Anno 2 / Numero 3
2021

CYBER MAGAZINE

In questo numero:

Cybersecurity: i dispositivi degli utenti sono in prima linea

Il ritorno di attualità della qualità e della sicurezza dei dati: la Data governance come disciplina emergente

I cambiamenti dei Cyber attacchi nell'anno del COVID-19

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

INDICE

3
I cambiamenti dei Cyber attacchi nell'anno del COVID-19
di Pierguido Iezzi, ***Swascan***

6
Cybersecurity: i dispositivi degli utenti sono in prima linea
di Stefano Zai, ***Ricoh***

9
La strategia di Cyber deterrenza europea nella programmazione del settennio 2021-2027
di Davide Maniscalco, ***Swascan***

12
Cos'è il Cryptojacking?
di Riccardo Paglia, **Swascan**

15
Italia quinta al mondo per attacchi macro malware (prima in Europa), settima per attacchi malware e undicesima per attacchi ransomware. Cosa succederà nei prossimi mesi?
di ***Trend Micro***

17
Factory 4.0: perché potrebbe essere importante avere un sistema di Gestione degli Allarmi.
di Enzo Maria Tieghi, ***ServiTecno***

20
Il ritorno di attualità della qualità e della sicurezza dei dati: la Data governance come disciplina emergente
di Carlo Guastone, ***Sernet***

23
La necessita' di tenere insieme tecnologia e fattore umano Impreparazione e overconfidence in cybersecurity
di Francesco Tieghi e Alessandro Pollini, ***ServiTecno***

25
Previsioni sulle minacce per il 2021. Attenzione a privacy, estorsioni e vaccini.
di ***Kaspersky Lab***

27
Tik tok e minori. Houston abbiamo un problema
di Valentina Arena, ***Ikran Services***

L'editoriale del Presidente Assintel

Paola Generali

Ad un anno dall'irruzione del Covid i cambiamenti avvenuti all'interno della società e del lavoro ci mettono di fronte ad alcune riflessioni. La Trasformazione Digitale ha subito un'accelerazione decisiva – e questo è uno degli effetti collaterali positivi – ma non si è avuto il giusto tempo per adeguare il mindset e l'approccio culturale al digitale. Come ogni processo attivato velocemente, spesso arriva prima la tecnologia rispetto alla piena consapevolezza dello strumento, e fra le sue pieghe possono insinuarsi le minacce che sfruttano nuove vulnerabilità dei sistemi informativi.

I nuovi contesti che lasciano il fianco scoperto sono quelli legati all'emergenza sanitaria, all'organizzazione del lavoro agile, alle piattaforme di videoconferenza e di file sharing. Ed altri se ne apriranno, perché se è vero che il Next Generation UE incentiva il Digitale, è altrettanto vero che parallelamente si apriranno continuamente nuovi contesti e target che saranno caratterizzati da nuove vulnerabilità e quindi nuove minacce.

Noi operatori del settore allora dobbiamo farci carico di una responsabilità etica, oltre che professionale: continuare a diffondere una cultura della security, nel nostro modo di comunicare, nelle nostre relazioni con i clienti, nelle iniziative di sensibilizzazione. E a livello politico dobbiamo continuare il pressing affinché il tema rientri a pieno titolo nei progetti di sostegno alla transizione digitale non solamente intesa per la PA ma anche e soprattutto per le MPMI che rappresentano il tessuto economico italiano.

I cambiamenti dei Cyber attacchi nell'anno del COVID-19

Un anno dopo l'inizio ufficiale della pandemia da COVID-19, i metodi e le tattiche utilizzati dai cybercriminali sono mutati drasticamente.

---

di ***Pierguido Iezzi - Swascan***

Le email di phishing a tema COVID, gli attacchi brute-force su dipendenti in smart working e un particolare focus nell'attaccare le svariate piattaforme di video conferenza e file sharing sono i tratti distintivi delle organizzazioni criminali al primo anniversario del virus che ha cambiato le nostre vite.

Un anno dopo l'inizio della crisi da COVID-19, il modo in cui le persone vivono e lavorano è cambiato radicalmente. E con loro anche i metodi e le tattiche utilizzati dai criminali per cercare di sfruttare l'enorme aumento di traffico online.

Le truffe di phishing che fanno leva sul COVID-19

Le truffe via email (e il phishing in particolare) sono ancora uno dei metodi di attacco più efficaci nell'era della pandemia, dato che la paura e l'ansia sono due delle emozioni su cui è più facile fare leva per questo tipo di attacchi di social-engineering.

Le campagne come quelle che sostengono di voler offrire mascherine e igienizzante per mani (che richiedevano ai destinatari di inserire i dettagli di pagamento) sono diventate molto comuni nel corso dell'ultimo anno. Fra gli approcci abituali c'è anche stato l'impersonare le autorità mediche da parte dei cybercriminali, con l'offerta di "importanti" aggiornamenti. Ma invece di news di valore arrivavano i malware.

I cybercriminali hanno anche utilizzato il tema dei ritardi nelle consegne per celare l'esca dei loro attacchi. Questo perché, specie durante il picco pandemico, la catena di trasmissione della fornitura si era inceppata proprio a livello delle consegne a domicilio. Non a caso nel 2020, proprio i corrieri, i fornitori di servizi di consegna a domicilio, sono entrati a far parte della top 10 delle organizzazioni più soggette allo spoofing.

