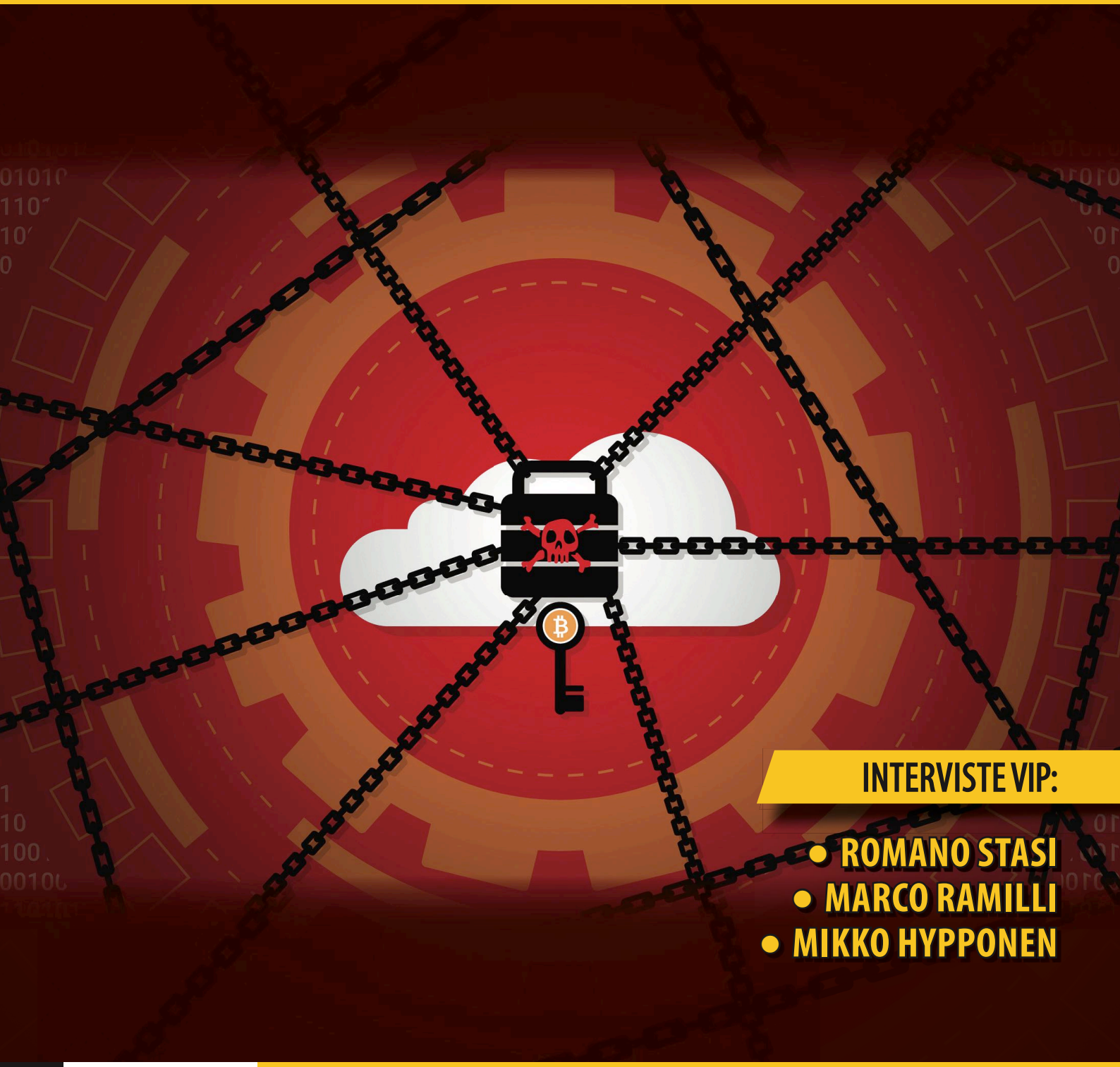
Cybersecurity Trends

Edizione italiana, N. 3 / 2023



INTERVISTE VIP:

- ROMANO STASI
- MARCO RAMILLI
- MIKKO HYPPONEN

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Folder centrale:

RANSOMWARE

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

Ransomware una minaccia crescente.

Autore: Nicola Sotira

Negli ultimi anni, il ransomware è diventato una delle minacce digitali più pericolose e costose per individui e aziende. Anche quest'anno il tema è stato presente nelle cronache giornalistiche e sfortunatamente anche in molte aziende italiane e nel mondo.

Il ransomware è un tipo di malware che si diffonde attraverso e-mail infette, link dannosi o exploit di sicurezza. Anche qui ricordiamoci che il fattore umano conta e, ancora una volta, un click sbagliato può costare caro. Una volta che il ransomware infetta un dispositivo, esfiltra i dati, crittografa file e richiede poi un riscatto per ripristinare l'accesso a questi ultimi.

Questa forma di estorsione digitale è in continua crescita perché offre ai criminali informatici un modo semplice e redditizio per ottenere guadagni finanziari illeciti.

Purtroppo, oltre all'impatto finanziario, il ransomware può causare danni significativi a livello aziendale. Le vittime, infatti, possono subire perdite finanziarie, reputazionali e di clientela. Inoltre, ci sono spese legate alla risposta dell'incidente, al ripristino dei sistemi e dei dati, che possono essere estremamente onerose.

Per affrontare il ransomware, esistono diverse misure preventive che possono essere adottate. In primo luogo, è essenziale mantenere tutti i sistemi operativi e i software di sicurezza sempre aggiornati per proteggere le falle di sicurezza conosciute, le vulnerabilità possono essere fatali. Inoltre, sempre lo stesso annoso problema, una solida politica di gestione delle password, che preveda password uniche e complesse, può ridurre le possibilità di cadere preda di attacchi di phishing. L'ingresso continua, purtroppo, ad essere sempre un account compromesso.

Ovviamente, ma non è sempre così ovvio da quello che leggiamo, una efficace strategia di backup e disaster recovery può ridurre notevolmente l'impatto del ransomware. Mantenere copie regolari dei dati rilevanti su dispositivi esterni, server remoti può consentire di ripristinare rapidamente i file crittografati senza dover pagare il riscatto. Tuttavia, è fondamentale assicurarsi che i backup siano adeguatamente protetti e segmentati dalla rete principale per evitare che anche i file di backup vengano compromessi.

La formazione e l'educazione degli utenti diventano elementi cruciali nella lotta contro il ransomware. Gli utenti devono essere consapevoli dei rischi associati all'apertura di allegati o link sospetti e devono essere istruiti su come identificare gli indicatori di phishing.

L'aumento del ransomware rappresenta una minaccia crescente per individui e aziende di tutto il mondo. Tuttavia, adottando misure preventive efficaci, è possibile mitigare gli effetti di questi attacchi informatici. Investire nella sicurezza informatica, nell'aggiornamento dei software, nell'implementazione di solide politiche di gestione delle password e nella formazione degli utenti può aiutare a ridurre le possibilità di cadere vittima di un attacco ransomware. Ovviamente, nonostante l'aumento del ransomware, la consapevolezza e l'attenzione costante alla sicurezza possono fare la differenza nella protezione dei nostri dati preziosi e per la vostra organizzazione. ■

BIO

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

Mitigare i Rischi Ransomware: Strategie Efficaci che le Organizzazioni Possono Adottare per Proteggersi dagli Attacchi Ransomware.

Autore: Lisa Ventura

Gli attacchi ransomware sono emersi come una significativa minaccia per la cybersecurity, causando danni diffusi alle organizzazioni di vari settori. Il ransomware è un software dannoso che crittografa i dati della vittima e richiede il pagamento di un riscatto in cambio della chiave di decrittazione. Questi attacchi possono portare a gravi perdite finanziarie, data breach, interruzioni operative e danni alla reputazione.

Gli attacchi ransomware spesso sfruttano le vulnerabilità nell'infrastruttura di sicurezza di un'organizzazione. Possono essere diffusi tramite e-mail di phishing, allegati dannosi, siti Web compromessi o sfruttando vulnerabilità di software senza patch. Una volta che un sistema viene compromesso, il ransomware crittografa i file e richiede un pagamento del riscatto, in genere mediante criptovalute, per fornire la chiave di decrittazione.

Con quale frequenza si verificano gli attacchi ransomware?

Secondo una ricerca di Astra, ogni giorno si verificano 1,7 milioni di attacchi ransomware, il che significa 19 attacchi ransomware ogni secondo. Nella prima metà del 2022 si sono verificati quasi 236,7 milioni di attacchi ransomware in tutto il mondo. Si prevede che il ransomware costerà alle sue vittime circa 265 miliardi di dollari all'anno entro il 2031.

La natura di alto profilo di alcuni attacchi, come quelli contro infrastrutture critiche, multinazionali e strutture sanitarie, ha sottolineato l'impatto significativo che gli attacchi ransomware possono avere sulle società e sulle economie. Gli attaccanti spesso richiedono ingenti riscatti, con conseguenti perdite finanziarie e potenziale esposizione dei dati se le organizzazioni scelgono di non pagare.

È importante notare che il panorama dei ransomware può evolversi rapidamente, con nuove tecniche di attacco, tipologie di ransomware e cambiamenti continui negli obiettivi e nelle tattiche utilizzate. Di

BIO

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

conseguenza, la prevalenza e l'impatto degli attacchi ransomware potrebbero essere cambiati dal mio ultimo aggiornamento. Per ottenere le informazioni più accurate e aggiornate, si consiglia di fare riferimento ai recenti report sulla cybersecurity, alle analisi di settore e alle fonti di notizie che trattano gli incidenti di cybersecurity.

Pensi che un attacco ransomware non possa colpire la tua organizzazione? Pensaci bene….

Gli attacchi ransomware stanno aumentando in modo esponenziale; ogni giorno vengono annunciati attacchi di alto profilo o data breach. Secondo un recente studio di Thales, gli attacchi ransomware sono aumentati a livello globale e di pari passo con l'aumento dei rischi per i dati sensibili nel cloud.

Quasi la metà (47%) dei professionisti IT intervistati ritiene che le minacce alla sicurezza stiano aumentando in volume o gravità con il 48% che segnala un aumento degli attacchi ransomware. Più di un terzo (37%) ha subito una data breach negli ultimi 12 mesi, tra cui il 22% ha segnalato che la propria organizzazione è stata vittima di un attacco ransomware.

Gli intervistati hanno inoltre individuato negli asset cloud il principale obiettivo degli attacchi cyber. Oltre un quarto (28%) ha affermato che le app SaaS e il cloud-based storage erano gli obiettivi principali, seguiti dalle applicazioni ospitate sul cloud (26%) e dalla gestione dell'infrastruttura cloud (25%). L'aumento dello sfruttamento e degli attacchi al cloud è direttamente dovuto all'aumento dei carichi di lavoro spostati nel cloud poiché il 75% degli intervistati ha affermato che il 40% dei dati archiviati nel cloud è ora classificato come sensibile rispetto al 49% degli intervistati nel 2022.

Anche in Italia gli attacchi ransomware sono in aumento. Nel febbraio 2023 migliaia di server sono stati presi di mira da un attacco ransomware globale, secondo l'Agenzia nazionale per la cybersicurezza nazionale (ACN), che ha avvertito le organizzazioni di operarsi per proteggere i propri sistemi.

Attacco hacker globale, cosa sappiamo degli impatti in Italia

Home > Attacchi hacker e Malware: le ultime news in tempo reale

Condividi questo articolo

Decine di server/siti italiani e migliaia nel mondo sono inaccessibili per colpa di un attacco "hacker" globale. L'ha segnalato Csirt Italia (Agenzia cyber nazionale), come già venerdì sera lo Csirt francese. Al centro ci sono numerose vulnerabilità, note da anni, dei server VMWare ESXi, molto utilizzati. Gli impatti possono essere l'indisponibilità di servizi pubblici e privati anche essenziali

L'agenzia italiana ANSA, citando ACN, ha riferito che a seguito di questo attacco ransomware sono stati compromessi i server in altri paesi europei, come Francia e Finlandia, nonché Stati Uniti e Canada. Milioni di utenti sono rimasti senza Internet e sono stati segnalati disservizi agli sportelli bancomat; decine di organizzazioni italiane probabilmente sono state colpite, e molte altre sono state avvisate di agire per evitare di essere bloccate fuori dai loro sistemi.

L'enorme impatto degli attacchi ransomware

Gli attacchi ransomware possono avere conseguenze devastanti per le organizzazioni, che vanno dalle perdite finanziarie alle interruzioni operative e ai danni alla reputazione a lungo termine. L'impatto di tali attacchi può variare a seconda delle dimensioni dell'organizzazione, del settore, della preparazione e della gravità dell'attacco.

Alcuni modi in cui un attacco ransomware può colpire le organizzazioni includono:

- **Perdite finanziarie:** gli attacchi ransomware spesso richiedono ingenti pagamenti di riscatto, il che può mettere a dura prova le risorse finanziarie di un'organizzazione. Anche se viene pagato un riscatto, non vi è alcuna garanzia che gli attaccanti forniscano una chiave di decrittazione funzionante. Inoltre, i costi associati al ripristino di un attacco, come il ripristino dei sistemi IT, le spese legali e le potenziali sanzioni normative, possono aumentare rapidamente.
- **Interruzione operativa:** il ransomware può paralizzare le operazioni di un'organizzazione crittografando dati e sistemi critici. Ciò può portare a tempi di inattività, interruzione della produzione, interruzione dei servizi e ritardi nei progetti. Quanto più tempo è necessario per riprendere il controllo, tanto più grave può essere l'impatto operativo.
- **Perdita e danneggiamento dei dati:** in alcuni casi, gli attaccanti potrebbero non fornire una chiave di decrittazione anche dopo il pagamento del riscatto, oppure il processo di decrittazione potrebbe inavvertitamente provocare la perdita o il danneggiamento dei dati. Le organizzazioni potrebbero perdere informazioni sensibili, proprietà intellettuale, dati dei clienti e importanti documenti aziendali.
- **Danni alla Reputazione:** la notizia di un attacco ransomware può minare la fiducia dei clienti e danneggiare la reputazione di un'organizzazione. I clienti potrebbero mettere in dubbio la capacità dell'organizzazione di salvaguardare i propri dati, portando potenzialmente all'abbandono dei clienti e a un'immagine del marchio danneggiata che è difficile da ripristinare.
- **Conseguenze Legali e Normative:** le organizzazioni sono legalmente obbligate a proteggere i dati sensibili e a rispettare le normative sulla protezione dei dati. Un attacco ransomware che porta a un data breach può innescare responsabilità legali, indagini normative e multe. Dimostrare negligenza nella cybersecurity può ulteriormente inasprire i problemi legali.
- **Perdita di produttività:** poiché i sistemi rimangono inaccessibili, i dipendenti possono avere difficoltà a svolgere i propri compiti in modo efficiente, con conseguente riduzione della produttività. Inoltre, il tempo e gli sforzi necessari per il ripristino possono distogliere risorse dalle attività aziendali principali.
- **Impatto sulla supply chain:** gli attacchi ransomware possono diffondersi ai partner delle organizzazioni o ai fornitori, interrompendo l'intera supply chain. Ciò può portare a ritardi nella ricezione di beni o servizi critici e, di conseguenza, influire sulla capacità di un'organizzazione di soddisfare le richieste dei clienti.
- **Perdita di vantaggio competitivo:** se le informazioni sensibili o la proprietà intellettuale vengono compromesse, un'organizzazione può perdere il proprio vantaggio competitivo. Segreti commerciali rubati o informazioni proprietarie potrebbero essere sfruttati dai concorrenti.
- **Costi della cyber security:** la remedation post-attacco implica non solo il ripristino dei sistemi ma anche l'investimento per rafforzare le misure di cybersecurity per prevenire incidenti futuri. Ciò può includere l'aggiornamento dell'infrastruttura di sicurezza, l'implementazione dell'advanced threat detection e il potenziamento della formazione dei dipendenti.
- **Clima Aziendale:** lo stress e l'incertezza derivanti da un attacco ransomware possono avere un impatto negativo sul morale dei dipendenti. Se l'attacco porta a licenziamenti o cambiamenti nella forza lavoro, i dipendenti rimanenti potrebbero demoralizzarsi, influenzando la produttività e la fidelizzazione dei talenti.

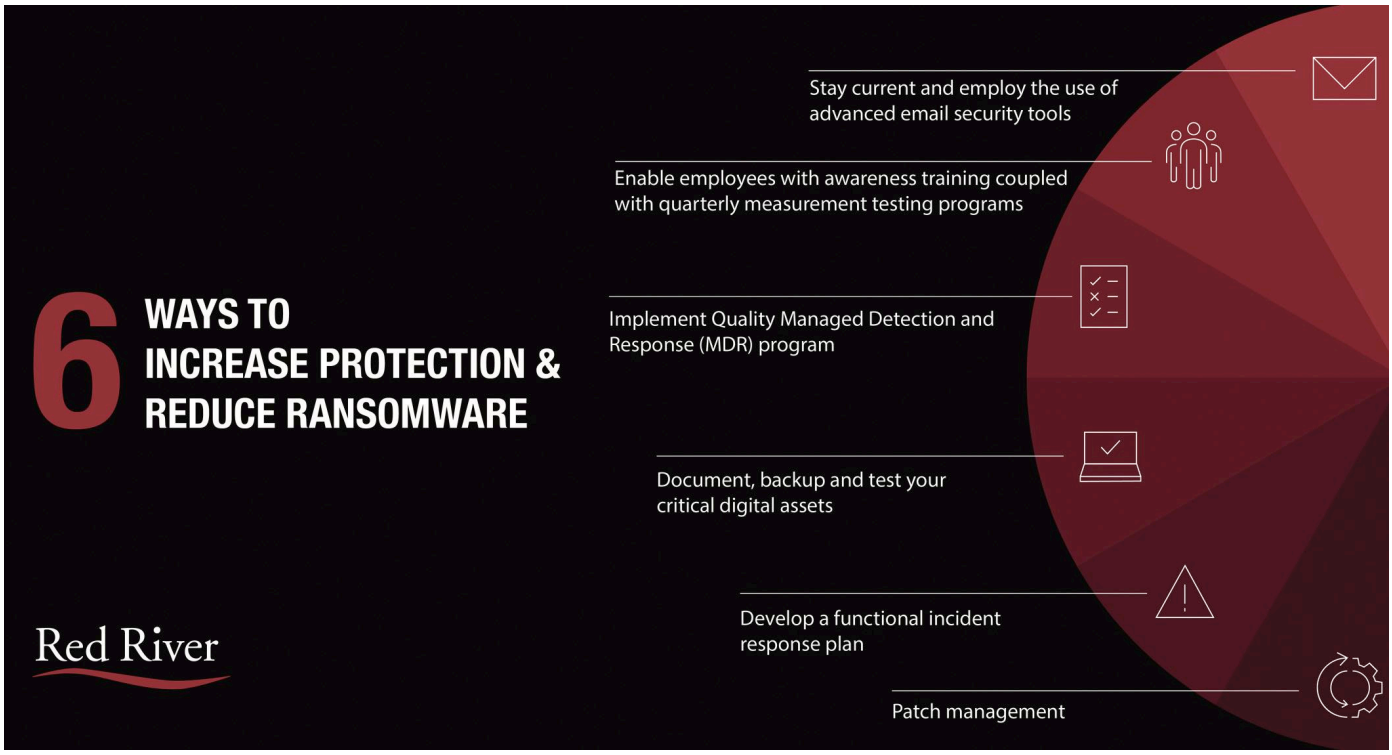
Considerata la potenziale portata di questi impatti, le organizzazioni dovrebbero quindi adottare misure proattive per mitigare il rischio di attacchi ransomware.

In che modo le organizzazioni possono mitigare la possibilità di un attacco ransomware?

Gli attacchi ransomware rappresentano una minaccia significativa per le organizzazioni di tutte le dimensioni, quindi, per mitigare efficacemente questi rischi e ridurre il potenziale impatto di tali attacchi, le organizzazioni devono adottare un approccio completo e proattivo per mitigarli. Migliorare la loro resilienza agli attacchi ransomware è fondamentale, ma richiede un enorme sforzo continuo, un adattamento continuo all'evoluzione delle minacce e il perfezionamento delle misure di mitigazione.

Alcune strategie chiave da considerare includono:

- **Effettuare backup regolari:** le organizzazioni dovrebbero effettuare backup regolari dei dati e sistemi critici in ambienti offline o isolati. Ciò garantisce che, anche se i dati fossero compromessi, potrebbero essere ripristinati senza pagare il riscatto.
- **Patch di sicurezza:** mantenere aggiornati software e sistemi operativi con le ultime patch di sicurezza è fondamentale. La maggior parte degli attacchi ransomware sfruttano vulnerabilità note che sarebbero potute essere prevenute con aggiornamenti tempestivi.
- **Organizza regolarmente corsi di cyber security awareness:** forma i tuoi dipendenti su come riconoscere le e-mail di phishing, gli allegati sospetti e come adottare un comportamento online sicuro. I dipendenti rappresentano spesso la prima linea di difesa contro gli attacchi ransomware, non l'anello più debole.
- **Email filtering and web protection:** implementa robuste soluzioni di email filtering and web protection per impedire ai dipendenti di accedere a siti Web dannosi e scaricare file infetti.



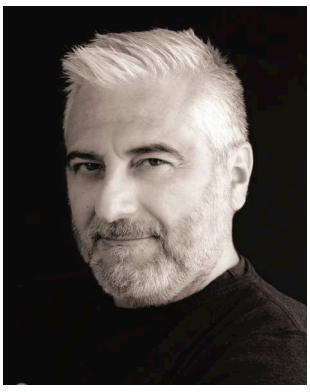
- **Segmentazione della rete:** separare le reti in segmenti con diversi livelli di accesso. Ciò limita il movimento laterale del ransomware all'interno della rete, diminuendo il potenziale impatto.
- **Protezione degli endpoint:** installa e mantieni software antivirus e antimalware avanzati su tutti gli endpoint per rilevare e prevenire le infezioni da ransomware.
- **Pianificazione della risposta agli incidenti:** sviluppare un piano completo di risposta agli incidenti che delinei gli step da intraprendere in caso di attacco ransomware. Questo piano dovrebbe comprendere strategie di comunicazione, implicazioni legali e procedure tecniche per il contenimento e il recupero.
- **Crittografia e autenticazione:** implementare una crittografia robusta per i dati sensibili e applicare l'autenticazione a più fattori (MFA) per migliorare la sicurezza dell'accesso.
- **Gestione delle vulnerabilità:** valutare regolarmente e dare priorità alle vulnerabilità all'interno dei sistemi, delle applicazioni e dell'infrastruttura dell'organizzazione. Affrontare tempestivamente le vulnerabilità identificate per ridurre la superficie di attacco.
- **Cyber Security Partnership:** collabora strettamente con esperti di cybersecurity, provider di threat intelligence e forze dell'ordine per rimanere aggiornato sulle ultime minacce e tendenze. Promuovere una maggiore collaborazione nel settore della cybersecurity può aiutare a proteggersi dai ransomware e da altri attacchi cyber: insieme si è più forti.
- **Esercitazioni per la gestione degli attacchi ransomware:** conduci esercitazioni in cui simulare attacchi ransomware per valutare la preparazione della tua organizzazione per un simile attacco e identificare e rimediare a potenziali punti deboli.

Conclusioni

Gli attacchi ransomware rappresentano una seria minaccia per le operazioni, le finanze e la reputazione delle aziende. Se le organizzazioni

implementano una strategia globale che comprenda la formazione dei dipendenti, solide misure di cybersecurity, backup regolari e piani efficaci di risposta agli incidenti, possono ridurre significativamente le loro vulnerabilità agli attacchi ransomware. La cybersecurity è uno sforzo continuo che richiede vigilanza e adattamento continui per contrastare le minacce in evoluzione nel panorama digitale. ■

Evoluzione del ransomware e attività di prevenzione. Opportuno separare le funzioni organizzative ICT e Cybersecurity.



Autore: Gerardo Costabile

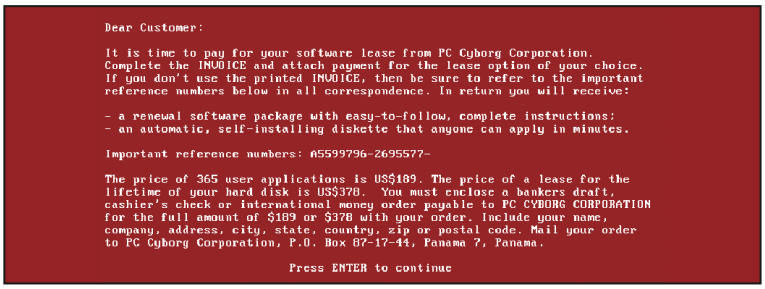
Introduzione

Negli ultimi anni, come ulteriormente confermato nell'ultima relazione dell'Agenzia per la cybersicurezza nazionale (ACN), il ransomware si è affermato come una delle minacce più pericolose nel panorama della sicurezza informatica. Le organizzazioni di ogni settore sono state colpite da attacchi di ransomware che hanno causato danni significativi, tra cui perdite finanziarie, interruzioni delle operazioni commerciali e compromissione dei dati sensibili. Solo dall'osservatorio dell'ACN – che è comunque parziale - sono stati gestiti nel 2022 oltre 1094 attacchi cyber, condotti soprattutto attraverso ransomware.

Il ransomware: evoluzione della specie

Il ransomware si è molto evoluto negli anni, diventando sempre più sofisticato e pericoloso.

Inizialmente, era sinonimo di malware che crittografava i file sul computer dell'utente e richiedeva il pagamento di un riscatto per ripristinare l'accesso ai dati. I primi esempi di ransomware risalgono ai primi anni '90, quando sono stati creati programmi come "AIDS Trojan" e "PC Cyborg". Questi programmi crittografavano i file sui computer delle vittime e chiedevano un pagamento per ripristinarne l'accesso. Nel corso degli anni, il ransomware è diventato sempre più avanzato, attraverso l'utilizzo di tecniche come la crittografia asimmetrica e il pagamento in criptovalute per rendere più difficile il tracciamento delle transazioni.



Ma l'evoluzione più importante si è avuta con il cambio di *target:* dal singolo utente si è passati a organizzazioni aziendali e pubblica amministrazione, portando il ransomware a diventare una sorta di sinonimo di accesso abusivo a una rete di una organizzazione, per operare un *data*

BIO

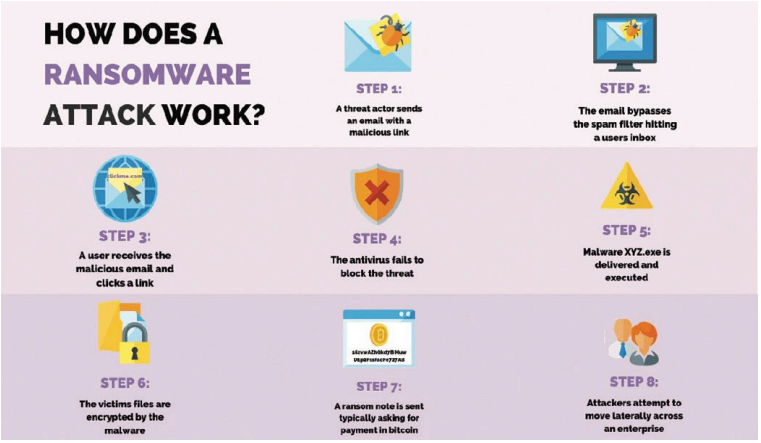
Gerardo Costabile è Amministratore delegato di DeepCyber. Co-inventore di un brevetto, depositato sia negli Stati Uniti che in Europa, sulla cyber security *(vulnerabilty management)* nel settore IOT/ICS/SCADA. Precedentemente, è stato Chief Security Officer di British Telecom e Fastweb spa, Executive Director della practice "Forensic Techonology and Discovery Services" di EY (Ernst & Young) per l'Europa dell'Ovest, Chief Information Security Officer del Gruppo Poste Italiane e investigatore nel Gruppo Repressione Frodi della Guardia di Finanza di Milano. Membro del Team che ha catturato i primi virus writer italiani (2001 e 2003), bloccato le due crew di bad actor che avevano bucato NASA, Us Army, US Navy e oltre 1000 macchine governative in tutto il mondo (2001) ed ha effettuato le prime indagini in Italia su phishing e money laundering (2005-2006). Nel 2009, ha contribuito alla creazione dell'European Electronic Crime Task Force, fondata da Poste Italiane, Polizia Postale e United State Secret Service, coordinandone i lavori sul piano tecnico-scientitico. È tuttora membro del New York Electronic Crime Task Force (NYECTF) dell'United States Secret Service. Presidente dell'Italian Chapter di IISFA (associazione no profit che raggruppa gli specializzati in informatica forense), Professore a contratto in cyber security e digital forensics per alcune università, relatore in diversi consessi tecnico-specialistici e altresì autore di numerose pubblicazioni scientifiche su cybersecurity, cyberintelligence, digital forensics, compliance, Privacy, IT risk management, IT audit, criminalità informatica. Ha conseguito, negli anni, alcune certificazioni internazionali, tra cui: Certified Information Forensics Investigator (CIFI), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), Certified Hacking Forensics Investigation (CHFI) e AccessData Certified Examiner (ACE) riconosciute in ambito internazionale e conseguite rispettivamente presso l'IISFA International, EC-Council, ISACA ed Accessdata.

breach e una (e spesso, più) richieste di riscatto. Quindi, non ci troviamo più davanti a un utente al quale si blocca il pc, ma gli attaccanti operano una penetrazione nella rete della vittima, sfruttando diverse strade, al fine di operare illecitamente sui dati. Solo in conclusione, di fatto, si cifreranno tutti i sistemi disponibili in rete (backup compresi, se accessibili).

