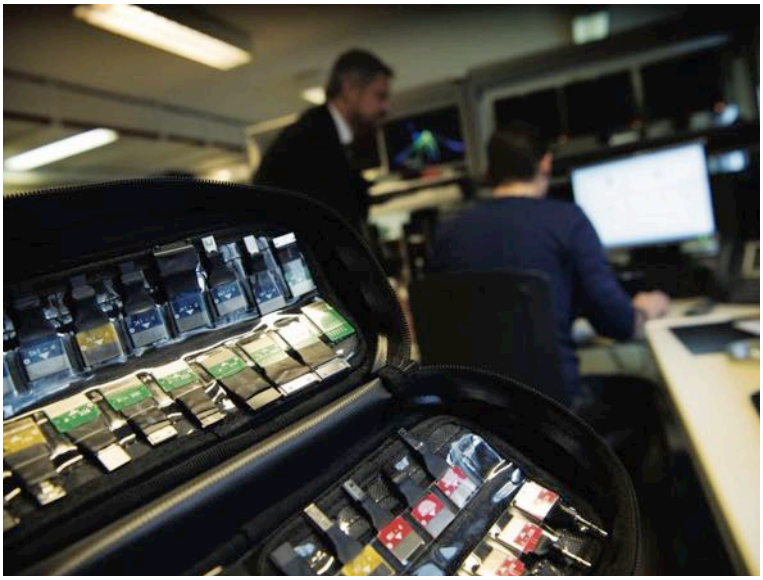
Una delle questioni fondamentali nella gestione delle denunce di crimini informatici è sempre stata la valutazione dei benefici della gestione centralizzata rispetto alla gestione affidata a gruppi specifici.

Fino ad ora, tutte le denunce relative alla criminalità informatica sono state gestite da gruppi secondo il loro ambito di azione. Per esempio, le denunce di *Romance Scam* sono state gestite dal gruppo dedicato ai reati contro la persona, mentre le denunce contro le frodi su Internet sono state gestite da quello antifrode e i casi di Ransomware dal nucleo per la repressione della criminalità.



Il dilemma per molto tempo è stato quello di chiarire se fosse più efficiente far trattare le denunce ai nuclei secondo il loro reato o raggruppare tutte le denunce cyber e farle trattare da agenti di polizia specializzati.

La polizia cantonale di Ginevra ha ora preso la decisione di creare una «Brigata» specializzata nella criminalità informatica, raggruppandola in un'unica entità e professionalizzando gli agenti di polizia attraverso una formazione accademica.

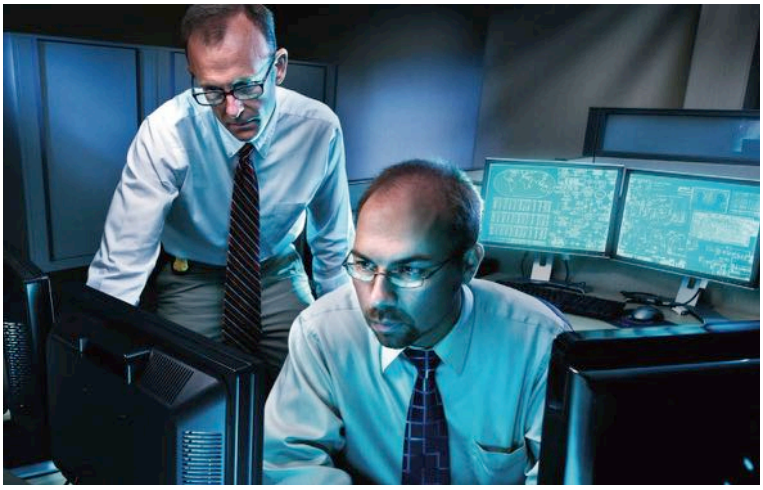


Personale in grado di affrontare le sfide

La BCE sarà composta da 17 ispettrici ed ispettori specializzati e di un segretario. Creata il 1° settembre 2021 con un organico di 12 poliziotte e poliziotti, con inserimento di nuovo personale nel corso del 2022.