Attacchi brute-force verso i dipendenti che lavorano in Smart Working

Con la creazione improvvisa e a volte improvvisata di milioni di uffici in abitazioni di tutto il mondo, le misure di cybersecurity sono passate in secondo piano per molte aziende. I cybercriminali, consci di ciò, hanno messo nel mirino

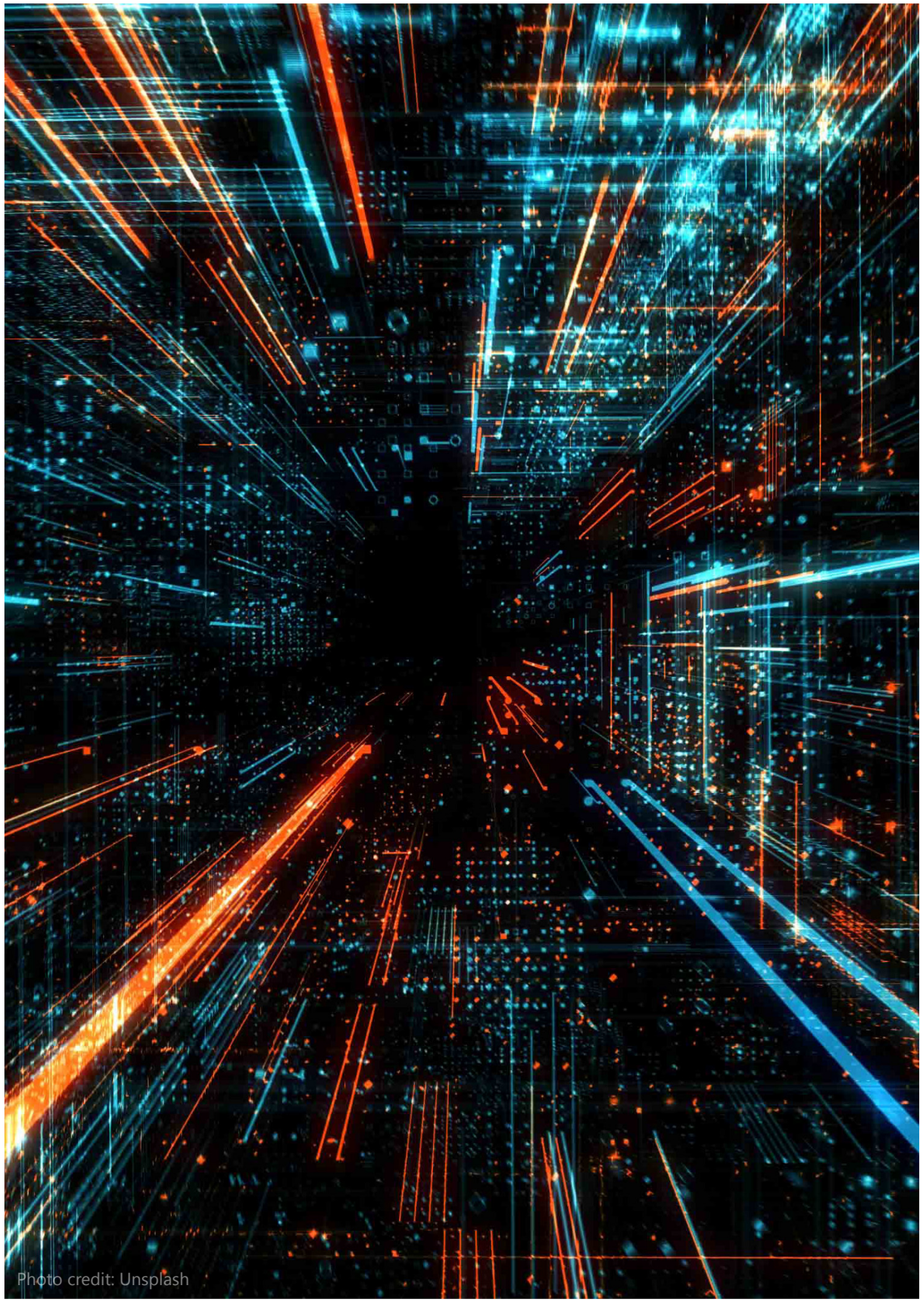


Photo credit: Unsplash

i dipendenti che accedono ad account di lavoro attraverso dispositivi personali in reti domestiche non protette.
Nello specifico, gli attacchi brute-force (in cui l'aggressore prova nomi utente e password in maniera randomica per ottenere l'accesso a un account) su connessioni Remote Desktop Protocol (RDP) sono aumentati in modo esponenziale, con un incremento del 197% dall'anno precedente, arrivando a 277,4 milioni totali a marzo. RDP è il protocollo di Microsoft che permette agli utenti di accedere a postazioni di lavoro di questo sistema operativo da remoto. RDP è proprio uno dei protocolli di maggiore successo per l'accesso da remoto usato dalle aziende, diventando di conseguenza il preferito anche da parte dei criminali.

L'aumento degli attacchi sulle piattaforme

I cyberattacker si sono anche messi all'inseguimento di utenti di vari servizi di cloud, in particolare di app per il lavoro in team come Flock, GotoMeeting, HighFive, Join.me, Lifesize, Teams di Microsoft, Slack, Webex e Zoom.
Kaspersky ha rilevato che a maggio del 2020, il numero medio degli attacchi giornalieri a questo tipo di servizi era cresciuto del 25% a partire da febbraio. E la tendenza non ha subito rallentamenti.
La maggior parte di questi attacchi prevedono la diffusione di file dannosi rinominati in modo da ingannare i destinatari, convinti di stare scaricando o aprendo una di queste famose app. A gennaio sono stati rilevati ben 1,15 milioni di file di questo tipo, il numero più alto dall'inizio del lockdown. Spesso vengono creati dei veri e propri insiemi di file che imitano con fedeltà i file d'installazione dei programmi legittimi, per poi essere diffusi attraverso email di phishing, conditi con presunte offerte speciali dalle piattaforme, o attraverso pagine web.

Cosa dobbiamo aspettarci dal futuro dei cyberattacchi?

Con la pandemia diretta verso la nuova fase delle vaccinazioni, sorgono nuovi argomenti che possono essere sfruttati da truffatori ed esperti di phishing per nuove macchinazioni criminali. Ad esempio, la creazione di passaporti a certificare lo stato di buona salute per poter viaggiare, o messaggi a tema vaccino.