Questa evoluzione dei *bad actor*, inoltre, ha portato a uno sviluppo del business opportunistico dei criminali, spingendo da un lato questi ultimi a organizzarsi in realtà che potremmo definire un misto tra una azienda e una organizzazione militare. Dall'altro, come noto agli addetti ai lavori, alcuni di loro si sono organizzati con *"ransomware as a service"* (come avviene per il *phishing* ed il *carding*, da anni), permettendo ad altri di creare e distribuire il proprio ransomware in cambio di una percentuale del riscatto.

Le tipiche tecniche di attacco

Le tipiche fasi di un moderno attacco ransomware sono le seguenti:



a. Fase di Inizializzazione: In questa fase, gli aggressori utilizzano varie tecniche di ingegneria sociale e tecniche di exploit per compromettere il sistema della vittima. Le due principali modalità sono lo *spear-phishing* per inviare e-mail con link e allegati malevoli e/o sfruttare vulnerabilità tecnologiche dell'infrastruttura dell'organizzazione (spesso nei sistemi di accesso a sistemi esposti in rete, modalità ancora più presente a seguito dell'enorme richiesta di smart working).

b. Fase di Esecuzione: Una volta che gli aggressori hanno accesso al sistema, possono utilizzare tecniche di exploitation per ottenere i permessi di root o di amministratore e diffondere il loro malware attraverso la rete dell'organizzazione. Lo scopo dell'attaccante, infatti, è quello di cercare utenze di amministratore, perché è con quelle utenze che potrà fare alcune azioni più pervasive nella rete della vittima. A tale scopo, possono utilizzare tool di exploit come Metasploit per trovare e sfruttare le vulnerabilità dei sistemi, utilizzare il malware per installare agenti di remote access trojan (RAT) o backdoor, o utilizzare tecniche di password guessing o stealing per ottenere le credenziali di accesso dei sistemi.

c. Fase di Persistenza: Una volta che gli aggressori hanno ottenuto l'accesso alla rete, cercano di mantenere l'accesso e il controllo sulla rete. Possono utilizzare tecniche di rootkit per nascondere il malware dal rilevamento delle soluzioni di sicurezza, utilizzare tecniche di obfuscation per mascherare il loro codice malevolo, o utilizzare tecniche di backdoor per garantire che possano mantenere l'accesso alla rete anche dopo il riavvio dei sistemi o il ripristino dei dati.

d. Fase di Evasione: Gli aggressori cercano di evitare il rilevamento da parte delle soluzioni di sicurezza dell'organizzazione e di bypassare le misure di sicurezza implementate. Possono utilizzare tecniche di packer per mascherare il malware in modo che non sia rilevabile dalle soluzioni

di sicurezza, utilizzare tecniche di cifratura per criptare il codice malevolo o utilizzare tecniche di "living off the land" (LOL) per utilizzare strumenti di sistema legittimi per eseguire il malware.

e. Fase di Data Breach: In questa fase, gli attaccanti hanno l'obiettivo di esfiltrare più dati possibili, per poi poter ricattare la vittima con una doppia estorsione e/o per pubblicare o vendere i dati sul dark market. Per questo obiettivo, sarà importante aggirare gli eventuali sistemi di alert per grandi flussi di dati verso l'esterno.

f. Fase di Cifratura: In questa fase, gli aggressori utilizzano il malware per cifrare i dati della vittima e richiedere un riscatto per il ripristino dei dati. Possono utilizzare algoritmi di crittografia avanzati come AES o RSA per cifrare i dati della vittima, creare una chiave di decrittazione personalizzata per ogni vittima, e utilizzare un sistema di pagamento anonimo come Bitcoin per ricevere il pagamento del riscatto.

g. Fase di Richiesta di Riscatto: Dopo aver rubato e cifrato i dati della vittima, gli aggressori inviano un messaggio di avviso alla vittima e richiedono il pagamento del riscatto. Possono utilizzare servizi di chat e messaggistica per comunicare con la vittima, offrendo la chiave di decrittazione in cambio del pagamento del riscatto. Spesso, gli aggressori minacciano di distruggere o pubblicare i dati della vittima se non viene pagato il riscatto entro un certo periodo di tempo. E questo avviene sia per la vittima che per gli interessati a cui si riferiscono i dati (si parla, appunto di doppia o tripla estorsione).

h. Fase di Post-attacco: Dopo aver ricevuto il pagamento del riscatto, gli aggressori potranno fornire alla vittima la chiave di decrittazione e la istruiscono su come decifrare i dati. Tuttavia, non c'è alcuna garanzia che la vittima riceverà effettivamente la chiave di decrittazione o che i dati saranno completamente decifrati. Inoltre, anche se la vittima paga il riscatto, gli aggressori avranno comunque copia dei dati e, se non risolto il problema del cosiddetto "malato zero", questi potranno teoricamente mantenere l'accesso al sistema e rubare ulteriori dati sensibili, oltre che cifrare nuovamente la rete.

Analisi delle cause

Nei numerosi casi che abbiamo analizzato nel panorama nazionale, ci sono alcuni punti di attenzione che si avvicendano di frequente e che potremmo sintetizzare in queste azioni:

a. le tecnologie di sicurezza non coprono mai tutto il perimetro, i progetti sono troppo spesso a rilento;

b. le configurazioni sono "al minimo", per asseriti – e non meglio precisati, né documentati - problemi di business o ICT;

c. il monitoraggio non è efficace, sia in termini di use case (cosa monitorare) che di analisti (seniority e competenze);

d. la *cyber threat intelligence* è spesso poco più di una rassegna stampa ("per restare aggiornati"!) e non esistono processi che favoriscono una postura più adeguata con l'evolversi delle minacce cyber (uno degli scopi primari dell'intelligence e del cyber threat hunting);

e. le reti sono "piatte"(con relativa eccessiva fiducia implicita): raramente esistono soluzioni di NDR (Network Detection & Response) e i progetti sulla gestione delle utenze privilegiate e amministrative con Multi Factor Authentication faticano a partire (o a completarsi);

f. le persone sono poco formate, sia in generale che in alcune aree più professionali;

g. le vulnerabilità sono migliaia, aumentano più velocemente di quelle che si risolvono;

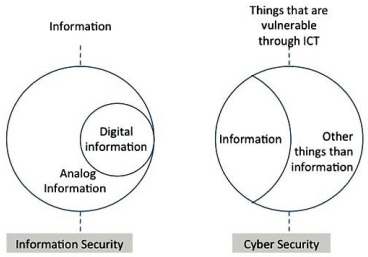
h. i vertici aziendali non vengono adeguatamente informati (e quindi sono inconsapevoli del rischio reale).

Spesso, al contrario, c'è un mantra di rassicurazione e questo accade molto più frequentemente in organizzazioni che hanno la cyber security all'interno dell'ICT, per fisiologico conflitto di interessi.

Ed è su quest'ultimo punto, molto importante, che c'è un'opportunità chiave per il top management, per influire alla riduzione del rischio ransomware (ed in generale per una migliore cybersecurity).

È necessario, a parere di chi scrive, separare le funzioni organizzative ICT e Cybersecurity.

La separazione tra ICT e Cybersecurity: una sfida possibile



La separazione delle funzioni organizzative ICT e Cybersecurity è fondamentale per garantire una gestione efficace del rischio ransomware. La materia richiede competenze specialistiche e una profonda comprensione delle minacce informatiche emergenti. Affidare la responsabilità della cybersecurity a una struttura separata consente di concentrarsi specificamente sulla prevenzione, la rilevazione e la risposta agli attacchi informatici. Inoltre, come già accennato, aiuta a evitare conflitti di interesse e a garantire un controllo adeguato sulle misure di sicurezza adottate.

La Cybersecurity, in questa nuova veste organizzativa, potrà esercitare liberamente l'autorità e utilizzare le risorse necessarie per implementare le migliori pratiche di sicurezza, condurre test di vulnerabilità, portare il cyber risk management all'attenzione del vertice aziendale e fornire formazione continua al personale ed al management.

È bene dire, allo stesso tempo, che nonostante la separazione delle funzioni, è fondamentale promuovere una stretta collaborazione e una comunicazione efficace tra il team ICT e il team di Cybersecurity. Questo garantirà una comprensione condivisa delle esigenze e delle sfide di entrambi i reparti, consentendo una gestione integrata del rischio cyber (ed in questo caso, del ransomware).

Esistono, di contro, alcuni aspetti di riflessione che vanno valutati, per operare una determinata trasformazione organizzativa. In particolare:

- Qual è il miglior modello organizzativo?
- Quali sono i rischi/svantaggi che si innestano in questo cambiamento?

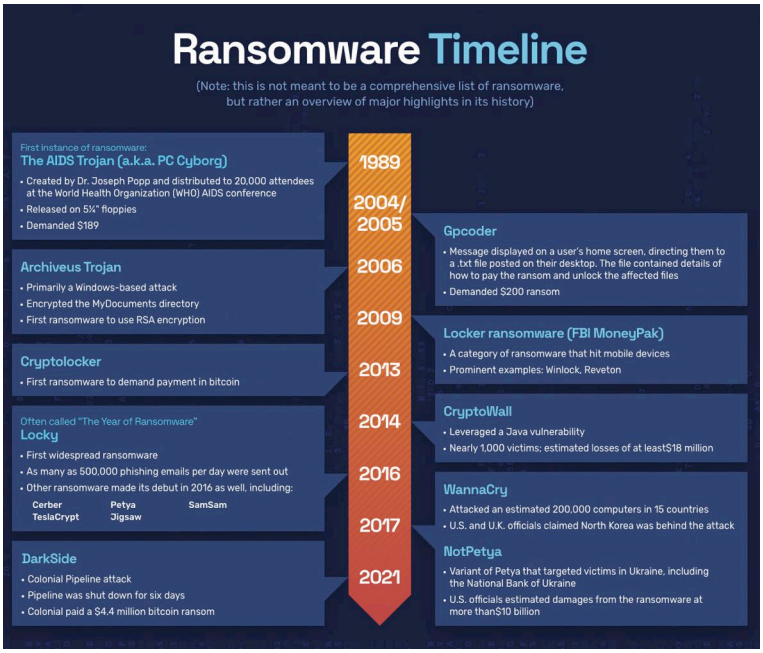
Le risposte non sono semplici, in un contesto teorico, in quanto è necessario ragionare caso per caso. Per esperienza, possiamo tracciare alcune riflessioni, non necessariamente applicabili a tutti i contesti. Prima di tutto, non esiste un unico modello organizzativo: in alcuni scenari del settore telecomunicazioni o bancari, ad esempio, sono state create – già molti anni or sono - delle strutture di Tutela Aziendale *(et similia)*, con all'interno le "varie" sicurezze, da quella fisica a quella cyber, con talvolta il fraud management, sicurezza sul lavoro, qualità ed altro ancora. In questi modelli, dove il rischio conflittuale esiste ed è vivo, è molto importante stabilire il perimetro delle attività e quindi definire i relativi centri di costo.

Nonostante tale modello, ci sono organizzazioni che preferiscono tenere al di fuori dell'ICT gli aspetti di governance, risk e compliance della cybersecurity, lasciando nell'ICT quelli implementativi (progettuali) e operativi (compreso il SOC). In altri esempi - ad avviso di chi scrive i più interessanti - lasciano al di fuori dell'ICT quasi tutti gli aspetti di cybersecurity, preferibilmente identificando un CISO con forti doti di leadership (interna ed esterna), mantenendo nell'ICT alcune parti più operative della quotidianità nella gestione della sicurezza. In questo modello, il top management non avrà dubbi organizzativi, saprà a chi chiedere aggiornamenti, avrà la consapevolezza di aver ridotto al minimo i conflitti di interesse (con una buona dose di *segregation of duty*).

Quest'ultimo approccio, in alcune organizzazioni, ha iniziato a far riflettere sulla posizione organizzativa del CISO la quale, per meglio operare, potrà anche riferire direttamente al board e quindi ai vertici aziendali, preferibilmente senza filtri. Questo orientamento, ad ogni buon conto, deve anche essere valutato (come sempre accade) rispetto ai manager presenti. Un CISO, organizzativamente all'interno di una struttura di Tutela Aziendale molto "analogica", farà fatica a comunicare al board per il tramite di questo schema "di gioco". A fine di ridurre il rischio di "filtro analogico" di tematiche cyber complesse, quindi, potrà essere decisa una modalità più snella e meno "militare" dell'organizzazione, con una maggiore libertà del CISO nelle relazioni con i vertici. In casi particolari, si potrà anche decidere di mettere il CISO a pari livello di Tutela Aziendale o del CIO: questo disegno ha anche l'indubbio vantaggio di avere, specialmente in alcune culture organizzative italiane, un maggiore equilibrio tra i manager, in modo che la stessa ICT si senta di fatto "alla pari" della cybersecurity anche sul piano politico-organizzativo aziendale.

Il tema, come ovvio, è complesso e in questa sede si può solo ipotizzare la necessità di una riflessione, lasciando caso per caso la scelta del design organizzativo e dei manager a un progetto *ad hoc*, lasciando alla sensibilità organizzativa della singola azienda la scelta dello schema più adeguato.

Conclusioni



Il ransomware - negli ultimi anni - ha subito un'enorme evoluzione tecnica e di scelta dei target, sempre più complessi e quindi interessanti sul piano opportunistico.

Al contempo, gli attacchi ransomware, nelle organizzazioni pubbliche e private, hanno enorme efficacia per alcune cause comuni, spesso dipendenti da problematiche architetturali, progettuali, formative e vulnerabilità che possono restare "sotto al tappeto", anche a causa di modelli organizzativi e di leadership che vedono la cybersecurity all'interno dell'ICT.

Per tale motivo, è opinione di chi scrive che la separazione delle funzioni organizzative ICT e Cybersecurity rappresenta un'opportunità strategica per ridurre il rischio ransomware. L'implementazione di soluzioni organizzative come la creazione di un team dedicato alla Cybersecurity, una collaborazione efficace tra i reparti, politiche di accesso e privilegi ben definite, monitoraggio delle minacce e formazione del personale può aiutare a migliorare la sicurezza informatica e mitigare il rischio di attacchi ransomware. Affrontare questa sfida richiede un impegno continuo da parte dell'organizzazione nel rafforzare le difese e nel promuovere una cultura della sicurezza informatica in tutti i livelli dell'azienda.

La scelta del modello organizzativo più adeguato e delle persone all'interno di questo processo è molto importante e, nonostante la diffusione dell'intelligenza artificiale (che permea anche le soluzioni di cybersecurity), ad oggi il fattore umano resta ancora il punto di forza e di debolezza di questo ecosistema. E le organizzazioni, come noto, sono fatte di persone. ■

Un'autenticazione avanzata e l'utilizzo di strumenti di AI per prevenire i continui attacchi ransomware.

Autore: Paolo Cecchi

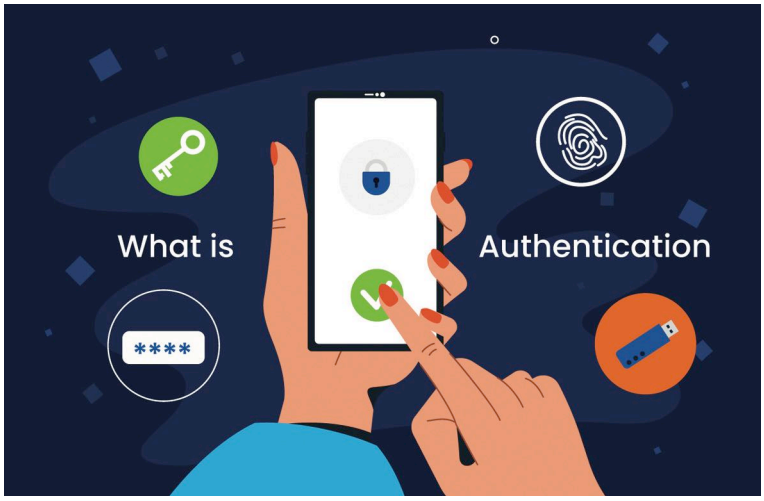
Adottare robuste tecniche di autenticazione e i più innovativi strumenti di AI possono contribuire sensibilmente nell'aiutare le imprese a prevenire l'accesso non autorizzato ai sistemi e a proteggere i dati sensibili dalle mani sbagliate. Cerchiamo quindi di fare chiarezza sulle best practices da implementare.

L'Italia è tra le nazioni maggiormente prese di mira dai cybercriminali e, secondo il recente rapporto Clusit, nel 2022 circa l'8% degli attacchi risultati vincenti sono stati indirizzati a enti della PA e imprese del settore manifatturiero. Purtroppo, nonostante negli anni la consapevolezza del rischio sia aumentata in modo significativo, molte organizzazioni non sono ancora pronte a fronteggiare le minacce e, tra i sistemi più colpiti si evidenziano gli ambienti OT, che risultano essere più critici da proteggere rispetto ai tradizionali strumenti IT. Inoltre, gli attacchi si manifestano con maggiore gravità e i cybercriminali sono diventati abili nello sfruttare ogni piccola vulnerabilità per compromettere i sistemi.

Gli esperti ritengono che, quando le imprese vogliono migliorare la propria resilienza informatica, uno dei primi interventi da adottare per proteggersi efficacemente dagli attacchi informatici sia quello di implementare validi protocolli di autenticazione. Allo stesso tempo, anche gli innovativi strumenti di intelligenza artificiale generativa dedicata al threat hunting, all'analisi e alla risposta alle minacce, possono diventare essenziali per aiutare le imprese a prevenire gli attacchi informatici.

Cosa si intende per "autenticazione"?

L'autenticazione consiste nel verificare le identità di un utente o di un dispositivo prima di concedere l'accesso a un sistema o a una rete. In genere



si ottiene richiedendo agli utenti di fornire una forma di identificazione, come nome utente e password. Tuttavia, è ben noto come sia difficile per gli utenti rispettare alcune regole per impostare le password e come sia

BIO

Paolo Cecchi è Regional Sales Directory Mediterranean Region di SentinelOne. Cecchi è entrato in SentinelOne nell'Ottobre 2022 con il ruolo di Regional Sales Director per l'Italia, mentre a Maggio 2023 è diventato responsabile della Mediterranean Region, che include Italia, Iberia e Israele. La sua mission è quella di coordinare il team vendite e di canale della region per sviluppare ulteriormente il business di SentinelOne sul mercato Enterprise e della Pubblica Amministrazione, anche mediante accordi strategici con i principali player di mercato. Il manager vanta un'esperienza commerciale ultraventennale maturata in aziende del settore ICT, con un'ottima specializzazione sui temi della cybersecurity orientati alle imprese Enterprise, alle Telco e agli enti della Pubblica Amministrazione. Ha inoltre forti competenze nello sviluppo delle strategie commerciali idonee a implementare i canali di vendita necessari attraverso i quali veicolare le migliori soluzioni ICT. Possiede elevate doti manageriali di coordinamento, abilità di negoziazione e capacità di consolidamento delle relazioni a livello CxO che negli anni gli hanno consentito di posizionarsi come 'trusted advisor' dei propri clienti. Cecchi ha avviato il percorso professionale alla fine degli anni '90 come Account Manager in primari System Integrator operanti a livello nazionale per poi approdare ad aziende multinazionali come Telindus e Juniper Networks, mantenendo sempre la responsabilità commerciale per l'acquisizione di nuovi clienti. Nel 2013 entra in FireEye, azienda leader nel settore della cybersecurity, aprendo di fatto la filiale italiana e, con il ruolo di Territory Manager, delinea le strategie di go-to-market per acquisire i clienti nel centro-sud Italia. Prima di arrivare in SentinelOne ha avviato le attività della startup Carbon Black, come Country Manager Italia e Regional Sales Manager per l'Adriatic Region, e successivamente quelle di Exabeam, con il ruolo di Regional Sales Director, per sviluppare il business della regione che include i paesi Italia, Iberia e Malta. Cecchi ha conseguito una laurea in ingegneria delle telecomunicazioni presso l'Università della Sapienza di Roma.

semplice per gli hacker entrare nei sistemi utilizzando tecniche di ingegneria sociale o sistemi di forzatura. Di conseguenza, negli anni, le aziende hanno compreso la necessità di ricorrere a metodi di autenticazione più potenti, indicati come MFA o autenticazione a più fattori.

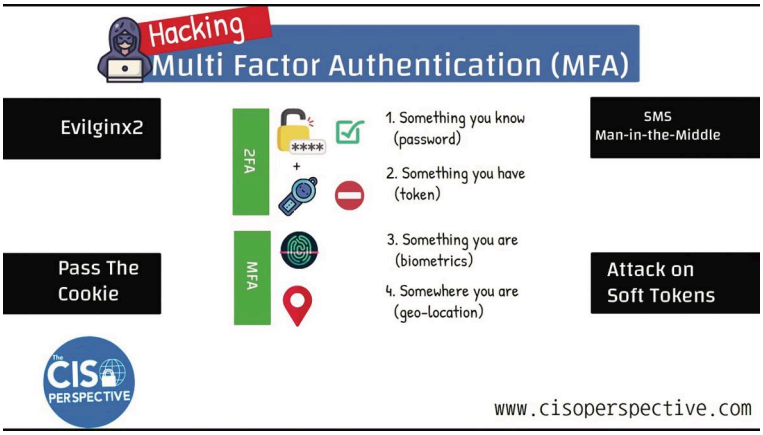
Alcuni metodi MFA di uso comune oggi coinvolgono un fattore biometrico come l'impronta digitale o la scansione del riconoscimento facciale. Anche le app di autenticazione che generano codici unici a tempo e le chiavi USB hardware stanno diventando sempre più popolari tra le aziende attente alla sicurezza.

Quali sono le migliori procedure per ottenere un'autenticazione avanzata?

L'autenticazione avanzata è essenziale per proteggersi dagli attacchi. Ecco alcuni esempi:

1. **Utilizzare l'autenticazione a più fattori (MFA):** l'implementazione dell'MFA può ridurre notevolmente il rischio di furto di credenziali.
2. **Applicare policy con password più sicure:** le password sono ancora una delle forme di autenticazione più comuni, quindi è importante generarne più complesse.
3. **Implementare l'autenticazione biometrica:** l'autenticazione biometrica, come le scansioni delle impronte digitali o del riconoscimento facciale, è molto più difficile da replicare rispetto alle password e garantisce una protezione aggiuntiva.
4. **Monitorare e analizzare i registri di autenticazione:** Il monitoraggio può aiutare a rilevare e prevenire i tentativi di accesso non autorizzati. L'analisi dei registri di autenticazione fornisce indicazioni preziose su potenziali vulnerabilità della sicurezza.

Come i cybercriminali riescono ad aggirare l'MFA?



Di fronte alla crescente consapevolezza delle aziende di dover implementare le proprie misure di autenticazione, i cybercriminali hanno trovato nuovi modi per aggirare le tecnologie. Per questo è necessario comprendere punti di forza e di debolezza dell'MFA, che si distinguono in:

- **Stress da MFA:** alcune procedure di MFA richiedono all'utente di approvare l'accesso su un altro dispositivo o in una specifica app di autenticazione.
- **Attacchi Pass-the-Cookie:** molte applicazioni popolari per l'ambiente di lavoro che richiedono l'autenticazione, per esempio Slack o Teams, funzionano inserendo cookie di sessione sul dispositivo dell'utente dopo l'avvenuta autenticazione. Se un hacker è in grado di rubare cookie di sessioni valide da un dispositivo, può essere in grado di accedere come utente su un altro dispositivo senza autenticazione.

- **Attacchi Adversary-in-the-Middle:** in questi attacchi (AiTM), i cybercriminali intercettano la comunicazione tra un utente e un sistema e, inserendo un server proxy, possono raccogliere le credenziali dell'utente e rubare il cookie di sessione restituito dal sistema di autenticazione.
- **SIM Swapping:** lo scambio di SIM sfrutta il processo con cui i provider di telefonia cellulare assegnano i numeri ai nuovi dispositivi. Gli attaccanti si fingono vittime per convincere il provider a riassegnare il numero dalla carta SIM della vittima a una controllata dall'aggressore. In questo modo riescono a intercettare i codici di autenticazione e altri messaggi 2FA inviati all'utente.

Come difendersi dagli attacchi MFA Bypass

È probabile che gli hacker continuino a ideare nuovi attacchi di bypass dell'MFA, ma le seguenti best practice possono aiutare a mitigare i rischi associati ai bypass già noti:

- Limitare o disabilitare le notifiche push MFA;
- Assicurarsi che i cookie di sessione scadano a intervalli più brevi;
- Utilizzare almeno una forma di autenticazione biometrica;
- Considerare l'utilizzo di chiavi hardware per la massima sicurezza.

Inoltre, le aziende possono rafforzare le proprie superfici di identità e proteggere le credenziali con strumenti ITDR (Identity Threat Detection and Response) in grado di rilevare e prevenire in modo proattivo le minacce basate sulle identità.

Strumenti di AI per aumentare il potenziale degli analisti con funzioni di threat hunting

Quando si tratta di threat hunting, vale a dire identificare, isolare e neutralizzare in maniera proattiva le minacce informatiche più avanzate, è indispensabile poter utilizzare la query giusta per ottenere i migliori risultati. È necessario quindi che l'analista capisca quali siano gli schemi da ricercare e abbia una buona conoscenza delle sintassi della query per tradurre domande apparentemente semplici in qualcosa di comprensibile per il sistema. Oggi, le innovative tecnologie di AI generativa ci vengono incontro offrendoci una varietà di modelli e ci consentono di aumentare l'efficienza dell'organizzazione fornendo agli analisti della sicurezza un motore AI che aiuta a identificare, analizzare e mitigare le minacce utilizzando prompt e dialoghi interattivi.

Ad esempio, l'analista può fare una domanda tipo "Il mio ambiente è infettato da SmoothOperator?", oppure "Ho qualche indicatore di SmoothOperator sui miei endpoint?" al fine di individuare una minaccia specifica. In risposta, i moderni sistemi di AI generativa consentono di fornire una

tabella di risultati con approfondimenti contestuali basati sul comportamento osservato e sulle anomalie identificate nei dati restituiti. Inoltre, vengono fornite domande di follow-up e consigli su come procedere.

L'analisi delle minacce diventa più semplice con gli strumenti di AI

È risaputo che un eccessivo numero di segnalazioni o falsi positivi sia una delle sfide che i moderni centri operativi di sicurezza (SOC) devono gestire ogni giorno. La maggior parte dei team riceve più avvisi di sicurezza di quanti ne possa esaminare e risolvere. La questione è chiara: il problema della sicurezza è un problema di dati. Le informazioni si trasformano in conoscenza solo quando si applicano collegamenti significativi tra più punti di informazione, assemblando i dati contestualizzati in risultati utilizzabili.

Oltre ad aiutare i team di sicurezza a porre domande complesse per il threat hunting e a eseguire comandi operativi per gestire l'intero ambiente aziendale utilizzando il linguaggio naturale, le nuove tecnologie di AI semplificano in modo significativo anche il processo di analisi delle minacce, per determinare rapidamente ciò che sta accadendo.

Conclusioni

I protocolli di robuste autenticazioni sono fondamentali per proteggersi dagli attacchi informatici come il ransomware e, l'implementazione di misure come l'MFA con autenticazione biometrica può ridurre notevolmente il rischio di accesso non autorizzato e protegge dati e risorse sensibili. Inoltre, le nuove tecnologie di AI permettono agli analisti di sicurezza non solo di trovare rapidamente tutti gli eventi associati a una specifica attività sospetta, ma anche di poter disporre di un resoconto e di una valutazione della pericolosità in un batter d'occhio.

In particolare, SentinelOne, fornitore leader di una piattaforma di cybersecurity con capacità di autonomous response, ha recentemente presentato Purple AI, un'intelligenza artificiale generativa dedicata al threat hunting, all'analisi e alla risposta alle minacce che consente agli analisti di ottenere risposte rapide, precise e dettagliate a qualsiasi domanda e in qualsiasi lingua. Purple AI è un'intelligenza artificiale generativa integrata che consente a threat hunters e analisti dei SOC di sfruttare la potenza degli LLM (large language models) all'interno della console SentinelOne per identificare e rispondere agli attacchi in modo più rapido e semplificato.

Per ulteriori informazioni consultare www.sentinelone.com ■

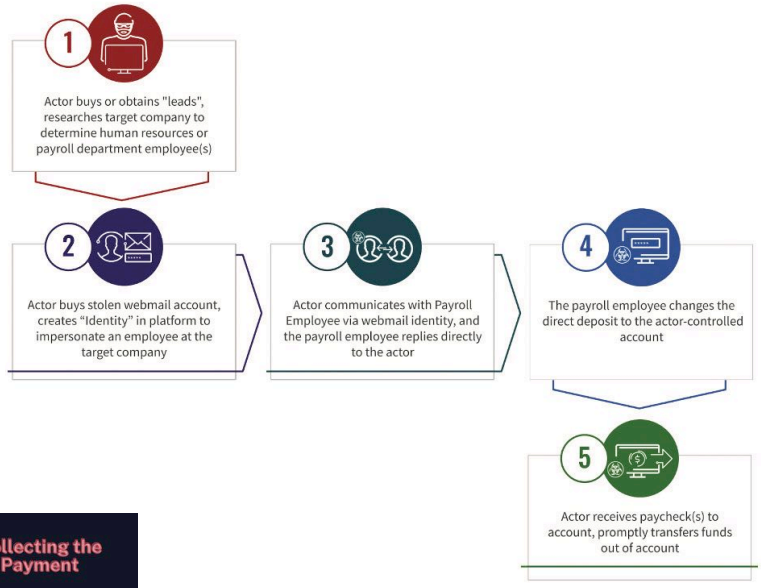
Strategie dei criminali informatici per attaccare gli istituti scolastici.

Autore: CrowdStrike Counter Adversary Operations Team

La Counter Adversary Operations di CrowdStrike monitora e tenta di neutralizzare un ampio spettro di attività di intrusione degli attori eCrime, che variano da sofisticate campagne ransomware a forme di frode più semplici ma comunque molto efficaci.

