ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ANNO 1
Numero 2
2020

CYBER Magazine

L'Italia continua a essere **bersagliata** da **malware** e **ransomware**

Cybersecurity, gestione integrata del rischio **ICT** **e impatti sul business.**

Riconoscimento Facciale e GDPR: considerazioni sulle linee guida del comitato **europeo**

Indice

Paola
Generali

L'editoriale del Presidente Assintel

"Siamo a 9 mesi dall'inizio della Pandemia, che ha avuto il merito – almeno uno – di accelerare il Digitale come mai era accaduto prima.

Da un giorno all'altro, tanto le organizzazioni quanto i singoli si sono trovati costretti ad un uso estensivo del digitale, dallo smart working al social commerce, dalla didattica a distanza agli eventi, per garantire una continuità che il Covid stava minando. Il mondo si è riorganizzato in fretta, e come sempre accade quando si è in urgenza non si pensa ad alcuni aspetti importanti come alla Cybersecurity ma esclusivamente all'operatività.

Il Digitale è una prateria sconfinata, dalle mille opportunità ma anche dai mille rischi, come ben sa chi si occupa di cybersecurity: l'uso imponente del digitale ha fatto sì e farà sì, che i possibili oggetti di "attacco" soprattutto in ambito e-commerce, servizi SaaS, App e tutti i servizi esposti via web stiano "deliziando" tutti coloro i quali vivono per violare tali sistemi per appropriarsi di dati che poi vengono rivenduti, oppure per minare i brand e per finire per dare luogo a vere e proprie azioni criminali.

La sicurezza va progettata, pianificata, e ancor prima va percepita e capita come bisogno "essenziale", un "sine qua non". È un'operazione prima di tutto culturale, che passa per le organizzazioni, gli imprenditori, i cittadini, ma anche e soprattutto dai vertici della Pubblica Amministrazione e dei suoi Enti, che hanno un ruolo decisivo in questa catena. La Commissione Europea infatti ritiene che gli investimenti futuri per il Sistema Paese Europa dovranno vertere su questi argomenti:

- Cybersecurity
- AI
- Potenziamento di Calcolo e quindi Creazione di Super Computer

La motivazione della scelta di queste 3 tematiche è evidente e molto chiara: per potenziare l'AI sono necessari un numero massimo di dati che la medesima deve utilizzare; per elaborarli, l'AI ha necessità di una rilevante potenza di calcolo che può essere soddisfatta grazie ai Super Computer; e per finire, poiché tutto questo implica un trattamento di una quantità massiva di dati, è necessario elevare la protezione delle infrastrutture informatiche come anche dei software che li elaborano. Ecco perché la Cybersecurity è una "Condicio sine qua non".
Le aziende di cybersecurity sono quindi un anello fondamentale e strategico di questa catena, con una mission tecnologica primaria che corre in parallelo al ruolo culturale. Buona lettura"

Il Ransomware prende le scorciatoie

di ***Pierguido Iezzi***

Una delle parti più critiche – e più difficili se guardiamo la vicenda dalla parte del Criminal Hacker – nella catena d'infezione di un Ransomware è proprio la prima fase; quella che permette loro di "entrare" nelle reti dei loro target.

Magari si tratta di cercare porte RDP esposte in Rete, magari si tratta di campagne di phishing. Attività che comunque prevedono un certo "effort" e una certa spesa da parte dei gruppi dediti al ransomware.

E non illudiamoci che i Criminal Hacking non operino sotto uno strettissimo regime di "costo-beneficio", non dissimile a quello che utilizzano tutte le attività "in chiaro".
Per questo la notizia che gli accessi diretti ai network sono adesso in vendita nel Dark Web – per cifre che a volte sono di appena 300$ - non dovrebbe farci dormire sogni tranquilli.

Soprattutto perché molti gruppi tra i più noti come Maze e NetWalker potrebbero essere lì pronti in attesa di comprare.
Togliere la parte di "infiltration" nella catena di attacco del ransomware, da ancora più tempo ai gruppi di Criminal Hacker per perfezionare la loro persistenza nel sistema e di muoversi lateralmente.

L'accesso ai network venduto come "item" separato è solo divenuto recentemente una "hot comodity" anche se a dire la verità le prime tracce di questo fenomeno erano state tracciate per la prima volta nel dark web nel 2017.

I "venditori" in questo caso, ça va sans dir, sono a loro volta Criminal Hacker che hanno expoitato una vulnerabilità per ottenere accesso completo ai network di una serie di target – magari senza particolari obiettivi in mente.

Fatto questo, invece che passare alla fase di attacco si fermano e mettono in vendita quanto ottenuto sul Dark Web con il prezzo basato sul fatturato e la dimensione dell'azienda da loro colpita.

"L'annuncio" di vendita solitamente è ben dettagliato con tutte le informazioni della vittima: dal tipo di industry in cui opera (per esempio banking o manifatturiero) passando per il tipo di accesso ottenuto sfruttando la vulnerabilità (potrebbero essere stati in grado di "bucare una VPN, un RDP esposto…), fino a dettagli come il numero di macchine, la nazione e molto altro ancora…

I numeri del fenomeno

All'inizio di settembre, per meglio contestualizzare il fenomeno, un gruppo di ricercatori ha "scandagliato" il Dark e Deep Web alla ricerca dei reseller di accessi alle Reti.
Al tempo della ricerca erano riusciti a trovarne circa 25, ma con la precisazione che molti altri stavano entrando sul mercato.

Curiosamente o forse in maniera preoccupante, tutti questi threat actors operavano negli stessi forum e ambienti solitamente popolati dai "big hitters" del Ransomware come Maze, Avaddon, Sodiniokibi, NetWalker e molti altri. Certo, non è semplicissimo risalire - durante la fase forense di un'investigazione post incident – al se e quando gli accessi che hanno permesso ai Criminal Hacker di colpire arrivano da queste vendite sul Dark Web. L'unica certezza è che questi sono in vendita e che i gruppi ransomware stanno iniziando a comprare in massa. Tornando alla "merce" in vendita, al momento il "top seller" rimane l'accesso a reti RDP compromesse, anche se ultimamente sono in forte crescita accessi a VPN come Pulse e Citrix.
Non a caso sono servizi che hanno visto un'impennata nel loro utilizzo negli ultimi mesi di Pandemia.

Zero day

Come se non bastasse, adesso queste offerte vengono accoppiate anche a nuovi zero-day – invece che essere vendute separatamente.
Per esempio, secondo i ricercatori, un gruppo di Criminal Hacker noto come Frankknox ha messo in vendita uno Zero day per un noto client di posta a circa 250mila dollari.

Ma, sorprendentemente, ha poi deciso di vendere la sua offerta e iniziare a vedere gli accessi separati a circa 36 aziende differenti ottenuti grazie allo sfruttamento di questi zero day.

Una mossa che ha fruttato al Criminal Hacker tra i 2mila e i 20mila dollari per accesso venduto (il gruppo ha dichiarato di aver venduto – ad oggi – 11 di questi accessi).

Come difendersi

Ovviamente la prima linea di difesa deve essere un perimetro di difesa resiliente e – vista la loro particolare incidenza nell'elenco della mercanzia in "vendita" – cercare di eliminare o limitare il più possibile l'utilizzo di protocolli RDP all'interno del perimetro aziendale. In particolare se non si utilizzano in proprio è imperativo disattivarle e chiudere la porta 3389.
Certo, se proprio non ci sono alternative, la loro corretta configurazione deve essere il primo punto d'attenzione. Ecco alcune misure e best practice per rendere sicuro il protocollo RDP:

- utilizzare password forti;
- rendere disponibile l'RDP solo attraverso una VPN aziendale;
- utilizzare l'autenticazione a livello di rete (Network Level Authentication);
- se possibile, abilitare l'autenticazione a due fattori;

Si dovrebbero anche abilitare i criteri di blocco degli account per intercettare eventuali attacchi di forza bruta, poiché questi bloccheranno temporaneamente i login sugli account dopo un certo numero di tentativi falliti.

L'abilitazione delle politiche di revisione degli account può allo stesso modo aiutare a prevenire tali attacchi, permettendo agli amministratori di vedere quali account mostrano ripetutamente errori di login e sono quindi potenzialmente oggetto di attacco.Certo, se il network è già stato "bucato", queste potrebbero essere solo misure "pro futuro". In questo caso però potrebbe esserci un delta di tempo cruciale in cui intercettare informazioni riguardanti il nostro network, prima che queste vengano acquistate e soprattutto riuscendo a rimediare alla vulnerabilità.
Qui, giocano un ruolo fondamentale i servizi di Threat Intelligence, in grado di fornire quell'Actionable intelligence necessaria per prevenire e anticipare devastanti attacchi ransomware, monitorando l'attività sul dark web che menziona la nostra azienda…
Non abbassiamo la guardia!