Molto probabilmente questi nuovi canali verranno sfruttati: è importante che gli utenti guardino a ogni email a tema pandemia con occhio scettico.
I recenti eventi ci hanno dimostrato praticamente come i criminali siano pronti ad approfittare della crisi per il proprio tornaconto personale.
L'uso dell'RDP non è destinato a svanire nel nulla, così come accadrà agli attacchi contro questo protocollo. Questo significa che le aziende devono rivalutare l'utilizzo di questo strumento in modo da garantire un accesso da remoto sicuro.
Tutto questo nel bel mezzo del can can mediatico generato dall'hackeraggio di Exchange Server, altro prodotto di Microsoft, con potenziali ramificazioni politiche a livello globale, visto il numero e l'entità dei player coinvolti da questa ultima offensiva.
Insomma, non una prospettiva "rosea", ma neppure un'offensiva di fronte alla quale non abbiamo strumenti per difenderci. La chiave è sempre la stessa: la Cyber Security di oggi e del futuro deve prevedere tre pilastri:

- Sicurezza Predittiva,
- Sicurezza Preventiva,
- Sicurezza Proattiva.

Tre pilastri fondamentali che devono appoggiarsi su competenze, tecnologie e processi.

Non abbassiamo la guardia!

Cybersecurity: i dispositivi degli utenti sono in prima linea

di ***Stefano Zai - Ricoh***

Tutte le grandi rivoluzioni prendono le mosse e vengono accelerate da accadimenti inaspettati e che potremmo definire "traumatici". Che fosse in atto un'evoluzione nell'ambito dei servizi informativi e della comunicazione era palese da anni, ma gli eventi recenti ne hanno accelerato l'adozione.
Dall'oggi al domani, l'emergenza ha spostato l'attenzione sulla produttività personale al di fuori del perimetro aziendale, in una scala di gran lunga superiore alle previsioni.
La necessità di dare continuità alle attività aziendali ha portato all'adozione del lavoro da remoto con misure veloci ed eccezionali quali:

- connettività privata per collegarsi in azienda in VPN / SSL;
- dispositivi condivisi e pc privati (un BYOD "forzato");
- repository cloud ad uso privato per lo scambio di documentazione aziendale;
- applicazioni VNC (Virtual Network Computing) al di fuori di collegamenti sicuri malgrado vulnerabilità note fin dagli anni 2000;
- dispositivi con sistemi operativi vari e di versioni diverse (da Windows Xp in avanti, Android, iOS e MacOS tra i più diffusi);
- sistemi di videoconferenza anche gratuiti che poi si sono rivelati non del tutto sicuri.

In questo nuovo contesto, ed in tempi brevissimi, la superficie "attaccabile" di un'azienda si è estesa velocemente, sfuggendo al controllo dei responsabili IT e DPO che hanno dovuto garantire comunque la continuità operativa.

Lavoro da remoto: la sicurezza prima di tutto
Gli effetti della situazione appena descritta sono risultati deleteri e hanno confermato come le minacce più pericolose vengano indirizzate sull'utente finale, sulle sue abitudini d'uso e sui suoi dispositivi che sovente sono ad uso promiscuo aziendale e privato.
Le attività di consulenza e di Threat Intelligence condotte su diverse aziende mostrano come le credenziali di dominio di un numero crescente di aziende vengano violate, fenomeno dovuto anche all'utilizzo del SaaS (Software as a Service) al di fuori di connettività sicure (per le quali è sempre comunque importante implementare policy di multifactor authentication, sistemi DLP e cambi password frequenti impedendo il riutilizzo delle stesse).
Gli exploit più pericolosi, ad esempio, hanno portato a furti d'identità e ransomware sia su dispositivi personali che su dati ed infrastrutture centrali.

Una risposta concreta
In prima battuta le aziende

dovrebbero selezionare soluzioni e servizi che consentono di implementare gli standard di sicurezza necessari negli attuali scenari in cui il nuovo perimetro di sicurezza aziendale è rappresentato dai dispositivi personali.
In particolare soluzioni EMM (Enterprise Mobility Management) consentano di:

- operare su un ampio spettro di dispositivi mobili/ personali e IoT, evitando così di frammentare la gestione tra diverse soluzioni;
- gestire l'inventario dei dispositivi di proprietà dell'azienda o personali ma comunque abilitati ad operare nel perimetro di sicurezza aziendale;
- rilevare lo stato di aggiornamento di sistemi operativi, antivirus e patching degli applicativi;
- applicare per gruppi di utenza le configurazioni e policy di sicurezza (tra cui dati criptati, configurazioni per collegamenti sicuri in VPN o SSL, impostazioni per l'autenticazione, backup, etc…)
- attivare policy aziendali e aggiornamenti in modalità push, senza interazione diretta tra il personale IT e l'utente finale;
- distribuire applicativi con il controllo dell'avvenuta installazione e attivazione;
- suddividere dati e applicativi aziendali rispetto a quelli personali;
- inibire l'accesso a porte, accessori o estensioni che possono essere veicolo di minacce provenienti da periferiche: non solo la "classica" chiavetta USB, ma anche dispositivi di videoconferenza, gateway IoT e altre tecnologie emergenti (tipicamente dotati di sistemi operativi commerciali poco o addirittura mai aggiornati)
- cancellare dati e inibire l'utilizzo dei dispositivi a seguito di smarrimento o furto.