Nel periodo da ottobre 2022 all'estate 2023, CrowdStrike ha rilevato un incremento significativo e costante delle discussioni di attori eCrime sugli attacchi di payroll BEC, contenenti perfino informazioni dettagliate su alcuni istituti specifici. Il payroll BEC è un metodo di frode meno dispendioso in termini di tempo e più semplice rispetto al BEC tradizionale. Prevede che i criminali informatici contattino le risorse umane di un'azienda/istituto - in particolare il reparto che gestisce l'erogazione degli stipendi - impersonificando un dipendente, nel tentativo di sostituire le sue coordinate bancarie con quelle di un conto di propria gestione.

Struttura di una campagna di payroll BEC



Per l'inizio dell'anno scolastico, il personale delle risorse umane degli istituti scolastici dovrebbe prepararsi a riconoscere i segnali sospetti associabili alle campagne di payroll BEC, nonché ad implementare eventuali strategie rimediali per mitigare questo tipo di frode.

Spesso, gli attori eCrime condividono tutorial di campagne di payroll BEC su canali Telegram e su forum rintracciabili o del deep web. Di seguito, un esempio di questi tutorial, completo di tutti i passi da seguire per effettuare un attacco:

1. Ricerca e identificazione dell'obiettivo

a. Il tutorial suggerisce di sfruttare i motori di ricerca più diffusi per ottenere l'elenco del personale di un'azienda/istituto e identificare il responsabile del reparto dell'HR che si occupa dell'erogazione degli

stipendi. Il settore accademico è uno dei target più consigliati, visto il numero elevato di scuole di solito presenti nei paesi.

b. In seguito, è necessario utilizzare l'elenco del personale per impossessarsi dei nomi e degli indirizzi e-mail associati ai vari dipendenti da impersonificare.

2. Impersonificazione di un dipendente

a. Per impersonificare un dipendente di un'azienda/istituto, si consiglia di utilizzare un account di webmail e di creare un'identità fittizia che corrisponda al dipendente target.

b. Sfruttare il nome e l'account e-mail del dipendente preso di mira, inserendo l'indirizzo e-mail desiderato (gestito dall'attore eCrime) nel campo *"Rispondi a"* in modo tale che le risposte del thread vengano deviate e non arrivino al dipendente ma al criminale informatico e che l'azienda/istituto ne rimanga all'oscuro.

3. Interazione con l'obiettivo

a. In questa sezione viene indicato un modello di messaggio per gli aspiranti attori di BEC, ad esempio: *"Ho cambiato di recente le mie coordinate bancarie, potrebbe aggiornare le mie informazioni direttamente al momento del deposito in busta paga? Il conto precedente verrà disattivato pochi giorni prima dell'arrivo del prossimo stipendio".*

4. Sostituzione delle coordinate bancarie al momento del deposito

a. Gli operatori addetti alle buste paghe potrebbero richiedere all'attore della minaccia ulteriori informazioni per la modifica delle coordinate bancarie al momento del deposito, tra cui il numero di conto, il numero di routing e il tipo di conto (corrente o risparmio), oppure un assegno nullo che presenti il numero di routing e di conto. Viene quindi consigliato ai potenziali attori eCrime di scaricare online dei template di assegni e di modificarli in base alle proprie necessità per soddisfare la richiesta dell'operatore.

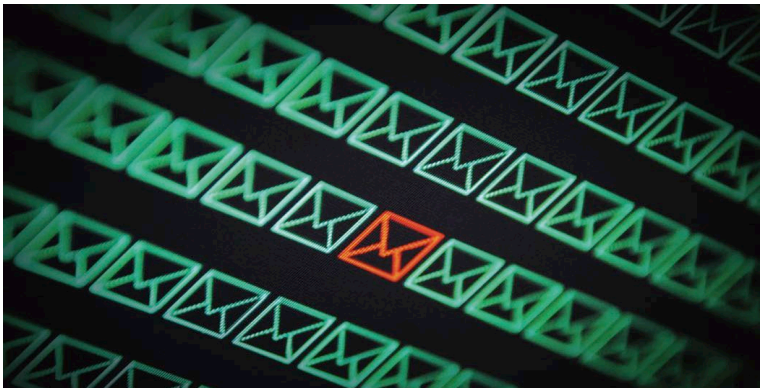
5. Incasso

a. Il tutorial suggerisce che è possibile *"utilizzare qualsiasi conto [bancario o prepagato] per ricevere lo stipendio, senza eccezioni"*. Tuttavia, alcuni sostengono che il campo dell'intestatario del conto indicato debba corrispondere a quello del dipendente impersonificato.

b. Se necessario, gli attori di payroll BEC possono collaborare con altri membri dell'ecosistema criminale che forniscono servizi di ricerca di informazioni di identificazione personale (PII) per ottenere le PII necessarie alla creazione di un account che presenti i dati del dipendente impersonificato, oppure per l'apertura diretta di un account.

Metodi di mitigazione del rischio di Payroll BEC Social Engineering

Le aziende/istituti che desiderano ridurre la probabilità che il dipartimento delle risorse umane che gestisce le buste paghe invii per errore i pagamenti dei dipendenti ad un attore eCrime possono prendere in considerazione l'implementazione delle seguenti procedure.



In primo luogo, i responsabili degli stipendi dovrebbero esaminare gli intestatari presenti nel campo *"Rispondi a"* delle e-mail in arrivo riguardanti cambiamenti delle coordinate bancarie, per verificare che le risposte all'e-mail vengano inviate solamente all'indirizzo e-mail aziendale interno del dipendente. Dato che le campagne payroll BEC si basano sull'usurpazione di indirizzi e-mail legittimi, questo passaggio può servire a comprovare che il destinatario coincida con il dipendente.

In secondo luogo, i responsabili degli stipendi o i dipendenti delle risorse umane dovrebbero prestare maggiore attenzione alle e-mail che presentano una struttura simile a quella indicata in precedenza. A causa della popolarità dei tutorial sulle campagne di payroll BEC, CrowdStrike ha verificato che gli attori eCrime di payroll BEC utilizzano le seguenti frasi *"Ho recentemente cambiato le mie coordinate bancarie"* oppure *"Il conto precedente verrà disattivato alcuni giorni prima dell'arrivo del prossimo stipendio"*, senza alcun stravolgimento. Pertanto, le aziende/istituti potrebbero implementare filtri antispam per le e-mail il cui testo del corpo corrisponde a queste frasi.

In terzo luogo, considerato che gli attori eCrime di payroll BEC sfruttano gli indirizzi e-mail, le aziende che utilizzano una piattaforma separata per le operazioni di pagamento sono intrinsecamente più protette da questo tipo di frode. Infatti, in questo secondo caso un attore eCrime dovrebbe riuscire ad ottenere le credenziali di un dipendente (probabilmente attraverso una campagna di phishing) e a eludere l'autenticazione multifattore (MFA) per accedere alla piattaforma di pagamento. Pertanto, a meno che non sia presente una specifica vulnerabilità all'interno di questa piattaforma, una tipica campagna di payroll BEC risulterebbe inefficace.

Per ulteriori informazioni sull'aumento degli attacchi di questo tipo agli istituti scolastici, ascoltare il podcast Adversary Universe, Ransomware Actors Mark Their Calendars for Back-to-School. Link all'articolo in inglese: https://www.crowdstrike.com/blog/ecriminals-use-payroll-bec-to-steal-paychecks/ ■

Navigazione strategica nell'era del digitale: oltre l'hype, tra innovazione e integrazione.

Autore: Rafy Meghnagi

In un'epoca in cui la tecnologia si evolve a un ritmo vertiginoso, è facile perdersi tra le migliaia di informazioni, nuovi termini e promesse di rivoluzione. Questo articolo non intende essere una guida tecnica dettagliata, ma piuttosto una riflessione sui meccanismi sottostanti che, spesso inconsciamente, possono distoglierci dalle reali esigenze e priorità. Esploriamo come l'euforia dell'innovazione possa talvolta offuscare la visione e come, con una prospettiva chiara e attenta, si possa navigare con prudenza nel vasto oceano digitale, mantenendo sempre la rotta verso ciò che è veramente rilevante.

Navigare l'oceano digitale: dall'euforia alla realistica visione strategica

Il panorama tecnologico odierno può essere paragonato a un vasto oceano, dove le correnti dell'innovazione possono facilmente sommergere chi è impreparato o deviarlo dalla rotta prefissata a causa di ostacoli incontrati lungo il percorso. In queste acque, ogni nuova "buzzword" agisce come una corrente seducente, promettendo velocità e direzione, ma potenzialmente trascinando le aziende lontano dalla loro rotta strategica.

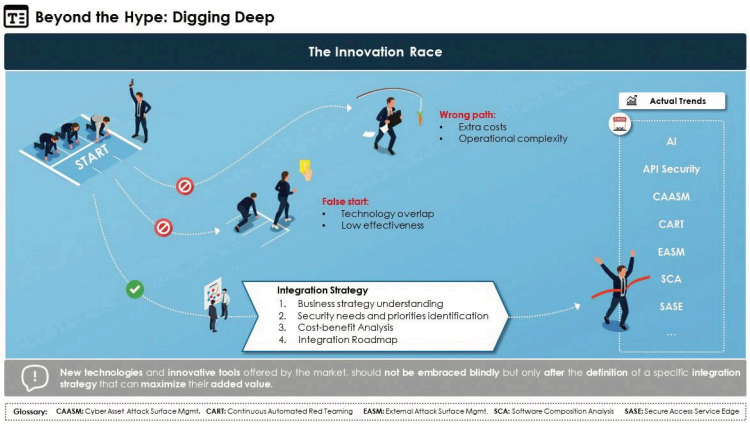
Molti leader aziendali si sentono come capitani di navi in questo vasto oceano, attirati dalle sirene delle nuove tecnologie e delle tendenze emergenti. Ma la domanda fondamentale che devono porsi è: "Sto seguendo la rotta chiara del mio business o mi sto lasciando semplicemente trascinare dalle correnti?".

Buzzword e tendenze: navigare o naufragare?

Parole come "Machine Learning", "Intelligenza Artificiale" e "Blockchain" non sono meri concetti astratti. Hanno la capacità di rivoluzionare interi settori e di reinventare le modalità di gestione del business. Tuttavia, proprio come una corrente potente, se non navigata correttamente, queste possono trascinare un'azienda lontano dalla sua destinazione desiderata.

La vera sfida per le aziende non risiede solamente nell'adottare queste tecnologie, ma comprendere quando, come e perché integrarle. Non si tratta di adottare una tecnologia perché è alla moda o perché la concorrenza lo sta facendo. Si tratta di valutare se e come quella tecnologia specifica può supportare, arricchire, migliorare o proteggere il proprio modello di business.

Oltre l'hype: scavare in profondità



Ogni nuova tecnologia, ogni nuova tendenza ha un hype associato. Spesso, ciò che viene presentato in superficie è solo l'apice di ciò che realmente esiste. E come un iceberg, ciò che giace sotto è molto più grande e rilevante.

Le aziende devono, quindi, imparare a scavare in profondità. Non si tratta solo di chiedere "Cosa può fare questa tecnologia?", ma piuttosto "Come questa

tecnologia si allinea con la nostra strategia e visione aziendale?". Ogni implementazione tecnologica dovrebbe derivare da una decisione riflessiva, fondata su una comprensione approfondita del valore che può apportare in sinergia con il proprio business.

Navigare con determinazione nel tumulto digitale

In questo paesaggio digitale in rapida evoluzione, le aziende non possono permettersi di essere semplicemente passeggeri. Devono prendere il timone, stabilire una rotta chiara e navigare con determinazione. Ciò richiede una solida comprensione non solo delle tecnologie emergenti, ma anche dei propri obiettivi di business, dei rischi associati e delle opportunità che queste tecnologie possono offrire.

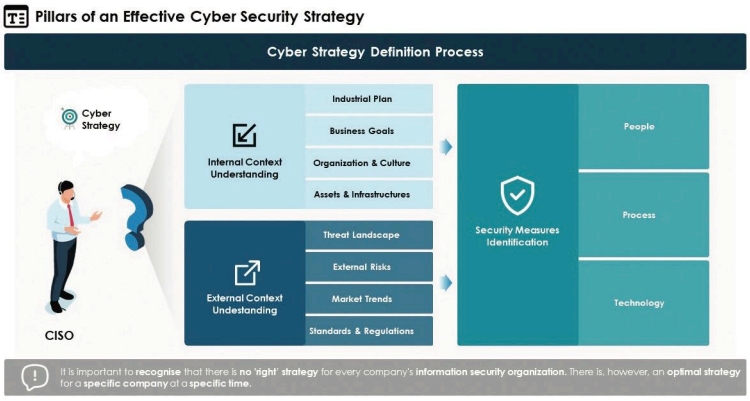
Mentre la tempesta digitale infuria è essenziale avere un faro, una chiara visione strategica, in questo tumultuoso oceano digitale. Non si tratta di resistere al cambiamento o di abbracciarlo ciecamente, ma di capire come quell'innovazione si inserisce nel quadro più ampio del viaggio (e del vantaggio) aziendale.

Il collegamento tra innovazione e sicurezza

La progressiva espansione dell'innovazione tecnologica porta con sé inevitabilmente l'esigenza di una sicurezza sempre più sofisticata. L'entusiasmo suscitato dalle nuove tecnologie non dovrebbe mai offuscare l'importanza di proteggere e garantire la sicurezza dei dati e delle infrastrutture. Proprio come l'adozione di nuove tecnologie dovrebbe essere basata su una profonda comprensione del valore aziendale, allo stesso modo la sicurezza dovrebbe essere integrata nella stessa fase di implementazione, garantendo che l'innovazione non si trasformi in una vulnerabilità e ponendo fiducia nelle pratiche di sicurezza sin dalla progettazione (security by design).

Pilastro nell'era digitale: strategia e business

La sicurezza, tuttavia, non dovrebbe essere l'unico focus. Mentre navighiamo in questo oceano digitale, dobbiamo anche assicurarci di mettere al centro le esigenze e le finalità del nostro business. Una strategia di Cyber Security non dovrebbe essere una reazione precipitosa alle ultime notizie di violazioni o una corsa all'adozione dell'ultima soluzione "rivoluzionaria" sul mercato. Deve essere un processo riflessivo, radicato in una profonda comprensione del DNA aziendale. Dopo tutto, se non comprendiamo pienamente ciò che è essenziale per il nostro business, come possiamo sperare di proteggerlo adeguatamente?



Pilastri di una strategia di Cyber Security efficace

Nel panorama diversificato della Cyber Security, non affrontiamo una soluzione unica o un prodotto isolato. Piuttosto, ci troviamo di fronte a un intricato mosaico, in cui ogni componente svolge un ruolo cruciale. Per garantire la robustezza di questo mosaico e il suo allineamento con le necessità aziendali, è essenziale costruire su tre pilastri fondamentali:

- Conoscenza Profonda del Business: L'azienda deve sempre avere la precedenza sulla tecnologia. È essenziale conoscere dettagliatamente gli asset, sia tangibili che intangibili, per poterli proteggere in modo appropriato.
- Comprensione delle Minacce e dei Rischi: Ogni minaccia è diversa e comporta un rischio potenziale specifico per l'organizzazione. Disporre di strumenti accurati per identificare e valutare minacce e rischi, sia quelli immediati che quelli nascosti, è fondamentale.
- Selezione dei Presidi Adeguati: Di fronte a un mercato in continua evoluzione di soluzioni, la questione chiave è se la soluzione scelta risponde veramente alle esigenze e ai rischi specifici dell'azienda. Senza dimenticare che i presidi non sono unicamente di natura tecnologica (non esiste solo il salvagente) ma anche in termini di ruoli, responsabilità e processi (l'intera imbarcazione deve essere solida e affidabile).

Durante questa fase di selezione, emerge spesso un gap critico. Nonostante molte aziende abbiano una solida comprensione del proprio ambito operativo e dei rischi associati, possono incorrere in errori nella scelta dei presidi tecnologici. Queste imprecisioni possono nascere non solo da una visione limitata delle ultime innovazioni tecnologiche, ma anche dall'essere fuorviati da buzzword e "hype" del momento, che distraggono dalla reale necessità di identificare e risolvere i problemi specifici.

In altre parole, è essenziale non farsi accecare dalle tendenze tecnologiche del momento, ma piuttosto concentrarsi su ciò che veramente conta: identificare e affrontare le minacce e i rischi che sono più rilevanti per il nostro business. Proprio in questo contesto di ricerca continua e di attenzione alle reali necessità, le start-up emergono come uno strumento prezioso.

L'innovazione delle start-up: oltre il tradizionale

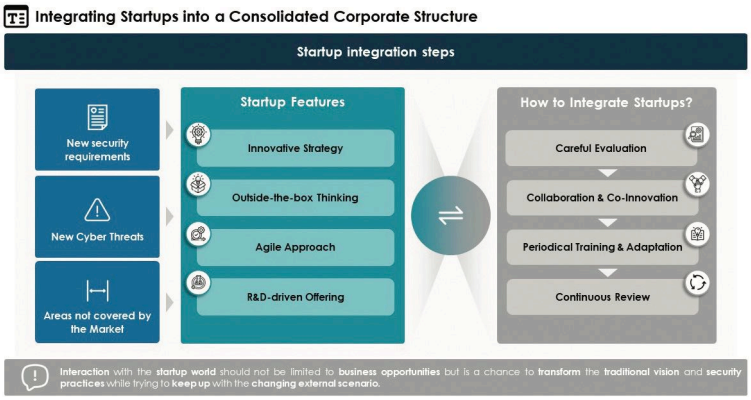
Nel dinamico mondo della Cyber Security, le start-up emergono come catalizzatori di trasformazione. Con il loro spirito intraprendente e visionario, sfidano lo status quo, rompendo schemi predefiniti e introducendo soluzioni inedite. Il loro approccio innovativo spesso ci costringe a rivedere e riformulare il modo in cui affrontiamo le sfide della sicurezza.

Queste aziende, agili e veloci nella risposta, sono in grado di adattarsi alle nuove sfide con una prontezza che molte aziende consolidate possono trovare stimolante. La loro passione per l'innovazione introduce continuamente nuovi strumenti e metodologie, apportando una ventata di freschezza nel panorama della Cyber Security.

Nell'attuale scenario, dove i "Pure Player" tecnologici dominano il mercato, esistono ancora lacune e aree non coperte. Qui entrano in gioco le start-up, che spesso propongono soluzioni e tecniche innovative in grado di colmare queste lacune, offrendo risposte a domande che i player tradizionali non hanno ancora considerato.

Ridurre le start-up a un semplice ruolo accessorio sarebbe un grave errore. Sono esse il fulcro delle idee più innovative e avanzate, capaci di rivoluzionare e completare l'approccio consolidato di un'organizzazione alla Cyber Security. Tuttavia, quando una soluzione innovativa viene adottata, è fondamentale che questa si integri armonicamente nell'ecosistema aziendale. Non si tratta di una mera inserzione di una nuova tecnologia, ma di un'integrazione attenta e mirata. Questa deve fondersi con l'infrastruttura esistente dell'organizzazione, assicurando che il suo valore aggiunto sia pienamente realizzato e capitalizzato.

Integrando le start-up in un tessuto aziendale consolidato



Le start-up, con la loro natura agile e l'approccio rivoluzionario, offrono spesso una visione fresca e una soluzione alle sfide emergenti nel mondo della Cyber Security. Questa capacità di "pensare fuori dagli schemi" può dare un valore incommensurabile, soprattutto quando le organizzazioni affrontano minacce in costante evoluzione. Ma come si fa a integrare queste nuove proposte in un ecosistema aziendale che potrebbe essere profondamente radicato in prassi e tecnologie consolidate?

- Valutazione attenta: Prima di adottare qualsiasi nuova soluzione proposta da una start-up, è vitale sottoporla a un'analisi approfondita. Questo permette di assicurarsi che la soluzione non solo risolva una sfida attuale ma sia anche sostenibile a lungo termine.
- Collaborazione e co-Innovation: Le start-up, con la loro mentalità aperta, sono spesso disposte a personalizzare le loro soluzioni in base alle esigenze specifiche di un'organizzazione. Avviare un dialogo produttivo può garantire che l'innovazione proposta si integri perfettamente nel tessuto esistente. Tale scenario può, inoltre, aprire a ulteriori sviluppi in termini di business.
- Formazione e adattabilità: L'introduzione di nuove soluzioni richiede spesso una formazione adeguata per gli utenti finali. Investire nella formazione assicura che la nuova tecnologia venga utilizzata al massimo delle sue potenzialità.
- Revisione continua: L'adozione di una soluzione innovativa non dovrebbe essere vista come un processo una tantum. Piuttosto, dovrebbe essere sottoposta a revisioni periodiche per assicurarsi che continui a soddisfare le esigenze dell'organizzazione.

BIO

Con un bagaglio di 11 anni nel mondo della consulenza, Rafy Meghnagi oggi è un Senior Manager nell'area Cyber Security di Deloitte. Gli esordi della sua carriera lo hanno visto immergersi profondamente in ruoli squisitamente tecnici, con una particolare enfasi sugli aspetti infrastrutturali e di sicurezza. Questa formazione gli ha conferito una solida base, su cui ha costruito la sua identità nel tempo. La traiettoria professionale di Rafy non si è limitata solo all'aspetto tecnico. Infatti, spinto da un innato desiderio di affrontare e superare nuove sfide, ha successivamente intrapreso un percorso consulenziale più strategico e orientato al cliente.
In questo contesto, come advisor, Rafy si dedica con passione e determinazione a trasferire tutto il suo know-how ai clienti, puntando a generare un reale impatto e valore aggiunto in ogni singolo progetto che lo vede coinvolto.La dualità della sua formazione, che combina competenze tecniche con capacità consulenziali, rende Rafy un professionista equilibrato, in grado di affrontare con metodo, profondità e precisione le diverse sfide che il mondo della consulenza presenta ogni giorno.

Orientarsi nell'innovazione: la bussola nel digitale

Navigare nel tumultuoso oceano del digitale richiede ben più di un semplice capitano; necessita di un vero timoniere, una figura che non si perda nel canto delle sirene tecnologiche, ma che sappia orientarsi tra le onde dell'innovazione. Le aziende non devono cadere nella trappola di inseguire ciecamente ogni nuovo trend, perdendo di vista la propria bussola strategica. È fondamentale porsi le giuste domande, scavando oltre l'apparente e l'hype per identificare reali opportunità che rispecchiano e potenziano il DNA aziendale. Inoltre, nell'ambito della Cyber Security, l'orizzonte sempre in evoluzione delle start-up può offrire nuovi percorsi e soluzioni, ma è cruciale integrarli con cura e consapevolezza nel tessuto dell'organizzazione. Alla fine, essere proattivi piuttosto che reattivi, guardando oltre il consolidato, può fare la differenza tra una navigazione sicura e un naufragio nel vasto mare del digitale. ■

Ransomware.

Autore: Leonardo Casubolo

Cosa si intende per Ransomware

Anche se immagino siamo tutti allineati sul significato del termine "Ransomware", preferisco chiarire l'argomento di cui voglio trattare.

Per ransomware si intende quella famiglia di malware che "rapiscono" i dati e li rendono nuovamente disponibili dopo il pagamento di un riscatto.

BIO

Ancora studente di Ingegneria Elettronica al Politecnico di Milano, Leonardo Casubolo inizia a lavorare come sviluppatore di software per l'industria dei videogiochi e dell'integrazione di sistemi. Terminato il percorso accademico, inizia la sua carriera professionale, coordinando gruppi di sviluppo impegnati in diverse aree di sviluppo software come videogiochi, automazione, archiviazione di documenti... Nel 2001 entra in OM Carrelli Elevatori S.p.A. come responsabile dei sistemi informatici. Nel 2008 ha assunto il ruolo di Chief Security Officer nel Gruppo KION. Da ottobre 2014 è Direttore Globale Infrastruttura IT e Sicurezza di Burckhardt Compression AG.

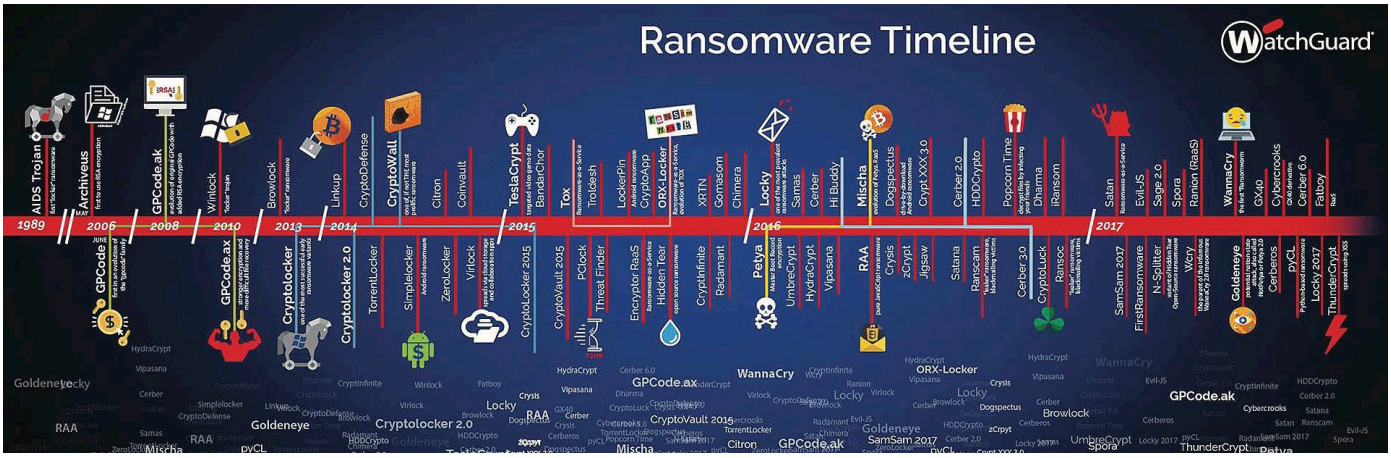
Questo viene realizzato lasciando i file dove si trovano ma crittografandoli. La chiave crittografica necessaria per accedere al contenuto è nota all'attaccante fino al pagamento di un riscatto.

Nel tempo si è aggiunta la pratica di esportare i dati, aggiungendo la minaccia di pubblicarli, e la «conquista» dei servizi di directory, controllando così tutti gli account e i computer della rete attaccata.

Come funziona il tutto?

Esistono varie implementazioni, ma la modalità operativa più comune è costituita da un certo numero di fasi:

- un primo elemento infettante, spesso molto limitato e, quindi, piccolo, inviato via e-mail e reso disponibile su un sito web;
- questo, sfruttando vulnerabilità del sistema attaccato o eccessivi diritti amministrativi dell'utente, si installa localmente;
- a questo punto, il software cerca di accedere ad Internet per scaricare da un "centro servizi" la versione completa dell'infezione e le chiavi di crittografia personalizzate per lo specifico bersaglio. Le chiavi sono personalizzate per evitare che sia possibile riutilizzate chiavi crittografiche di sblocco concesse ad un'altra vittima;
- tale software, tenta anche di stabilire un canale sicuro di comunicazione per ricevere comandi e per eventualmente trasferire in uscita informazioni sull'architettura, dati veri e propri e credenziali di accesso;



- quindi esso tenta di replicarsi sulla rete locale installando le sue componenti su altri client con una azione di lateral movement;
- durante la diffusione, l'attacco cerca di estrarre copie locali di credenziali di amministrazione per poter accrescere le sue capacità amministrative (privilege escalation). Con l'obiettivo, passo dopo passo, di prendere controllo dei domain controllers. Anche qui, patch mancanti o diritti ammnistrativi troppo generosi, agevolano l'attaccante;
- una volta riuscito a diffondersi adeguatamente, e avendo raccolto opportune credenziali amministrative, attende il momento propizio (magari una festività locale, quando si può supporre una minore presenza di supervisione tecnica) per effettuare la crittografia dei dati e comunicare alle vittime che potranno accedere nuovamente ai dati fronte il pagamento di un riscatto.

Nel corso del tempo, all'attacco base, si sono aggiunti:

- estrazione di dati più o meno sensibili. O dal punto di vista business o legale.
- questi serviranno ad accrescere la pressione sulla vittima. Vuoi mostrandoli come prova, vuoi minacciando la pubblicazione;
- alterazione dei sistemi di backup. Spesso le copie di backup non vengono verificate, l'infezione dei sistemi di backup può generare copie di backup compromesse. In alcuni casi, sfruttando il fatto che le copie di backup per essere rilette necessitano di un "indice" delle versioni (noto anche come catalogo), è sufficiente attaccare tale database per rendere inutilizzabili, o almeno difficilmente utilizzabili, le copie di backup. Anche quelle offline;
- disattivazione delle credenziali amministrative. Compromettendo le capacità di reazione della vittima e inibendo l'accesso a multiple funzioni aziendali;
- compromissione dei sistemi di produzione. Anche se il ransomware non è specializzato nei sistemi di supporto/controllo della produzione, può compromettere l'operatività della produzione aziendali rendendo inutilizzabili le console di gestione dei macchinari, spesso dei semplici PC (più o meno protetti da polvere e altre condizioni ambientali avverse).

Perché "ransomware" è oggetto di così tante attenzioni

Le ragioni sono multiple. A differenza di un classico virus che può "limitarsi" a rendere i sistemi non funzionanti, nel caso del ransomware sono i dati

ad essere compromessi. Con danni diretti (cessazione delle attività) ed indiretti (pubblicazione dei dati o delle credenziali estratte), con implicazione come la violazione di accordi di riservatezza. Inoltre, l'ammontare del riscatto può non essere banale. Un ulteriore danno collaterale, conseguente sia al fermo di produzione che alla pubblicazione dei dati, è la compromissione dell'immagine aziendale.

Non ultimo, in molti contesti legali la pubblicazione di dati oggetto di accordi di riservatezza o personali/sensibili, comporta ulteriori danni economici e conseguenze legali.