Gli specialisti che compongono la Brigata di investigazione informatica sono stati selezionati sulla base della loro motivazione, autonomia e capacità di sottoporsi alla formazione accademica relativa ai loro nuovi compiti.

Sono veri e propri investigatori che formano una triade operativa con gli analisti della Brigata di intelligence criminale (BRC) e gli specialisti forensi della Brigata di criminalità informatica (BCI).



È certo che lo sviluppo della criminalità informatica a Ginevra e in tutto il mondo continuerà a crescere e non si conoscono ancora gli effetti delle nuove tecnologie come il 5G, l'intelligenza artificiale o l'uso dei computer quantistici a fini criminali.

Tuttavia, l'organico dei poliziotti non è ampliabile e il loro numero non dovrebbe essere l'unico criterio per lo sviluppo della brigata. Per questa ragione lavoreremo anche sui processi automatizzati, l'ottimizzazione del trattamento dei reclami e lo sviluppo di partenariati pubblico-privato (PPP) al fine di essere veramente al servizio della popolazione ginevrina.

Un insieme di compiti ricco e vario

Le missioni affidate alla BCI sono le stesse di qualsiasi ispettore di polizia giudiziaria. Le cui missioni principali sono: stabilire i fatti, cercare e arrestare gli autori di crimini e reati nel dominio cibernetico.

Gli argomenti principali saranno quelli relativi al **Cybercrime economico,** come il phishing, le truffe su Internet, il Romance Scam e le frodi sugli investimenti online. Un'altra parte delle loro missioni si occuperà di alcuni aspetti dei **crimini sessuali cibernetici**, come la Sextortion. Infine, si occuperanno anche di casi di **danno alla reputazione e di pratiche sleali**, nonché di Cyber bullismo e mobbing.

Come gli altri ispettori di polizia, avranno compiti aggiuntivi, quali la protezione personale dei VIP e le pattuglie sul campo.

In generale, le truffe su Internet sono uno dei principali obiettivi del lavoro della polizia, questo perchè sono convinto che la tecnologia ha i suoi limiti quando si tratta di proteggere gli utenti. Naturalmente è molto

importante avere una protezione antivirus aggiornata, un firewall efficace e sistemi operativi regolarmente aggiornati, proprio come il software utilizzato.

La Prevenzione: un aspetto chiave della lotta contro il crimine informatico

Tuttavia, se vogliamo davvero aumentare il livello di consapevolezza degli utenti, si deve partire da un'adeguata prevenzione. Questo significa, per esempio, informazioni ripetute e messaggi differenziati secondo l'età degli utenti. Il ruolo dei media è cruciale in questa prevenzione, in quanto sono in grado di raggiungere la popolazione in modo regolare e su larga scala. Lato polizia cantonale ginevrina, si sta pensando di rafforzare i nostri partenariati pubblico-privato per sostenere i messaggi di prevenzione e limitare i danni causati da queste truffe.

Una formazione specifica indispensabile

Grazie al sostegno della Direzione della polizia, tutti gli agenti di polizia informatica seguiranno una formazione accademica sotto forma di un ***certificato di studi avanzati in criminalità informatica,***