Photo credit: Unsplash

Photo credit: Unsplash

L'utilizzo di soluzioni di EMM applicate sia a dispositivi mobili che a pc e notebook con sistemi Next Generation EDR (Endpoint Detection and Response) consente di implementare efficacemente il concetto di "Zero Thrust Security" dal punto di vista organizzativo, fisico e tecnologico.
E' preferibile l'adozione di sistemi Next Generation EDR per l'intera infrastruttura, anche cloud. Tipicamente basati su AI (Artificial Intelligence), si dimostrano di efficacia superiore nel caso di attacchi "Zero Day" in cui la firma del malware non è stata ancora classificata e resa riconoscibile da parte dei sistemi EDR più tradizionali. Le soluzioni Next Generation EDR si dimostrano efficaci anche quando si devono contrastare attività sospette con eventi non riconducibili alle abitudini dell'utente e ai suoi tempi e modalità d'utilizzo di dati e funzionalità (esempio: l'inoltro di migliaia di e-mail in millisecondi da un notebook, cripting di un disco, modifiche o integrazioni a funzionalità del sistema operativo o del browser,...).
Per ridurre i rischi in ambito Cybersecurity per le aziende oggi è bene attuare un framework operativo che comprenda assessment periodici a scopo preventivo e predittivo sulle minacce più attuali e che implementino sistemi di gestione e controllo che consentano risposte automatizzate. Tra le misure tradizionali, sono sempre necessarie procedure e soluzioni di ripristino alla situazione precedente ad un evento di databreach.

La strategia di Cyber deterrenza europea nella programmazione del settennio 2021-2027

di ***Davide Maniscalco - Swascan***

Lo scorso dicembre la Commissione Europea e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza hanno presentato una nuova strategia dell'UE per la cybersecurity, che si innesta nel più ampio percorso europeo proteso definizione del Digital Single Market. La nuova strategia completa il prolifico framework programmatico europeo che vede tra le sue componenti anche la strategia digitale dell'UE "Plasmare il futuro digitale dell'Europa", il "piano per la ripresa dell'Europa" e la "strategia dell'UE per l'Unione della sicurezza". La minaccia cibernetica diventa sempre più pervasiva, anonima e polimorfa e si caratterizza per uno scenario ibrido preordinato spesso alla destabilizzazione di sistemi democratici, anche attraverso mirate campagne di disinformazione, nonché all'attività di spionaggio e di sabotaggio di presidi strategici di uno Stato. L'attuale scenario pandemico a livello globale ha ulteriormente confermato l'imprescindibile esigenza di proteggere i sistemi informatici ed informativi che costituiscono ormai da anni un elemento chiave per la sicurezza di qualsiasi organizzazione a prescindere dal settore di riferimento, tanto più in quelli cosiddetti "critici o strategici".
Per queste ragioni, la natura transnazionale della minaccia e la sua connotazione asimmetrica, hanno richiesto e continuano a richiedere una risposta di sistema, per mitigare le vulnerabilità e le esternalità negative.
Del resto, l'espansione delle tecnologie di ICT unita alla forte esigenza di presidiare le infrastrutture critiche di un Paese, nonché l'evoluzione progressiva dell'economia digitale "data driven", al cui progressivo sviluppo contribuirà l'avvento delle reti di quinta (e sesta) generazione con l'aumento della potenza di calcolo "in locale" (edge computing), attraverso le interconnessioni sempre più eterogenee dei devices dell'Internet of (every) Things, configurano, su scala europea, una road map verso la costruzione di un mercato unico digitale sicuro ed affidabile.
In ambito industriale, infatti, l'aumento degli attacchi alle cosiddette Operational Technologies (Ot)/ICS risulta particolarmente preoccupante di fronte all'intrinseca vulnerabilità dei sistemi OT che, invero, non sono progettati per difendersi da attività informatiche dannose.
E' pertanto intuitivo che in tale scenario le normative e le regolamentazioni esistenti in materia di sicurezza delle reti e dei sistemi diventano un punto di riferimento per tutte le imprese che intendono aumentare il loro livello di sicurezza e la consapevolezza riguardante le minacce e i rischi informatici e, pertanto, diventa fondamentale configurare un approccio efficace alla mitigazione del rischio e alla resilienza dei processi primari.
Già la strategia per la cybersicurezza del 2013, sottoposta a revisione nel 2017, e l'agenda europea sulla sicurezza 2015-2020 della Commissione europea andavano nella direzione di una maggiore efficacia delle misure di cyber deterrenza e resilienza, seppur in uno scenario di riferimento diverso per livelli di pervasività e superficie esposta al rischio.
Per queste ragioni, nell'ambito del Cybersecurity Act (Regolamento UE 2019/881) viene delineato un nuovo mandato permanente per l'ENISA, l'Agenzia Europea per la Sicurezza Informatica, che in virtù dell'art. 48(2) del Regolamento è chiamata a preparare il primo programma europeo di certificazione della cybersecurity, il "Common Criteria based European candidate cybersecurity certification scheme" (EUCC), che mira a sostituire i sistemi esistenti che operano nell'ambito del SOG-IS - MRA (Senior Officials Group – Information Systems Security - Mutual Recognition Agreement) per i prodotti ICT, aggiungendo nuovi elementi e rendendolo applicabile per tutti gli Stati membri dell'Unione.
In seguito a tale richiesta, l'ENISA ha istituito un gruppo


Photo Credit: Unsplash

di lavoro ad hoc composto dai rappresentanti delle parti interessate (AHWG) per essere di supporto alla preparazione del programma di certificazione, e grazie anche al confronto continuo con il Gruppo Europeo per la Certificazione di Sicurezza (ECCG) , istituito dal Regolamento come organo consultivo dell'Agenzia, ha consolidato uno Schema di Certificazione europeo per la sicurezza dei servizi, processi e prodotti ICT, che sarà applicabile da giugno 2021, avrà carattere volontario, e prevede il rilascio di certificati aventi validità per 5 anni, rinnovabili.