Inoltre, oggidì esistono dei "kit" acquistabili nel Darknet. Tali kit sono dei veri e propri Malware As A Service e permettono di effettuare attacchi pur disponendo di limitate conoscenze tecnologiche.

Questo permette ad un maggior numero di individui di effettuare attacchi e garantisce ai veri artefici un ulteriore livello di separazione dalla vittima. E un conseguente incremento della impunità (nonché un aumento della "potenza di fuoco" e conseguenti guadagni).

Quali sono le vie di accesso per un attacco ransomware

Come accennato in precedenza, un attacco ransomware necessità un metodo di ingresso per una prima, piccola, infezione: una e-mail, una pagina web, una chiavetta USB.

Quindi richiede un accesso ad Internet per procedere con i passi successivi.

Effettua poi dei movimenti laterali per diffondersi e cerca di sfruttare vulnerabilità per estrarre credenziali amministrative.

Come vedete, non è un attacco semplice. Richiede multipli passaggi e può essere individuato e fermato in ognuno di essi.

Ed è, in genere, un attacco lento. In molti casi permane per mesi nei sistemi. Collezionando e trasferendo informazioni, prima di bloccare i dati.

Per quanto è importante indagare eventuali anomalie.

Questo può essere fatto con vari strumenti. Alcuni sono:

- **Network Detection and Response**

Gli NDR funzionano catturando e analizzando il traffico di rete. Il traffico viene quindi scansionato alla ricerca di attività sospette, come l'uso di porte non standard o l'invio di grandi quantità di dati o cambi di attività, effettuando la comparazione con le passate attività. Se viene rilevata attività sospetta, l'NDR può essere configurato per generare avvisi o intraprendere azioni per bloccare l'attacco.

- **Endpoint Detection and Response**

Gli EDR funzionano raccogliendo dati dagli endpoint, come registri di sistema, file e attività dei processi. I dati vengono quindi analizzati alla ricerca di attività sospette, come l'esecuzione di malware o l'accesso a file non autorizzati. Anche qui, la comparazione con il passato può aiutare a determinare anomalie. Se viene rilevata attività sospetta, l'EDR può essere configurato per generare avvisi o intraprendere azioni per bloccare l'attacco.

- **eXtended Detection and Response**

Gli XDR sono una evoluzione degli EDR. Il traffico di rete è un elemento addizionale nelle attività di analisi/individuazione.

Come proteggersi dagli attacchi ransomware

Come per qualsiasi attacco informatico, bisogna tenere in considerazione che non esiste una protezione al 100%. Un attaccante giustamente motivato potrà

sempre trovare un "punto di ingresso": una vulnerabilità non corretta (applicate tutte le patch?,quanto tempo passa dalla pubblicazione di una patch all'applicazione della stessa su tutti i computer interessati?), un utente non attento, …

Focalizzandosi sugli attacchi "commodity", che sono indubbiamente la maggioranza, molto fa la normale "igiene":

- sistemi operativi ed applicazioni aggiornate;
- diritti amministrativi limitati alle reali attività dell'amministratore e dell'utente;
- accesso ai dati limitato a chi necessità di tale accesso;
- protezione delle identità degli utenti, con obbligo di Multifactor Authentication quando al di fuori di reti gestite;
- limitazione dell'accesso ai dati solo con macchine dotate di un adeguato livello di sicurezza;
- verifica periodica delle impostazioni di sicurezza;
- penetration test;
- predisposizione di un piano di reazione agli attacchi informatici ed esercitazione sullo stesso. Nel piano non vanno dimenticati passi che appaiono secondari, ma che non lo sono quando i problemi accadono (chi contattare e come, non dimenticando fornitori, partner, assicurazione e autorità), la sequenza di ricostruzione dei sistemi, come verificare che gli stessi siano puliti prima di rimetterlo in linea (altrimenti correte il rischio di ripartire da capo) e, molto importante, chi ha il diritto di decidere quali sistemi mettere offline per proteggerli dall'attacco in corso e chi può decidere se tentare una "ripulitura" e ripartire dalle copie di sicurezza.

Inoltre, oggidì sono necessari (non solo per gli attacchi ransomware):

- sistemi di identificazione e soppressione delle minacce (accettando qualche falso positivo) come EDR e XDR;
- uno spam filter che possa prevenire email infette;
- verifica e limitazione dell'accesso ad Internet;
- soluzioni di browsing sicuro (oggi offerte, almeno nella versione "entry level", dai più noti browser);
- sistemi di monitoraggio (solo se avete la reale possibilità di sfruttarli, altrimenti forniscono solo un falso senso di sicurezza);
- avere accordi con una società di Cybersicurezza che possa aiutarvi nell'identificare l'attacco, nella mitigazione dei danni e nella ripartenza.

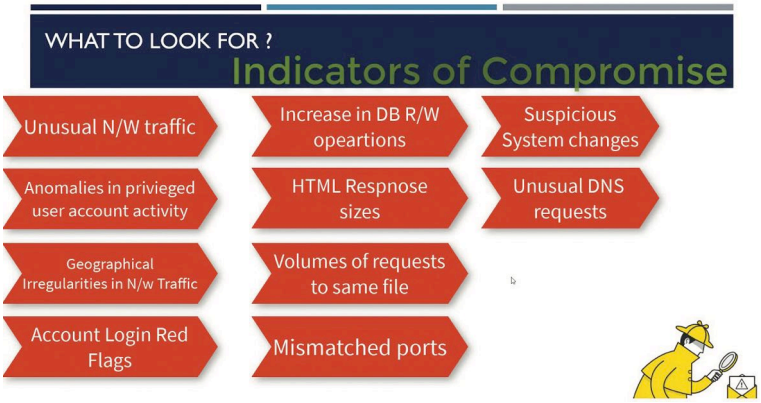
Reputo che la predisposizione di un piano di reazione e la sua simulazione siano un elemento fondamentale. Permettono di reagire in modo organizzato, non caotico. Sicuramente non alleggeriscono la tensione in un caso reale. Ma almeno vi danno la certezza che le azioni introdotte sono note, di sapere dove sono i vari strumenti/contatti e come usarli, e ciascuno conosce le reazioni degli altri colleghi che contribuiscono al risultato.

Come limitare i danni

E se le varie contromisure falliscono e siete vittima di un attacco ransomware? Scoprirete che è estremamente utile aver redatto un piano di reazione, averlo simulato e sapere chi e come contattare le varie persone.

Soprattutto, se l'attacco viene individuato sul nascere, sarà fondamentale che sia già stato individuato chi e a quali condizioni possa decidere di fermare i servizi salvando il salvabile e lo faccia con la sequenza corretta per evitare corruzioni dei dati. Questo è un elemento per niente secondario. Il tempo per l'esecuzione dell'encryption dei dati non è zero. Ma non è di giorni. Il tutto si compie in minuti/ore in dipendenza delle dimensioni (numero dei sistemi, presenza di sistemi remoti, mole di dati). Non dimenticate che l'attaccante fino all'ultimo cercherà di non essere individuato. E sa che azioni repentine possono destare la vostra attenzione. Questo, almeno in parte, lo forza ad un approccio non troppo aggressivo/rapido.

Una volta che i sistemi sono stati fermati (o resi inutilizzabili) dovrete verificare che le ultime azioni di "estrema difesa" siano state completate correttamente (leggi: backup). Accertatevi di essere nelle condizioni di farlo. Considero utile avere una copia dell'active directory e un secondo server di backup per avviare le operazioni di ripristino. Tale server e i domain controller che contengono copia dell'active directory possono essere sincronizzati periodicamente. Sicuramente la sincronizzazione periodica è la fase più rischiosa, ma avere questi elementi in uno stato quiescente vi può permettere di ripartire molto più rapidamente. E, essendo quiescenti, potrete accertarvi di aver individuato l'infezione prima di attivarli nuovamente. E non sono utili solo in caso di attacco ransomware.



È vitale identificare gli indicatori di compromissione, ovvero quanto permette di individuare con certezza l'attacco. Infatti, dovrete accertarvi di averlo rimosso dai sistemi prima di effettuare le operazioni di ripristino e, ogni volta che un sistema viene ripristinato, dovrete accertarvi che la copia ripristinata sia priva (o venga ripulita) dall'infezione prima di collegarla alla rete.

Come potete immaginare, in questa fase è fondamentale poter contare del supporto di una società di consulenza informatica con opportuna esperienza nel settore e con cui avete un rapporto regolare. Solo così potete essere certi che conoscano i vostri sistemi e siano in grado di fornire istruzioni ritagliate sulla vostra realtà.

Pagare o non pagare?

La più grande incognita rimane: pagare o non pagare?

In alcune legislazioni pagare significa anche incorrere in sanzioni per violazioni sulle norme che regolano i pagamenti non tracciati, il sostegno ad attività criminali ...

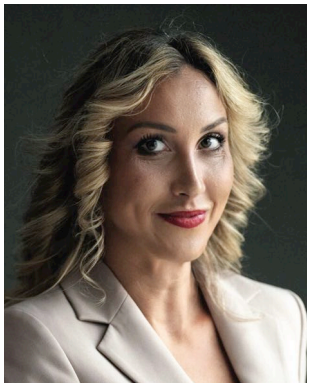
Inoltre, visto che state trattando con persone di non proprio specchiata moralità, cosa evita loro di usare dei dati sottratti in precedenza allo scopo di mostrarvi la capacità di decrittare, ma in ultimo non rilasciare alcuna soluzione per rimuovere la cifratura dei dati?

Anche se, ad oggi, sono stati rari i casi in cui ad un pagamento non sia corrisposto uno sblocco dei dati. Forse perché chi ha pagato una volta è un ottimo candidato per un successivo attacco in tempi di magra.

Certo che se non avete copie, non riuscite ad individuare il codice infettante e siete oggetto anche della minaccia di pubblicare dati sensibili…

Ergo, preparatevi al meglio e verificate se le vostre strategie di backup sono allineate con le esigenze di business. Inclusa una valutazione sui danni d'immagine. Se non reputate di essere in grado di implementare delle soluzioni sufficientemente robuste, considerate di trasferire le vostre soluzioni on premise in soluzioni Cloud SaaS. Seppure le certificazioni non siano di per sé un sinonimo di robustezza, una società che eroga servizi SaaS che rispondano a certificazioni multiple e che faccia di tali servizi il proprio core business ha buone probabilità di aver implementato opportune soluzioni. ■

Conoscere i Ransomware: Minacce, Prevenzione e Ripristino.



Autore: Jelena Zelenovic Matone

Introduzione

Il ransomware, un software dannoso che crittografa i file e richiede un pagamento per il loro rilascio, ha una storia lunga e leggendaria che risale a diversi decenni fa. Il primo esempio conosciuto di ransomware, il "Trojan AIDS", è emerso alla fine degli anni '80 come presagio delle future minacce digitali. Tuttavia, è stato solo a metà degli anni 2000 che il ransomware ha iniziato a catturare veramente l'attenzione sia degli esperti di cybersecurity che dell'opinione pubblica, segnando l'inizio del suo significativo aumento di popolarità e prevalenza.

Durante le fasi evolutive del ransomware, una particolare variante nota come "Reveton" ha raggiunto un famigerato status intorno al 2012. Questa variante ha adottato una metodo particolarmente sinistro impiegando messaggi a tema di polizia per intimidire le vittime e indurle a cedere alle sue richieste di pagamento. La manipolazione psicologica associata a tali messaggi ha aggiunto un nuovo livello di minaccia al panorama dei ransomware.

Il panorama dei ransomware ha subito un cambiamento sostanzaile con l'emergere di varianti più sofisticate come "CryptoLocker" nel 2013. Questi ceppi avanzati di ransomware sfruttavano tecniche di crittografia avanzate rendendo i file delle vittime praticamente resistenti alla decrittazione senza l'intervento degli aggressori. Questa nuove tecniche hanno alzato considerevolmente la posta in gioco, poiché le vittime si sono trovate di fronte alla prospettiva di perdere per sempre i loro preziosi dati se non avessero pagato il riscatto.

Negli ultimi anni, la minaccia rappresentata dal ransomware è aumentata notevolmente, catturando l'attenzione globale a causa di incidenti di alto profilo come gli attacchi WannaCry e NotPetya. Questi attacchi su larga scala hanno dimostrato il caos e i blocchi che gli operatori di ransomware potrebbero scatenare. Ad aggravare il rischio, gli operatori di ransomware hanno evoluto le loro tattiche, includendo il concetto di doppia estorsione. Questa tecnica prevede non solo la crittografia dei file delle vittime, ma anche la minaccia di rendere pubblici dati sensibili e riservati, aumentando così in modo esponenziale la pressione sulle vittime affinché vengano rispettate le richieste di riscatto.

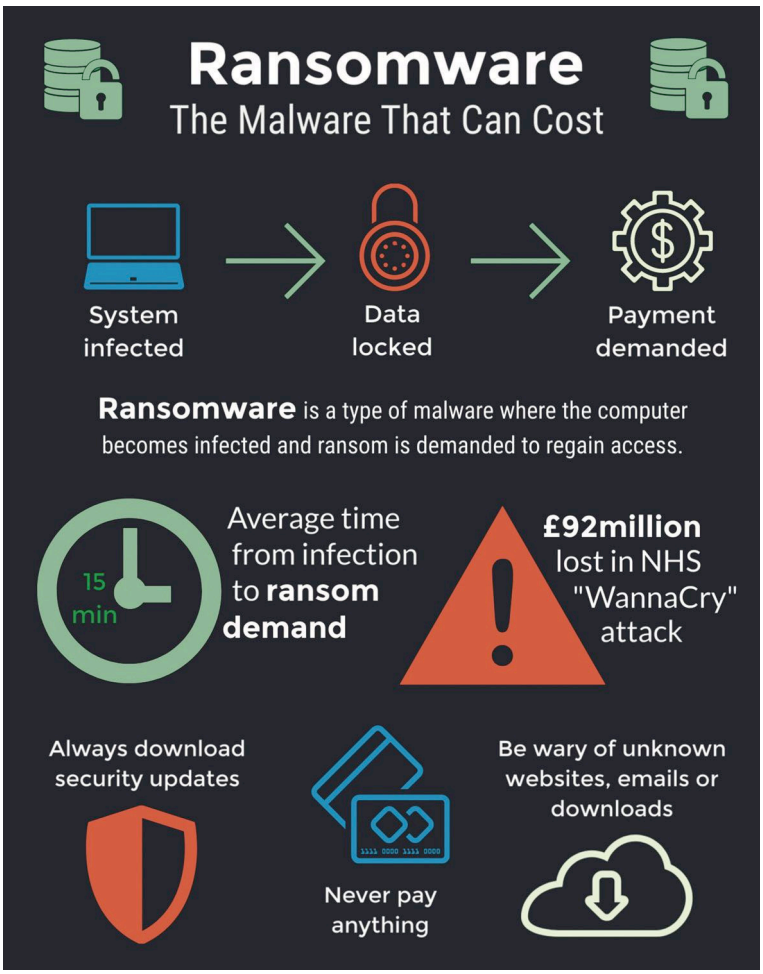
In questo panorama sempre più ostile, le infrastrutture critiche, le aziende di tutte le dimensioni, gli ospedali e le organizzazioni governative sono diventati tutti obiettivi primari per gli attacchi ransomware. Anche gli importi dei riscatti richiesti sono cresciuti in modo esponenziale, raggiungendo spesso cifre astronomiche, il tutto con pagamenti in criptovalute in grado di garantire un livello di anonimato agli autori dei reati.

Per contrastare efficacemente la crescente minaccia del ransomware, è essenziale un approccio globale e multiforme. Questo approccio richiede gli sforzi congiunti di esperti di cybersecurity, forze dell'ordine e cooperazione internazionale. Le difese tecnologiche devono essere continuamente rafforzate per proteggersi dalle strategie in continua evoluzione degli operatori di ransomware. Altrettanto importanti sono gli sforzi delle forze dell'ordine volti a rintracciare e ritenere questi cybercriminali responsabili delle loro azioni.

Poiché le minacce ransomware continuano a evolversi e mutare, mantenere uno stato di attenzione è fondamentale. Le misure proattive sono componenti essenziali di qualsiasi strategia di difesa. Rimanendo informati, preparati e coesi di fronte a questa piaga digitale, gli individui e le organizzazioni possono proteggere meglio se stessi e i propri dati dalla morsa insidiosa del ransomware.

Gli attacchi ransomware possono infatti scatenare un'ondata di conseguenze distruttive che si ripercuotono sia sulla vita individuale che sul panorama organizzativo. L'intricata rete di impatti che questi attacchi possono avere è di vasta portata e comprende vari aspetti del benessere degli individui:

Impatto sugli Individui



1 **Perdita di Dati:** il ransomware non si limita a crittografare i file; interrompe l'accesso a ricordi preziosi e documenti importanti, lasciando le vittime con un evidente senso di perdita. Foto dal valore inestimabile, documenti cari e altri ricordi digitali possono essere rinchiusi a tempo indeterminato, privando le persone della loro eredità digitale.

2 **Perdita Finanziaria:** le vittime si trovano a un bivio: pagare il riscatto o rischiare di perdere i propri dati per sempre. Il pagamento del riscatto può portare a significative difficoltà finanziarie, mentre la scelta di non pagare spesso comporta costi ingenti per il recupero dei dati e la riparazione del sistema. In entrambi i casi, le implicazioni finanziarie possono persistere a lungo anche dopo la fine dell'attacco.

3 **Violazione della Privacy:** la minaccia del ransomware di esporre dati privati è simile a una violazione degli aspetti più intimi della propria vita. La semplice idea che informazioni sensibili vengano esposte ad attori malevoli può portare a una profonda violazione dei confini personali e a una compromissione della fiducia nelle piattaforme digitali.

BIO

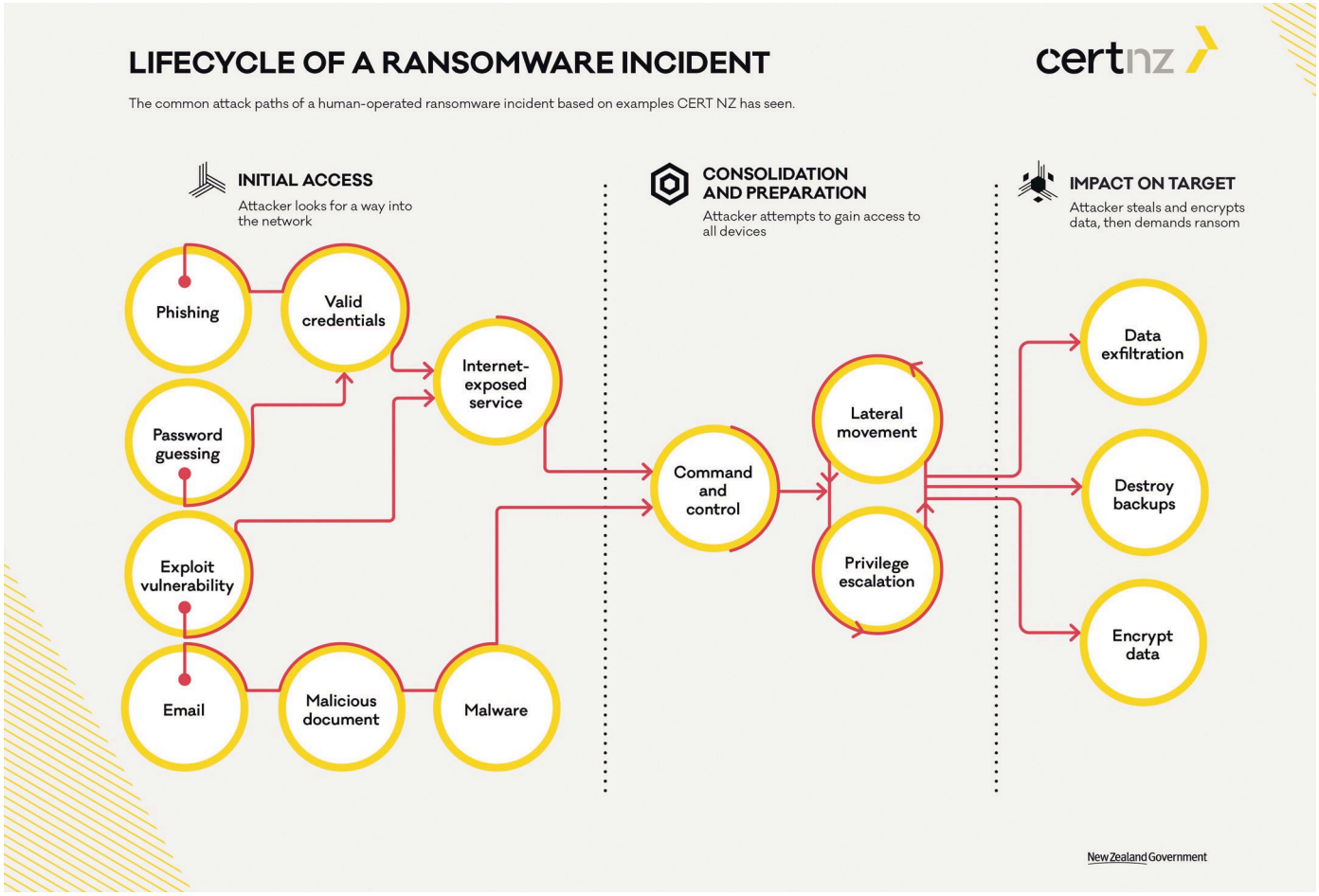
Rispettata leader CISO, insignita del CISO dell'anno per il 2019 in Lussemburgo, Sentinel CISO Global 2020, EU CISO 2020 e Ambasciatore dell'anno 2021 in Lussemburgo, Jelena è esperta di Cybersecurity versatile e innovativa con enfasi sulla gestione del rischio di sicurezza informatica/ risk management,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

4 **Impatto Emotivo:** il carico emotivo conseguente a un attacco ransomware può essere molto pesante. I sentimenti simultanei di impotenza, ansia e frustrazione possono mettere a dura prova il benessere mentale. L'incapacità di accedere ai file personali, unita alla paura di una potenziale esposizione dei dati, può sfociare in stress, depressione e altri problemi emotivi.

5 **Furto di Identità:** il furto di informazioni personali in un attacco ransomware può avere effetti a lungo termine. Le vittime potrebbero scoprire che i loro conti finanziari sono compromessi, le loro informazioni personali sfruttate e il loro senso di sicurezza distrutto. Ricostruire la fiducia nelle interazioni digitali e nei sistemi finanziari diventa una battaglia difficile.

Impatto sulle Organizzazioni

1 **Interruzione Operativa:** l'impatto del ransomware sulle organizzazioni va oltre il mondo digitale. La paralisi dei sistemi e dei dati importanti può tradursi in interruzioni operative nel mondo reale. Questi attacchi possono bloccare la produttività, bloccare l'evasione degli ordini dei clienti e portare a ritardi nelle tempistiche dei progetti. In casi estremi, la portata dell'interruzione può costringere le organizzazioni a confrontarsi con la triste possibilità di interrompere completamente le loro attività.



2 **Danni Finanziari:** le conseguenze finanziarie di un attacco ransomware possono essere impressionanti. La combinazione dei tempi di inattività, dei costi associati al ripristino dei dati e del sistema e delle potenziali azioni legali può infliggere un duro colpo ai profitti di un'organizzazione. Gli effetti a catena di tale danno finanziario possono ripercuotersi per anni, influenzando le opportunità di investimento, i piani di crescita e la stabilità economica complessiva.

3 **Danni alla Reputazione:** gli effetti a catena delle violazioni dei ransomware si estendono al mondo dell'opinione pubblica. La divulgazione pubblica di un attacco può distruggere la reputazione di un'organizzazione, erodendo la fiducia di clienti, partner e stakeholder. La compromissione della fiducia può avere implicazioni di vasta portata, influenzando i tassi di fidelizzazione dei clienti, attirando l'attenzione negativa dei media e provocando potenzialmente un calo a lungo termine delle entrate.

4 **Ripercussioni Normativi e Legali:** per i settori che gestiscono dati sensibili, come quello sanitario e finanziario, le conseguenze di un attacco ransomware possono oltrepassare le crisi finanziarie e operative. La mancata protezione dei dati sensibili può portare a sanzioni normative, azioni legali e problemi di conformità. Le conseguenze legali potrebbero coinvolgere non solo i clienti che chiedono risarcimenti, ma anche le autorità di regolamentazione che esaminano attentamente le procedure di protezione dei dati dell'organizzazione.

5 **Perdita di Dati:** nei casi in cui le organizzazioni scelgono di non pagare il riscatto o non dispongono di backup completi, la perdita di dati importanti diventa una triste realtà. Questa perdita può interrompere la business continuity, ostacolare i processi decisionali e impedire la pianificazione futura. Il vuoto lasciato da dati insostituibili può avere un profondo impatto sugli obiettivi strategici a lungo termine dell'organizzazione.

6 **Interruzione della Supply Chain:** la natura interconnessa del ransomware può trasformarlo in un'infezione a catena, diffondendosi attraverso la rete di un'organizzazione e penetrando nelle reti dei suoi partner e fornitori. La conseguente interruzione della supply chain può estendersi a tutti i settori, colpendo più organizzazioni ed aggravando l'impatto iniziale sul soggetto target.

L'interconnettività

La violazione iniziale del ransomware nelle difese di un'organizzazione è simile al paziente zero in una pandemia. Una volta dentro, cerca di propagarsi, sfruttando la natura interconnessa della rete. Ma non si ferma all'host interessato; si infiltra nelle reti di partner, fornitori ed entità interconnesse. Questo contagio digitale trasforma una singola violazione in un attacco diffuso, un incidente isolato in una crisi sistemica.

Reazione a catena dell'impatto

L'interruzione all'interno della rete di un'organizzazione è solo l'inizio. Man mano che il ransomware prolifera attraverso le reti interconnesse,

innesca una reazione a catena, causando danni a tutti i settori. Alla supply chain, alla produzione, alla distribuzione, ai fornitori di servizi, ai rivenditori. Gli effetti si moltiplicano, amplificando esponenzialmente l'impatto iniziale.

Un parallelo nel mondo reale: NotPetya

Il famigerato ransomware NotPetya è un chiaro esempio della portata dell'interruzione della supply chain. Nel 2017, questo wiper distruttivo, mascherato da ransomware, ha preso di mira inizialmente le organizzazioni ucraine attraverso un software di preparazione fiscale. Tuttavia, la sua furia non si è limitata all'Ucraina. NotPetya si è propagato attraverso un colosso mondiale delle spedizioni, Maersk, paralizzandone le operazioni in tutto il mondo. L'infezione ha oltrepassato i confini, colpendo il colosso farmaceutico Merck, interrompendo la produzione e causando perdite finanziarie miliardarie.

L'azione interconnessa del ransomware intensifica l'impatto dell'interruzione. Le organizzazioni, già alle prese con le conseguenze della propria violazione, si ritrovano a subire il peso delle vulnerabilità dei partner della supply chain. Gli effetti a cascata dei tempi di inattività, perdita di dati e conseguenze finanziarie diventano un groviglio intricato, poiché ogni soggetto coinvolto lotta per mitigare la crescente tensione.

7 **L'impegno delle Risorse IT:** La battaglia contro il ransomware richiede un notevole impiego di risorse IT, sottraendo attenzione e impegno ad altri progetti strategici. I team IT devono destreggiarsi nel complesso panorama della decrittazione, del recupero dei dati e del ripristino del sistema, spesso lavorando 24 ore su 24 per ridurre al minimo i tempi di inattività. Questa modifica può compromettere la strategia IT complessiva di un'organizzazione e rallentare l'innovazione tecnologica.

8 **Impatto sulle Assicurazioni Cyber:** Le conseguenze di un attacco ransomware possono ripercuotersi nel campo delle assicurazioni cyber. Le organizzazioni che ne sono rimaste vittime potrebbero riscontrare un aumento dei premi o addirittura avere difficoltà a garantire la copertura in futuro. Ciò aumenta ulteriormente la posta in gioco, rendendo il recupero post-attacco ancora più oneroso dal punto di vista finanziario.

Noti Attacchi Ransomware – Uno Sguardo al loro Impatto

WannaCry (2017): questo famigerato attacco, sfruttando una vulnerabilità di Windows, si è diffuso a livello globale, colpendo centinaia di migliaia di sistemi in 150 paesi. L'attacco ha interrotto servizi essenziali come l'assistenza sanitaria, i trasporti e le agenzie governative, lasciando dietro di sé una scia di caos.

NotPetya (2017): inizialmente mascherato da ransomware Petya, NotPetya ha rivelato il suo vero intento di wiper distruttivo. Ha sfruttato le vulnerabilità di Windows utilizzando metodi di propagazione alternativi, colpendo aziende di tutto il mondo, comprese società importanti come Maersk e Merck.

Attacco Colonial Pipeline (2021): il gruppo DarkSide ha preso di mira la Colonial Pipeline, forzandone la chiusura e provocando carenza di carburante in tutti gli stati. Questo incidente ha sottolineato il potenziale impatto del ransomware sulle infrastrutture critiche, scuotendo le fondamenta della distribuzione energetica.

Attacco Ransomware JBS (2021): colpendo una delle più grandi aziende di lavorazione di carne al mondo, l'attacco JBS ha interrotto la produzione di carne negli Stati Uniti e in Australia, evidenziando le vulnerabilità all'interno della supply chain alimentare.

Vulnerabilità del Settore Sanitario: il ransomware ha una particolare preferenza per il settore sanitario, poiché sfrutta i dati sensibili dei pazienti archiviati al suo interno. Gli ospedali e le strutture mediche diventano obiettivi primari, causando un'interruzione dell'assistenza ai pazienti, ritardando i trattamenti e mettendo a repentaglio la documentazione sanitaria.

In tutti questi casi, le ripercussioni degli attacchi ransomware si riversano su settori critici, causando interruzioni operative, perdite finanziarie e preoccupazioni per la sicurezza pubblica. La collaborazione sinergica tra governi, industrie ed esperti di cybersecurity resta fondamentale per bloccare l'ondata di queste minacce digitali.