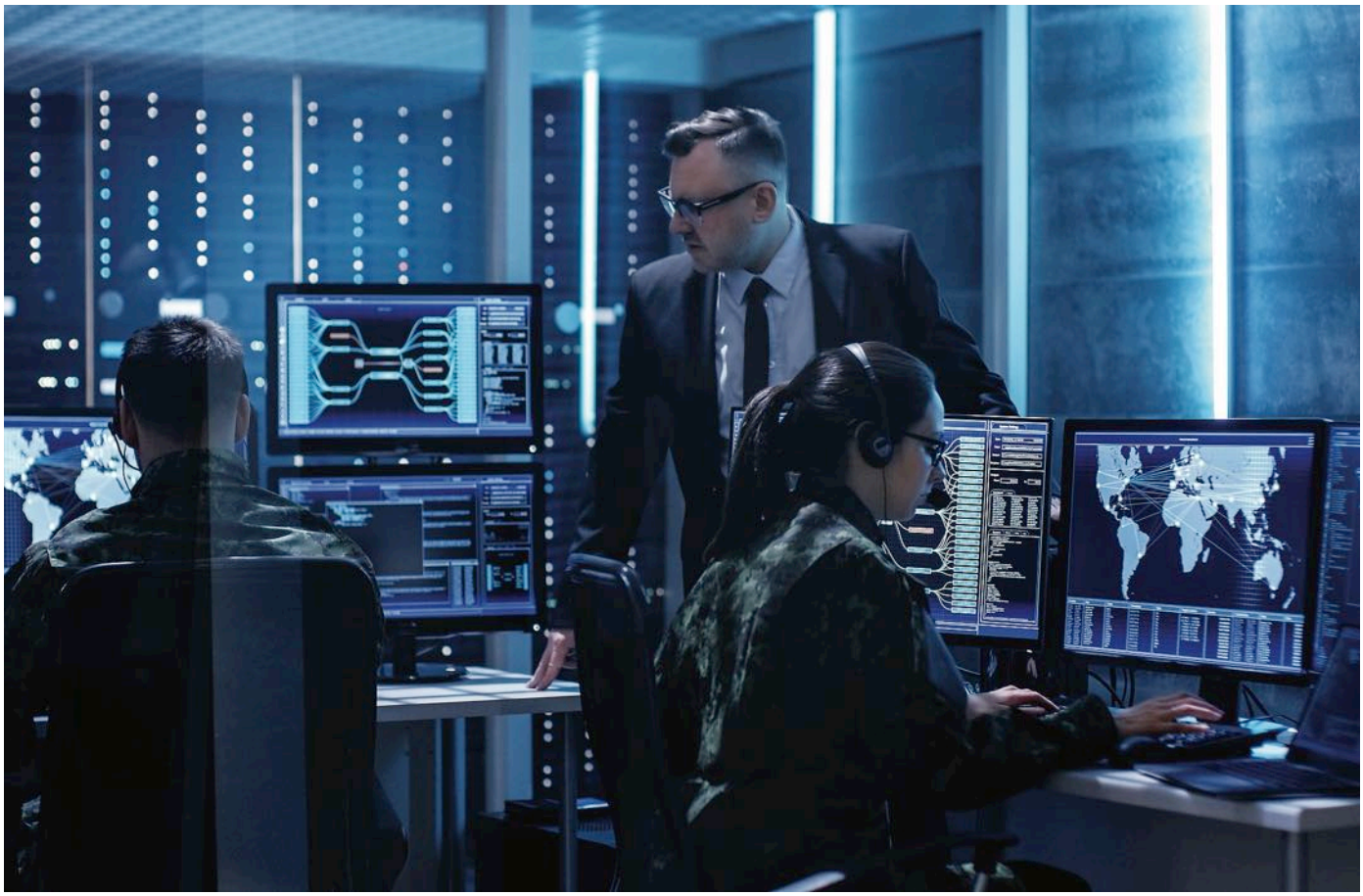
specializzato in indagini informatiche (CAS CY-E) presso l'HES-SO della Svizzera occidentale.

Il programma molto ricco e aggiornato comprenderà una parte centrale comune sulle reti informatiche e Internet in generale, il contesto cybercriminale e le misure operative in particolare.

La specializzazione in investigazioni informatiche includerà corsi sul mondo della criminalità informatica come la Darknet, le reti di criminalità informatica, i flussi finanziari con le criptovalute e le neo-banche.

Uno degli aspetti innovativi che tendono a svilupparsi sono gli aspetti di protezione attiva. Chiaramente, se non si è in grado di arrestare i sospetti per ragioni tecniche o legali, è importante essere in grado di contrastare le attività criminali per ridurre il numero delle vittime.