A ciò si aggiunga che lo scorso 24 luglio 2020, è stata adottata la nuova strategia UE sulla sicurezza 2020-2025 relativa alla protezione e resilienza delle infrastrutture nella direzione di una importante revisione della Direttiva europea 2008/114/CE dell'8 dicembre 2008 relativa alle infrastrutture critiche europee.
In tale contesto, lo scorso anno si è dato anche avvio al processo di revisione della Direttiva europea 2016/1148 Network and Information Security (NIS), passando per la consultazione pubblica, conclusasi il 2 ottobre scorso, per affrontare la questione della resilienza sia informatica che fisica dei soggetti critici e delle reti essenziali (specie in ambito supply chain) attraverso la "proposta di Direttiva europea sulle misure per un elevato livello comune di cybersicurezza in tutta l'Unione (NIS 2)".
E' evidente che la strategia europea sulla cybersecurity mira a rafforzare ulteriormente ed in modo strutturato la resilienza collettiva dell'Europa contro le minacce informatiche attraverso l'accesso a servizi e strumenti digitali sempre più affidabili ed un rafforzamento della sovranità digitale e della leadership su norme e standard internazionali del dominio cibernetico anche sulla base di best practices di information sharing.
In questa linea d'azione l

a NIS 2 ha l'importante obiettivo di aumentare il livello di cyber resilienza dei settori pubblici e privati essenziali, anche attraverso la strutturazione di un network di centri operativi per la sicurezza in tutta l'UE, caratterizzati da un approccio proattivo e di tipo analitico-predittivo con l'ausilio di sistemi di intelligenza artificiale e l'introduzione di nuovi strumenti di diplomazia informatica per la più ampia diffusione della vision europea sul cyberspazio.
La strategia passa anche per una più ampia valorizzazione delle PMI nel quadro del sostegno che verrà accordato con la creazione dei poli dell'innovazione digitale preordinati a migliorare le competenze e a stimolare l'innovazione e la competitività.
Imponente il commitment economico-finanziario europeo a sostegno della nuova strategia per il prossimo settennio 2021-2027, coerentemente con il Quadro Finanziario Pluriennale.

L'UE si è infatti impegnata con investimenti storicamente senza precedenti attraverso il programma Europa digitale, Orizzonte Europa e il piano per la ripresa dell'Europa, con l'obiettivo di raggiungere fino a 4,5 miliardi di Euro di investimenti combinati da parte dell'UE, degli Stati membri e dell'industria, con particolare riguardo allo sviluppo del Centro di competenza sulla cybersecurity e della rete dei centri di coordinamento.
Nel contesto politico europeo che vede avvicendarsi il Portogallo nel semestre europeo di presidenza, si prevede una compiuta attuazione della nuova strategia nel breve periodo.

All'esito del negoziato tra Parlamento europeo e Consiglio sulla proposta afferente alla NIS 2, gli Stati membri avranno una deadline di 18 mesi dall'entrata in vigore per il conseguenziale recepimento nei rispettivi ordinamenti giuridici.

Cos'è il cryptojacking?

Il cryptojacking è l'uso non autorizzato del computer altrui per minare criptovaluta.

*di **Riccardo Paglia - Swascan***

I criminal hacker si macchiano di cryptojacking attraverso 2 approcci: convincendo la vittima a cliccare su di un link dannoso presente in un'email, il quale scaricherà e installerà il codice del cripto minatore sul computer, oppure infettando un sito o una pubblicità online con del codice JavaScript in grado di auto-eseguirsi una volta caricato nel browser della vittima. Indipendentemente dall'approccio usato, il codice di cryptomining continua a essere eseguito in background mentre le vittime utilizzano il proprio dispositivo senza sospettare nulla. Potrebbero notare solo una maggiore lentezza nelle performance o qualche ritardo nell'esecuzione dei programmi.
Perché il cryptojacking va per la maggiore?