Varianti e meccanismi

La storia del ransomware dalle sue fasi nascenti alla sua attuale importanza è stata segnata da un'evoluzione di tattiche e strategie, mentre i cybercriminali perfezionano continuamente i loro metodi per massimizzare il guadagno finanziario. Con caratteristiche e metodi distinti, sono emersi tre tipi principali di ransomware come avanguardie dell'estorsione digitale.

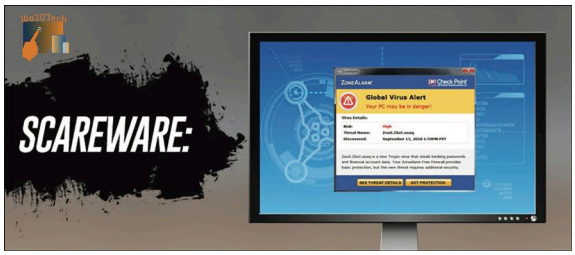
1. Ransomware con Crittografia – I Digital Locksmiths

Il ransomware basato su crittografia, spesso definito cripto-ransomware, ha consolidato la sua posizione come minaccia principale nel panorama dei ransomware. Funziona come un digital locksmith, impiegando potenti algoritmi di crittografia per bloccare i file delle vittime oltre a renderli inaccessibili. Il processo di crittografia trasforma i file in parole senza senso, rendendoli incomprensibili senza la chiave crittografica in mano agli aggressori. Una volta che i file vengono intrappolati in questo labirinto crittografico, sullo schermo della vittima si visualizza una richiesta di pagamento del riscatto in criptovaluta. Il pagamento promette la chiave di decifrazione, mettendo le vittime davanti alla scelta di: pagare o perdere i propri file per sempre. I ransomware crittografici più rappresentativi, come CryptoLocker, CryptoWall e Ryuk, hanno portato questa variante in prima linea nell'estorsione digitale.

2. Locker Ransomware – I Digital Gatekeepers

Il ransomware Locker, simile a un digital gatekeeper, esercita il controllo sui sistemi operativi delle vittime. Invece di prendere di mira i file, requisisce l'accesso all'intero sistema. Il mondo digitale della vittima è bloccato dietro una barriera imposta dal ransomware, accompagnato da un annuncio a schermo intero che potrebbe imitare in modo convincente la comunicazione delle forze dell'ordine. Questo messaggio accusa la vittima di cattiva condotta e sollecita il pagamento come unica modalità di accesso al sistema. In sostanza, il sistema stesso diventa ostaggio e il riscatto richiesto è il prezzo per la sua liberazione. I più importanti rappresentanti dei locker ransomware comprendono varianti come WinLocker e i ransomware a tema Police.

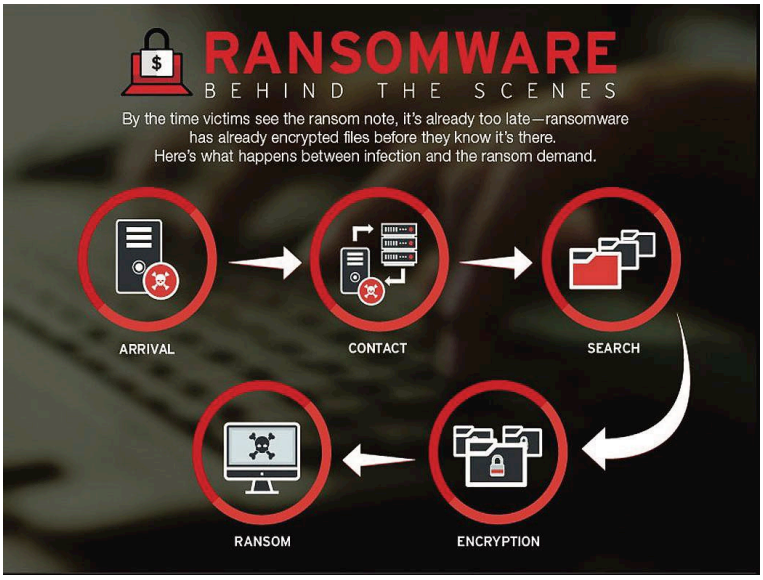
3. Scareware – La Minaccia Fittizia



Lo scareware adotta un approccio completamente diverso, mascherandosi da virtual ghost con l'unico intento di seminare il panico. A differenza dei suoi omologhi, lo scareware non crittografa i file né immobilizza i sistemi. Al contrario, condiziona psicologicamente gli utenti, evocando scenari falsi di infestazione da malware o attacchi virali. Messaggi allarmanti, che ricordano segnali di pericolo, emergono sotto forma di pop-up, chiedendo all'utente di usare i propri fondi per l'acquisto di una soluzione pseudo-antivirus. Il social engineering fa da padrone nel mondo dello scareware, convincendo le vittime a pagare per la risoluzione di un problema che, in verità, non è mai esistito.

Un Filo Comune: l'Estorsione e le sue Complesse Ramificazioni

Nonostante la diversità delle loro tecniche, tutti e tre i tipi di ransomware fanno risalire la loro genesi all'arte malevola dell'estorsione. Attraverso l'intimidazione, la guerra psicologica o la coercizione diretta, i cybercriminali fanno pressione sulle vittime affinché soddisfino le loro richieste. Tuttavia, il pagamento del riscatto non garantisce che i sistemi vengano riparati o che i dati vengano recuperati; potrebbe essere data la chiave di decrittazione o il silenzio assoluto. Pagare il riscatto non fa che alimentare il circolo vizioso, incoraggiando i cybercriminali a perfezionare le loro tattiche e a creare ceppi di ransomware sempre più sofisticati.



Come Funziona il Ransomware: Svelare le Complessità della Crittografia e dell'Estorsione

Quando il ransomware si infiltra in un sistema, inizia la sua malevola dance di crittografia ed estorsione, orchestrata da intricati meccanismi progettati per massimizzare il suo impatto.

1. La Dance della Crittografia

La prima mossa del ransomware è scansionare i file della vittima, selezionandola da un mare di dati. Utilizzando sofisticati algoritmi di crittografia, il ransomware blocca i file all'interno di una fortezza inespugnabile. A ogni file viene assegnata una chiave di crittografia univoca, un talismano digitale necessario per sbloccarne il contenuto. Queste chiavi vengono conservate sul server dell'aggressore, garantendone l'esclusività.

2. L'Inquietante Trasformazione

Una volta che il ransomware inizia a crittografare, i file delle vittime subiscono una trasformazione inquietante. I dati si trasformano in parole incomprensibili senza senso, ed è come se il ransomware avvolgessi i contenuti con un velo digitale. Le identità dei file vengono riscritte, le estensioni modificate o vengono aggiunte nuove estensioni, segnalando il loro stato crittografato. Un file come "document.docx" si trasforma in "document.docx.encrypted", contrassegnando così l'avvenuta crittografia.

3. L'arrivo Minaccioso della Richiesta di Riscatto

Dopo questa trasformazione, la minacciosa richiesta di riscatto appare sul sullo schermo. Arrivando in varie forme (file di testo, pop-up, immagini), informa le vittime della crittografia irrevocabile e fornisce precise condizioni da rispettare per tornare in possesso dei propri dati o del proprio sistema. Non mancano le istruzioni per creare un portafoglio di criptovaluta, spesso in Bitcoin, dove le vittime devono trasferire il riscatto richiesto, per riconquistare il patrimonio digitale.

4. Il Conto alla rovescia

Il tempo diventa un protagonista inevitabile nel mondo del ransomware. Il messaggio fissa una scadenza per il pagamento, simile a una clessidra la cui sabbia sottile scorre inesorabilmente. Un minaccioso conto alla rovescia incombe, avvertendo le vittime di terribili conseguenze se il riscatto non verrà effettuato in tempo. Aleggia un agghiacciante ultimatum: rispettalo o

rischierai la scomparsa permanente della chiave di decrittazione o l'aumento del prezzo del riscatto.

5. Lo Stratagemma della Doppia Estorsione

L'evoluzione della strategia ransomware introduce un'arma a doppio taglio: la doppia estorsione. Gli aggressori, assetati di maggiore potere, oltrepassano i confini della crittografia. Prima di nascondere i file sotto il velo della crittografia, rubano silenziosamente i dati sensibili dal dominio della vittima. Questo patrimonio, che comprende informazioni riservate sui clienti, segreti industriali e documenti finanziari, diventa una spada da brandire. Emerge un nefasto ultimatum: paga il riscatto o affronta la diffusione di questi dati rubati sul web.

La Complessa Dance del Cybercrime

La dualità del ransomware, che intreccia crittografia ed estorsione, presenta una coreografia sofisticata. Unisce la manipolazione psicologica con l'abilità tecnologica, creando un'intricata sinfonia di terrore e coercizione. Questa strategia è rafforzata dalla minaccia incombente non solo della perdita di dati ma anche della potenziale reazione a catena che si innesca dopo la violazione di dati sensibili come danni alla reputazione, sanzioni normative e battaglie legali.

Metodi di Distribuzione Comuni: Smascherare i canali di infezione

L'evoluzione del ransomware è intrinsecamente legata ai suoi metodi di distribuzione innovativi. I cybercriminali sfruttano abilmente le debolezze umane e le vulnerabilità tecnologiche per infiltrarsi nei sistemi con i loro payload dannosi.

1. Email di Phishing

Le email di phishing rimangono uno dei vettori di infezione più diffusi per la distribuzione di ransomware. Queste email ingannevoli si mascherano da corrispondenza legittima, inducendo gli utenti a fare clic su allegati o collegamenti dannosi. All'insaputa del destinatario, questa azione apparentemente innocua avvia il download e l'esecuzione del ransomware sul proprio sistema.

2. Siti Web Compromessi e Malvertising

I siti Web compromessi fungono da trappole ignare, obbligando a download automatici del ransomware. Il malvertising, sfrutta gli annunci online per reindirizzare gli utenti a tali siti web. Un singolo clic errato può avviare l'installazione nascosta del ransomware.

3. Drive-By Download

Navigare in modo inesperto sul web può portare ad un'infezione involontaria di ransomware. I cybercriminali si infiltrano nei siti Web, aspettando di sfruttare le vulnerabilità dei browser o del software. Il semplice atto di visitare un sito compromesso può inavvertitamente distribuire il ransomware attraverso questi "drive-by" download.

4. Sfruttare il Remote Desktop Protocol (RDP) - Backdoor Intrusion

Le connessioni RDP debolmente protette offrono ai cybercriminali un percorso diretto verso i sistemi delle vittime. Sfruttando misure di sicurezza deboli, gli attaccanti possono installare silenziosamente ransomware sul computer della vittima, aggirando le difese tradizionali.

5. Exploit kit: a Caccia di Vulnerabilità

Gli exploit, pacchetti di codice dannoso, setacciano software alla ricerca di vulnerabilità ben note da sfruttare. Quando vengono rilevate, queste vulnerabilità fungono da gateway per la distribuzione del ransomware. Prendendo di mira meticolosamente i punti deboli del software, gli attaccanti utilizzano gli exploit kit come armi per infiltrarsi nei sistemi.

6. Supporti Rimovibili e Social Engineering

Le unità USB infette e altri supporti rimovibili possono introdurre involontariamente ransomware nei sistemi. Il social engineering, d'altro canto, manipola gli utenti inducendoli a scaricare o eseguire volontariamente ransomware, spesso mascherati da aggiornamenti software legittimi.

Prevenzione e Mitigazione: Protezione Contro l'Attacco Ransomware

Lo studio attento delle tecniche del ransomware sottolinea l'urgenza di misure proattive di cybersecurity.

Una difesa solida implica non solo pratiche preventive ma anche l'implementazione di soluzioni di backup resilienti. La inviolabilità dei dati e la sovranità digitale dipendono dall'attenta navigazione in questo labirinto

informatico, dalla salvaguardia contro le complessità della crittografia, dell'estorsione e delle tattiche in continua evoluzione dei cybercriminali.

La battaglia contro il ransomware richiede un approccio su più fronti, in cui controllo, conoscenza e misure proattive costituiscono il baluardo contro questa minaccia digitale.

1. La Protezione con gli Aggiornamenti Software

Gli aggiornamenti regolari del software rappresentano una difesa fondamentale contro il ransomware. Mitigando le vulnerabilità note nei software obsoleti, i punti di ingresso sfruttati dai cybercriminali diventano obsoleti. Questi aggiornamenti creano una barriera contro la minaccia del ransomware, impedendogli un facile accesso ai sistemi.

2. Le Misure di Cybersecurity

L'adozione di solide procedure di cybersecurity costituisce la base della difesa. Ciò include dotare i sistemi di software antivirus e antimalware affidabili, installare firewall per respingere intrusioni non autorizzate, implementare l'autenticazione a due fattori per un ulteriore livello di sicurezza, limitare i privilegi dell'utente per ridurre potenziali violazioni e perfezionare continuamente i controlli di accesso per proteggere i dati sensibili.

3. La Formazione degli Utenti

Fornire ai singoli individui le conoscenze necessarie per riconoscere e contrastare gli attacchi di phishing e di social engineering è fondamentale. La maggior parte degli attacchi ransomware avviene attraverso e-mail di phishing o tattiche di social engineering. Gli utenti formati rappresentano un baluardo impenetrabile, in grado di identificare collegamenti dannosi, allegati ed e-mail sospette che preavvisano un attacco ransomware.

4. La Solida Strategia di Backup

Una solida strategia di backup rappresenta una protezione contro il blocco dei ransomware. La creazione di questa difesa implica diverse pratiche: eseguire regolarmente il backup dei dati per garantire una perdita minima di dati, archiviare i backup offline o all'interno di segmenti di rete sicuri e isolati per impedire l'invasione del ransomware sui file di backup, mantenere più versioni di backup per consentire il corretto ripristino, programmare regolari test dei backup per verificarne la funzionalità e adozione della regola 3-2-1 che salvaguarda tre copie dei dati, di cui due su supporti distinti e una archiviata fuori sede.

Il Monitoraggio Costante

La difesa dal ransomware è incessante. Richiede controllo costante e collaborazione ininterrotta in tutti gli livelli di un'organizzazione, dagli executive ai singoli utenti, rafforzando la convinzione che la sovranità digitale sia responsabilità collettiva di tutti.

Prevenzione

In un panorama in cui le minacce cyber si evolvono e mutano, la prevenzione operante su più fronti rappresenta la cosa più importante.

Aggiornamenti software regolari, pratiche di cybersecurity, formazione degli utenti e una strategia di backup formano uno scudo impenetrabile contro gli attacchi del ransomware. Questa collaborazione guida individui e organizzazioni nel labirinto delle minacce cyber, garantendo che escano illesi dalla morsa del ransomware.

Rispondere agli Attacchi Ransomware

Nelle temibili conseguenze di un attacco ransomware, riuscire nella attività di risposta diventa fondamentale, una riposta in grado di aiutare le vittime immerse nelle acque tumultuose dell'incertezza.

1. Isola e Proteggi

Il primo imperativo di fronte a un attacco ransomware è fermarsi. Isola rapidamente il sistema infetto per interrompere la sua connessione all'ecosistema digitale, impedendo all'infezione di diffondersi ad altri dispositivi. Questo isolamento richiede una quarantena digitale, per proteggere i sistemi ancora non infettati.

2. Valutare e Comprendere

Il secondo step prevede una meticolosa valutazione dell'attacco. Individua quali file e sistemi sono stati intaccati. Scopri l'estensione dell'intrusione, accertando l'entità del danno per tracciare una strada da seguire. Questa comprensione è la base per un processo decisionale strategico.

3. Valutare la Richiesta di Riscatto

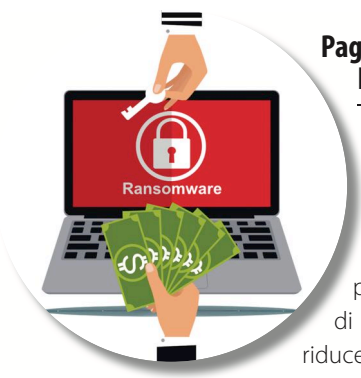
In mezzo al caos, incombe lo spettro della richiesta di riscatto, che promette la liberazione in cambio di un pagamento. Tuttavia, la cautela deve prevalere sulla fretta. Valuta altre opzioni oltre quella del pagamento del riscatto, cercando tool o soluzioni di decifrazione che potrebbero sbloccare i file in ostaggio. Per non parlare del fatto che in molti paesi il pagamento del ransomware è considerato illegale. Questa riflessione equilibrata apre la strada a una scelta consapevole.

4. Segnala e Coinvolgi gli Esperti

Un valido aiuto arriva dalle forze dell'ordine. Segnala prontamente l'attacco, contribuendo in maniera significativa alla lotta al cybercrime. Il coinvolgimento degli esperti della cybersecurity è imperativo; infatti, questi sono in grado di destreggiarsi negli intricati labirinti dei ransomware. La loro competenza nell'analizzare la situazione e nel tracciare il percorso di ripristino può essere la bussola durante la tempesta.

5. Ripristino da Backup

Se hai a disposizione il backup dei dati, il ripristino diventa la tua ancora di salvezza. Backup puliti e non contaminati diventano la soluzione all'azione del ransomware, rivitalizzeranno i sistemi e daranno nuova vita ai file crittografati.



Pagare o Non Pagare: Il Dilemma Fatidico

La decisione di pagare il riscatto si pone come un crocevia di emozioni. Si hanno davanti sia pro che contro, creando un dilemma fatidico. Il pagamento può fornire l'ambita chiave di decrittazione, accelerando il ripristino e riducendo al minimo le interruzioni operative. Tuttavia, questo percorso è pieno di rischi. Non vi è alcuna garanzia che la chiave sarà consegnata o che la decrittazione vada a buon fine. Ricordando, inoltre, che ogni pagamento finanzia le imprese cybercriminali perpetuando un ciclo di estorsioni. Inoltre, pagare una volta potrebbe contrassegnarti come bersaglio per attacchi futuri.

Collaborazione e Risposte Personalizzate

Il coinvolgimento delle forze dell'ordine e degli esperti di cybersecurity supera gli ambiti individuali, e si trasforma in un'armoniosa difesa collettiva. Questa collaborazione è indispensabile per monitorare e perseguire i cybercriminali, fornire indicazioni sulle migliori pratiche e rafforzare il proprio mondo digitale contro future incursioni.

L'Odissea Individualizzata

Non esistono due incidenti ransomware uguali. Ogni attacco è unico, regolato da variabili come il valore dei dati, l'importo del riscatto, la disponibilità del backup e le implicazioni legali. Personalizza la tua risposta, elaborando una strategia che rispecchi le tue condizioni specifiche, armandoti di conoscenza, supporto e una determinazione incrollabile.

Trend Recenti e Prospettive Future: Orientarsi tra le Mutevoli Tendenze dei Ransomware

Nel panorama in continua evoluzione delle minacce cyber, il mondo del ransomware presenta mutevoli tendenze, caratterizzato dai trend recenti e contrassegnato dagli sviluppi emergenti.

1. Ransomware-as-a-Service (RaaS)

È emerso un mercato oscuro, segnato dal minaccioso fenomeno del Ransomware-as-a-Service (RaaS). In questo mercato, attaccanti vendono toolkit e piattaforme ransomware agli aspiranti cybercriminali, chiedendo in cambio una quota dei profitti. Questo sinistro modello di business ha compromesso la difesa iniziale, limitando le conoscenze tecniche necessarie per lanciare campagne ransomware. Con interfacce intuitive, supporto tecnico e persino servizio clienti, le piattaforme RaaS hanno reso accessibile a tutti il ransomware, consentendo un'ondata di attacchi diffusi.

2.Targeting specifico

La storia del ransomware è passata da generica a strategica. I cybercriminali hanno affinato le loro tattiche, puntando su settori che da cui potrebbero ricavare riscatti più alti. Il targeting strategico comprende l'assistenza sanitaria, gli enti governativi, le istituzioni finanziarie

e le infrastrutture critiche. Questi attacchi sfruttano le vulnerabilità insite nella natura critica delle operazioni o dalla sensibilità dei dati. Sfruttando la minaccia del data breach o degli sconvolgimenti operativi, gli aggressori esercitano una pressione che spesso si traduce in sostanziali ricompense.

3. Difese Tecnologiche

Per contrastare efficacemente il ransomware sono emersi efficaci strumenti di difesa tecnologica:

- Behavioral Analysis: l'attività del trovare tracce del ransomware prima che colpisca, identificando le attività anomale e contrastandole all'inizio.
- Deception Technology: i dati e i sistemi esca svolgono un ruolo fondamentale, attirando gli aggressori in labirinti di informazioni fuorvianti distogliendo i loro sforzi da risorse preziose.
- Intelligenza Artificiale (AI) e Machine Learning (ML): questi alleati tecnologici esercitano un potere predittivo, portando alla luce modelli nel labirinto di dati, identificando anomalie e prevedendo imminenti incursioni di ransomware.
- Architettura Zero Trust: questa paradigma comporta il passaggio dalla fiducia intrinseca alla verifica rigorosa. Impone severi controlli di accesso, verifica continua e accesso con privilegi minimi, limitando le potenziali superfici di attacco del ransomware.

4. Sguardo sul Futuro: Convergenza delle Forze

La futura lotta contro il ransomware vedrà probabilmente una convergenza di forze. La tecnologia svolgerà un ruolo fondamentale, affiancandosi a meccanismi di prevenzione avanzati e promuovendo al tempo stesso la collaborazione internazionale.

5. L'imperativo Strategico della Collaborazione

a. Progressi Tecnologici: man mano che il ransomware affina le sue tattiche, la cybersecurity deve evolversi di pari passo. L'intelligenza artificiale, il machine learning, l'analisi comportamentale e la deception technology matureranno, operando con maggiore precisione e capacità di previsione.

b. Collaborazione Internazionale: le maree digitali non conoscono confini. Rintracciare e arrestare i cybercriminali richiede la cooperazione internazionale, che trascende i confini giurisdizionali.

c. Controllo a Tutti i Livelli: il crogiolo della difesa si estende dall'individuo all'organizzazione. La missione della cybersecurity deve essere solida, diventando parte intrinseca della vita digitale quotidiana.

d. Controllo Proattvo: man mano che le trame del ransomware diventano sempre più fitte, lo scudo di prevenzione deve innalzarsi sempre più. Controllo, monitoraggio continuo e risposta rapida agli incidenti saranno fondamentali per mitigarne l'impatto.

Sintesi: Comprensione delle Minacce e delle Difese Ransomware

Il ransomware, un software dannoso che richiede un pagamento per i file crittografati, si è evoluto nel tempo. Varianti come "Reveton" e "CryptoLocker" segnano la sua evoluzione. Gli incidenti recenti evidenziano impatti globali e la richiesta di riscatti elevati in criptovaluta. La difesa necessita di collaborazione, tecnologia e azioni legali.

Gli impatti includono perdita di dati, impiego di risorse finanziarie, violazioni della privacy, impatto emotivo e furto di identità per gli individui. Le organizzazioni devono affrontare interruzioni operative, danni finanziari, perdita di reputazione, conseguenze legali, perdita di dati e interruzione della supply chain.

Il ransomware si diffonde in modo contagioso attraverso le reti, colpendo molteplici settori. La distribuzione avviene attraverso phishing, siti web dannosi e exploit kit.

I meccanismi includono crittografia, richieste di riscatto, manipolazione psicologica e doppia estorsione. La prevenzione prevede aggiornamenti, cybersecurity, formazione e backup robusti. La risposta richiede isolamento, valutazione, reporting e ripristino dai backup. Pagare il riscatto è un dilemma; la collaborazione di esperti è fondamentale.

Tendenze recenti: Ransomware-as-a-Service (RaaS), targeting del settore, progressi nella difesa tecnologica e cooperazione internazionale.

Meccanismi di Difesa

- Aggiornamenti Software: Regolari aggiornamenti eliminano le vulnerabilità del software obsoleto.
- Pratiche di Cybersecurity: utilizzare antivirus, firewall, autenticazione a due fattori, limitare i privilegi utente e perfezionare i controlli di accesso.
- Formazione degli Utenti: forma gli utenti a riconoscere gli attacchi di phishing e di social engineering.
- Backup Robusti: backup regolari, isolati e testati proteggono dalla perdita di dati.
- Behavioral Analysis: rileva le anomalie prima che il ransomware colpisca.
- Deception Technology: inganna gli attaccanti con sistemi e dati ingannevoli.
- AI e ML: prevede modelli e identificare anomalie.
- Architettura Zero Trust: rigorosa verifica e severi controlli di accesso.
- Collaborazione Internazionale: rintracciare e arrestare i cybercriminali richiede cooperazione.
- Controllo e Risposta agli Incidenti: il monitoraggio continuo e la risposta rapida sono decisivi.

In un panorama dinamico, la lotta contro il ransomware richiede una difesa proattiva, collaborazione e incessante ricerca della sicurezza. Nel cuore dell'evoluzione della narrativa del ransomware, risuona una chiamata alle armi. La difesa è multiforme, la risposta sincronizzata e la risolutezza incrollabile. In una società in cui il mondo digitale e quello tangibile si intrecciano, la lotta contro il ransomware è una testimonianza della resilienza dell'umanità e della costante ricerca della sicurezza. ■

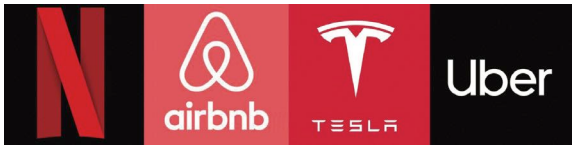
I nuovi ransomware nel loro quadro globale: l'uso di cyber-mercenari dell'intelligenza artificiale nella guerra economica.

Autore: **Stéphane Mortier**

L'intelligenza artificiale richiede grandi quantità di dati per essere sviluppata. Non è un segreto che i GAFAM, i BATX ed i NATU raccolgano dati dai loro utenti per sviluppare nuovi strumenti basati su di essi. Nessuno si lascia ingannare dal fatto che Tik Tok sia stato creato per raccogliere dati, ad esempio[1]. Allo stesso tempo, gli attacchi informatici sembrano essere sempre più focalizzati sul furto di dati: dati sanitari[2], dati di laboratori di ricerca, dati finanziari, dati personali... e persino dati dei casinò[3]! In breve, qualsiasi tipo di dati può essere rubato... e venduto a chi lo richiede. A parte i casi di spionaggio (soprattutto economico o militare), si può scommettere che questi dati rubati possano anche essere utilizzati come dati di addestramento per futuri strumenti di intelligenza artificiale. I criminali informatici sono ladri e/o destinatari di dati rubati venduti sul darkweb o altrove, oppure sono "mercenari" che agiscono per conto di un cliente (potenze straniere, industrie, laboratori, ecc.). In entrambi i casi, l'IA è al centro del problema: è sia uno strumento per ottenere dati che un richiedente di dati per il suo sviluppo. Abbiamo quindi belligeranti (Stati, industrie digitali, laboratori), combattenti (criminali informatici), armi e munizioni (strumenti e dati informatici) e un obiettivo strategico (l'intelligenza artificiale). Insomma, tutti gli elementi necessari per una vera e propria guerra economica e tecnologica.

BIO

Stéphane Mortier è attualmente direttore aggiunto del Centro di Sicurezza Economica e Protezione delle Imprese (CSECOPE) presso la Direzione Generale della Gendarmerie Française; è membro della Comunità di Ricerca della Gendarmerie Nationale (CREOGN), nonché docente all'Università Gustave Eiffel. È laureato in scienze politiche, sociologia e relazioni internazionali presso l'Université Libre de Bruxelles (ULB), in gestione strategica e intelligence economica presso l'École de Guerre Économique e ha conseguito un dottorato in management presso Paris 1 Panthéon-Sorbonne. È anche rappresentante delle sezioni estere dell'ULB Alumni Union e presiede la sezione francese (UAEF). In questa veste, sviluppa progetti di cooperazione in Africa. È docente presso l'Ecole de Guerre Économique (lotta al riciclaggio di denaro) e presso l'Università di Likasi - Repubblica Democratica del Congo (strategia, diritto commerciale). È membro fondatore del Cercle K2 e membro attivo dell'Association pour l'Unification du Droit en Afrique (UNIDA). È autore di diverse pubblicazioni sulla business intelligence.