Di conseguenza, stiamo assistendo ad una vera e propria professionalizzazione della gestione delle indagini giudiziarie sulla criminalità informatica presso la polizia cantonale di Ginevra per arrivare ad un sistema coerente e unico in Svizzera, a beneficio della popolazione. ■



Bibliografia

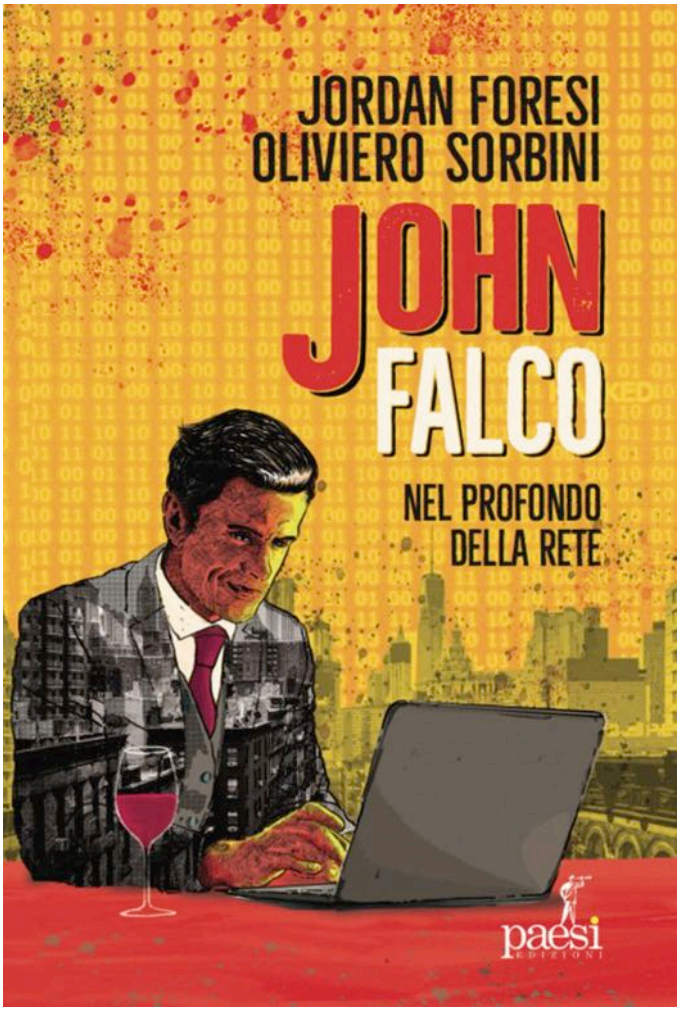
Jordan Foresi – Oliviero Sorbini
John Falco. Nel profondo della rete
Paesi Edizioni

Autore: Massimiliano Cannata

Aziende imparate a gestire il rischio
La cyber security tra il reale e l'immaginario

"È normale ispirarsi alla realtà che viviamo. Pochi anni fa la maggior parte di noi ignorava del tutto la problematica della cyber sicurezza. Il cinema, però, da tempo aveva rilevato e usato il fenomeno. Ovviamente nella creazione della fiction gli sceneggiatori hanno potuto liberare la loro fantasia creando situazioni anche irreali. D'altra parte, in questi anni, abbiamo visto un crescendo di ottimi e autorevoli saggi incentrati sulla sicurezza informatica. Questo ha consentito anche a chi scrive narrativa di individuare un campo estremamente vasto e da scoprire dove misurarsi. Uno scrittore può anche non essere un esperto della materia che tratta in un romanzo, deve però contare su informazioni attendibili, per fare bene il suo lavoro".