Nessuno sa precisamente quanta criptovaluta venga

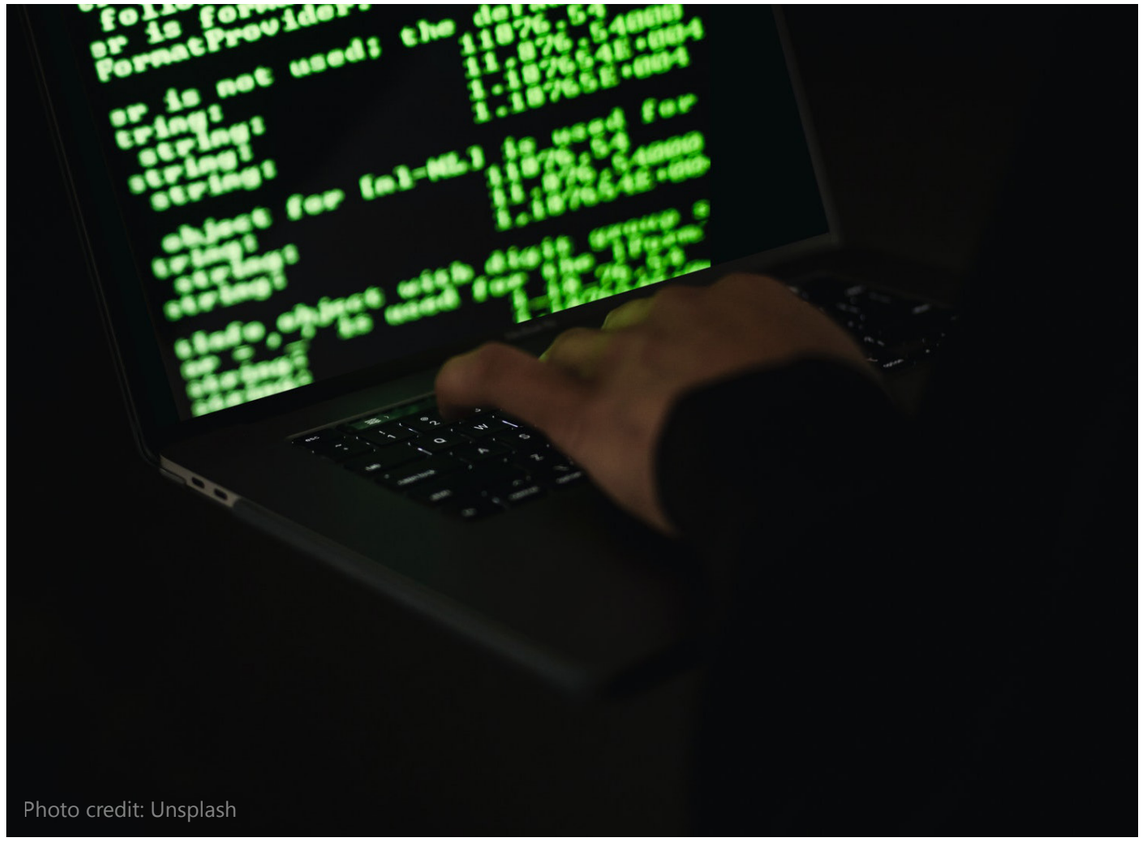


Photo credit: Unsplash

minata attraverso questa pratica illecita ma non c'è dubbio che la tendenza sia al rialzo. Il cryptojacking basato su attacchi via browser ha avuto un'esplosione iniziale ma ora sembra in calo, probabilmente perché la volatilità del valore delle criptovalute e la chiusura di Coinhive, il principale miner Javascript, utilizzato anche in operazioni lecite, hanno reso meno conveniente tale approccio.

Il SonicWall Cyber Threat Report del 2020 ha rivelato che il volume di attacchi di cryptojacking è sceso del 78% nella seconda metà del 2019 proprio in virtù di tale chiusura. Nonostante questo calo, il fenomeno è considerato ancora in fase "infantile", ovvero è destinato a crescere ed evolversi.

Nel gennaio del 2018, i ricercatori hanno scoperto che la botnet Smominru focalizzata sul cryptomining aveva infettato più di 500mila macchine, principalmente in Russia, India e Taiwan. La rete aveva messo nel mirino server Windows per estrarre Monero, generando un incasso totale stimato di oltre 3,5 milioni di dollari.

E l'aspetto preoccupante è che il cryptojacking non richiede nemmeno particolari competenze tecniche. Per dare un esempio pratico, i kit per il cryptojacking per novizi sono venduti sulla dark web con prezzi a partire da 30 $.

Il motivo per cui tante organizzazioni criminali adottano tale approccio è che il rischio di essere colti sul fatto e identificati è minore rispetto a un'offensiva basata su un ransomware. Il codice di cryptomining viene eseguito segretamente e tale attività può continuare per lunghi periodi

Photo credit: Unsplash

senza essere rilevato. Una volta scoperto, è comunque molto complesso rintracciare la fonte e le vittime sono poco incentivate a denunciare il fatto dato che non c'è stato alcun furto materiale (e nessun dato è stato cifrato o reso indisponibile).

Esempi reali di cryptojacking:

I cryptojackers sono molto scaltri e hanno ideato una serie di schemi criminali per accedere nei computer altrui ed estrarre criptovaluta. Molti non sono innovativi: i metodi di rilascio dei malware derivano spesso da tecniche utilizzate in offensive basate su ransomware o adware.

Ecco qualche esempio pratico:

PowerGhost ruba le credenziali di Windows

Il report pubblicato da Cyber Threat Alliance, denominato The Illicit Cryptocurrency Mining Threat, descrive nel dettaglio PowerGhost, analizzato per la prima volta da Fortinet, un malware molto elusivo che può evitare il rilevamento in diverse modalità. Inizialmente usa tecniche di "spear phishing" per entrare in un sistema informatico e in seguito ruba le credenziali di Windows al fine di sfruttare gli strumenti gestionali del sistema operativo e l'exploit EternalBlue per diffondersi. In seguito prova a disattivare il software antivirus ed eventuali cryptominatori già presenti nel sistema.
Graboid, il worm criptominatore che si diffonde rapidamente

A ottobre, Palo Alto Networks ha pubblicato un report nel quale veniva descritta una botnet attiva nel cryptojacking in grado di autodiffondersi. Denominata Graboid, è stato definito come il primo worm criptominatore nella storia. Questo malware si diffonde attraverso i cosiddetti Docker deployments e sarebbe riuscito a colpirne più di 2.000 nella sua breve esistenza.

Come prevenire il cryptojacking e difendersi da questa minaccia

Consigliamo di seguire questi step per minimizzare il rischio di cadere preda di cryptojacking:

Incorporare tale minaccia nel proprio programma formativo di cybersecurity, concentrandosi sui tentativi di accesso tramite phishing, finalizzati al rilascio di script dannosi nei computer degli utenti. Tale formazione potrebbe tornare utile nel caso in cui i sistemi tecnologici automatizzati lasciassero passare fra le loro maglie messaggi via email dannosi. Secondo le previsioni degli esperti, il phishing è destinato a rimanere il metodo primario di diffusione di questo e di tanti altri tipi di malware.

La formazione delle risorse aziendali non avrà alcun impatto in caso di attacchi cryptojacking ad esecuzione automatica qualora si visitino siti legittimi ma con frammenti di codice dannoso. In questo caso sarebbe difficile dire ai propri utenti quali siti visitare e quali evitare, dato che quelli dannosi sono del tutto indistinguibili da quelli legittimi (in questo caso specifico).

Installare un'estensione di ad-blocking o anti-cryptomining sui propri browser di navigazione. Dato che gli script dei criptominatori sono spesso rilasciati attraverso le pubblicità su internet, installando un ad blocker è possibile bloccare tale minaccia. Alcune estensioni che bloccano la pubblicità, come ad esempio Ad Blocker Plus sono in grado, in una certa misura, di rilevare gli script dei cryptominatori.

Italia quinta al mondo per attacchi macro malware (prima in Europa), settima per attacchi malware e undicesima per attacchi ransomware. Cosa succederà nei prossimi mesi?

Trend Micro ha presentato il report 2020 delle minacce e lo studio sugli attacchi che colpiranno prossimamente.