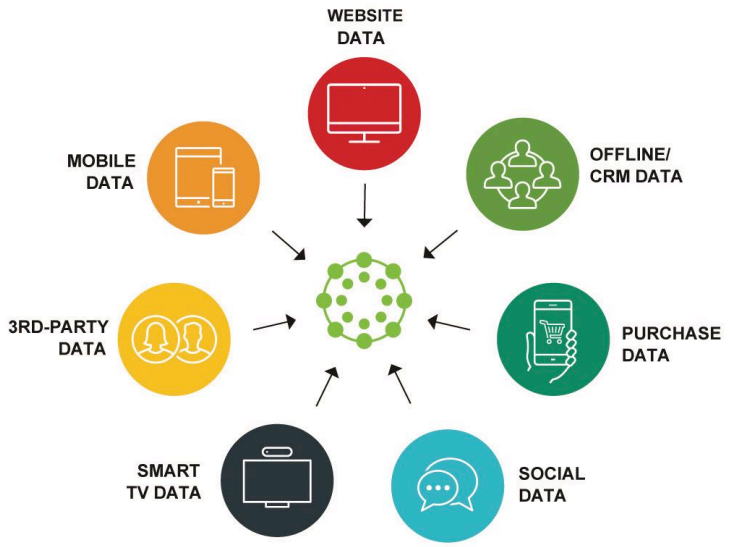
L'intelligenza artificiale come strumento per i criminali informatici

I criminali informatici utilizzano sempre più spesso strumenti di intelligenza artificiale per commettere i loro crimini. Basta dare un'occhiata ai principali modus operandi:

- **Phishing:** fino a qualche anno fa, gli utenti erano in grado di individuare un phishing principalmente identificando la scarsa qualità del messaggio contenuto nell'e-mail ricevuta (errori ortografici o grammaticali, immagini e loghi di scarsa qualità, aziende strane, ecc.). Oggi, i criminali informatici utilizzano modelli linguistici estesi (LLM) per redigere i loro messaggi. Tali modelli generano un testo virtualmente indistinguibile da quello scritto da un autore umano. Tecnicamente, si tratta di una rete neurale basata sulla trasformazione[4]. Questi modelli di base utilizzano l'intelligenza artificiale generativa per l'elaborazione del linguaggio naturale (NLP[5]) e la generazione del linguaggio naturale **(NLG)**. Ciò rende quasi impossibile per un utente distinguere tra un'e-mail scritta da un autore umano e quella scritta dall'intelligenza artificiale, questo aumenta notevolmente le possibilità di successo dei criminali.
- **Bypassare i filtri anti-spam e creare indirizzi e-mail:** l'intelligenza artificiale può anche consentire ai criminali informatici di aggirare i filtri anti-spam e creare indirizzi e-mail apparentemente legittimi. I filtri antispam si basano sul *machine learning* per valutare la reputazione del mittente e il contenuto dell'e-mail e quindi assegnare un grado di minaccia al destinatario. I criminali informatici utilizzano un'enorme diversità di tecniche per ingannare l'intelligenza artificiale che filtra lo spam (utilizzo di servizi con una buona reputazione pubblica, come Gmail, Dropbox, ecc.; utilizzo di soluzioni *warm-up*[6]; moltiplicazione degli indirizzi IP di invio; compromissione a cascata di *account* per beneficiare della reputazione del primo account; occultamento del contenuto del messaggio dietro un sito affidabile o reindirizzamento / accorciamento dell'URL; occultamento del contenuto dietro un captcha; utilizzo di malware di evasione dei sandbox[7]). Per quanto riguarda la creazione di indirizzi e-mail affidabili, si tratta semplicemente di generare un indirizzo che abbia una "buona reputazione" e che quindi neutralizzi le capacità di rilevamento dei filtri anti-spam.
- **Ransomware e crittografia:** gli attacchi ransomware diventano ogni giorno più efficaci. I criminali informatici utilizzano l'intelligenza artificiale per crittografare i file eludendo i software antivirus e, soprattutto, individuando i file più sensibili e strategici per la loro vittima. La maggior parte delle vittime di ransomware sono aziende o istituzioni che detengono dati strategici o sensibili. L'intelligenza artificiale può essere utilizzata per identificare i file di molta importanza per la vittima, esercitando una pressione particolarmente forte su quest'ultima, che sarà quindi più propensa a pagare il riscatto.
- **Ingegneria sociale:** in un attacco informatico di ingegneria sociale, in cui l'attaccante sfrutta le vulnerabilità della vittima attraverso l'interazione sociale, la confusione tra finzione e realtà, resa possibile dall'IA, è inarrestabile nel raggiungere l'obiettivo prefissato. La vittima, ingannata da una «falsa realtà virtuale», si trova quindi in una situazione in cui, naturalmente, il suo comportamento porterà inconsapevolmente alla compromissione di un sistema informatico o, più semplicemente, a subire un'estorsione. Questo uso abusivo dell'IA può essere praticato in varie fasi di un attacco informatico tramite l'ingegneria sociale: dalla ricerca di informazioni sull'obiettivo all'esecuzione dell'attacco, passando per la fase di approccio[8].
- **Deepfakes:** i deepfakes sono generalmente generati dall'intelligenza artificiale. I criminali informatici creano video, immagini e registrazioni audio falsi, sufficientemente realistici da ingannare qualsiasi utente o destinatario (vedi social engineering sopra). Questi mezzi di comunicazione ingannevoli e manipolatori vengono utilizzati per mettere in atto truffe (frode che compromettono un CEO, ad esempio), per diffondere propaganda e false informazioni, ecc. L'intelligenza artificiale consente di manipolare le espressioni facciali, le voci e i gesti, sia nelle immagini, sia nei video o nelle colonne sonore, confondendo il confine tra realtà e illusione.

Creazione e gestione di botnet: L'intelligenza artificiale svolge un ruolo centrale nella creazione, gestione, razionalizzazione, coordinamento e ottimizzazione delle attività delle botnet. Queste possono essere utilizzate per attacchi DDoS, distribuzione di spam e, naturalmente, furto di dati.

A questi modus operandi si aggiunge il fatto che i criminali informatici possono tentare di sfruttare l'IA attraverso il reverse-engineering dei motori di IA. Se riescono a simulare i sistemi di IA, sapranno se un attacco che stanno pianificando sarà rilevato da un sistema[9]. In breve, l'IA sta diventando uno strumento al servizio della criminalità informatica ed il suo il modus operandi, sebbene identico da molti anni, diventa ogni giorno più complesso e sempre più difficile da contrastare. La maggior parte di questi attacchi ha come obiettivo *finale* l'acquisizione di dati ed eventualmente la loro falsificazione. La domanda è: Qual è la destinazione finale di questi dati? Vengono solo "commercializzati" sul darkweb oppure hanno uno scopo più strategico? Potrebbero essere utilizzati, in un modo o nell'altro, per alimentare lo sviluppo di nuove intelligenze artificiali, usati come dati di addestramento?



Necessità di dati per sviluppare strumenti di intelligenza artificiale

Facciamo un passo indietro di qualche anno: al Web Summit 2016, il direttore della sicurezza IS di Facebook ha dichiarato che la sua azienda acquistava i dati di login disponibili per la vendita sui mercati darkweb[10], una pratica in atto dal... 2013[11]. Facebook acquista dati di login compromessi per identificare quali dei suoi utenti utilizzano password deboli. Questi utenti vengono quindi invitati a cambiare la loro password con una più complessa e unica[12], sulla base di informazioni ottenute illegalmente... Tutto questo va avanti dal 2013, ma qual è la situazione oggi? I dati regolarmente rubati saranno utilizzati come dati di addestramento per futuri strumenti di intelligenza artificiale, che saranno venduti proprio alle persone a cui sono stati rubati i dati? Nell'esempio di cui sopra, Facebook è coinvolto, ma più in generale, al di là dei terna di dati raccolti legalmente (o con "giochi di prestigio" purtroppo legali - aggirando il RGPD, il Cloud Act, ecc.) dai GAFAM, dai BATX e dai NATU, i dati risultanti dagli attacchi informatici non sono forse prelevabili da queste stesse aziende? La questione rimane aperta, ma l'ipotesi è stata avanzata.

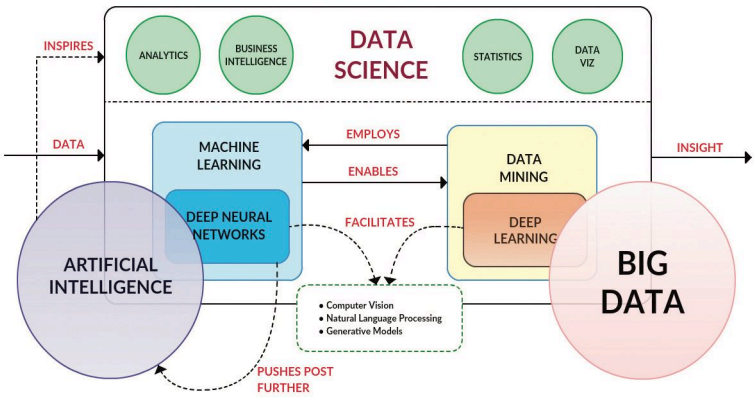
Sebbene si riconosca che gli Stati Uniti sono nella posizione migliore per vincere questa corsa all'IA, grazie al loro impressionante bacino di ingegneri altamente qualificati, alle loro aziende innovative particolarmente dinamiche e al loro esercito, che sta già iniziando a integrare alcune applicazioni tecnologiche, la Cina sembra comunque in grado di superarli. Questa ambizione è chiaramente visibile nel "Piano di sviluppo

dell'intelligenza artificiale di nuova generazione (AIDP)", presentato dal governo cinese nel luglio 2017. Il piano prevede che la Cina diventi la prima potenza mondiale dell'IA entro il 2025 e il primo polo di innovazione entro il 2030[13]. L'AIDP stabilisce tre tappe fondamentali, ognuna delle quali contiene una serie di obiettivi, alcuni dei quali sono definiti in modo preciso, mentre altri sono più vaghi[14]:

- entro il 2020, la Cina intende rimanere competitiva con le altre grandi potenze e ottimizzare il proprio ambiente di sviluppo dell'IA. In termini monetari, la Cina intende creare un'industria dell'IA del valore di oltre 150 miliardi di yuan (circa 21 miliardi di dollari). Infine, sta cercando di stabilire standard etici, politiche e regolamenti iniziali per le aree vitali dell'IA;
- entro il 2025, la Cina mira a raggiungere una "svolta importante" (come indicato nel documento) nella teoria di base dell'IA e a guidare il mondo in alcune applicazioni (alcune tecnologie e applicazioni raggiungono un livello di leadership mondiale). La Cina mira anche ad aumentare il valore della sua industria principale dell'IA a più di 400 miliardi di yuan (circa 58 miliardi di dollari) e prevede di sviluppare e codificare in legge standard etici per l'IA;
- entro il 2030, la Cina mira a diventare il centro globale dell'innovazione dell'IA. Per quella data, si prevede che la crescita dell'industria dell'IA di base raddoppierà di nuovo e sarà valutata a 1.000 miliardi di yuan (circa 147 miliardi di dollari), e si prevedono anche ulteriori miglioramenti nelle leggi e negli standard, al fine di affrontare le nuove sfide emergenti.

In altre parole, il Piano di Sviluppo dell'Intelligenza Artificiale di Prossima Generazione è inteso come un progetto per un ecosistema completo di IA per il Paese[15]. In breve, la Cina sta cercando di creare sistemi di IA in grado di analizzare e reagire ai cambiamenti geopolitici, dando un vantaggio competitivo rispetto agli altri Stati[16]. Ci sono poi le materie prime (metalli rari in particolare) che sono essenziali per i componenti elettronici, compresi i semiconduttori necessari per gli strumenti di IA. Senza questi componenti, lo sviluppo dell'IA è impossibile e i loro produttori hanno a disposizione una vera e propria arma di guerra economica. L'accesso e la capacità di produzione di questi componenti sono una questione di guerra economica.

Per raggiungere tali obiettivi, in un lasso di tempo così breve e con tali risorse finanziarie, è necessario raccogliere dati in quantità quasi infinite e, soprattutto, ottenere risultati. È legittimo chiedersi quale sia l'origine dei dati utilizzati come dati di addestramento nei programmi di sviluppo di strumenti di IA. Naturalmente non si tratta di lanciare accuse semplicistiche all'uno o



all'altro protagonista, ma è chiaro che esiste una linea sottile tra legalità e illegalità, come dimostra l'esempio di Facebook citato *in precedenza*. Sarebbe inoltre ingiusto puntare il dito solo contro i GAFAM, i BATX ed i NATU o anche contro le grandi potenze come Cina e Stati Uniti. In effetti, ogni potenza di stato ha ambizioni di IA, ogni settore dell'attività economica ha bisogno di strumenti di IA e ogni attore malintenzionato (criminalità organizzata, terrorismo ideologico, ecc.) cerca di migliorare il proprio modus operandi. Ci troviamo quindi di fronte a un mondo di guerra economica ad alta intensità, in cui l'uso di mercenari è una realtà pari a quella di un conflitto militare tradizionale, e in cui i dati sono al centro del conflitto. ■

1 https://www.lebigdata.fr/tiktok-donnees-proteger
2 Si veda il nostro articolo sull'argomento https://www.blockapt.com/health-data-from-raiding-to-reselling/
3 https://www.theregister.com/2023/09/14/caesars_mgm_hacks/
4 I trasformatori, o modelli sequenza-sequenza (Seq2seq), sono modelli di Deep Learning che appartengono a una classe speciale di architetture di reti neurali ricorrenti. Sono reti che trasformano una data sequenza di elementi, come la sequenza di parole in una frase, in un'altra sequenza. Vedere https://blent.ai/blog/a/transformers-deep-learning
5 L'elaborazione del linguaggio naturale (NLP) è una branca dell'intelligenza artificiale. Si tratta di addestrare i computer a comprendere, elaborare e generare il linguaggio umano. L'NLP si basa su una combinazione di apprendimento automatico e linguistica computazionale. I sistemi vengono addestrati sui testi per imparare a riconoscere le parole e il modo in cui sono messe insieme. Per alimentare i sistemi di ML si utilizzano frasi, estratti di testo o addirittura interi libri. Questi dati di addestramento vengono elaborati e il sistema impara a prevedere il resto del testo identificando i modelli. Vedere https://datascientest.com/introduction-au-nlp-natural-language-processing
6 Il riscaldamento dell'indirizzo IP consiste nell'invio progressivo di e-mail, anziché in un unico blocco, ottenendo comunque un alto tasso di coinvolgimento. Questo processo consente di costruire una reputazione positiva del mittente e quindi di aggirare i filtri antispam.
7 Una sandbox è una macchina virtuale isolata in cui il codice software potenzialmente pericoloso può essere eseguito senza influire sulle risorse di rete o sulle applicazioni locali.
8 https://incyber.org/ia-une-aubaine-pour-ingenierie-sociale/
9 https://mpost.io/fr/data-heists-evolve-how-cybercriminals-are-using-artificial-intelligence-to-steal-your-data/
10 https://www.cnet.com/news/privacy/facebook-chief-security-officer-alex-stamos-web-summit-lisbon-hackers/
11 https://nakedsecurity.sophos.com/2016/11/11/facebook-is-buying-up-stolen-passwords-on-the-black-market/
12 Stamboliyska, Rayna (2017), La face cachée d'internet, Larousse.
13 Thibout, C. (2018), " L'intelligence artificielle, une géopolitique des fantasmes", Etudes digitales, n°5 - 1.
14 Roberts, H.; Cowls, J.; Morley, J. et al. (2021), "The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation", AI & Society, n. 36.
15 Wu, F. ; Lu, C. ; Zhu, M. et al. (2020), "Towards a new generation of artificial intelligence in China", Nature Machine Intelligence, n°2.
16 Frankopan, P. (2018), Les nouvelles routes de la soie. L'émergence d'un nouveau monde, Flammarion, Champs Histoire.

Ransomware: le fasi di Prevention, Detection e Response.



Autori: Marco Di Costanzo, Camilla Salini, Giuseppe Brando

Nel corso degli ultimi anni, il ransomware ha ricevuto una significativa rilevanza mediatica. I criminali informatici, spinti dalla sete di profitto, hanno preso di mira un'ampia gamma di organizzazioni, istituzioni e industrie, influenzando praticamente ogni aspetto della vita quotidiana e causando notevoli perdite finanziarie e danni alla reputazione. Secondo il rapporto «IT Security Economics» di Kaspersky, più del 40% delle aziende ha subito almeno un attacco ransomware nel corso del 2022. Questo dato sottolinea l'ampia portata e l'impatto significativo che i ransomware hanno avuto sulle organizzazioni durante quell'anno.

Nonostante gli sforzi di contrasto, questi gruppi continuano a sviluppare nuove tecniche sempre più sofisticate ed efficienti, talvolta adottando anche caratteristiche delle precedenti bande di ransomware che hanno cessato la loro attività.

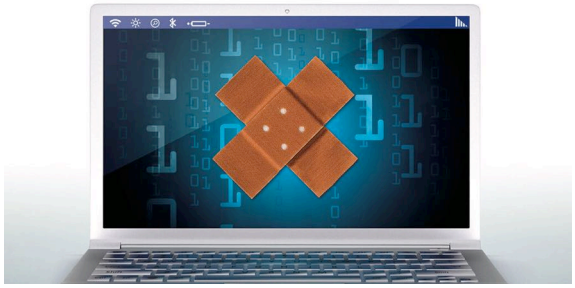
Il processo di messa in sicurezza delle informazioni prevede un rafforzamento continuamente strutturato in più fasi. Per combattere efficacemente questa minaccia, è fondamentale comprendere le fasi di prevenzione, rilevamento e risposta degli attacchi ransomware.

Ogni fase richiede strategie e attività che si basano l'una sull'altra. Qualsiasi modifica apportata a una delle fasi si ripercuoterà sulla successiva e quindi su tutto il processo. Ad esempio, le modifiche proattive apportate nella fase di prevenzione influenzeranno anche le attività di rilevamento e risposta.

Un aspetto cruciale nella prevenzione del ransomware è garantire che i dipendenti siano ben informati sulle pratiche di sicurezza informatica, conducendo sessioni di formazione per aumentare la consapevolezza riguardo i possibili vettori di attacco dei criminali informatici. Ma anche l'aggiornamento e il patching regolare di tutti i sistemi, delle applicazioni e del firmware aiutano a ridurre al minimo l'impatto di un attacco.

BIO

- **Marco Di Costanzo è Security Researcher presso l'ICS CERT di Kaspersky**
- **Camilla Salini è Cyber Threat Intelligence Analyst all'Eni**
- **Giuseppe Brando è Head of Cyber Threat Analysis & Research all'Eni**



Altre pratiche di prevenzione possono essere la limitazione dei privilegi amministrativi, la concessione agli utenti solo dei permessi necessari a svolgere le attività di competenza e l'utilizzo di backup offline o basati su cloud.

Infine, l'implementazione dell'autenticazione a più fattori in tutti i sistemi e le applicazioni aumenta i livelli di sicurezza complessivi.

La sicurezza al 100% non esiste e sappiamo bene che nonostante gli sforzi, possono verificarsi situazioni in cui non si riesce a prevenire un attacco a mezzo ransomware. Per questo motivo è fondamentale disporre di misure come il monitoraggio e il rilevamento di attività anomale mediante specifici strumenti di sicurezza, al fine di agire tempestivamente a una potenziale minaccia.

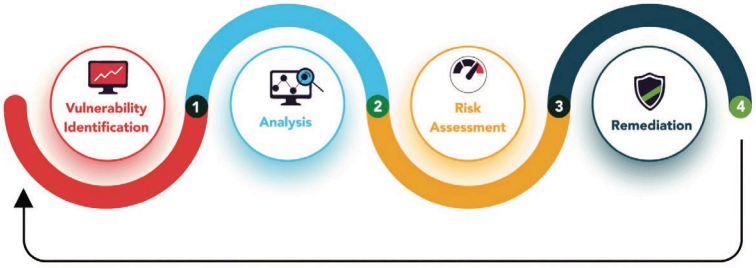
Avere la capacità di isolare i sistemi infetti ed evitare, quindi, un'ulteriore diffusione, da modo di intervenire rapidamente in caso di rilevamento di un attacco informatico, contrastando efficacemente la minaccia del ransomware qualora avesse eluso le misure di prevenzione.

Dobbiamo ricordare che l'avversario non è quello che spesso il mondo cinematografico ci propone, cioè singoli soggetti che operano da un garage o da uno scantinato, ma da vere e proprie aziende illegali con la propria gerarchia aziendale, salari, bonus e premi per i propri dipendenti. È stato possibile analizzare queste dinamiche interne dopo la pubblicazione dei dati trafugati al collettivo ransomware Conti, ne abbiamo ampiamente parlato nel nostro libro "Il ransomware nell'economia del cybercrime: analisi d'intelligence sul gruppo Conti".

Possiamo quindi trovarci di fronte a situazioni in cui le misure di prevenzione e rilevamento messe in atto non siano state sufficienti e il ransomware sia riuscito a cifrare i dati sistemi e/o dati nella nostra infrastruttura.

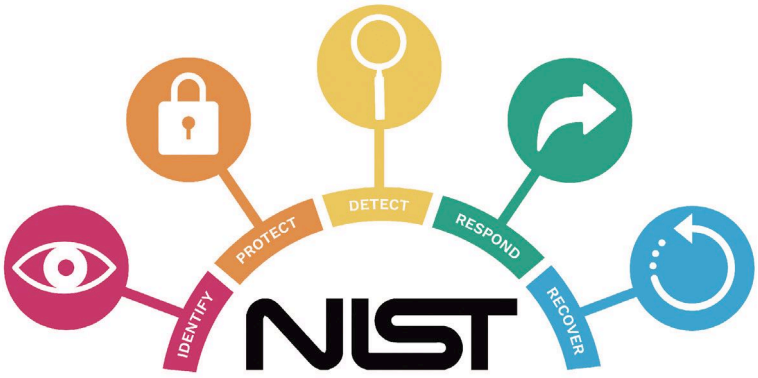
In questo caso è essenziale avere un piano di risposta e di recupero ben definito, aggiornato costantemente e che delinei le misure e le procedure da adottare. Come accennato in precedenza sarà importante attuare tutte le misure di contenimento a nostra disposizione, come l'isolamento dei sistemi infetti, per ridurre al minimo la propagazione del ransomware. Una volta neutralizzato e isolato, bisognerà avviare il processo di ripristino dei sistemi e dei dati dai backup precedentemente predisposti.

Per concludere, bisognerà condurre un'analisi approfondita per identificare le vulnerabilità sfruttate e individuare dove migliorare le misure di sicurezza.



In parallelo a quanto detto è importante non tralasciare la comunicazione, sia verso l'interno dell'organizzazione che verso l'esterno, per garantire una rapida segnalazione verso gli organismi competenti.

L'adozione di una strategia di difesa completa, che comprenda le fasi di prevenzione, rilevamento e risposta con misure di sicurezza multilivello è fondamentale per proteggere i sistemi e i dati da questa crescente minaccia informatica.

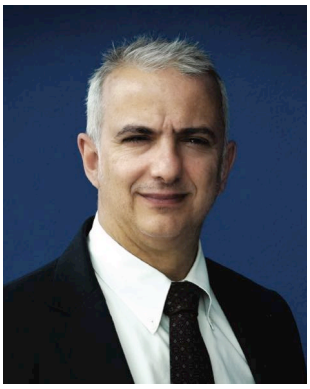


Seguire le raccomandazioni e linee guida prodotte dal NIST e l'ENISA è essenziale per garantire la sicurezza informatica e la corretta gestione dei sistemi informativi. Ma anche comitati per la normazione ISO e ISACA svolgono un importante lavoro di ricerca, divulgazione e sviluppo di metodologie efficaci in questo campo.

È importante dare la giusta attenzione a questi organismi e alle loro pubblicazioni, in quanto forniscono strumenti e conoscenze fondamentali per affrontare le sfide della sicurezza informatica e garantire una gestione efficace. Rimanere vigili e preparati rimane una priorità fondamentale. ■

Le banche nel mirino del cybercrimine rispondono con investimenti in ricerca e capitale umano.

Intervista VIP a Romano Stasi.



Autore: Massimiliano Cannata

Banche e sicurezza un binomio strategico sempre più sotto osservazione a causa del susseguirsi di attacchi sempre più sofisticati che vengono portati a reti e sistemi. "Quello finanziario –spiega nell'intervista Romano Stasi, Segretario generale del Centro di Ricerca e Innovazione ABI Lab, è da sempre tra i settori maggiormente presi di mira. Per tale ragione le banche seguono con pari attenzione i cambiamenti tecnologici e di business e l'evoluzione del panorama delle minacce, al fine di rispondere al meglio alle esigenze della clientela e mantenere livelli di sicurezza adeguati in termini di protezione non solo del denaro ma anche delle informazioni. Elemento centrale nella lotta al crimine informatico è rappresentato dalla capacità di agire in maniera strutturata e coordinata, facendo tesoro non dell'esperienza limitata del singolo ma piuttosto della continua condivisione delle esperienze da parte di tutti. Su questa base, opera dal 2017 il CERTFin – CERT Finanziario Italiano, un'iniziativa nata dalla cooperazione pubblico - privato che ha l'obiettivo di innalzare la capacità di gestione dei rischi cibernetici degli operatori bancari e finanziari".

Ing. Stasi, la tutela degli asset ha bisogno di investimenti. I nostri istituti di credito come si stanno muovendo su questo delicato ambito?

L'elevata attenzione verso i temi della sicurezza trova conferma proprio negli investimenti dedicati: dallo studio del CERTFin *"Sicurezza e frodi informatiche in banca - Come prevenire e contrastare attacchi informatici e frodi sui canali digitali"* emerge che la maggior parte delle realtà ha previsto per il 2023 un aumento o comunque un generale mantenimento dei livelli della spesa destinata sia alla sicurezza dei canali remoti, sia al rafforzamento dei sistemi di monitoraggio e protezione interni a ciascuna banca. Entrando più nel dettaglio: il 55% delle risorse stanziate dalle realtà rispondenti per progetti/interventi legati al contrasto e alla prevenzione

BIO

Romano Stasi è il Segretario generale di ABI Lab, il centro di ricerca e innovazione per la banca, promosso dall'ABI. Dopo aver conseguito la Laurea in Ingegneria Meccanica presso l'Università La Sapienza e un MBA presso la SDA Bocconi School of Management, ha ricoperto vari ruoli in società di consulenza internazionali come Accenture, Capgemini ed Ernst & Young, sviluppando e implementando progetti nei servizi finanziari e il settore ICT. Partecipa a diversi gruppi di lavoro a livello europeo, tra cui EBF, Europol, Enisa. A partire dal 2017 ha coordinato diverse iniziative volte a promuovere l'utilizzo della DLT nel settore finanziario basata su una infrastruttura comune denominata ABILabChain. È inoltre fondatore e Direttore del CERTFin, il centro nazionale di eccellenza sulla sicurezza informatica per il settore bancario presieduto da ABI e Banca d'Italia.

delle frodi informatiche sarà destinato a interventi volti a incrementare i livelli di sicurezza dei servizi, mentre il 26% sarà destinato all'evoluzione sicura dei servizi per la clientela anche in ottica business (servizi che mirano a migliorare l'esperienza del cliente e che al contempo facilitano la promozione di ulteriori servizi non ancora sottoscritti dal cliente). La quota di budget destinata a interventi per l'adeguamento ai requisiti previsti dalla normativa resta stabile al 19%.

Prevention, detection, response: ***come si affrontano queste fasi quando si ha a che fare con la minaccia che in questo momento più impensierisce aziende e istituzioni?***

Nel tempo gli attacchi ransomware si sono evoluti, oggi i nuovi attacchi anziché limitarsi a crittografare semplicemente i dati su alcune unità disco spesso prendono di mira l'infrastruttura, cifrano anche i backup ed esfiltrano informazioni sensibili minacciando di divulgarle al contesto esterno. Significa che si rendono necessari giorni, quando non settimane per recuperare i dati, risolvere i problemi di sicurezza e riavviare tutte le attività. Le aziende per rispondere devono focalizzarsi sui tre momenti chiave, che caratterizzano la gestione di un attacco ransomware: preparazione, risposta, ripristino. Facciamo un esempio per capirci: un'organizzazione che investe per potenziare la propria resilience rispetto a un attacco ransomware può significativamente mitigarne gli impatti intraprendendo azioni preventive, tramite la realizzazione di backup periodici dei dati critici e sviluppando e testando un piano di risposta degli incidenti ransomware.

Quali azioni vanno intraprese e quali vanno evitate per attuare una corretta tutela degli asset strategici del settore bancario?

Una *preparazione adeguata* serve a prevenire dolorosi insuccessi, è dunque fondamentale che l'azienda investa nello sviluppo di un *Ransomware Recovery Plan* che funzioni in condizioni reali e in ambiente che si caratterizzano per elevati livelli di stress. Un ransomware recovery plan non può anticipare tutte le circostanze che devono affrontare i decisori ma la preparazione stessa del piano offre all'organizzazione l'opportunità di considerare attentamente le alternative e definire policy e procedure in atmosfere sufficientemente "tranquille", piuttosto che in contesti attraversati da tensione e stress, tipicamente alimentati dagli attacchi in corso.

Il piano di difesa come si articola?

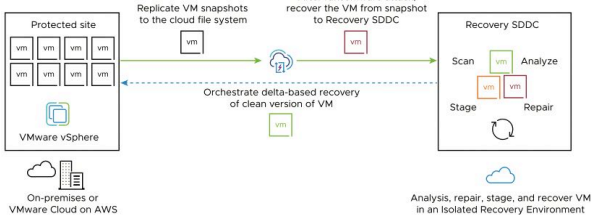
Il piano garantisce che vengano presi in giusta considerazione gli aspetti di compliance, che vengano definite opportune politiche aziendali e che sia valutato il coinvolgimento di terze parti, come il fornitore dei servizi di cyber insurance o una società di consulenza specializzata. Quando si è colpiti

da un attacco ransomware, dovrebbe essere già disponibile un piano di risposta e gestione della crisi e la presenza di alcune risorse essenziali, quali: il Backup dei dati effettuati prima dell'attacco in infrastrutture segregate e sicure; gli Strumenti per analizzare la portata e l'impatto degli attacchi; un'area di ripristino sicura (Recovery Zone) dove riavviare dati e applicazioni.

La resilienza: definizione difficile

In caso di attacco ransomware che misure vanno adottate perché si possa definire resiliente un'istituzione o un'impresa?

Se non si è dedicato tempo sufficiente alla fase di Preparazione, difficilmente la Risposta si rivelerà pienamente efficace. La risposta a un attacco ransomware dovrebbe prevedere il coinvolgimento di diverse figure chiave, idealmente quelle che dovrebbero comporre il Ransomware Response Team. Tra i passaggi più tecnici vale la pena citare l'importanza della **fase di contenimento** che resta senza dubbio una parte fondamentale del piano di risposta agli incidenti. L'impossibilità di isolare rapidamente dalla rete i sistemi infetti (negli stadi iniziali dell'attacco) può contribuire ad aggravare l'incidente, permettendo al malware di diffondersi ulteriormente all'interno dell'infrastruttura. Una metodologia di analisi basata sull'individuazione delle Tattiche, Tecniche e Procedure (TTP), favorita e supportata dalla Threat Intelligence (TI), può agevolare le azioni di mitigazione, permettendo un'identificazione proattiva delle minacce e una risposta tempestiva ed efficace. Alla luce di queste considerazioni possiamo immaginare di poter definire davvero "Resiliente" un'azienda quando quest'ultima si è dotata



di una **Recovery Zone**, corredata di tutte le procedure (magari anche testate) per il suo corretto utilizzo.