Credit image: Unsplash

L’Italia continua a essere bersagliata da malware e ransomware

Trend Micro presenta il report semestrale delle minacce. Il nostro Paese è l’ottavo al mondo più colpito dai malware e l’undicesimo (secondo in Europa) per quanto riguarda gli attacchi ransomware

*di **Trend Micro***

I malware e i ransomware continuano ad abbattersi sull’Italia, che risulta ai primi posti delle classifiche mondiali per questo genere di attacchi.

Il nostro Paese è infatti, al mondo, l’ottavo più colpito dai malware e l’undicesimo (secondo in Europa) per quanto riguarda le incursioni ransomware.

Il dato emerge da “Securing the Pandemic-Disrupted Workplace”, il report sulle minacce informatiche del primo semestre 2020, a cura di Trend Micro Research.

Le minacce a tema pandemia imperversano in tutto il mondo.

A livello globale il tema più utilizzato dai cybercriminali è stato quello legato alla pandemia. Trend Micro ha infatti bloccato 8,8 milioni di minacce in sei mesi, di cui il 92% via e-mail.

Tra le minacce più rilevate le truffe Business Email Compromise (BEC), che hanno cercato di capitalizzare al meglio le pratiche di smart working introdotte negli ultimi mesi e i ransomware, che hanno visto le nuove famiglie crescere del 45%.

Anche le vulnerabilità sono aumentate e la Trend Micro Zero Day Initiative (ZDI) ha pubblicato un totale di 786 avvisi, ovvero il 74% in più rispetto alla seconda metà del 2019, e con un particolare focus sui sistemi di controllo industriali.

Italia: i numeri della prima metà del 2020

- **Malware –** Il numero totale di malware intercettati in Italia nella prima metà del 2020 è di 6.955.764. L’Italia è l’ottavo Paese più colpito al mondo
- **Ransomware –** Nel primo semestre 2020 l’Italia è l’undicesimo Paese più colpito al mondo con una percentuale di attacchi del’1,33%. In Europa è seconda solo alla Germania con il 18,67% di attacchi subiti
- **Le minacce arrivate via mail** sono state 151.884.242, tra cui 107.684 erano messaggi spam a tema COVID
- **Gli URL maligni** visitati sono stati 6.064.101
- Il numero di **app maligne** scaricate nella prima metà del 2020 è di 127.690
- Nella prima metà del 2020 sono stati 2.907 i malware di **online banking** che hanno colpito l’Italia

In tutto il mondo, Trend Micro ha bloccato nel primo semestre un totale di 28 miliardi di minacce (27.823.212.959), quasi un miliardo in più rispetto allo stesso periodo dell’anno precedente. Il 93% di queste minacce è arrivato via mail.

SECURING THE PANDEMIC-DISRUPTED WORKPLACE

H1 2020 CYBERSECURITY REPORT

Nei primi sei mesi dell'anno, il tema più utilizzato dai cybercriminali è stato quello legato alla pandemia. Trend Micro ha infatti bloccato in tutto il mondo **8,8 milioni di minacce**, di cui il 92% via e-mail.

TREND MICRO | research

Cyber Security, gestione integrata del rischio ICT e impatti sul business

Tecnologie digitali, processi aziendali e Cyber security

di ***Carlo Guastone***

La pervasività dell'informatica nella società e nelle aziende è un fenomeno sotto gli occhi di tutti, per gli impatti sulle aziende e sulla vita degli individui, tematica che non può non essere all'attenzione del management e del Vertice aziendale. Management e vertice aziendale non possono chiamarsi fuori , devono indirizzare le scelte aziendali non solo in domini tradizionali come l'automazione di base dei processi gestionali (i sistemi ERP, per fare un esempio), o l'automazione di fabbrica, ma anche sulle tematiche emergenti, dalla digitalizzazione dei processi, ai Sistemi IOT, all'Intelligenza artificiale, che avranno sicuramente un impatto sul sistema competitivo che l'azienda dovrà fronteggiare.

Il tutto in un contesto nel quale cresce l'utilizzo dei social anche per finalità di business e il valore economico delle informazioni assume rilevanza crescente per gestire le opportunità e le dinamiche di mercato.

Le aziende si stanno progressivamente orientando verso due tendenze ineluttabili: i servizi Cloud e l'adozione delle tecnologie abilitanti della quarta rivoluzione industriale, fra le quali il Web 4.0, l'IoT (Internet delle cose) e l'intelligenza artificiale, che presentano impatti di sicurezza per le aziende e per gli individui. In questo contesto cresce l'attualità della Cybersecurity per fronteggiare gli attacchi che provengono dalla rete, fenomeno sempre più ripreso dai mass media, unitamente alla diffusione dei Social Network e dei dispositivi mobili, fonte non secondaria di minacce alla sicurezza delle informazioni aziendali e degli individui.

Il Rischio integrato dei servizi ICT

La Cybersecurity nasce molti anni dopo rispetto all'Information security: la Norma ISO 27001 (Sistema di gestione Sicurezza delle informazioni) è stata infatti pubblicata nel 2005 (facendo seguito ad una Norma BSI pubblicata 10 anni prima), e già considerava la sicurezza delle reti di telecomunicazioni. La prima Norma ISO dedicata alla Cybersecurity è del 2012 (norma ISO/IEC 27032), e, per semplificare, si può considerarla una Linea guida che delinea l'impatto sull'Information security dagli attacchi provenienti dal cyberspazio (in pratica dal mondo Internet).

I rischi di information security e cybersecurity presentano molte aree di sovrapposizione ed è opportuno considerarli in logica integrata (come suggerisce la Norma ISO 27001), tenendo presente che la sicurezza di funzionamento dell'azienda dipende non solo dall'efficacia delle misure di Information security e cybersecurity, ma anche dalle soluzioni aziendali di Business Continuity che ne assicurano la continuità operativa anche a fronte di disastri e gravi disservizi. La dipendenza del business dall'efficienza e dalla qualità dei servizi ICT aziendali (interni o terziarizzati) è un'altra componente fondamentale da considerare, unitamente alla compliance a leggi e regolamenti, con particolare riferimento al Regolamento Europeo in materia di protezione dati personali (GDPR) per la rilevanza che la sicurezza ICT ha per i trattamenti di dati personali. L'idea di svolgere valutazioni di rischio considerando gli ambiti citati in logica integrata è favorita da due fenomeni convergenti: il vantaggio di poter presentare al Vertice aziendale un risultato completo che consideri le principali minacce che possono determinare criticità nei servizi ICT aziendali e nei processi di business, e la presenza di Norme ISO che rappresentano best practices cui l'azienda può fare riferimento.

Ci riferiamo alla Norme ISO 27001:2013 (Sistema di gestione sicurezza delle informazioni), ISO 20000:2019 (Sistema di gestione IT Service management), ISO 22301: 2019 (Sistema di gestione business continuity), e ISO 27701: 2020 (Sistema di gestione sicurezza dei dati personali). Nell'ambito del risk assessment integrato è prevista una specifica focalizzazione sulla Application security e sulla Cybersecurity, attraverso lo svolgimento di Vulnerability Assessment e Penetration Test sulle infrastrutture e sulle applicazioni esposte al web. Inoltre si potrà valutare l'adeguatezza delle soluzioni di mitigazione dei più significativi rischi di cybersecurity , come i cosiddetti APT- Advanced Permanent Threat, e DDoS-Distribuited Denial of Service, etc.), valutando anche l'opportunità di adottare soluzioni identificate come SOC-Security Operation Center, aziendali o gestite in outsourcing, per il monitoraggio degli eventi e degli attacchi di sicurezza.