*di **Trend Mirco***

Le minacce informatiche continuano a flagellare l'Italia, che nel 2020 a livello mondiale risulta il quinto Paese più colpito dai macro malware (primo in Europa) il settimo per attacchi malware e l'undicesimo per attacchi ransomware.

I dati emergono da "A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report", il report di Trend Micro Research sulle minacce informatiche che hanno colpito nel corso dell'anno passato.

Nel 2020, in tutto il mondo, Trend Micro ha rilevato 119.000 minacce al minuto, facendo registrare un +20% rispetto al 2019, per un totale di 62,6 miliardi di minacce.

Le cause di questo incremento sono da ricercarsi nel lavoro da remoto che ha determinato l'incremento della pressione cybercriminale su molte infrastrutture.

Gli attacchi alle reti domestiche sono infatti cresciuti del 210% raggiungendo i 2,9 miliardi.

Il phishing continua a essere una delle tattiche più sfruttate dai cybercriminali, il 91% di tutte le minacce è arrivato infatti via email e gli URL unici di phishing intercettati sono stati 14 milioni.

Il numero di vulnerabilità pubblicate dalla Zero Day Initiative di Trend Micro è cresciuto del 40%, per un totale di 1.453 vulnerabilità, l'80% delle quali è stato etichettato "ad alto rischio".

Cosa potrebbe succedere nel 2021?

Secondo gli esperti Trend Micro, i prossimi mesi saranno caratterizzati da una uova ondata di attacchi che colpiranno i software utilizzati per il lavoro da remoto e i sistemi cloud. Le reti domestiche, in particolar modo, verranno utilizzate dai cybercriminali come teste di ponte per compromettere le infrastrutture aziendali e IoT. Il dato emerge dal report "Turning the tide - La marea è salita, è ora di invertire la tendenza".

Lo studio indica che gli utenti che hanno un accesso regolare ai dati sensibili, sono più a rischio. Ad esempio, i professionisti HR che trattano dati personali o i direttori vendite che custodiscono le informazioni dei clienti.

Gli attacchi potrebbero sfruttare vulnerabilità conosciute all'interno dei software di collaborazione online, ma questo una volta rese pubbliche, piuttosto che in modalità zero-days.

I modelli di business cybercriminali "Access-as-a-service" sono destinati a crescere e prenderanno di mira le reti domestiche dei dipendenti, l'IT corporate e le reti IoT.

I team di security dovranno rivedere le policy del lavoro da remoto e le contromisure, per affrontare la complessità degli ambienti ibridi nei quali il lavoro e i dati personali convivono in un unico punto.
Le integrazioni di terze parti sono sempre più importanti, per questo Trend Micro avvisa che le API's esposte diventeranno il nuovo vettore di attacco preferito dai cybercriminali, che avranno così accesso a dati sensibili, codici sorgente e servizi back-end.
Un'altra area dove le minacce persisteranno è quella dei sistemi cloud, tra utenti inconsapevoli, configurazioni errate e criminali intenti a prendere il controllo dei server cloud per distribuire immagini di container dannose.
Come difendersi?

Per affrontare con successo le minacce, gli esperti Trend Micro raccomandano quindi di favorire la user education e i corsi di formazione, controllare severamente gli accessi alle reti corporate e all'home office, rafforzare le misure di security e i programmi di patch management e migliorare il rilevamento delle minacce, aumentando le competenze in materia di sicurezza così come adottando controlli estesi di rilevamento e risposta (XDR).

Photo credit: Unsplash

Factory 4.0: perché potrebbe essere importante avere un sistema di Gestione degli Allarmi

di ***Enzo Maria Tieghi - ServiTecno***

I sistemi di controllo processo ed automazione di fabbrica sono sempre più raffinati, potenti e purtroppo anche complessi.

Le configurazioni attuali, oltre ai PLC e sistemi HMI/SCADA collegati su bus e reti industriali, vedono attuatori e sensori sempre più evoluti ed anche macchine ed impianti con a bordo dispositivi IIoT (Industrial Internet of Things) che generano ulteriori misure, ed allarmi.

Il rischio è che la moltitudine di misure ed allarmi possano diventare un intralcio per gli operatori. Ecco allora alcune domande da porsi:

- Gli operatori di impianto utilizzano correttamente gli allarmi per controllare processi importanti e critici?
- Gli operatori vedono e ricevono troppi allarmi ("inondazione di allarmi") o, peggio, ignorano gli allarmi provenienti dai sistemi HMI/SCADA perché ne arrivano troppi e poco rilevanti?
- Gli operatori hanno i corretti strumenti e lavorano in un ambiente che consenta la concentrazione e un buon processo decisionale?
- Siamo conformi con le regole di sicurezza/safety, obblighi assicurativi e/o a standard del settore?

L'evoluzione dei processi di automazione e il cambiamento delle tecnologie ha fatto diventare il sovraccarico di allarmi un problema diffuso ed i vantaggi di una gestione efficace degli allarmi sono spesso sottovalutati. Un sistema di allarme ben progettato, monitorato e ottimizzato nel tempo migliorerà safety e sicurezza di un impianto, le prestazioni dei macchinari e del sistema di allarme e aumenterà la produttività di un impianto, il tutto con ripercussioni su efficienza, produttività e redditività.

Il tema è conosciuto da tempo e si sono attivati comitati ed organismi internazionali per affrontare in modo sistematico il problema: per questo sono stati rilasciati prima lo standard ISA 18.2 divenuto ANSI, poi EEMUA191 ed in definitiva lo standard IEC62682. (vedi le White Paper specifiche sul sito www.servitecno.it).