Ricorro sempre a un esempio per essere più chiaro: avviare il ripristino direttamente sull'infrastruttura che è stata compromessa da un attacco ransomware non è una buona idea. Si dovrebbe invece lavorare in una Recovery Zone con una rete segregata e server, strumenti e software "puliti". La zona di ripristino dovrebbe, in particolare disporre di strutture di backup complete. Sebbene le applicazioni risiederanno lì solo temporaneamente, dovranno essere in grado, per un certo periodo di tempo, di generare dati di produzione in tempo reale. Come best practice si suggerisce di configurare una recovery zone con hardware e software dedicati in standby, per poter rispondere rapidamente ad attacchi ransomware e ad altre minacce alla business continuity. Le organizzazioni possono anche valutare di configurare parte della recovery zone su piattaforma cloud.

Proviamo ad allargare lo sguardo. Oggi esiste un fitto intreccio tra cyber security, geopolitica, economia e diritto, lo stiamo vedendo ogni giorno basta sfogliare i giornali. L'adozione del* digital services act *che scenari potrà aprire?

Tra le varie aree toccate dal DSA evidenzio tre punti che, nelle aspettative della CE, dovrebbero produrre gli effetti più macroscopici. La prima stabilisce norme più chiare sulla **Responsabilità** delle piattaforme online per i contenuti ospitati sui loro servizi. Le piattaforme possono essere tenute responsabili per la rimozione tempestiva dei contenuti illegali o dannosi, il che produrrà principalmente due effetti: un maggiore controllo di sicurezza dei contenuti, anche attraverso l'implementazione di sistemi di segnalazione più efficaci, una più alta capacità di contrastare la diffusione di disinformazione e fake news online, ad esempio obbligando le piattaforme a processi per la rimozione tempestiva di contenuti falsi o inattendibili. Secondo aspetto importante è la **Protezione dei consumatori**: il DSA mira a rafforzare i diritti dei consumatori online, garantendo la sicurezza dei prodotti e dei servizi digitali. Questo migliorerà la fiducia dei consumatori nell'ecosistema digitale. Come terzo aspetto troviamo la **Cooperazione internazionale**: il DSA potrebbe aprire la strada a una maggiore cooperazione tra l'UE e altre giurisdizioni nel regolamentare le piattaforme digitali, poiché molte di queste piattaforme operano a livello globale. Lo dimostra il fatto che l'estensione del DSA a paesi extra-UE appare già nell'agenda del G7.

Il digital service Act: passo importante

In una recente intervista l'ex direttore di ACN Roberto Baldoni ha osservato: "con il DSA potremo avere un web più sicuro anche se si impone un bilanciamento tra la proliferazione e il coordinamento delle norme". ABI Lab ha nell'innovazione il suo epicentro. Quale deve essere il rapporto tra lo sviluppo della tecno-scienza e la ricerca di strumenti giuridici atti a garantire la sicurezza di reti e sistemi?

Questo rapporto dovrebbe essere dinamico, interconnesso e in costante evoluzione. Risulterà decisiva una collaborazione interdisciplinare e multisettoriale. La sicurezza informatica è un campo multidisciplinare che richiede la collaborazione tra esperti tecnici, giuristi, economisti e altre figure professionali. Per questo la ricerca di strumenti giuridici dovrebbe coinvolgere esperti in diversi campi per sviluppare soluzioni complete ed efficaci a valenza anche su più settori produttivi. Molta attenzione bisognerà rivolgere al Principio di proporzionalità: le leggi e i regolamenti sulla sicurezza informatica dovrebbero rispettare il principio di proporzionalità. Ciò significa che le misure devono essere adeguate alla minaccia e non eccessivamente restrittive per l'innovazione tecnologica. In altre parole, dovrebbero essere bilanciate e mirate. Centralità va poi riconosciuta agli Standard e alle norme generali che regolano la sicurezza, sviluppate da organizzazioni internazionali e settoriali che dovrebbero essere incorporati nei requisiti legali, consentendo alle imprese di avere riferimenti chiari e di adottare approcci basati su best practice. Non trascurerei, poi, la definizione degli Incentivi per la sicurezza. Gli strumenti giuridici dovrebbero essere utilizzati per promuovere l'adozione di una postura di sicurezza migliore e potrebbero prevedere incentivi per investimenti in sicurezza informatica.

In conclusione, mi soffermerei sulla riconosciuta fragilità del fattore umano. La sua esperienza la induce a pensare che su questo delicato terreno si siano fatti passi avanti apprezzabili?

Si tratta di una grande sfida per la sicurezza, motivo per il quale le iniziative di cybersecurity awareness giocano un ruolo centrale nel nostro mondo mobile e interconnesso. Le banche sono da sempre fortemente impegnate in iniziative di sensibilizzazione indirizzate alla propria clientela, comunicando in particolare sull'utilizzo sicuro degli strumenti di pagamento e dei dispositivi mobili e sulla gestione sicura dell'identità attraverso diversi canali: portali di internet banking, mobile app, e-mail e/o sms, filiali e social network. Un ulteriore ambito di impegno è quello delle iniziative di sensibilizzazione sui temi della sicurezza informatica condotte in collaborazione dalle istituzioni e dalle singole banche. Penso alla campagna di informazione *"I Navigati – Informati e Sicuri"* (www.inavigati.it) realizzata dal CERTFin per favorire l'uso sicuro e consapevole dei canali e degli strumenti digitali e sensibilizzare i clienti sui rischi di attacchi e frodi online nella fruizione di servizi finanziari. A tale iniziativa si aggiunge l'iniziativa "CyberSicuri" a cui il CERTFin sta lavorando in questi mesi: una campagna di *cybersecurity awareness* destinata alle piccole e medie imprese che punta attraverso video e materiale interattivo ad aumentare la sensibilità di manager e dipendenti di fronte ai rischi informatici che presentano impatti molto forti sugli asset aziendali. ■

Preparazione, competenza, condivisione, la sicurezza nella societa' complessa è un bene condiviso.

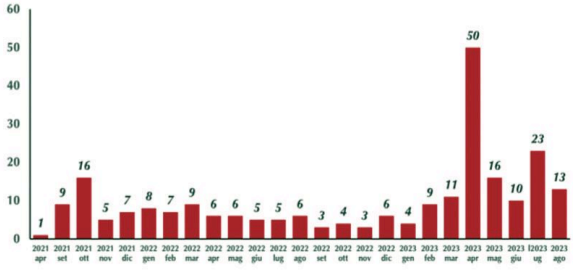
Intervista VIP a Marco Ramilli.

Autore: Massimiliano Cannata

Occhi puntati sul Ransomware, sofisticato software con cui si sottraggono informazioni, per chiedere poi il rilascio dietro compensi crescenti alle organizzazioni. Ne parliamo con Marco Ramilli, CEO di Yoroi.

Prevention, detection, response come si affrontano queste delicate fasi quando si ha a che fare con la minaccia che, in questa fase, sembra impensierire più di ogni altra cosa aziende e istituzioni: il ransomware?

Partirei dai dati che usualmente sono una buona base sulla quale strutturare ragionamenti difensivi. I gruppi Ransomware oggi conosciuti e monitorati sono 165, di cui 85 sono attivi negli ultimi 3 mesi. Dall'inizio del monitoraggio (2021) sono stati indicizzati circa 9000 vittime a livello globale di cui ben 3201 nei primi 8 mesi del 2023. Considerando che in tutto il 2022 le vittime dichiarate dai gruppi ransomware sono state 3081 a livello globale possiamo osservare una crescita molto significativa che probabilmente si avvicinerà a un "high double digit" verso la fine dell'anno.



Sul fronte italiano (vedi immagine sopra n.d.r.) i numeri sono ovviamente ridotti parliamo infatti di decine di vittime dichiarate per anno. Nei primi 8

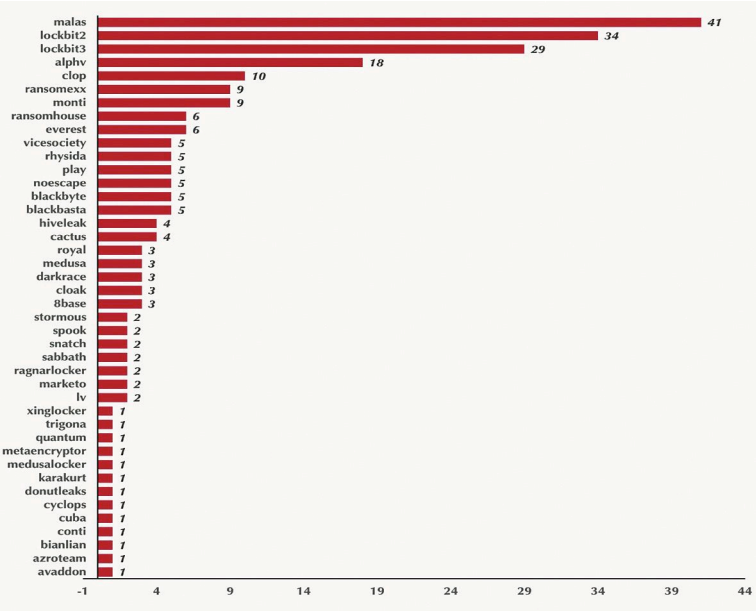
BIO

Esperto di sicurezza Informatica, specializzato in Malware Analysis e sistemi di evasione, Marco Ramilli ha ottenuto un PhD presso l'Università degli studi di Bologna in collaborazione con l'Università della California, Davis, dove ha realizzato alcune delle principali tecniche per individuare nuove famiglie di Malware ed alla messa in sicurezza di noti sistemi di voto elettronico. Ha lavorato per il Governo degli Stati Uniti d' America, dove ha contribuito alla realizzazione dell OEVT. CyberSecurity blogger dal 2007, autore di due libri sulla sicurezza informatica e sulle metodologie di penetrazione di sistemi informatici, autore di innumerevoli articoli scientifici pubblicati su note riviste quali IEEE ed ACM. CEO e fondatore di Yoroi, una delle aziende più innovative di Cybersecurity, appartenente al Gruppo Tinexta S.p.A. dal 2020.

mesi del 2023 sono state monitorate 127 tentativi di estorsione in aziende italiane per un totale di circa 242 su base totale, ma sappiamo bene che non tutte le organizzazioni colpite vengono pubblicate sui rispettivi blog dei gruppi criminali.

Qual è il livello reale di rischio che le organizzazioni devono fronteggiare?

La richiesta di riscatto varia molto da gruppo a gruppo, per fare solo alcuni esempi il gruppo Blackmatter ha effettuato delle richieste di riscatto nel range compreso da 5 milioni fino a 15 milioni di dollari, negoziate rispettivamente a 1.5 milioni e 13.5 milioni di dollari. Lockbit3 che assieme a Lockbit2 è molto presente in Italia, al netto di qualche richiesta di riscatto che ha superato i 10 milioni (come per esempio quelle effettuate a wabteccorp.com, samyang.com e royalmailgroup.com) mantiene un profilo più basso che in media (escludendo le top 10 negoziazioni pubbliche) resta in un *range* tra i 2milioni ed i 700k dollari per evitare che i dati aziendali vengano resi pubblici. I principali gruppi operanti in Italia risultano essere (in accordo all'immagine a seguire) MalasRansomware, Lockbit2, Lockbit3 ed Alphv.



I dati riportati si basano su fonti aperte e su monitoraggi attivi e pubblicamente dichiarati dai gruppi criminali stessi sulle rispettive sorgenti di informazioni ma è evidente che non tutto viene pubblicato, per questo motivo possiamo confermare con una certa sicurezza che questi numeri sono solo la punta di un iceberg ben più grande. Riassumendo possiamo dire che risulta evidente che la dimensione del fenomeno è ampia e di impatto per molte nostre organizzazioni, è un fenomeno che non possiamo più permetterci di sottovalutare e che deve essere incluso nel percorso di valutazione del rischio aziendale.

Per attuare una corretta tutela degli asset produttivi, cosa devono fare le aziende?

Credo sia importante avviare due modelli di attività simultanee. Un modello denominato "Top Down" che miri a organizzare i processi di difesa e un'attività denominata "Bottom Up" con obiettivo più tecnologico. Tipicamente la prima attività (TopDown) ha obiettivi di difesa a medio-lungo termine mentre la seconda ha obiettivi di difesa a corto-medio termine. Per questo motivo avviarli in parallelo offre all'organizzazione un duplice vantaggio: aumentare la difesa dell'oggi e contemporaneamente avere un team con overlook a 3 anni per la creazione di processi e procedure per una gestione di incidenti più matura e di continuo miglioramento tecnologico. Per affrontare il modello "Top Down" esistono numerosi strumenti metodologici come per esempio: DORA, NIS2 ed il cybersecurity framework del NIST (nella sua nuove versione) da applicare alla propria realtà in funzione della tipologia di business e dal grado di rischio al quale si vuole tendere.

In relazione al secondo modello, cosa possiamo dire?

Per attuare il modello "Bottom up" risulta importante avere ben chiaro il perimetro da difendere e avere una buona visibilità su di esso. Da non sottovalutare il "network". Esso può essere decisivo tanto quanto lo sono gli "agenti" installati sulle singole macchine. Un XDR può essere eluso (evaso/disattivato) mentre una traccia di rete persiste, essa può essere utilizzata sia per un "early detection" che per una analisi a posteriori. Oggi alcune organizzazioni tendono a mantenere XDR al posto di "probe di rete" ma non dobbiamo dimenticarci che non sono due alternative, sono piuttosto due oggetti a complemento.

Una definizione di resilienza

Per definire resiliente un'organizzazione complessa, che comportamenti deve attuare?

Per dare una risposta dividerei preliminarmente la gestione di un "attacco" con quella di un "incidente". Un attacco va gestito attraverso il team di difesa, per esempio, attraverso un Cybersecurity Defence Center o un tradizionale Security Operation Center (SOC). Esso ha le proprie strutture interne ed i propri metodi (e playbook) con il quale reagisce a un attacco. Scenario differente se stiamo affrontando un incidente, ovvero uno specifico sottoinsieme di attacchi. Un incidente è definibile come un attacco andato a buon fine con un impatto sulla vittima.

Cosa vuol dire in concreto?

Che se ci stiamo preparando per la gestione di un incidente informatico, allora dobbiamo prepararci in modo più specifico. Per prima cosa necessitiamo di un

team differente, un team di analisti DFIR (digital forensi and incident response). Tale team ha capacità trasversali sia su analisi forensi sia su risposta ad un attacco. Il team ha la necessità di collaborare con molte aree aziendali, per questo motivo un'organizzazione preparata a un incidente informatico, e vengo in maniera più diretta alla domanda, deve aver precedentemente effettuato una sequela di azioni.

Possiamo riassumerle?

In prima battuta la preparazione di un *incident response plan* (IRP). Ovvero un documento disponibile a tutte le figure chiave aziendali da seguire in caso di incidente. Obiettivo di tale documento è evitare ogni improvvisazione. Ogni figura (Chief Executive Officer, Chief Operation Officer, Chief Technology Officer, Chief Marketing Officer, Chief Salse Officer, Board of Director, Chief Human Resource) ha un ruolo all'interno dell'IRP, che è quello di seguire alla lettera il documento favorendo la velocità di intervento. Secondo: una corretta simulazione di un incidente, che vuol dire aver testato IRP almeno una volta per anno. Terzo: preoccuparsi che ci sia un adeguato *engagement* aziendale, che si misura da una puntuale comunicazione della presenza di un IRP all'interno dell'organizzazione, e contestualmente dall'avvenuta messa in esercizio di un processo di maturazione cibernetica del personale. Sono questi gli step principali, che ogni organizzazione, sia essa privata o pubblica dovrebbe adottare per garantire un livello standard di sicurezza digitale.

Allarghiamo lo sguardo. Su quali basi va costruito un ecosistema della sicurezza all'altezza delle sfide di oggi?

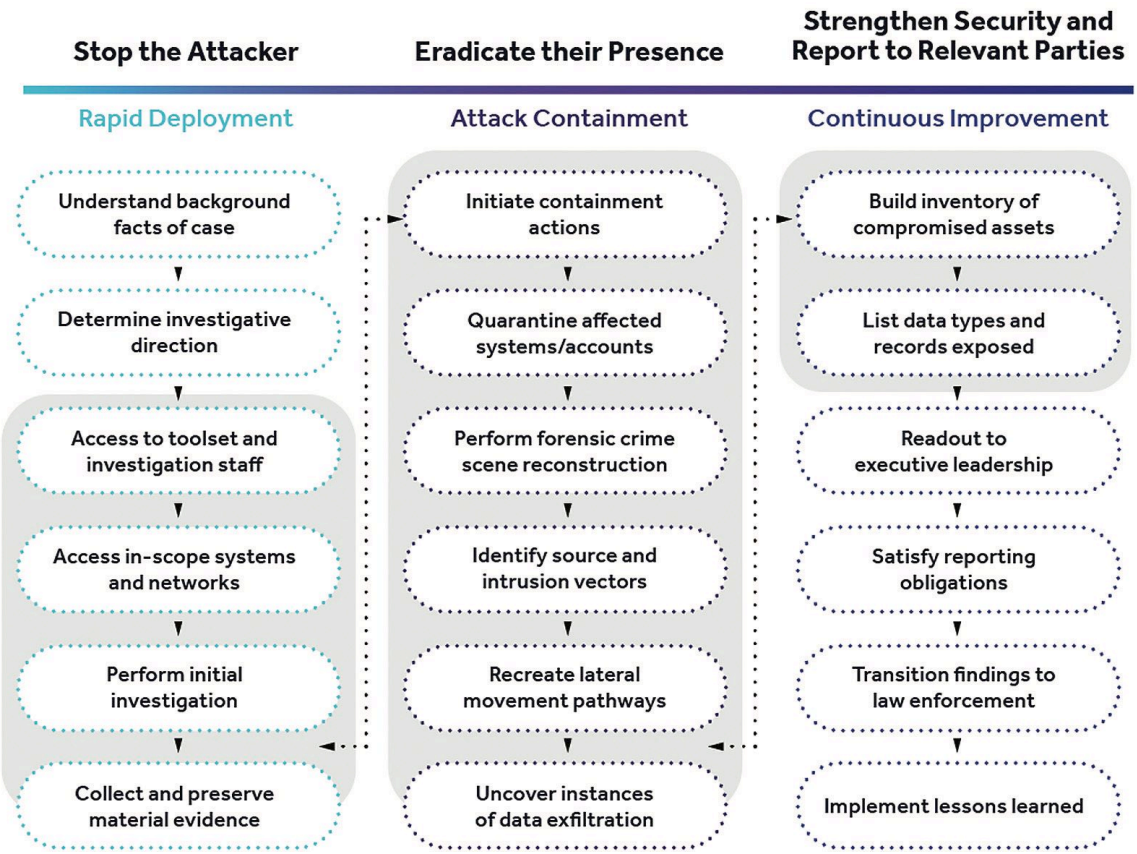
Durante la storia della *cybersecurity* abbiamo vissuto numerose "mode", dagli antivirus agli XDR, passando per efficaci tecnologie di "prevention", "detonazione" e "deception". Oggi credo che la principale attività sulla quale fondare la propria difesa cibernetica sia il rafforzamento della conoscenza. Conoscere come operano gli avversari credo siano i fondamenti di ogni attività di difesa "ragionata" ancora prima che l'automatismo o l'inserimento dell'intelligenza artificiale. Sotto questo aspetto la *"threat intelligence"* risulta essere la pietra miliare per ogni difesa contemporanea. La difesa "ragionata" non è tuttavia l'unica difesa possibile. È possibile adottare una difesa "veloce", ovvero una difesa che decida di favorire la velocità piuttosto che l'azione meditata.

Come si riconosce questa seconda modalità?

Molto semplice. Il lettore potrebbe pensare all'*Incident Response Plan*, modalità fondata sul "ragionamento" a priori, che consente un'azione conseguente "veloce" e "ragionata", termini che insieme possono confondere. In questo contesto un IRP ha assolutamente il massimo del rispetto ma è altamente improbabile trovare un IRP che riesca a mappare ogni decisione per ogni scenario di attacco, esso infatti offre delle linee guida e dei principi sui quali muoversi agilmente. Ma quanto mi riferisco a difesa ragionata o difesa veloce mi riferisco alle azioni tecniche da adottare durante il corso di un incidente, non certo a un incidente compiuto.

Possiamo fare un esempio per capirci meglio?

Il team DFIR ha individuato l'attaccante, la macchina dalla quale impartisce i comandi (proxy). L'attaccante è in una fase di footprint



augmentation e quindi si muove lateralmente per aumentare il proprio dominio interno alla rete vittima ancora nessun dato esfiltrato e nessun ransomware installato sul sistema. Una possibile risposta veloce potrebbe essere quella di bloccare il threat actor, fare una copia di tutte le macchine coinvolte per analisi più attenta, riportare la rete allo stato iniziale in attesa di comprendere il vettore di ingresso per poi bloccarlo definitivamente. Una risposta ragionata (specialmente valida in alcuni settori governativi) potrebbe essere quella di attirare il threat actor verso un perimetro specifico, coinvolgerlo in attività a bassa intensità e mantenerlo occupato il più a lungo possibile. Nel frattempo, salvare gli eventuali sistemi coinvolti nel perimetro di "vero interesse aziendale" e riportare alla normale operatività la specifica parte di rete mentre l'attaccante resta attivo all'interno di uno specifico perimetro aziendale. Tale scelta dipende da numerosi parametri tecnologici, dalla competenza degli operatori che sono coinvolti nel DFIR, dal momento storico dell'organizzazione coinvolta come vittima, dalla sua maturità nella gestione degli incidenti, nella natura della stessa e dalla volontà del management.

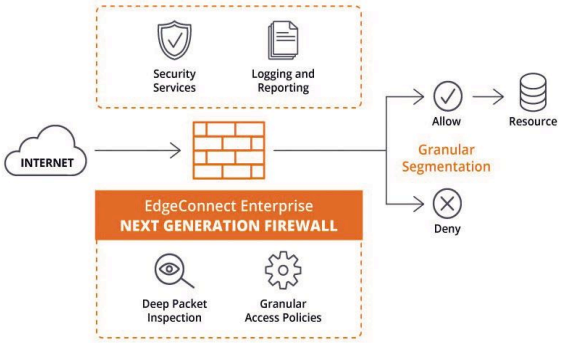
L'importanza della threat intelligence

La threat intelligence, cui Lei prima faceva riferimento, su cui Yoroi ha avuto un importante riconoscimento a livello continentale, può contribuire a innalzare il livello di difesa da minacce che hanno la tipologia del ransomware?

Avere indicatori di compromissione, indicatori di attacco o informazioni relative al "modus operandi" di collettivi ransomware gioca un ruolo molto rilevante. Gli indicatori di attacco possono aiutare ad anticipare l'attaccante dotando la futura vittima di "filtri" o di tecnologie adatte al tipo di attacco su cui sta investendo l'attaccante. Basti pensare che durante le ondate di DDOS di Killnet o Noname essere a conoscenza con anticipo delle prossime vittime, ha offerto la possibilità di innalzare deflettori per tempo o di attuare politiche di geo-fence nello stretto tempo necessario evitando o riducendo il più possibile perdite di business. Avere indicatori di compromissione ci offre, inoltre, l'opportunità di effettuare analisi migliori e di avere un dettaglio di attribuzione con maggiore accuratezza. Per esempio, essere a conoscenza che uno specifico crafted-tool appartiene all' attore X, aiuta notevolmente nell'attività di attribuzione e di conseguenza aiuta la remediation ovvero le azioni necessarie all'eradicazione del sistema compromesso. Oppure essere a conoscenza che l'attore Z ha compromesso i servers s1, s2 e s3 e che li utilizza come proxy per effettuare tentativi di *exploiting* è importante per il filtering-out ovvero configurare sistemi a perimetro per bloccare ogni richiesta proveniente da s1, s2 e s3.

Decisive anche le informazioni sul modus operandi, di chi attenta alla sicurezza. Qual è la sua opinione in merito?

È molto importante questo aspetto, perché dà la possibilità di investire in tecnologie o formazione specifica al fine di essere pronti al meglio durante un incidente. Essere, per esempio, a conoscenza che l'attore A utilizza sistemi di phishing come vettore iniziale, ci offre la possibilità di suggerire ai nostri clienti di investire nella sofisticazione della tecnologia anti-phishing piuttosto che (semplice esempio) sul Next generation firewall. Contemporaneamente essere a conoscenza che il nuovo collettivo sta migrando la sua operatività contro sistemi Linux offre alla nostra organizzazione l'opportunità di avviare corsi formativi per analisti Linux piuttosto che analisti Windows.



L'adozione del digital services act

Esiste un fitto intreccio tra cyber security, geopolitica, economia e diritto, lo stiamo vedendo ogni giorno basta sfogliare i giornali. L'adozione del* digital service act *che scenari potrà aprire?

L'adozione di tale norma permetterà la nascita di un ecosistema di organizzazioni operanti nel settore ancora più prolifera e specifica, determinando una sempre più forte coesione tra gli organi di polizia internazionale per la lotta al cyber crime. Nel contempo si farà strada una maggiore tutela per le vittime nell'orizzonte di un *framework* Europeo al quale attenersi per una maggiore trasparenza per chi vorrà costituire nuove organizzazioni nello spazio digitale.

Fragilità del fattore umano. Vede elementi di progresso su questo che rimane un terreno molto difficile e delicato da presidiare?

La stampa ha contribuito a far maturare una nuova coscienza del rischio: i giornalisti di settore hanno dei meriti su questo fronte. Trasmissioni televisive (anche se in tarda serata), articoli specialistici, rubriche su periodici, titoli spesso molto toccanti, hanno contribuito a maturare la consapevolezza che il digitale debba essere difeso e che sia compito di tutti, lavoratori, studenti, insegnanti, genitori e amministratori impegnarsi per innalzare gli standard di sicurezza. Altro plauso va dato alla *compliance*. In questi ultimi anni è maturata tantissimo. Mentre prima si occupava principalmente di processi organizzativi (cfr. 231, ISO 9000, n.d.r.) oggi si occupano, con successo, di regolamentazioni tecniche come ISO27k, DORA e NIS2 solo per citarne alcune. Si tratta di passi decisivi, che contribuiscono notevolmente a ridurre la fragilità umana e a difendere, attraverso processi e procedure, la forza delle nostre aziende. ■

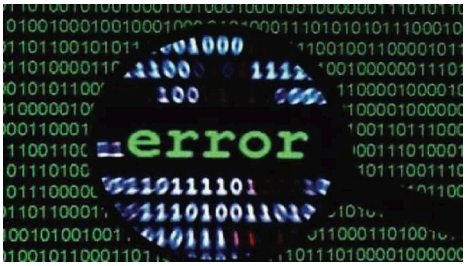
Stiamo vivendo un'epoca unica. Prepariamoci per essere protagonisti.

Intervista VIP a Mikko Hypponen.

Autore: Nicola Sotira

Stiamo assistendo, come viene detto nel suo libro, all'aumento della vulnerabilità di reti e sistemi. Come devono prepararsi le aziende?

La causa principale di qualsiasi violazione dei dati, incidente di ransomware, epidemia di natura tecnica, ha dietro una disattenzione. Ogni volta che parliamo di patch, aggiornamenti o vulnerabilità in sé, a volte mi viene la domanda: come mai non possiamo creare un sistema operativo o un'applicazione senza vulnerabilità? La risposta è molto semplice. Questi programmi sono scritti da esseri umani. Gli esseri umani commettono errori, quando i programmatori commettono errori, ci ritroviamo con dei bug, e quando abbiamo bug nei sistemi interconnessi, questi diventano facilmente vulnerabilità che possono essere sfruttate. E questo significa davvero che non ci libereremo dei bug. Ciò significa che non elimineremo le vulnerabilità tanto presto. Tutto questo non scomparirà finché tutto il codice che usiamo non sarà scritto dalle macchine. Ciò potrebbe accadere un giorno, ma non in un futuro molto prossimo. Non illudiamoci: anche le macchine commettono errori, che possono diventare vulnerabilità. Sono solo più difficili da sfruttare. Detto in estrema sintesi: più codice abbiamo, maggiore è la complessità, maggiori sono le vulnerabilità...



La complessità è nemica della sicurezza. Quando parliamo di violazione, non dobbiamo pensare solo ai dati. Può essere oggetto di attacco un pacemaker, una sala operatoria, un laboratorio chimico, persino un panificio. Quali contromisure adottare per un fronte così ampio di rischio?

Tutto è connesso in rete, difficile pensare a circoscrivere il rischio. Che ci piaccia o no, che siamo d'accordo o no, questa rivoluzione è già in atto. Anche se non ci piace, tutto ciò che colleghiamo alla rete elettrica si collegherà alla rete online per i vantaggi che offre al cliente. Non sono un grande sostenitore della regolamentazione, ma se non altro qui potrebbe avere una possibilità realistica di successo. Potremmo pensare a regolamentare la responsabilità dei danni causati da carenze di sicurezza nei dispositivi IOT. In questo momento noi regolamentiamo la sicurezza dei dispositivi (safety), ma non regolamentiamo la security su essi. Quindi se la tua lavatrice prende

BIO

Mikko Hypponen è Chief Research Officer di WithSecure, la più grande azienda di sicurezza informatica del Nord Europa. Lavora con i computer dagli anni '80 e con la sicurezza informatica dall'inizio degli anni '90. Vive in Finlandia a cento miglia dal confine russo, tenendo d'occhio il "gigante" e indagando nel contempo sulle strategie attuate dalle agenzie di intelligence e militari in tutto il mondo. È autore del saggio "If it's Smart, it's Vulnerable" da cui prende le mosse la nostra intervista.

fuoco, o la tua casa brucia, il produttore è responsabile dei danni. Ma se la tua lavatrice viene violata e ogni dispositivo della tua casa viene infettato da un ransomware, chi sono i responsabili? Credo che su questo bisogna cambiare molte cose.