Per quanto relativo all'IT service management si prevede di svolgere

una gap analysis sulla qualità dei servizi ICT aziendali focalizzando l'attenzione sulla corretta gestione dei processi IT che costituiscono un "servizio" verso clienti e processi aziendali, dal design e realizzazione delle applicazioni informatiche, alla loro gestione operativa, al change management, alle relazioni con i fornitori, etc. L'analisi relativa alla Business Continuity considera non solo le componenti ICT, ma anche il personale, gli impianti produttivi, le sedi aziendali, i fornitori, etc. Le valutazione dei rischi di non ottemperanza a GDPR può essere svolta tramite la Norma ISO 27701 che identifica i principali adempimenti di natura organizzativa, documentale, e tecnologica richiesti dal Regolamento. Nell'articolo non abbiamo fatto riferimento alle metodologie da adottare per la valutazione del rischio né a possibili strumenti di supporto. La metodologia generale di riferimento è la ISO 31000, da personalizzare alle diverse aree di rischio esaminate, considerando le minacce potenziali nei diversi ambiti (vulnerabilità dei controlli di Information security, carenza di misure di data protection per GDPR, assenza o carenze dei Piani di Business Continuity, adeguatezza dei processi di Service management). Il calcolo del rischio è svolto con valutazioni "semiquantitative" assegnando valori convenzionali a probabilità di manifestazione delle minacce, impatti e presenza di contromisure preventive. Al riguardo si sta registrando una recentissima tendenza di matrice USA, riportata da ISACA (Associazione internazionale di IT Governance) nel recente aggiornamento della pubblicazione "Risk IT Practioneer guide". LA pubblicazione suggerisce di utilizzare per il calcolo del rischio anche metodologie statistiche per la valorizzazione economica del rischio IT, facendo riferimento alla metodologia FAIR (Factor Analysis of information Risk) per raccolta di informazioni e al Metodo statistico Montecarlo per svolgere le simulazioni di rischio.

In sintesi la gestione integrata del rischio potrà favorire una valutazione oggettiva e completa della situazione aziendale rilevata in termini di sicurezza di funzionamento, fornendo anche utili informazioni al management relative ai progetti di innovazione in corso di realizzazione o pianificati.

Credit image: Unsplash

Riconoscimento Facciale e GDPR: considerazioni sulle linee guida del comitato europeo

di ***Federico Gabbricci***

Nell'ambito dei sistemi biometrici stanno acquisendo sempre maggior rilievo le tecniche di riconoscimento facciale ovverosia quelle tecnologie che permettono l'identificazione di un soggetto, mediante l'acquisizione e l'analisi delle caratteristiche del suo volto e la comparazione di queste ultime con una serie di modelli memorizzati in una banca dati.
Il riconoscimento facciale ha suscitato un forte interesse sia nel settore privato (è stato ad esempio utilizzato a fini pubblicitari e di profilazione della clientela al fine di individuare le preferenze dei consumatori e sottoporgli pubblicità mirate) che nel settore pubblico (alcuni Stati con l'aumentare dell'accuratezza di tali sistemi hanno fornito in dotazione alle loro forze di polizia sistemi di riconoscimento).
Tuttavia, pur prospettandosi nei confronti del riconoscimento facciale le più disparate applicazioni vi è da considerare l'impatto che esso possa avere sui diritti e le libertà dei cittadini soprattutto nel caso in cui il suo utilizzo non venga regolamentato.
La normativa comunitaria disciplina l'utilizzo di tale tecnologia sia da parte delle aziende che delle autorità statali, con particolare riguardo alla tutela dei dati personali che questi sistemi raccolgono. In particolare, sono da prendere in considerazione due atti:

- Il Regolamento 2016/679, General Data Protection Regulation ("GDPR");
- La Direttiva (UE) 2016/680 disciplinante il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali.

L'articolo 9 del GDPR pone espressamente delle limitazioni alla raccolta dei dati biometrici venendo questi espressamente ricompresi nella categoria dei dati personali particolari la quale presenta una tutela rafforzata, ben sintetizzata nel tenore del Considerando .51 del Regolamento:" Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di

Credit image: Unsplash

cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali".

Recentemente il Comitato europeo per la protezione dei dati il 29/01/2020 ha avuto modo di affrontare e approfondire la tematica in occasione dell'adozione delle "Guidelines on processing of personal data through video devices" nelle quali vengono fornite indicazioni e chiarimenti in merito all'applicazione del GDPR relativamente al trattamento dei dati personali raccolti tramite dispositivi video. Il capitolo 5 delle linee guida è infatti dedicato alla raccolta, tramite telecamere, dei dati biometrici compiuta al fine di identificare in maniera univoca una persona, attività che, per il comitato, "comporta elevati rischi per i diritti degli interessati".

In considerazione di tali rischi è fondamentale che l'utilizzo di tale tecnologia avvenga da un lato nel pieno rispetto dei principi generali sanciti dal GDPR (liceità, necessarietà, proporzionalità e minimizzazione dei dati) e dall'altro lato che i titolari del trattamento che volessero ricorrere a tali strumenti compiano sempre una valutazione d'impatto sui diritti e sulle libertà fondamentali considerando al contempo se il legittimo scopo del trattamento possa essere raggiunto con mezzi meno intrusivi.

Le linee guida dedicano poi una attenzione particolare all'utilizzo dei sistemi biometrici in luoghi aperti al pubblico, evidenziando il rischio che, in tali spazi, possano essere acquisiti i dati non solo di chi rientri in una delle esenzioni previste dall'articolo 9 ma anche di chi non vi sia ricompreso configurando così una acquisizione illegale dei dati di questi ultimi. Soffermandosi in particolare sull'esenzione del consenso esplicito dell'interessato (che è certamente la più utilizzata) le linee guida sottolineano come in tali ambienti non controllati sia importante segnalare e separare le aree adibite alle riprese del sistema biometrico[1]. E ancora, dal momento che il consenso non deve essere coartato bensì frutto della libera scelta del soggetto, il Comitato evidenzia come, qualora tale tecnologia venisse utilizzata per garantire l'accesso alle persone in determinati luoghi, il titolare dovrà sempre garantire modalità alternative di accesso che non prevedano il ricorso a sistemi biometrici.

Ultimo aspetto affrontato nelle guidelines sulla tematica riguarda le modalità di trattamento e conservazione dei dati biometrici al fine di minimizzare i rischi: i titolari del trattamento dovranno, conformemente al principio della minimizzazione dei dati garantire che i dati estratti da un'immagine digitale, per costruire il modello, non siano eccedenti e contengano soltanto le informazioni necessarie per la finalità specificata, evitando così ogni possibile trattamento ulteriore. Inoltre, è necessario che vengano adottate misure per garantire che i modelli non possano essere trasferiti tra diversi sistemi biometrici.

Infine, andranno prese tutte le precauzioni necessarie al fine di preservare la disponibilità, l'integrità e la riservatezza dei dati trattati; specificatamente si impone al titolare del trattamento di adottare le seguenti misure:

- trasmettere e conservare i dati in forma compartimentalizzata
- conservare modelli biometrici, dati grezzi[2] e dati di identità in banche dati distinte,
- cifrare i dati biometrici avendo cura di definire una politica per la cifratura e la gestione delle chiavi.
- prevedere misure organizzative e tecnica per il rilevamento delle frodi,
- associare un codice di integrità ai dati (ad esempio, firma o codice hash)
- vietare qualsiasi accesso esterno ai dati biometrici.

Conclusivamente, dall'analisi congiunta delle linee guida e del GDPR emerge una ampia tutela per i cittadini in materia di dati biometrici acquisiti dalle aziende, garantiti da un lato dalla tutela rafforzata dell'articolo 9 del GDPR e dall'altro lato dalla procedura di acquisizione e gestione dei dati, specificata nelle linee guida, che impone l'origine ai titolari di verificare la necessarietà del ricorso a tale tecnologia per perseguire le finalità del trattamento nonché di trattare solo i dati necessari e conservarli tramite misure adeguate a scongiurare il verificarsi di un data breach. Solo il tempo ci permetterà di vedere quanto tali misure saranno efficaci nel tutelare il nostro diritto alla riservatezza; rimane comunque sempre valida una raccomandazione: non disponete con leggerezza dei vostri dati personali, soprattutto di quelli sensibili, ma abbiate sempre la consapevolezza che state per dare accesso a terzi ad uno dei vostri diritti della personalità.

[1] Immaginiamo ad esempio che una società aeroportuale decida di introdurre la possibilità per i passeggeri, che lo vogliano, di verificare la loro identità attraverso un sistema di riconoscimento facciale; sarà necessario che la società predisponga posti di controllo separati e segnalati per i passeggeri che abbiano prestato il loro consenso a tale modalità così da evitare che vengano acquisiti i dati biometrici di persone che non desiderino ricorrere a tale modalità di verifica.

[2] Tali sono da intendere quei dati quali ad esempio le immagini del volto, i segnali vocali, il portamento dell'individuo dalla cui analisi il sistema elabora il modello biometrico. La costituzione di database contenenti questi dati potrebbe rappresentare una minaccia addirittura maggiore ai diritti degli individui essendo questi molto più facili da leggere piuttosto che un modello biometrico del quale non si conoscono i dettagli della sua programmazione. Per tale motivo le guidelines affermano che i titolari del trattamento qualora non esista più una base giuridica per trattare di tali dati debbano cancellarli. Ciò garantisce una maggiore tutela ai soggetti che prestino il loro consenso all'utilizzo di questi sistemi dal momento che, il modello biometrico, una volta creato tramite l'acquisizione e l'elaborazione dei dati grezzi, non necessita più di questi ultimi permettendone la cancellazione.