Jordan Foresi giornalista di Sky TG 24 e Oliviero Sorbini autore televisivo ed esperto in comunicazione socio - istituzionale hanno dato alle stampe per Paesi editore *"Jonh Falco nel profondo della rete"* dando corpo a una sperimentazione linguistica e narrativa destinata a conquistare pubblici sempre più ampi al tema della cyber security. Come dimostra l'intervista ad Alessandro Curioni che pubblichiamo in questo numero di CST la sicurezza informatica sta diventando un genere letterario di successo. Foresi offre una sua spiegazione del fenomeno: "Il libro è *figlio* del saggio, pubblicato da De Agostini, *I Segreti del Cybermondo*, che ho firmato con Jack Caravelli. Jack Caravelli amava la divulgazione dei temi di cui si interessava. Con lui iniziammo a ragionare su un soggetto per una serie televisiva. John Falco nasce così. Decidemmo che il nostro hacker non doveva essere uno psicopatico o comunque un uomo fuori dal comune, ma il più possibile vicino ad una persona che possiamo definire *normale*. Naturalmente doveva possedere un background che lo rendesse capace di agire. Poi, dopo la morte di Jack Caravelli, ci siamo ritrovati con un John Falco che aveva assunto una sua identità e allora abbiamo lavorato al personaggio, creando una *timeline* della sua vita. E ci siamo appassionati a immaginare la sua crescita, le esperienze, i dolori e le gioie del suo passato. Quello del presente è un John che può contare su solide basi, con un suo passato e una sua personalità in normale evoluzione con il trascorrere degli anni. Lasciata la NSA, John è diventato un esperto e stimato critico di vini. E questa scelta di lavoro, che abbiamo fatto per lui, gli consente di muoversi in un mondo assolutamente diverso ma come vedremo non esente da possibili azioni di cyber intrusioni". Le minacce informatiche si evolvono molto velocemente e con un elevato livello di sofisticazione. Le strategie da affinare per rafforzare la capacità di difesa delle aziende devono essere continuamente aggiornate. "Quello che emerge – precisa Sorbini – è la mancanza di una *cultura* della cyber sicurezza. Le aziende devono prendere atto che tutti i loro collaboratori devono attenersi ai protocolli di sicurezza. Inoltre, debbono approntare dei piani preventivi per fronteggiare eventuali attacchi o comunque improvvisi stati di stallo del proprio sistema informatico. Ma in particolare devono essere pronte a *gestire il rischio*: identificazione, analisi e valutazione. La valutazione del rischio può comportare il passo successivo: evitarlo, se possibile, condividerlo, nel caso ci siano le condizioni,



oppure ridurlo o addirittura decidere di accettarlo, perché si giunge alla conclusione che è estremamente improbabile o ininfluente. Infine, dopo questo processo di valutazione, debbono mettere in atto un *Risk reduction program*, preventivo".

Alla vita e alle vittime innocenti: una dedica per riflettere

La "doppia" dedica con cu si apre la narrazione merita attenzione: "alla vita e alle vittime innocenti dell'avidità umana". Su questo aspetto i nostri autori offrono una risposta univoca: "sono due le ragioni che ci hanno portato a questa scelta. La prima è legata alla figura di Jack Caravelli. Abbiamo voluto rendergli omaggio anche con la scelta dei luoghi e in particolare dei ristoranti che amava frequentare a Roma. La seconda dedica, invece, ci introduce nella finzione del romanzo, invitando il lettore a soffermarsi sul concetto di *ferocia dell'avidità*. Il caso degli attacchi hacker alle strutture sanitarie ne è un esempio. John Falco è ben consapevole della cattiveria da parte degli uomini, teniamo presente che nelle regioni del cyber mondo la *ferocia* e purtroppo ben presente. Il mondo nascosto del cyber non è per altro molto diverso nelle dinamiche da quello che tutti conosciamo".