L'intelligenza artificiale, può aiutarci a risolvere o perlomeno a ridurre il rischio?

Nella sicurezza informatica, l'intelligenza artificiale credo sia l'unica soluzione. Ci sono troppi attacchi da bloccare. Troppi campioni da analizzare. Troppi exploit da affrontare. Non può più essere fatto dagli esseri umani. L'unico modo per farlo è attraverso l'automazione, ed è ciò che stanno già facendo tutte le società di sicurezza. Lo facciamo da anni. Tutto è iniziato con l'automazione semplice. Si è espanso nei framework di apprendimento automatico e oggi utilizziamo l'intelligenza artificiale per automatizzare le macchine, distinguendo tra buono e cattivo.

E da quando lo facciamo, aspettiamo che il nemico faccia la stessa mossa. Stiamo aspettando che queste bande organizzate di criminali informatici o i gruppi che distribuiscono ransomware o che attuano truffe più semplici, inizino ad automatizzare i loro attacchi. E un po', sorprendentemente, non l'hanno ancora fatto davvero. Abbiamo visto esempi isolati di utilizzo dell'intelligenza artificiale negli attacchi informatici come alcuni deepfake.

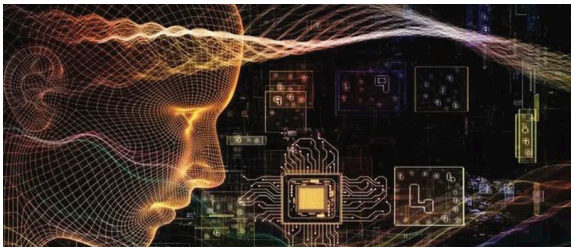
C'è stato un deepfake di Elon Musk su Twitter che cercava di convincere le persone ad acquistare bitcoin da un falso Bitcoin exchange, cosa che

è stata fatta con la tecnica del deepfake per il video e deepfake per la voce. Alcune cose le abbiamo viste, ma la maggior parte...le vedremo, devono ancora accadere. E ciò che mi preoccupa davvero, e che accadrà, sarà la completa automazione delle campagne malware in cui gli aggressori utilizzeranno l'automazione e il machine learning per reagire in modo automatico quando le società di sicurezza bloccheranno i loro attacchi. Quando accadrà vedremo se vincerà la buona o la cattiva IA.

Stiamo iniziando a utilizzare il machine learning, che è una parte dell'intelligenza artificiale e spingendo molto sull'automazione pensando che questa sia una delle aree in cui dobbiamo investire per ridurre il rischio. Quale approccio occorre avere nel prossimo futuro?

Nel prossimo futuro si parlerà di intelligenza artificiale e quantistica. Le tecnologie stanno diventando ogni giorno più intelligenti. Un giorno vedremo la super intelligenza artificiale, il che significherebbe che gli esseri umani sarebbero la seconda entità più intelligente del pianeta. Se ciò accadrà, dovremo stare molto attenti a come oltrepasseremo il limite. Possiamo oltrepassare quel confine solo una volta.

Altra cosa importante che cambia anche la sicurezza: l'informatica quantistica. Quando i computer quantistici diventeranno più realistici; quando avranno sempre più qubit, potranno eseguire calcoli sempre più grandi.



Avremo a disposizione la potenza di calcolo tale da decifrare tutti gli algoritmi di crittografia simmetrica che usiamo come l'RSA, per esempio. Dobbiamo semplicemente migrare dai vecchi algoritmi di crittografia deboli ai nuovi algoritmi di crittografia quantistici sicuri, che già esistono, sarà un progetto enorme, lungo un decennio, perché dobbiamo aggiornare ogni telefono cellulare, ogni computer, ogni server, ogni browser, ogni TV, ogni macchina. Discutendo di IOT, usano tutti il TSL in questo momento che utilizza algoritmi di crittografia deboli. Direi di più: siamo in ritardo, perché avremmo già dovuto farlo. I computer quantistici potranno insegnare algoritmi di apprendimento automatico molto, molto più potenti; quindi, potrebbero accelerare la velocità dell'intelligenza artificiale. Chi lo può dire? Sappiamo solo che stiamo vivendo tempi molto emozionanti e di certo spaventosi, attrezziamoci al meglio per affrontarli. ■

Security Mind

La Cyber Security incontra La Psicologia

A cura di Veronica Patron Co-Founder di Security Mind

Ransomware - Quando la Tecnologia Incontra la Psicologia Comportamentale

Cresce costantemente la diffusione del ransomware come minaccia digitale, poichè oltre all'aspetto tecnologico vengono sfruttati anche gli aspetti comportamentali delle potenziali vittime.
Per raggiungere il loro obbiettivo, i cybercriminali utilizzano una serie di strategie psicologiche per spingere i loro utenti target a pagare il riscatto.

Questo evidenzia l'importanza anche del fattore umano per difenderci da questa tipologia di attacchi: il nostro comportamento e la nostra capacità di prendere decisioni ragionate, piuttosto che impulsivamente, diventano fondamentali per evitare di aprire le porte ai cybercriminali.

Ma quali sono le Leve Psicologiche utilizzate per colpirci?

1

Paura e Panico
Vedere i propri dati inaccessibili può scatenare paura e panico nella vittima, spingendola a pagare il riscatto.

2

Pressione Emotiva
Il ransomware sfrutta spesso il tempo come leva emotiva, costringendo la vittima a prendere decisioni rapide.

3

Curiosità
Alcuni attacchi di ransomware iniziano con l'invio di email che incuriosiscono le vittime. Questo può portare le persone a cliccare su link dannosi.

4

Fiducia Violata
Dopo un attacco di ransomware, le vittime potrebbero avere difficoltà a fidarsi delle nuove tecnologie o delle comunicazioni online.

5

Isolamento
Bloccare l'accesso ai file e ai dati, fa sentire la vittima isolata e impotente, ritenendo che il pagamento sia l'unica via d'uscita.

La nostra Missone è passare dall' Informazione alla Trasformazione

www.securitymind.cloud

Bibliografia

Henry A. Kissinger
Eric Schimdt
Daniel Huttenlocher
L'era dell'intelligenza artificiale
Ed. Mondadori

Lo sviluppo dell'IA, tra rischi e opportunità

Cosa non abbiamo capito dell'Intelligenza artificiale, materia delicata che attraversa la contemporaneità, polarizzando l'attenzione dei media di tutto il mondo? Henry A. Kissinger, insieme a Eric Schmidt e Daniel Huttenlocher offrono delle risposte di urgente attualità. Non finisce di stupire la lucidità di Kissinger, già consigliere di Stato americano dei Presidenti: Nixon e Ford, Nobel per la Pace nel 1973, medaglia presidenziale delle libertà nel 1977, eminente figura del Novecento, componente di una classe dirigente che non può più vantare, purtroppo, protagonisti di uguale statura. Lo studio ha un sottotitolo significativo: il futuro dell'identità umana, perché appare ormai evidente, anche agli osservatori più distratti, che la diffusione delle tecnologie imporrà di riportare lo sguardo sull'uomo e sul suo destino. Sono diverse le tipologie di IA di cui disponiamo, quelle che hanno un grado avanzato di sviluppo entrano in "dialogo" con l'individuo, mimando le facoltà superiori, per questa non banale ragione richiedono un'analisi attenta, se vogliamo gestirle, senza subirne il potere di controllo. Rischi e opportunità dell'innovazione, è sempre la stessa dicotomia che mette sotto scacco le civiltà di ogni tempo e latitudine. Di fronte a questa "ventata" che Luciano Floridi ha ben descritto nel saggio dedicato alla "Quarta rivoluzione", stiamo assistendo a una polarizzazione di atteggiamenti: chiusura e pessimismo da un lato, eccesso di ottimismo dall'altro. Lo studio "L'Era dell'IA" si colloca in un'area mediana, non nasconde le paure, ma nello stesso tempo invita a guardare con spirito cautamente ottimistico i fenomeni di trasformazione della società. "Dove siamo", il primo capitolo della trattazione offre una ricognizione, per capire l'iter che ha portato agli straordinari risultati di oggi. La macchina di Turing è il *primum movens* che ha aperto il confronto tra logica, filosofia e scienza, che continua a dominare l'attuale ricerca sull'intelligenza generativa. Il nodo della questione rimane il delicato rapporto tra sicurezza e IA, aspetto che si riflette sulla capacità che dimostreremo di possedere nella protezione di reti, sistemi e infrastrutture critiche.

Intanto nuovi orizzonti di sfida si fanno strada nel campo della riproduzione artificiale di immagini e di notizie non veritiere, realtà e finzione ormai si rincorrono disorientando un'opinione pubblica frammentata, confusa, smarrita. Non si fa a tempo a definire un passaggio evolutivo, che subito bisogna fare i conti con qualcos'altro. Il rapporto tra IA e *quantum computing*, per esempio. Dovremo prepararci a dovere sull'argomento, mentre giunge notizia che anche i Codici di Leonardo sono stati passati allo scanner dell'intelligenza generativa. Anche la creatività umana è stata "riletta" dalla macchina, che ha cercato di riprodurre la fitta trama di connessioni che avrebbe portato il grande scienziato ad anticipare secoli di ricerca, con il "folle volo" della sua genialità unica. Giuristi, filosofi, scienziati l'agorà di riflessione è divenuta una piazza interdisciplinare. Tutti gli ambiti del vivere civile, del lavoro, dalla salute allo svago, vivono una metamorfosi in cerca di approdi stabili. Innalzare i livelli di consapevolezza, allenarsi a esercitare un agire comunicativo rispettoso della diversità delle opinioni, fa parte di un indirizzo di metodo che bisognerà applicare se vogliamo governare la macchina senza esserne travolti. Va misurata con strumenti adeguati, come ha più volte sottolineato Pasquale Stanzione, la tassonomia del rischio, nel tentativo di avvicinare l'evoluzione della tecno-scienza, alla nostra capacità di regolazione. Non c'è una sola etica che può ispirare il regolatore, più visioni del mondo e sensibilità devono portare un punto di convergenza, se vogliamo la crescita di quella che Morin chiama "comune umanità". Decisivo sarà lavorare per la generazione "z" immersa nel digitale, per questo ignara dei pericoli. Il confronto tra vecchi e giovani è un altro aspetto della strategia da mettere in campo. La sicurezza è visione, condivisione, consapevolezza. Preoccupiamoci, in conclusione, del "posto dell'uomo nel mondo", tra ordine naturale e disordine antropologico, per usare l'immagine dell'ultimo libro del filosofo Salvatore Natoli. Perché la definizione dell'identità, su cui ci interrogavamo all'inizio, è frutto di un continuo processo di immunizzazione e adattamento all'ecosistema, che non conoscerà mai soste. ■

Byung-Chul Han
Infocrazia
Ed. Einaudi

Vite in rete nel tempo frammentato del digitale

Il saggio di Syung-Chul Han solleva degli interrogativi forti su una nuova tipologia di regime, cui tutti siamo sottoposti: quella dell'informazione. L'esercizio della sovranità nell'universo digitale, la tesi di fondo su cui si regge l'impianto dello studio, può degenerare nel capitalismo della sorveglianza, declassando gli esseri umani a *bestie di dati e di consumo*. Del tema ci aveva parlato Shoshana Zuboff in un'opera pubblicata in Italia dalla

Luiss University Press che aveva indagato sui nuovi poteri legati alla digitalizzazione, suscitando un vivace dibattito. Il pensatore di Seoul riprende la forza di quell'analisi, spingendosi oltre. Han aveva già offerto un "assaggio" ai lettori dei suoi interessi teoretici in un agile scritto: "Le non cose", in cui ci ha fatto notare, senza usare mezzi termini, che il digitale è una continua epifania, che ci affascina facendoci perdere l'abitudine di vivere il reale. Con *Infocrazia* lo studioso torna sulle "malattie" della società tecnologica, entrando nel "sacrario" più difficile da maneggiare: il potere e i suoi simboli. "Nei regimi premoderni - spiega – nel Panopticon, il carcere perfetto di Faucault sono i corpi, portatori di energia che vanno controllati e soffocati. Le insegne di quel potere che ha fondato lo stato moderno, si nutre di biopolitica, toglie libertà, esercita, in uno spazio misurabile, la sua forza coercitiva, vuole visibilità per essere esemplare.

Canone inverso quello della società digitale: altri linguaggi e strumenti, diverse le modalità di affermazione della leadership. "Abbiamo a che fare con i grandi samurai digitali – commenta Michele Mezza – hanno scavallato gli stati, gestiscono direttamente le relazioni internazionali dallo spazio alla guerra, per arrivare alla sanità e all'informazione". Una metamorfosi delle classi dirigenti resa possibile dal tramonto del Leviatano di Hobbes, che identificava il potere sovrano nel territorio, nella spada, nella moneta, insegne di superiorità attorno a cui si organizzava lo sviluppo del corpo collettivo. Il digitale è un potere asimmetrico, diffuso apparentemente docile, in cui libertà e sorveglianza coincidono. Le grandi piattaforme ci lasciano apparentemente liberi, quando in realtà navighiamo in una prigione trasparente. Tra i tanti esempi richiamati dall'autore, che conduce il lettore fino alle estreme conseguenze della "crisi della verità", colpisce la contrapposizione tra Apple Store e la Ka'ba della Mecca. Contenitori diversi. Il potere rimane arcano, nascosto, pochi eletti lo manovrano. Apple è però una scatola di vetro, trasparente che rimanda un blackbox: l'algoritmo. Il controllo del dato da potere, il link media escludendo la rivoluzione, perché si piega a un dominio di velluto. Viviamo dentro lo smartphone, la nostra stessa casa è una home smart permeabile ai controlli esterni. Non serve tanto "Sorvegliare e punire" come ci ha insegnato Foucault, oggi bisogna motivare e performare. Gli *influencer* sono i sacerdoti di una nuova religione, salvatori di anime digitali, impalpabili fluttuanti, persino l'individuo è un onduscolo che barcolla, incapace di appigliarsi a orizzonti stabili di valore. In questa dinamica, i social media sono una chiesa", i processi di sharing una comunione, il consumo ci salva in questa dinamica. La rivoluzione non alberga, in questo complesso scenario tratteggiato da Byung-Chul Han, perché consumo e rivoluzione si elidono. La narrazione delle grandi ideologie, ha teorizzato la trasformazione del mondo, l'algoritmo è totalitarismo senza ideologia.

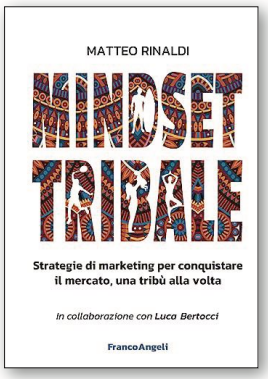
La stessa definizione di opinione pubblica non ha più nulla a che vedere con la modernità. Il libro, strumento ha formato l'opinione pubblica, la stampa ha permesso che ci fosse l'illuminismo. Habermas soffermandosi sull'etica del discorso pubblico, ha studiato a fondo i percorsi di costruzione del consenso. La mediocrazia nell'intreccio di informazione e intrattenimento ha sgonfiato di senso il discorso pubblico. L'esplosione dei media e della tv ha generato la malattia dell'infotainment, la società digitale deve curare un altro virus: l'infodemia, perché ha una struttura rizomatica, che si sostituisce a quella anfiteatrale, rappresentata dal grande fratello di Orwell.

Le architetture portanti del tempo sono ormai frammentate. Le pratiche del sapere, dell'esperienza della conoscenza sono eluse dal tempo liquido della comunicazione nell'era dell'IA. Ha ragione Maurizio Ferraris, che si è chiesto sulle colonne del Corsera, quale può essere il patto utile per il progresso. Più crescono i dati, di maggiore teoria abbiamo bisogno per decriptarli. Certo fa paura la "verità che si disintegra in polvere di informazioni, spazzata dal vento digitale", immagine con cui si chiude il saggio. Questo non deve però arrestare la ricerca verso approdi più alti, il cammino della civiltà continua anche a dispetto dello sfaldamento dell'agire comunicativo e della razionalità. Si tratta di individuare forme nuove di acquisizione della conoscenza, nel rispetto della dignità umana, che è il termine di valore indefettibile, da cui ogni ragionamento sul nostro modo di essere nel mondo deve sempre prendere le mosse. ■

Matteo Rinaldi
Mindset Tribale: strategie di marketing per conquistare il mercato, una tribù alla volta
Ed. Franco Angeli

Autore: Matteo Rinaldi

"Augh"



Vale la pena ascoltare questo suono evocativo, prima di addentrarci nelle pagine di questo volume che anche in quelle sillabe radica il suo pensiero, per ricordare che sempre, e oggi con grande evidenza, gli uomini hanno il bisogno di unirsi in community e altre forme di aggregazione. E che gli stessi concetti dei quali quel piccolo canto è intriso sono da tenere ben presenti nel rapporto con le nuove tribù di riferimento, *"che nel tempo hanno conservato il loro potere e la loro magia"*. Nel libro si parla di questo "Augh", articolato anche come un iniziale saluto ai lettori. Un invito a un viaggio importante, lungo, nella sua musicalità evocativa. Il saluto "Augh" degli Indiani d'America era originariamente pronunciato come un lungo suono gutturale - spiega l'autore nell'introduzione che riportiamo integralmente che simboleggiava la pace e la benedizione della Madre Terra. Era un modo per mostrare rispetto e gratitudine per la vita ed è, da sempre, simbolo di pace e di armonia.

Si può imparare tanto dalle tribù e non solo da quella degli Indiani d'America; infatti, se dovessi riassumere l'essenza di questo libro in

una frase direi: *Un manuale pratico di marketing per creare delle tribù o integrarsi in quelle già esistenti.*

Il bisogno di sentirsi parte di un gruppo è da sempre insito nella natura dell'uomo. Nella preistoria gli esseri umani vivevano in ambienti pericolosi e incerti, in cui la sopravvivenza dipendeva dalla capacità di proteggersi dagli animali feroci, dalle intemperie e dalle insidie degli altri gruppi umani. Per far fronte a queste sfide, i nostri antenati impararono a collaborare tra loro, unendo le loro forze per difendersi, cacciare, raccogliere cibo e costruire rifugi. In questo modo, la tribù riusciva a soddisfare tutti i bisogni primari dei suoi membri, garantendo la sopravvivenza della specie.

Sono passati migliaia di anni, ma l'istinto dell'uomo a raggrupparsi con persone simili, con abitudini e interessi in comune, non è mai cambiato. Al giorno d'oggi, internet e le nuove tecnologie hanno reso ancora più facile la creazione di community e di altre forme di aggregazione, rendendo il concetto di tribù estremamente interessante per l'economia attuale.

Ogni giorno, tutti noi ci interfacciamo con tribù diverse, di alcune ne facciamo parte, altre le osserviamo e ammiriamo da lontano, alcune ci incuriosiscono mentre altre ancora ci intimoriscono.

Pensiamo a quando apriamo la finestra del balcone di casa appena svegli e, affacciandoci, guardiamo con un misto di ammirazione e incredulità la tribù dei *runner* correre insieme per la città, mentre questa si sta svegliando; oppure quando vediamo la nostra collega in pausa pranzo ordinare piatti rigorosamente *vegani*, la stessa che dopo il lavoro corre per non fare tardi a lezione con gli altri *yogin*. Sono sicuro, inoltre, che tutti noi, nelle nostre famiglie, abbiamo un figlio, un nipote o un cuginetto che passa le ore a giocare ai videogiochi e a ritrovarsi online con gli altri amici *gamers*. Poi, di sicuro, tutti, ma proprio tutti, abbiamo quell'amico che vuole convincerci a giocare a padel, e che con ogni probabilità sarà anche riuscito a fare di voi dei *padelisti*. Ci innervosiamo quando sentiamo parlare di *terrapiattisti e complottisti* mentre, in cuor nostro, sappiamo anche noi che dovremmo essere un po' più *ambientalisti*.

La nostra vita è piena di *tribes* che nel tempo hanno conservato il loro potere e la loro magia.

Oggi, le aziende che riescono a interagire e integrarsi con loro, o addirittura a crearne di nuove, grazie ai loro brand, sono quelle in grado di crescere più velocemente e in maniera più duratura.

Ho raccolto le testimonianze di una psicoanalista, di un regista, di alcuni CEO, General Manager e Marketing Director, per portarvi con me in questo viaggio all'interno di alcune tribù che popolano il nostro Paese. Con me c'è anche Luca Bertocci, fedele amico e compagno di viaggio, che con la sua esperienza alcune tematiche con dei casi che mostrano come passare dalla teoria alla pratica.

Preparatevi a scoprire come il *mindset* tribale stia diventando la chiave del successo del marketing contemporaneo. Unitevi a noi in questo viaggio all'interno delle comunità che popolano il nostro mondo e scoprirete come costruire relazioni durature con i vostri clienti attraverso le tribes.

È tutto pronto, prepariamo gli archi e le frecce, insieme impareremo a centrare i cuori delle persone con i nostri brand. ■

The Tinder Swindler

(Felicity Morris, Regno Unito 2022)

Simon Leviev, figlio del magnate russo-israeliano Lev, re del commercio dei diamanti, è un ricchissimo playboy giramondo: viaggia per l'Europa, si sposta su jet privati, ostenta la sua favolosa ricchezza e seduce donne su donne attraverso la nota app di Tinder: una vita perfetta per lui e anche per le sue numerose fidanzate (per loro, almeno per il tempo in cui restano tali).

C'è solo un problema: Simon Leviev non esiste. Il suo vero nome è Shimon Hayut, viene sì da Israele ma non ha alcun legame di parentela con il magnate russo, non è affatto ricchissimo e i soldi che ostenta, tra regali sontuosi alle sue conquiste e jet privati, sono quelli che si è fatto «prestare» dai suoi amori precedenti. Le sue prede.

Su Tinder, Shimon Hayut è un truffatore. Ha convinto decine di donne, dopo averle sedotte, che per problemi legati alla sua sicurezza personale da rampollo di plutocrate aveva i conti temporaneamente bloccati e nemici pronti ad approfittarne, e si è fatto prestare da loro (anche facendole indebitare) somme considerevoli, che naturalmente non hanno più rivisto. Erano innamorate di Simon Leviev, del resto. Erano innamorate della sua maschera.

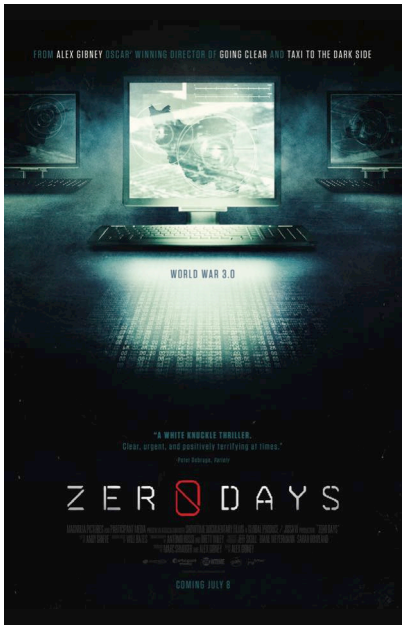
Questa è la trama di *The Tinder Swindler,* documentario britannico Netflix del 2022 che vede alla regia Felicity Morris e segue l'intera, incredibile vicenda del truffatore simbolo del XXI secolo: un uomo che rievoca in parte il mito intramontabile di Casanova, reinterpretandolo in chiave moderna grazie alle attualissime app di incontri e a un mondo eternamente connesso via web e aggiungendoci di suo l'indubbio tornaconto economico delle sue truffe abbastanza crudeli. Secondo le stime, sono stati circa dieci milioni di dollari i proventi delle sue poco edificanti imprese "romantiche".

Messaggi d'amore, richieste di aiuto, immagini di minacce nei suoi confronti con un coltello da parte dei suoi misteriosi "nemici", prestiti ingenti e poi bonifici falsi per fingere con le vittime di aver onorato il debito: il tutto condito da vita di lusso in prima classe. Non si è fatto mancare nulla Shimon Hayut, il truffatore di Tinder, e il

documentario non tralascia alcun dettaglio: soprattutto non manca di insegnare a non fidarsi mai. Nel web non si può mai sapere davvero chi ci sia dall'altra parte. ■

Zero Days

(Alex Gibney, USA 2016)



Il documentario di Gibney racconta al grande pubblico i segreti che si celano dietro la diffusione del virus informatico Stuxnet, creato dal lavoro congiunto delle intelligence americana e israeliana allo scopo di sabotare nel 2010 una centrale nucleare iraniana e poi, dopo che i suoi stessi creatori ne hanno perso il controllo, diffusosi nelle reti di tutto il mondo in maniera incontrollabile, provocando danni ingenti. Una storia di cui per molto tempo siamo stati all'oscuro viene così finalmente divulgata, facendoci comprendere come persino un'attività umana tra le più antiche, la guerra, abbia ormai un risvolto tecnologico tale da trasferirsi dai campi di battaglia ai microchip dei computer e alle reti informatiche.

Scopriamo così, attraverso il lavoro del documentarista, che dietro la creazione di uno dei virus più dannosi della storia tecnologica ci sono i servizi segreti di due Paesi capofila dell'Occidente considerato "buono", che però, come i servizi segreti di tutto il mondo, non si sono fatti scrupolo di ingenerare danni in una centrale nucleare "nemica" (con tutto ciò che una simile condotta può comportare, anche se non ci fossero state ulteriori conseguenze); né si sono dati pena di prevedere cosa sarebbe potuto succedere se, come poi si è probabilmente verificato, un innocente ingegnere nucleare iraniano avesse portato fuori dalla centrale il virus, annidato in una chiavetta USB e pronto a diffondersi da lì praticamente ovunque.

Il documentario di Gibney narra, attraverso ricostruzioni, interviste e testimonianze, questa storia controversa. Probabilmente non sarà né la prima né l'ultima che ci toccherà di conoscere (magari ancora con anni di ritardo), oggi che l'umanità è così immersa e così dipendente dalle sue reti informatiche, e questi veri e propri atti di guerra saranno, se non lo sono già, la prassi del futuro prossimo venturo. ■

Una pubblicazione

web for business
swiss webacademy

Redazione:

Laurent Chrzanovski e Romulus Maier (†)

(tutte le edizioni)

Per l'edizione italiana:

Nicola Sotira, Elena Agresti

ISSN 2559 - 1797

ISSN-L 2559 - 1797

Indirizzi:

info@cybertrends.it

Şcoala de Înot nr.18, 550005,

Sibiu, Romania

www.swissacademy.eu

www.cybertrends.it

CYBERSECURITY TRENDS

SOSTIENI IL GIORNALISMO INDIPENDENTE

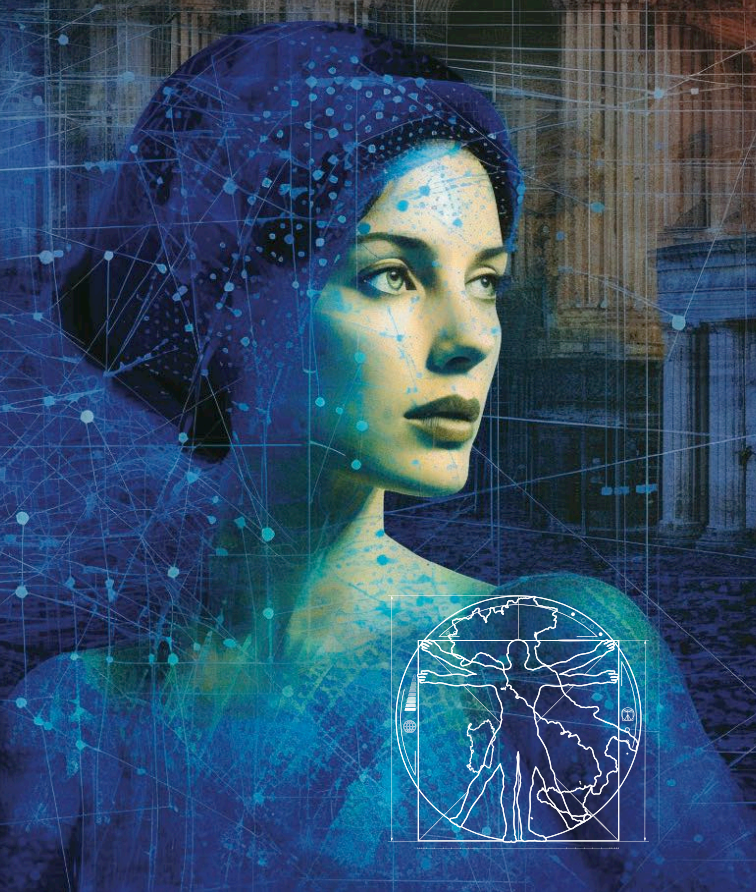
DONA ORA

Il tuo contributo è prezioso 💎
www.cybertrends.it/donate/

DIGITAL ITALY SUMMIT 2023

COSTRUIRE LA NAZIONE DIGITALE

14–16 NOVEMBRE ROMA



Piazza della Pilotta 4, Roma

Il più autorevole evento in cui Imprese, Governo, Pubblica Amministrazione, Università e Centri di Ricerca si confrontano sulle strategie per accelerare i processi di innovazione del nostro Paese.

INQUADRA IL QR CODE
PER CONSULTARE L'AGENDA
E ISCRIVERTI GRATUITAMENTE
ALL'EVENTO

PER INFORMAZIONI:

Alessandra Mosconi
alessandra.mosconi@theinnovationgroup.it

The Innovation Group Srl
Via Palermo 5, 20121 Milano

The Innovation Group
Innovating business and organizations through ICT