Un Assessment sulla cyber security non deve essere una foto. Deve essere un video.

di ***Francesco Tieghi***

"*Un'immagine vale più di mille parole*". Quante volte avrete sentito questa espressione da alcuni attribuita a Mao Tse Tung, che però sembra l'abbia "clonata" dal saggio Confucio.

Per la Cyber Security, soprattutto OT, finora una delle prime attività consigliate da fare per mettere in sicurezza una rete industriale, di automazione di fabbrica o di controllo di processo, nell'industria come nelle utility era: "*fai una bella foto della tua rete, ove si possano vedere tutti i partecipanti, i nodi, dispositivi connessi, switch, router, ecc*."

Poi ci aspettiamo una bella relazione (di 1000 o più parole?) ove trovo indicati quelli che "*pensi*" possano essere i punti critici che sono stati trovati nella "*foto*".

Più di recente si è visto che la foto risulta utile, ma propone la situazione "*as-is*" nell'istante in cui si fa la foto. Come dire oggi: fai il tampone alla ricerca del Covid19, domani o dopo hai il risultato. Che molto probabilmente sarà negativo, ma è una "*foto*" di due giorni fa. Chissà se oggi sono ancora negativo…

Ora abbiamo disponibili strumenti molto più efficaci e risolutivi: tool che ci fanno un video in continuo e, se lasciati attivi, continuano a registrare per noi, per poi indicarci in "*real-time*", tutto quello che (molto probabilmente) non va sulla nostra rete di fabbrica. Mi sono permesso di mettere "*molto probabilmente*" tra parentesi, perché, nonostante tutti gli algoritmi di ML (Machine Learning) e di AI (Artificial Intelligence), falsi positivi/negativi sono ancora possibili: è qui che viene d'aiuto il nostro cervello per meglio identificare e capire cosa ci stanno indicando questi meravigliosi e potenti tool.

Proprio come uno strumento di video sorveglianza installato in un varco da monitorare: per ore, giorni, mesi inquadra tramite telecamere sempre gli stessi luoghi, persone, veicoli, passaggi, senza magari che succeda alcunché. Poi improvvisamente ci indica che stà succedendo "*qualcosa di strano*" che richiede la nostra attenzione. E lì vediamo se davvero è entrato qualcuno che non avrebbe dovuto aver accesso, cosa stà facendo e quali sono le contromisure da mettere in gioco.

Questi tool appositamente studiati e sviluppati per il mondo industriale OT ed IIoT, oggi sono già disponibili sul mercato a cifre accessibili, sono potenti e già riconoscono tanti "*comportamenti sospetti*", tracciano vulnerabilità, identificano minacce ed ogni giorno sono sempre più ricchi di informazioni, in continuo apprendimento tramite il Machine Learning, sia sulla vostra rete che su tante in giro per il mondo.

Se volete sapere se possono essere impiegate con efficacia anche sulla vostra rete di fabbrica più critica, provate a parlarcene: siamo sicuri che un nostro esperto di OT cyber Security può aiutarvi!

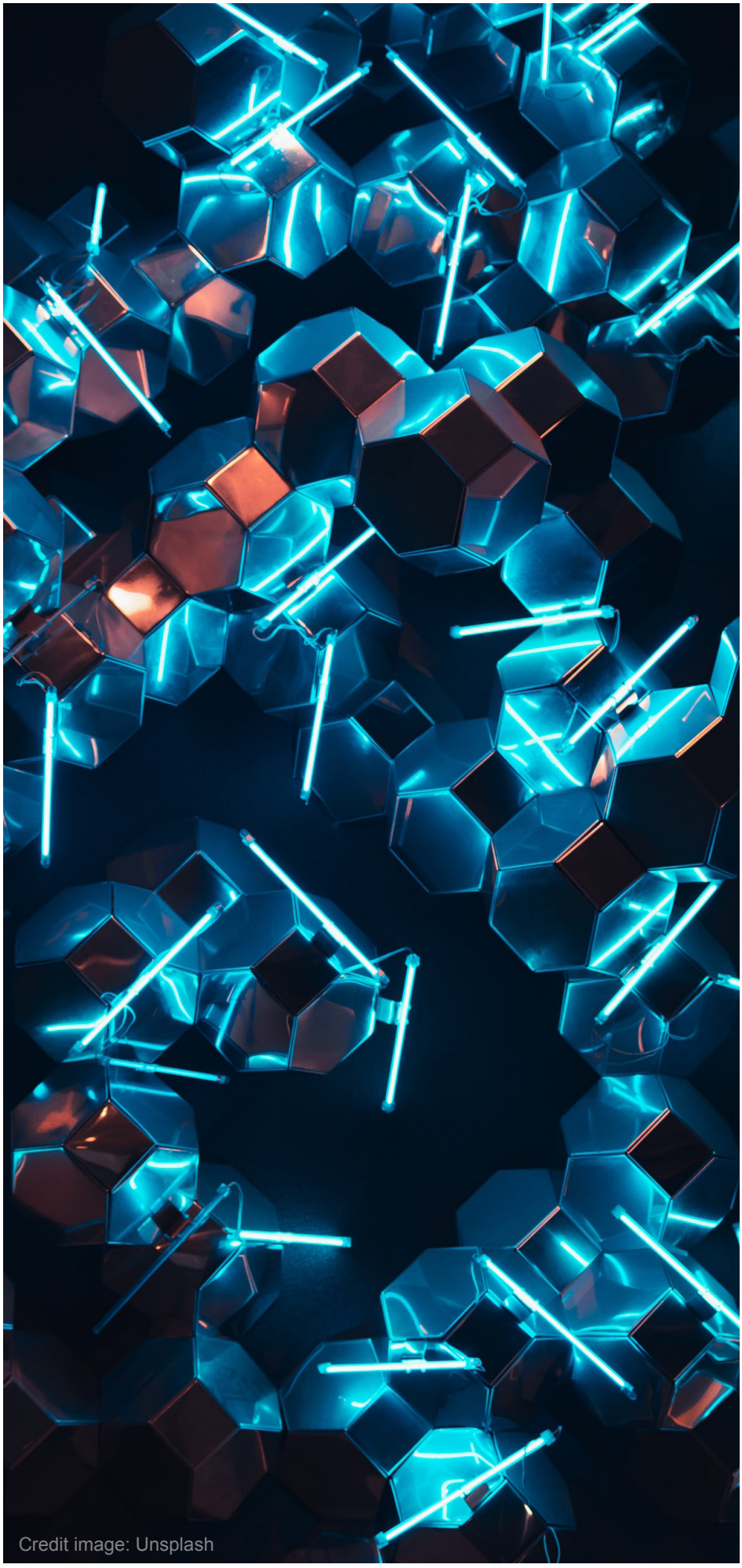
Tre immagini da ricordare per proteggere i tuoi impianti
Ultima Linea di Difesa, Anomaly Detection e Piano B.

Queste sono tre immagini che possono aiutarvi a rendere sicura la vostra architettura di rete industriale ed aumentare l'UPTIME delle vostre applicazioni di supervisione e controllo.

Cosa intendiamo dire? È presto detto!

- **ULTIMA LINEA DI DIFESA**: quando prendiamo un aereo veniamo controllati diverse volte per verificare la nostra identità (documento) e l'autorizzazione per accedere al gate (biglietto). Tuttavia quello che davvero ci separa dalla cabina di pilotaggio (e dunque dalla possibilità di prendere realmente il controllo) è una porta blindata. Per "fortificare" i tuoi sistemi di fabbrica servono dispositivi dedicati: non firewall generici dunque ma firewall industriali che siano adatti sia dal punto di vista hardware (per risiedere nei quadri a bordo macchina) che da quello software (protocolli di comunicazione e dinamiche sono spesso particolari)

- **FAI UN VIDEO DELLA TUA ARCHITETTURA**: Anomaly detection, ovvero…conosci davvero il tuo impianto? Per quanto gli operatori di linea e i supervisori siano esperti del processo, ci sono livelli che difficilmente possono essere monitorati costantemente: quali sono i pacchetti dati che possono viaggiare lecitamente tra la rete e le apparecchiature di campo? Quali sono le vulnerabilità presenti? Una volta


Credit image: Unsplash

stabilito il comportamento "tipo" dell'impianto, siamo in grado di rivelare anomalie e vulnerabilità? Non è sufficiente la "fotografia" per definire dunque la situazione generale della vostra architettura di fabbrica: è molto più indicato un monitoraggio prolungato che faccia emergere dinamiche lecite e non…più che una foto, un "video"

- **PIANO B**: quante volte hai sentito dire che "gli attaccanti saranno sempre più avanti dei difensori"? Non esistono sistemi sicuri al 100%, l'attacco (o incidente) informatico potrebbe nascondersi dietro ogni angolo: quello che fa la differenza è il tempo che ci mettono i tuoi impianti a tornare efficienti. Quante aziende manifatturiere o di processo hanno mai fatto una prova di ripartenza a seguito di downtime? Bisogna essere in grado di ripartire (almeno con le performance minime) nel minor tempo possibile, avendo dunque pensato ad una ridondanza fisica dei sistemi ed un adeguato versioning degli applicativi.