A riflettere bene sul messaggio che arriva da questo lavoro ci si rende pienamente conto che siamo di fronte a un cambio di paradigma che non riguarda solo il modo di concepire la sicurezza, ma il modo di pensare e concepire l'impresa. In tanti si chiedono, non solo tra gli addetti ai lavori, se il nostro sistema economico e sociale è pronto a questo profondo cambiamento d'epoca. Foresi mostra un certo razionale scetticismo in merito: "mi pare che non siamo pronti o meglio non lo siamo nel modo che ognuno di noi potrebbe augurarsi. Con l'esplosione dei diversi e molteplici fenomeni di intrusione nel privato e nel pubblico, le attività hacker criminali stanno determinando una linea di demarcazione preoccupante fra soggetti. In altre parole, abbiamo una nuova e pericolosa problematica di *digital divide*. Nel romanzo, John e i suoi amici, più volte sottolineano la complessità del mondo degli hacker. I buoni molto spesso si servono dei cattivi e viceversa. Questo avviene per motivi di interesse commerciale o per semplice convenienza, perché di fronte a determinate situazioni anche uno stato democratico si trova nelle condizioni di rivolgersi a … chiunque risolva il problema… ma la storia non si ferma qui…va anche oltre… John Falco è ben consapevole che chi possiede una informazione preziosa, ad esempio una falla su un determinato software, spesso mantiene l'informazione per sé stesso, in attesa di poter sfruttare il proprio know how nel modo più opportuno. Faccio un esempio per capirci: se un centro di ricerca, o anche un singolo hacker, scoprono che tutti i cellulari di una certa marca sono penetrabili con facilità, non è detto che l'azienda produttrice ne venga a sua volta informata. Oppure se la si informa … magari lo si fa per ricattarla…".

Il fattore tempo è cruciale nell'orizzonte della sicurezza. Anche Falco ha il su rapporto con il tempo: "John è consapevole che nella cyber sicurezza è estremamente improbabile potersi muovere da soli. Per questo, uscito dalla NSA, costituisce un gruppo internazionale di hacker. Ma ognuno dei componenti ha una sua specifica peculiarità per la quale risulta funzionale. Michael, è il presidente di una compagnia di cyber sicurezza, con sede inizialmente a Singapore, che agisce apertamente sul mercato. Frank, anch'egli ex NSA, è un funzionario dello US Cyber Command. Edmond è un ricercatore universitario che può contare su una potente macchina di ricerca dati (quantistica?) e infine Batya è un'agente del Mossad. Senza questa rete, John sa che il suo know how non potrebbe tenere il passo con l'evolversi quotidiano del cyber mondo".

La storia non è certo finita …

Gli autori non sono comunque sazi, la storia del personaggio, già movimentata, si apre a nuovi orizzonti. Jonh Falco due è già all'orizzonte. Foresi e Sorbini ne danno un'anticipazione per Cybersecurity Trends: "John non è solo uomo dei nostri tempi ma dei nostri giorni commentano - Il primo romanzo finisce con una battuta: *che fai ridi*? È quello che domanda John a Uncle Charlie, che non ritiene possibile che il suo ristorante a Manhattan possa chiudere per via del Covid-19. Il secondo romanzo riprende da John che, non appena possibile, se ne è volato in Italia. Il suo mercato come wine writer americano è fermo e spaventato e, dopo le vicende conclusive del libro, il terreno statunitense tende a scottare un po' troppo per lui. Quindi ha deciso di prendersi un po' di riposo e per lui non c'è posto migliore al mondo della campagna toscana di sua zia Francesca. Ma ovviamente non sarà lasciato in pace, altrimenti che cosa potremmo far leggere? Servizi segreti italiani, americani e hacker di tutto il mondo faranno di tutto per rovinargli la vita. Quello che possiamo anticipare è che comunque non riusciranno a toglierli il gusto di una buona degustazione dei suoi amati vini". ■

Ikujiro Nonaka Hirotaka Takeuchi L'impresa saggia Ed. Guerini NEXT

Autore: Fabio Corno*

Al mondo della "pratica" si indirizza *L'impresa saggia,* libro che si rifà all'impianto teorico di un primo testo The Knowledge-Creating Company con il quale Nonaka e Takeuchi erano già andati oltre le teorie sull'informazione, evidenziando il ruolo fondamentale della conoscenza nella creazione dell'innovazione, nelle organizzazioni così come nelle comunità. A distanza di venticinque anni, gli autori hanno messo a fattor comune il frutto di un rigoroso lavoro accademico e di un costante contatto con imprese dinamiche quali

Honda, Fast Retailing, Japan Airlines, Eisai, Toyota, Shimano, ykk, Mitsui & Company, Fuji Xerox, Apple, Walmart, Disney e MIT Media Lab. In particolare, questo nuovo lavoro si pone l'obiettivo di aiutare chi opera in un'impresa a tramutare la teoria in pratica, applicando la conoscenza all'azione.