L'Europa dedica un mese intero alla Sicurezza Cyber

di ***Mario Pinna***

Ottobre è il mese che associamo ai raccolti, alle vendemmie e ai tramonti intrisi dei colori caldi dal celebre Vincent Van Gogh che rappresentava i viali ricoperti dal fogliame autunnale con le sue sfumature rossastre e dorate. Ma ottobre, a partire dal secolo scorso, si tinge anche delle tinte più macabre per i preparativi della festa più spaventosa dell'anno: Halloween. E proprio come conviene fare nella notte degli spiriti per non rimanere vittime di qualche simpatico scherzo, è importante mantenere un atteggiamento sempre vigile a ciò che ci circonda. Non a caso, o forse è solo una coincidenza, il mese di ottobre è da qualche anno il mese dedicato alla diffusione della consapevolezza riguardo la Sicurezza informatica per cittadini ed imprese nel mondo digitale. Essere consapevoli significa avere le capacità di comprendere, prevenire ed eventualmente gestire adeguatamente le trappole dei criminali digitali, non certamente simpatiche come il trick-or-treat (dolcetto o scherzetto) halloweeniano. Parte anche quest'anno, come ogni ottobre, la campagna dell'Unione Europea per sensibilizzare cittadini e aziende sulle minacce informatiche. Clusit, l'Associazione Italiana per la Sicurezza Informatica, richiama anche nel nostro Paese l'attenzione al corretto comportamento e alla gestione dei rischi associati al digitale, promuovendo eventi per approfondire le tematiche di cyber security, in collaborazione con esperti, centri di ricerca e università, e in accordo con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Ancor più in questo momento storico in cui l'emergenza sanitaria è alta e diverse attività continuano a migrare dallo spazio analogico a quello digitale, la tecnologia è ormai imprescindibile protagonista della vita quotidiana. Ricordando che per i cybercriminali chiunque può essere un potenziale bersaglio, dal funzionario governativo, alla celebrità, al CEO tecnologico, allo studente, fino alla semplice casalinga di paese, è sempre bene ricordare quanto sia importante proteggere le nostre vite digitali dalle

Credit image: Unsplash

minacce informatiche. Utilizziamo assistenti vocali per gestire le nostre attività quotidiane, gli smartphone sono collegati alle nostre telecamere di sicurezza e ai campanelli, nonché agli elettrodomestici intelligenti, controlliamo se la lavatrice ha terminato il suo ciclo o se la cena è stata riscaldata correttamente. Tutto ciò è disponibile con il semplice tocco di un dito sullo schermo del nostro smartphone. Ecco che anche la più blasonata azienda, seppur protetta da sistemi sofisticati e manager capaci, può essere bersaglio dei cybercriminali, l'unica discriminante - così come accade per quanto riguarda la sicurezza fisica - è solo quanto i black-hat siano disposti ad investire in termini di risorse (tecnologiche, finanziarie o temporali) per conquistare il loro target. La prevenzione riguarda tutti, in ogni ambito e per qualsiasi uso si faccia dei dati. Aumentando la consapevolezza collettiva di queste minacce e fragilità tecnologiche, organizzative o a volte anche psicologiche, le iniziative del Mese Europeo della Sicurezza Informatica mirano a garantire che tutti facciano la loro parte e contribuiscano a una maggiore sicurezza e protezione online. Perché' la sicurezza informatica non è solo tecnologia, ma è anche e soprattutto organizzazione nei processi e consapevolezza del personale.

Proprio in occasione del mese dedicato alla sicurezza informatica, abbiamo preparato un vademecum con qualche consiglio di "cyber igiene" per una gestione consapevole delle proprie attività online, al fine di prevenire data-breach, dispersione indebita di dati personali, truffe ed altre spiacevoli conseguenze.

- Mantenere sempre aggiornati i sistemi software e utilizzare un buon programma antivirus, badando bene a non utilizzare mai software non correttamente licenziati: possono essere un meraviglioso portale di accesso per i malintenzionati.

- Esaminare puntualmente gli indirizzi e-mail e le URL contenuti nelle e-mail in arrivo: i truffatori spesso imitano un sito o un indirizzo e-mail legittimo utilizzando una leggera variazione nell'ortografia per il loro fine criminale.

- Controllare o verificare le informazioni sull'account, nel caso in cui un messaggio di testo, un'e-mail o una telefonata non richiesti chiedono un aggiornamento: non bisogna mai seguire il collegamento fornito nel messaggio stesso oppure chiamare i numeri di telefono forniti nel messaggio. È bene collegarsi al sito web dell'azienda per accedere al proprio account oppure chiamare il numero di telefono indicato sul sito web ufficiale per vedere se qualcosa ha effettivamente bisogno della tua attenzione.

- Non aprire alcun allegato a meno che non si aspetti il file, il documento o la fattura e non si abbia verificato l'indirizzo e-mail del mittente.

- Esaminare tutte le richieste elettroniche di pagamento o trasferimento di fondi, soprattutto se ciò viene richiesto con un'azione immediata: chi attacca sa benissimo che la fretta non è un'ottima consigliera e fa leva sulle ansie del prossimo.

- Confermare le richieste di bonifici o pagamenti possibilmente di persona o anche per telefono come parte di un processo di autenticazione a due fattori. Non verificare queste richieste utilizzando il numero di telefono indicato nella richiesta di pagamento.

Se lo connetti, proteggilo.
#Takedigitalcare

Leak Source code di Windows XP: quali sono le conseguenze

*di **Riccardo Paglia***

Qualche settimana fa il mondo della Cyber Security e dell'IT è stato scosso dalla notizia che il source code di Windows XP era stato pubblicato per intero all'interno di un thread di 4chan.

I file, scaricabili tramite torrent, oltre a contenere la versione Service Pack 1 dell'OS, contenevano anche Windows Server 2003, MS DOS 3.30, MS DOS 6.0, Windows 2000, Windows CE 3, Windows CE 4, Windows CE 5, Windows Embedded 7, Windows Embedded CE, Windows NT 3.5 e Windows NT 4.

Era il 24 settembre.

Non sono passati che alcuni giorni e qualche researcher si era già cimentato nella compilazione dei file per creare una versione funzionante o quasi del sistema operativo.

L'importanza di un Source code

Ma cosa rende così pericoloso il fatto che il source code di un sistema operativo come windows sia ora pubblico.

Come dice il nome, il source code è la "sorgente" di un programma. Essenzialmente l'how to che definisce il flusso di esecuzione del programma stesso e la sua codifica software.
Logicamente avere tutto questo a disposizione e in chiaro può facilitare e non poco il lavoro dei Criminal Hacker in cerca di exploit e vulnerabilità.

Allo stesso modo facilita il modo la creazione di malware ad-hoc e molto più efficaci e devastanti.
Certo, potreste obiettare che Windows XP, con il suo end of life annunciato nel "lontano" 2014 non dovrebbe rappresentare un problema per nessuno.

La realtà è che a oggi nel nostro Paese rappresenta quasi l'1% degli OS Windows in utilizzo (0.91% secondo statcounter.com), il che rappresenta comunque una buona quantità di macchine.

Forse la giusta domanda da porsi è "che tipo di macchine ancora hanno installato Windows XP"? Difficile rispondere, ma esistono strumenti nel campo dell'Healthcare – come le macchine per fare la TAC – che non sono facilmente aggiornabili e che ancora usano la versione "embedded" di XP o ancora molti POS, bancomat, infrastrutture critiche… insomma quegli hardware "pesanti" che risultano molto difficili da aggiornare. Avere in mano l'arma del source code è una manna sia per chi si occupa di blackhat – in sostanza i Criminal Hacker – sia per chi si occupa di whitehat – quindi i security researcher e gli Ethical Hacker –.

Anche se il sistema operativo non è più supportato da anni, ci sono ancora moltissimi vantaggi nel curiosare al suo interno. Anzi, se la vulnerabilità che viene scoperta è comunque sufficientemente grave Microsoft non è estranea a rilasciare patch di sicurezza anche dopo l'end of life (com'è successo nel 2019 per una vulnerabilità RDP).