Consapevoli di come oggi i decisori abbiano a disposizione una "conoscenza più abbondante, globale, complessa, aperta, profonda e connessa", Nonaka e Takeuchi sottolineano come la gestione di questa complessità richieda una saggezza profonda, plasmata dai valori, dall'etica e dalla morale. Una saggezza pratica, ispirata alla phronesis aristotelica, della quale evidenziano il ruolo centrale nella gestione e nella vita delle organizzazioni. Una saggezza "agita" negli spazi (fisici, virtuali o mentali) condivisi, capaci di consentire a una comunità di condividere contesti ed esperienze e di creare nuova conoscenza e innovazione, a livello sia aziendale sia sociale. "Vogliamo fare della creazione di conoscenza uno stile di vita valido per ognuno", sintetizzano gli autori. "Uno scopo arduo, che richiede disciplina e perseveranza, ma anche empatia e amore". Un obiettivo capace di generare una innovazione continua, migliorando il rendimento delle organizzazioni e arricchendo al tempo stesso le nostre vite….

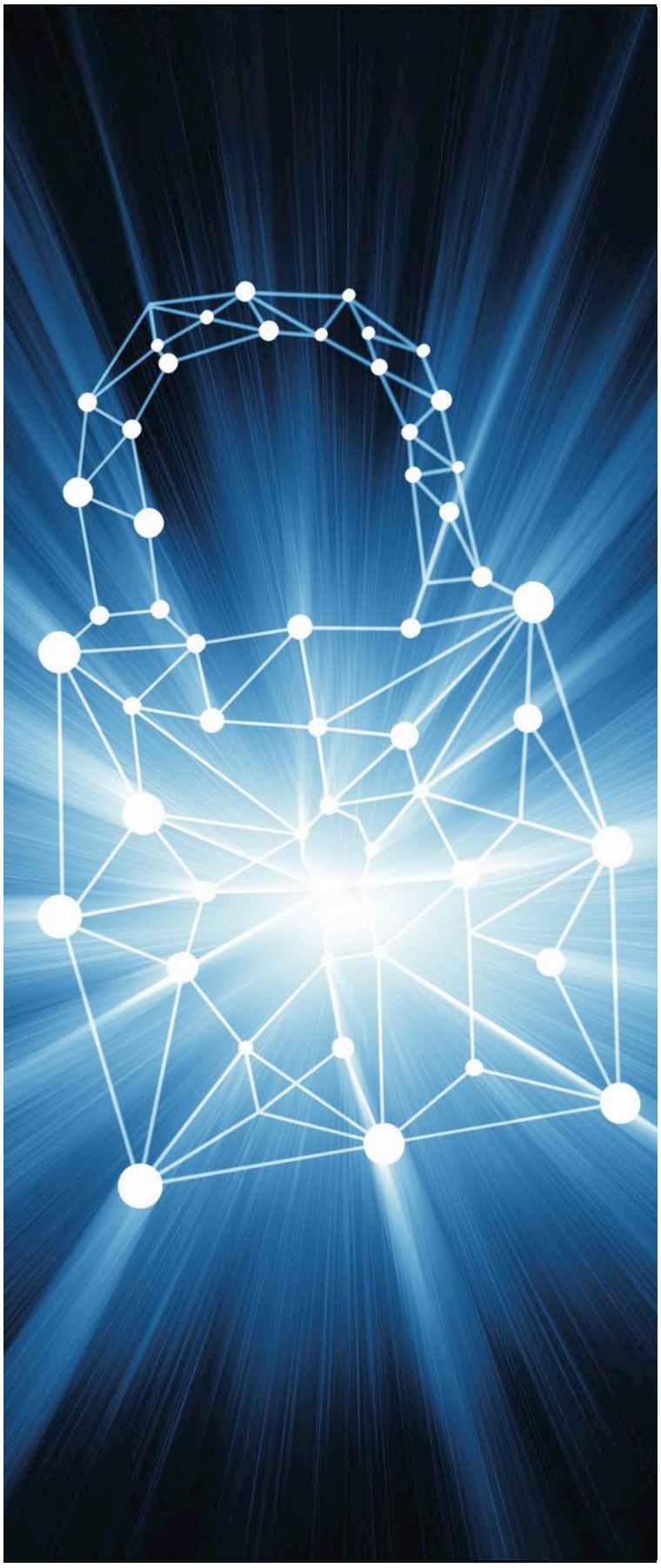
Sono gli stessi imprenditori, i manager, gli impiegati delle aziende esaminate nel testo che con la loro testimonianza, rendono credibili le proposte degli autori. Diventano così "eroi del loro quotidiano consapevole" – per citarne alcuni – il sig. Honda, dedito alla realizzazione di un motore pulito che gli consentisse di battere i suoi concorrenti americani; i venditori della Shimano, impegnati a testa bassa in un road-show finalizzato a conquistare il mercato americano; i camionisti della Yamato Transport e le "Yakult Ladies", attivati fino allo stremo per soccorrere le popolazioni della regione di Tohoku dopo il terremoto dell'11 marzo 2011. Si tratta di testimonianze belle e commoventi.