C'è anche il rischio che parte del codice utilizzato per Windows XP sia stato portato, come una sorta di eredità, anche nelle altre versioni successive dei sistemi operativi della casa di Seattle.

Chi lo sa; magari questo source code potrebbe essere la fonte di una vulnerabilità expoitabile anche su Windows 10.

Windows Server 2003, l'inosservato

Volendo fare un po' l'avvocato del diavolo, d'altra parte potremmo dire che, anche se la notizia è stata sicuramente da prima pagina, in fondo non c'è nulla di così sconvolgente visto e considerato che XP non è aggiornato da oltre 6 anni ed è già probabilmente pieno di vulnerabilità sfruttabili.

Anzi, se ancora sono presenti macchine che utilizzano windows all'interno del vostro perimetro dovreste mettere in cima alla lista delle priorità la loro dismissione immediata.

La parte più preoccupante della notizia, forse è una che è passata più in sordina.
All'interno degli oltre 40 gb di file che sono stati pubblicati, infatti, era presente anche il source code di Windows Server 2003.

Solo in italia, facendo una veloce ricerca con Shodan, sono presenti migliaia di Server che utilizzano questa versione dell'OS e sono esposti a Internet, quindi potenzialmente attaccabili.

Senza contare quelli non rilevabili immediatamente.

A differenza di un laptop o di un desktop aggiornare il sistema operativo di un server richiede un certo effort, motivo per cui ancora molte, troppe, organizzazioni ancora oggi utilizzano questa soluzione.

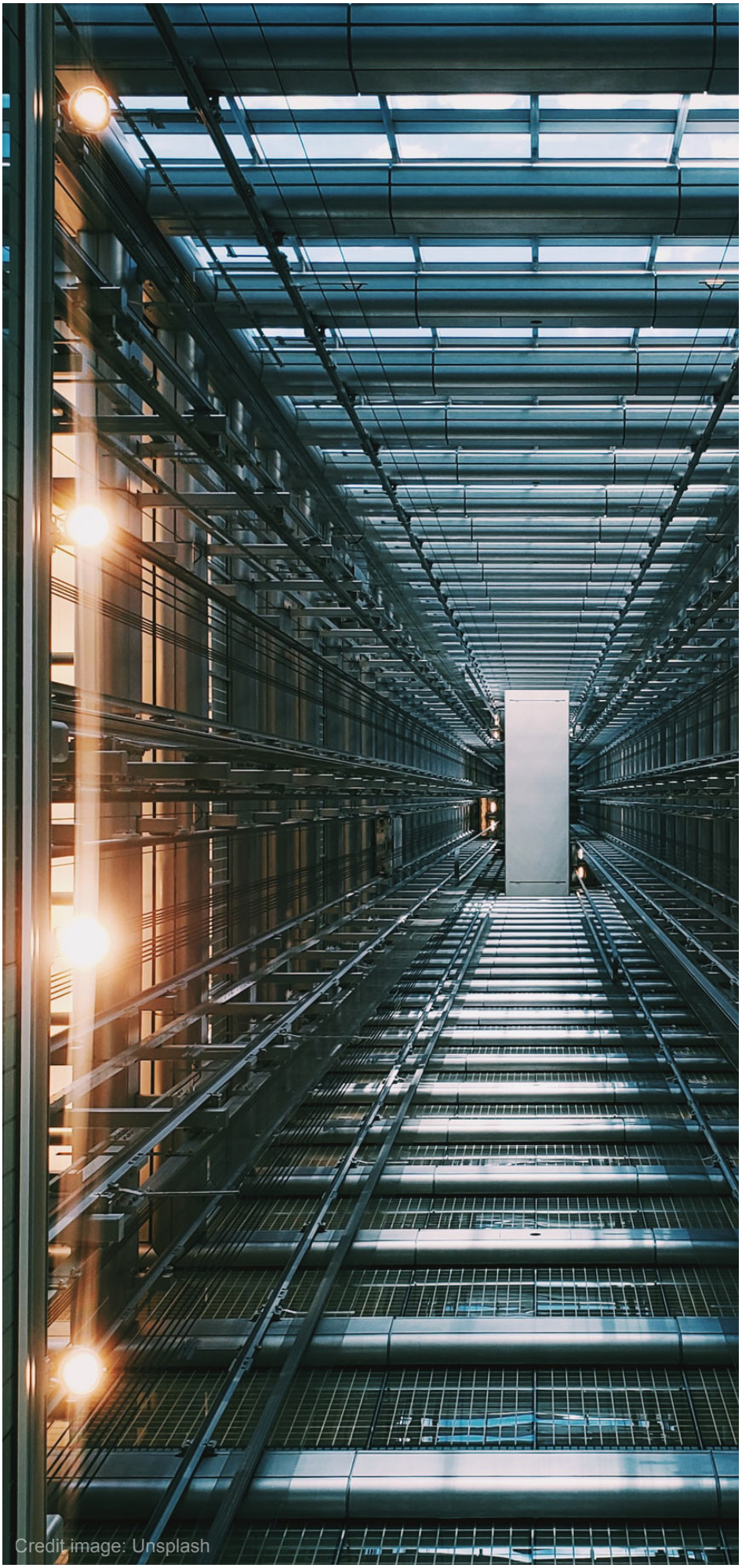
Se l'epidemia di WannaCry nel 2017 è un indicatore – visto e considerato che andava a colpire proprio Windows Server 2003 – il leak del source code potrebbe essere un gigantesco campanello d'allarme.

Al tempo – come è successo anche per Windows XP – c'era stata una patch di emergenza "fuori programma" per arginare l'epidemia, ma i danni erano stati quantificati in circa 200mila sistemi infettati in oltre 150 Paesi.
E quando in gioco c'è un server, non c'è bisogno di ricordarlo, a rischio è tutta l'organizzazione.

L'unico rimedio e non ci sono alternative e semplicemente aggiornare la propria infrastruttura. Anche solo volendo mantenere un'infrastruttura Windows, le ultime versioni dell'OS offrono una serie di vantaggi e strumenti come:

- Windows Defender – un'applicazione anti-malware che può rilevare in tempo reale le infezioni e garantisce aggiornamenti automatici
- Windows Device Guard – assicura che solo software affidabili possano essere fatti funzionare sul server
- Credential Guard – utilizza sistemi di virtualizzazione per proteggere le credenziali
- Improved Auditing Functionality – fornisce all'amministratore informazioni più dettagliate sui potenziali tentativi di violazione, consentendo all'amministratore di sistema di rispondere più rapidamente e di eseguire una migliore analisi forense.

Potrebbe essere una corsa contro il tempo, ma non ci sono alternative...


Credit image: Unsplash

La Sicurezza non è un'opinione: Data-Driven Computer Defence

di ***Adriana Franca***

"Immaginatevi due eserciti, uno buono e uno cattivo, impegnati in uno scontro decennale. L'esercito dei cattivi continua a vincere tutte le battaglie sferrate contro il fianco sinistro dell'avversario. In una guerra reale i buoni [...], dovrebbero dislocare più truppe e risorse proprio lì per contrastare i successi del nemico per non essere destinati a soccombere.

Ma nella guerra virtuale combattuta ogni giorno a difesa delle nostre reti, dopo aver compreso che il fianco sinistro viene costantemente battuto, inspiegabilmente i difensori dislocano truppe praticamente ovunque, tranne in quel punto. [...] Tutte le persone coinvolte possono constatare di stare perdendo a causa degli scontri che avvengono sul fianco sinistro, e si lamentano di questo, per poi rispondere facendo un sacco di cose tranne affrontare quegli attacchi." (Roger Grimes, A Data-Driven Computer Defense)

Purtroppo, questa è la situazione prevalente in materia di sicurezza informatica: la stragrande maggioranza delle aziende continua a spendere enormi budget in tecnologie software e hardware, ma continua a subire attacchi informatici in modo sempre più massiccio. Questo perché, nonostante tutta la tecnologia messa in campo, spesso si trascurano le più elementari misure di sicurezza e, soprattutto, si cercano di contenere i sintomi piuttosto che andare alla radice del problema.

Cyber Security in a Nutshell: i 3x3 Pilastri della Sicurezza

In breve, per ogni minaccia che dobbiamo affrontare, i controlli di sicurezza hanno tre principali obiettivi:

- Prevenire: vogliamo prevenire gli attacchi ed evitarne la diffusione
- Rilevare: se qualcosa passa, vogliamo ricevere notifiche tempestive e capire cosa sta accadendo
- Ripristinare: in caso di incidente, come possiamo rimediare al danno e prevenirlo la prossima volta?

Per ciascuno di questi obiettivi, dobbiamo fare tutto il possibile, distribuendo le migliori difese tra i tre tipi di controlli prescrittivi:

- Policy: dobbiamo avere delle linee guida in modo che chiunque possa comprendere quali sono le più probabili minacce, come possiamo mitigarle, e come attribuire l'accountability se qualcuno fa qualcosa di sbagliato. Se qualcosa va comunque storta, vorrà dire che avevamo trascurato qualcosa e dobbiamo rivedere i nostri controlli.

- Tecnologia: è l'insieme di tutti gli strumenti software e hardware che possiamo implementare e che servono a rendere più sicure determinate attività e mitigare i rischi in modo automatico. Ci teniamo a precisare, però, che essi dovrebbero evolvere al pari delle minacce per essere davvero efficaci. Ad esempio, gli antivirus tradizionali servono a poco o nulla contro le minacce non note (es. zero-days) e gli attacchi non basati su file.
- Training: i controlli tecnologici non sono infallibili e i cyber criminali troveranno il modo per bypassarli. Ancor meglio, dal momento che per violare un sistema ci possono volere settimane mentre per violare il 'sistema operativo uomo' ci vogliono pochi minuti, non è difficile indovinare quale strada un cyber criminale preferirà. Quindi, è oltremodo importante educare il nostro staff a riconoscere le minacce e sapere come difendersene.

Questa è la cyber security in a nutshell: semplice, no?

Creare una strategia efficace: I controlli 'top 3'

Sebbene tradizionalmente si citino i tre pilastri della cyber security secondo Ecco quindi l'elenco dei 3 controlli fondamentali da mettere in campo per primi:

- **Implementare un programma di security awareness.** Secondo le ultime statistiche, i data breach derivano da phishing e ingegneria sociale per il 70/90% (fig. 2). Questo dato di per sé dovrebbe rendere prioritario questo controllo eppure, di fatto, non lo è. Indipendentemente dalla tecnologia utilizzata, un'email di phishing su 10 arriva nella casella di posta dell'end-user. Ecco perché è importante

insegnare alle persone come riconoscerne la pericolosità e che fare appena se la trovano davanti. La formazione dovrebbe essere un processo continuo per rivelarsi in grado di ridurre significativamente il rischio, ed includere la simulazione di attacchi di phishing. Fare formazione one-shot significa soltanto perdere tempo: è come pretendere di avere dei muscoli ben torniti, facendo attività fisica una volta all'anno. I comportamenti di sicurezza sono 'muscoli' che vanno esercitati costantemente fino a diventare dei veri e propri riflessi automatici.

- **Monitoraggio continuo delle vulnerabilità** e dei programmi software non aggiornati costituiscono la seconda causa (20/40%, fig. 2) di data breach. La gestione delle vulnerabilità è quindi la nostra priorità numero 2. Ciò implica sia la rilevazione di vulnerabilità e patch non applicate che la massima automatizzazione degli aggiornamenti.

- Che cosa deve essere aggiornato? A livello client, le vulnerabilità più aggredite riguardano i browser e le loro componenti aggiuntive, seguite da quelle dei sistemi operativi. Lato server, le vulnerabilità sono maggiormente legate agli applicativi web e ai database. Aggiornando sistematicamente queste applicazioni, il nostro livello di rischio calerà considerevolmente.

- **Uso controllato dei privilegi d'accesso ai dati.** È opportuno seguire il principio del minimo privilegio perché i cyber criminali sanno che, violando gli account admin, possono provocare il maggior danno. Quindi:

  - Minimizziamo il numero di membri di ogni gruppo elevato
  - Imponiamo l'autenticazione multi-fattore
  - Imponiamo un limite di tempo per il log off
  - Monitoriamo inesorabilmente login e logoff

Concludendo, queste sembrano cose banali, di assoluto buon senso. Tuttavia, le principali cause di violazione (ingegneria sociale e mancati aggiornamenti) sono sempre state le stesse da quando è stato inventato il computer.


Credit image: Unsplash

L’importanza della continuità operativa in azienda

di ***Davide Giribaldi***

Se volessimo spiegare cosa sia la business continuity dovremmo dire che è l’insieme di attività da introdurre per minimizzare gli effetti negativi di un evento che ha colpito un’organizzazione o una sua parte.

Ma se davvero vogliamo capire cosa sia, dobbiamo porci alcune domande:

- Siamo a conoscenza di quanto siano importanti per il nostro successo imprenditoriale i dati e le informazioni che possediamo?
- Conosciamo i processi critici delle nostre organizzazioni?
- Per quanto tempo potremmo resistere senza averne l’accesso?
- Cosa succederebbe se d’improvviso non riuscissimo a raggiungere il 50% del nostro personale, della nostra infrastruttura o se perdessimo un fornitore strategico?

Si tratta di domande scomode, ma abbiamo investito tempo e denaro nella costruzione delle nostre imprese e se non vogliamo falliscano, dobbiamo essere pronti a gestire ciò che non è mai accaduto.

La business continuity è spesso associata ad un piano di gestione la cui mancanza potrà significare nella migliore delle ipotesi un tempo più lungo per riprendersi dall’evento dannoso e nella peggiore, fallire per sempre.

Un buon piano di continuità operativa può consentirci di superare un incidente con il minimo disagio possibile, ma da solo non basta, perché va mantenuto aggiornato nel tempo, collaudato di frequente e soprattutto integrato nel profondo della nostra organizzazione.

Quando parliamo di continuità operativa di solito commettiamo due leggerezze: la correliamo ad un disastro oppure la confondiamo con il concetto di resilienza che è più un obiettivo di medio/lungo periodo piuttosto che il risultato di una reazione ad un singolo episodio.

La continuità operativa non si occupa solo di disastri, anzi spesso si occupa di errori umani, attacchi informatici e soprattutto di piccoli incidenti all’apparenza insignificanti che se ripetuti con una certa frequenza nel tempo possono minare la stabilità aziendale nel suo profondo. Ad esempio, cosa succederebbe se il vostro sito di e-commerce fosse spesso irraggiungibile? Potreste perdere clienti, fatturato e soprattutto compromettere la vostra reputazione. Credete davvero si tratti di cose di poco conto?

Cosa è un piano di businness continuity

Un piano di continuità aziendale delinea le procedure e le istruzioni che un’organizzazione deve seguire al verificarsi di episodi imprevisti e deve essere in grado di coprire i processi aziendali, le risorse umane, quelle finanziarie e tutti i cosiddetti stakeholder.

Il metodo classico per determinare se possibili eventi legati ad un processo aziendale debbano rientrare nell’ambito di un piano di continuità operativa è quello della matrice probabilità per impatto.
L’approccio tiene in considerazione domande tipo: “cosa succederebbe se?” e si concentra maggiormente sulle cause degli eventi piuttosto che sulle loro conseguenze, ma quello che l’esperienza della pandemia ha insegnato è che esistono situazioni straordinarie, difficilmente prevedibili, ma dal forte impatto per le quali si rende necessario un nuovo approccio basato sulla comprensione degli effetti piuttosto che sulle cause.

Da ciò ne deriva l’esigenza di un’analisi che tenga conto di una terza dimensione, quella della “rilevabilità” ovvero del tempo necessario affinché un evento dannoso (già accaduto), manifesti la sua evidenza.

Cosa fare se non si dispone di un piano di bc

Se la nostra organizzazione non dispone di un piano BC, dobbiamo iniziare da una valutazione di tutti processi aziendali (Business Impact analysis) e dobbiamo stabilire quali aree siano maggiormente vulnerabili.
In poche parole, dobbiamo misurare l’impatto di uno o più eventi per un periodo di tempo non compatibile con i nostri obiettivi di business e dobbiamo farlo senza considerare la sua probabilità di accadimento.

La creazione di un piano di continuità è quindi solo l’ultimo di una serie di passaggi che per brevità riassumo qui di seguito:

Lo sviluppo di un piano di continuità dovrebbe partire dall’assunto che non

Business Continuity Plan

Business Impact Analysis

- Crea un questionario
- Istruisci il personale
- Analizza le risposte
- Valida con interviste
- Documenta
- Informa

Strategie di ripristino

- Identifica le risposte necessarie (BIA)
- GAP analysis tra requisiti di ripristino e capacità
- Valida con il management
- Informa
- Implementa la strategia

Piano di Business Continuity

- Sviluppa un Framework
- Organizza i gruppi di lavoro
- Scrivi procedure BC e DR
- Documenta
- Valida con il management
- Informa

Test Esercitazioni

- Stabilisci requisiti di test e di esercitazioni
- Istruisci i gruppi di lavoro
- Test ed esercitazioni
- Raccogli e verifica i risultati
- Informa
- Implementa il piano

è fondamentale avere il miglior piano possibile, ma quello più funzionale alle esigenze attuali della nostra organizzazione.