Il libro ribadisce con grande ricchezza argomentativa che per passare dall'informazione alla conoscenza e – infine – alla saggezza, serve una forma di leadership diffusa umana, fortemente coinvolta a livello personale, disponibile a esporsi in prima persona. Per questo risulterà sempre decisivo interrogandosi su ciò che è bene per l'organizzazione e per la società, prima di effettuare qualsiasi valutazione e di prendere qualsiasi decisione, facendo affidamento sul proprio intuito per capire la natura e il significato di persone, cose ed eventi, in modo da riuscire a cogliere rapidamente l'essenza di ogni situazione o problema…

Quello che gli autori propongono è il modello di un management umano-centrico, fondato sul contributo delle persone anche di fronte all'accelerazione estrema della tecnologia che caratterizza il nostro tempo. L'Impresa saggia chiude con un invito che le aziende e il mondo del business farebbero bene a mettere in pratica: "Non dimenticate mai che la vera saggezza del sapere si manifesta proprio nell'azione".

---

*Il testo di Fabio Corno Professore associato di economia aziendale all'Università Bicocca è tratto dall'introduzione del saggio. Ringraziamo l'editore Guerini e Associati per la gentile concessione. ■



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.cybersecuritytrends.ro

www.swissacademy.eu

www.cybertrends.it

CERT STAR

CERT STAR è un programma di incontri a porte chiuse dedicato ai **CERT** e ai **SOC** italiani volto ad alimentare le **competenze**, promuovere la **cooperazione** e la **condivisione** di esperienze. Nel corso degli incontri sono analizzate a livello tecnico **operativo** le principali **tematiche** "core" dei team di security.

LABORATORI 2021

- **Febbraio e dicembre** Competizione Red Team
- **31 Marzo** Intelligenza Artificiale e Cyber Security
- **Aprile** Cyber Threat Intelligence
- **Giugno** Kubernet Security
- **Luglio** Ransomware
- **Settembre** Supply Chain Attacks
- **Ottobre** Capture The Flag
- **Dicembre** Incident Response

NOVITÀ

- Incontri online
- Attività di laboratorio
- Competizioni Read Team
- Momenti di condivisione
- Webinar
- Momenti conviviali

save the date

DIGITAL ETHICS / FORUM / /

in streaming

18 / 19 novembre 2021

DEF

Sloweb