Uno dei pericoli maggiori dei piani di continuità è rappresentarlo con una fotografia di un determinato momento aziendale e di lasciarlo inalterato per anni.

Da imprenditori sappiamo che il business e di conseguenza le nostre organizzazioni cambiano ad una velocità tale per cui un piano efficace dovrebbe essere rivisto e testato più volte all'anno per poter essere costantemente allineato alle reali esigenze.
Purtroppo, non è così, ma testare un piano è l'unico modo che abbiamo per sapere se veramente saremo in grado di garantire la continuità del nostro business.

Se poi davvero volessimo provare un piano, non dovremmo scegliere uno scenario facile, ma provare a fare ipotesi complesse, renderle stimolanti e simulare ogni possibile correlazione tra eventi.
Dovremmo ovviamente darci obiettivi concreti e misurabili, coinvolgere sempre tutte le risorse, soprattutto quelle nuove perché solo così potremmo rendere credibile agli occhi dell'intera organizzazione il nostro test, migliorarlo e continuare a renderlo efficace.

Se vogliamo che un piano funzioni deve diventare parte della cultura aziendale.
Se i nostri collaboratori non lo conoscono come potranno reagire in modo appropriato durante una crisi?

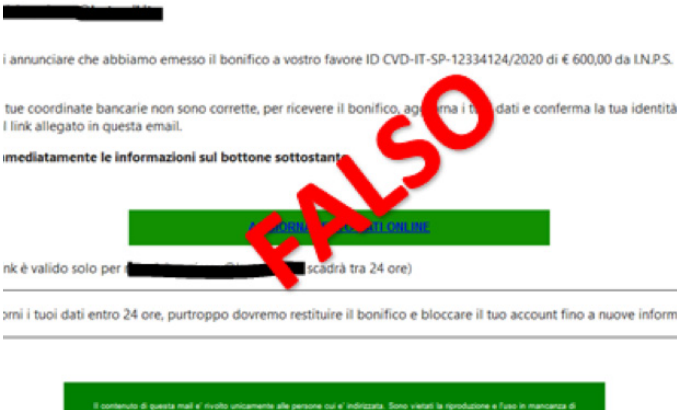
Se pensi di non avere tempo per occuparti della continuità operativa rifletti su cosa potrebbe accadere se un altro evento con implicazioni globali dovesse colpire la tua azienda: riusciresti a reagire?

Non chiederti se, ma preparati a quando accadrà di nuovo.

ATTENZIONE: INPS, NUOVA ONDATA DI PHISHING

Fonte: ***https://www.commissariatodips.it***

"Siamo lieti di annunciare che abbiamo emesso il bonifico a vostro favore ID CVD – IT –SP – 12334124/2020 di euro 600,00 da I.N.P.S. - purtroppo le tue coordinate bancarie non sono corrette per ricevere il bonifico - aggiorna i tuoi dati e conferma la tua identità accedendo al link allegato in questa email - Aggiorna immediatamente le informazioni sul bottone sottostante " È questo il contenuto di e-mail, a scopo di phishing, inviate in queste ore a ignari utenti con la finalità di sottrarre fraudolentemente dati sensibili.
Trattandosi di e-mail dal contenuto inaffidabile e ingannevole è consigliabile non dare alcun seguito, non cliccare su link e non fornire alcun dato personale. Si ricorda che le informazioni sulle prestazioni Inps sono consultabili esclusivamente accedendo direttamente dal portale www.inps.it e che l'INPS, per motivi di sicurezza, non invia in nessun caso mail contenenti link cliccabili.



ATTENZIONE ALLE FALSE OFFERTE DI LAVORO

Fonte: ***https://www.commissariatodips.it***

Giungono numerose segnalazioni di false offerte di lavoro veicolate tramite canali TELEGRAM che, utilizzando logo e intestazione di Agenzie che offrono servizi di somministrazione del lavoro traggono in inganno ignari candidati. A coloro che aderiscono alla proposta lavorativa viene inviata una bozza di contratto a tempo determinato con contestuale richiesta di documenti d'identità, codice fiscale e iban con la falsa promessa di un successivo accredito di un corrispettivo di euro 200 a settimana o in alternativa 800 euro al mese a fronte della pubblicazione, da parte del candidato, di un certo numero di annunci su gruppi di offerte lavorative presenti su noti social network. La Polizia Postale consiglia di: diffidare delle offerte pervenute tramite l'invio di mail o profili social e non precedute da alcuna richiesta; diffidare di richieste in denaro finalizzate alla copertura di ipotetiche "spese" per l'avvio dell'istruttoria; rifiutare richieste di apertura di conti correnti per "facilitare" trasferimenti di denaro; rifiutare la richiesta di reclutamento di altri soggetti cui rivolgere la medesima offerta di lavoro (cd schema "piramidale"); rifiutare offerte contrattuali particolarmente vantaggiose dal punto di vista economico. In presenza di uno di questi elementi è sicuramente consigliabile diffidare e non fornire dati personali.

Nuove campagne diffondono Formbook (AL01/20201023/CSIRT-ITA)

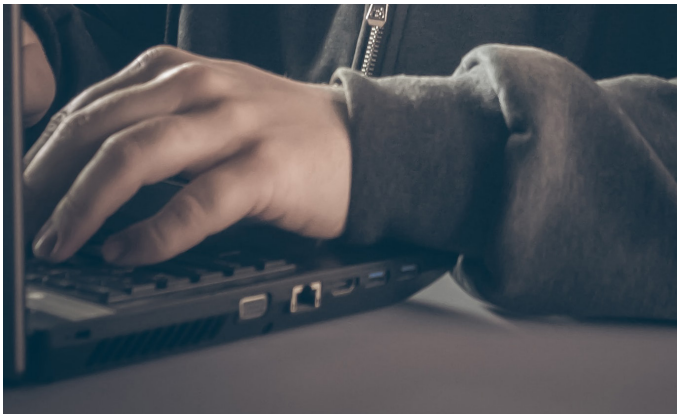
Fonte: ***https://csirt.gov.it***

Con riferimento alle precedenti informative, sono state individuate nuove campagne malspam dirette a utenze italiane e finalizzate alla distribuzione del malware Formbook, attraverso messaggi di posta elettronica con allegati malevoli. Per la diffusione del malware gli attaccanti utilizzano email esca contenenti riferimenti a società finanziarie realmente esistenti, al fine di indurre la vittima all'apertura dell'allegato. In particolare, nel messaggio si citano fatture fittizie e ricevute di pagamento. Gli allegati si presentano sottoforma di archivio compresso senza alcuna password di decrittazione. All'interno di quest'ultimo, risulta esservi sempre l'eseguibile contentente il malware Formbook.

Azioni consigliate
Si consiglia di valutare l'implementazione degli Indicatori di Compromissione (IoC) di seguito allegati sui propri apparati di sicurezza (https://csirt.gov.it/data/cms/posts/325/attachments/6084ad9f-8fb6-4c0d-b1a6-015ee0417257/download).

Campagna di malspam invia Dridex a nome di Intuit (AL03/201022/CSIRT-ITA)

Fonte: ***https://csirt.gov.it***



Descrizione e potenziali impatti
È stata individuata una campagna malspam che sfrutta, per la distribuzione del trojan bancario Dridex, i riferimenti di Intuit, una società americana di software commerciale e finanziario che fornisce servizi ad imprese e privati. Il messaggio di phishing, apparentemente inviato da una casella della citata azienda invita il destinatario a prendere visione di una fattura presente nel documento allegato (vds immagine sottostante). Le email inviate contengono un file con estensione .xlsm, denominato "Inv_XXXXX_from_XXXXXX.xlsm" (dove la X indica una parte numerica variabile), armato con macro malevole. Una volta aperto, viene visualizzato il logo dell'azienda Intuit (vds immagine sottostante). L'abilitazione della macro, che avvia di fatto la catena di infezione, provvede a contattare una risorsa internet, contattando un link malevolo che viene scelto da una corposa lista predefinita di URL, dalla quale viene prelevato ed installato il trojan bancario Dridex, uno tra i malware più diffusi in Italia. **Azioni consigliate** Gli utenti e le organizzazioni possono far fronte a questa tipologia di attacchi verificando scrupolosamente le email ricevute e attivando le seguenti misure aggiuntive:

- limitare le funzionalità delle macro che attivano connessioni verso internet;
- fornire periodiche sessioni di formazione finalizzate a riconoscere il phishing diffidando da allegati che invitano ad effettuare azioni con richiesta di abilitazione dei contenuti;

Credit image: Unsplash

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ANNO 1
Numero 2
2020

CYBER Magazine