Gestione allarmi e ANSI / ISA 18.2

ANSI/ISA 18.2 è uno standard di sicurezza per la gestione degli allarmi sviluppato da ISA (www.isa.org) per diversi settori dell'automazione, come industrie chimiche, petrolchimiche, farmaceutiche, minerarie e metallurgiche, elettriche e manifatturiere, ecc. Lo standard si concentra sulla sicurezza dell'operatore per i sistemi SCADA e presenta il "ciclo di vita della gestione degli allarmi" come linea guida per i requisiti per implementare e gestire efficacemente un sistema di allarme.

Ad esempio, ISA 18.2 consiglia "Monitoraggio e valutazione" come uno dei punti migliori per iniziare a comprendere e migliorare le pratiche di gestione degli allarmi. Gli strumenti di monitoraggio e la valutazione degli allarmi possono evidenziare le aree problematiche al fine di ridurre il "rumore" e migliorare le prestazioni del sistema di allarme, fornire approfondimenti per la manutenzione e la razionalizzazione degli allarmi e supportare la capacità di un operatore di rispondere in modo efficace, riducendo gli incidenti.

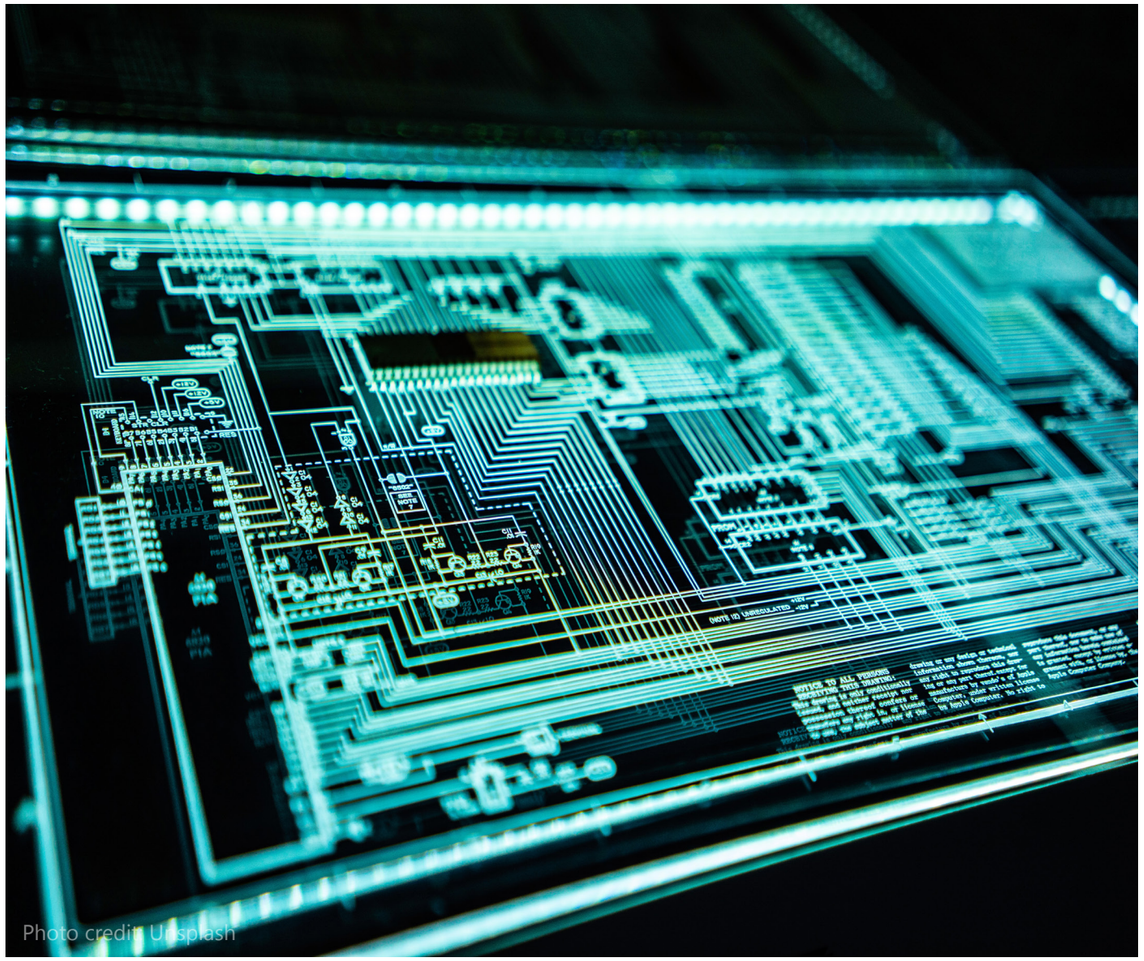


Photo credit: Unsplash

Migliorare la Gestione degli Allarmi con AlarmWatch

AlarmWatch è una soluzione studiata per migliorare le prestazioni del sistema di allarme e aumentare la sicurezza, la produttività e la redditività complessive di un impianto.

AlarmWatch è un componente software dinamico di monitoraggio e reportistica degli allarmi per una gestione efficace degli allarmi, facilmente integrabile con HMI/SCADA iFix di GE Digital, distribuito e supportato da ServiTecno (www.servitecno.it). Progettato per Operatori e Supervisori di impianti industriali e utility per valutare la situazione del proprio sistema di allarme e ridurre il sovraccarico di allarmi dell'operatore in conformità con lo standard ISA 18.2.

AlarmWatch è la soluzione più indicata se non si conoscono in dettaglio le pratiche di gestione degli allarmi secondo ISA18.2 e si renda necessaria una soluzione semplice e conveniente per il monitoraggio continuo delle prestazioni del sistema di allarme, la conformità verso il miglioramento continuo.

AlarmWatch con iFIX Productivity Tools aggrega i dati di allarme e di evento di GE Digital iFIX, analizza i dati di allarme (rispetto alle metriche di allarme consigliate da ISA 18.2) e visualizza il riepilogo degli allarmi su una dashboard interattiva, la "Dashboard KPI di AlarmWatch". Questa soluzione, pronta all'uso consente a Operatori e Supervisori di:

- Raccogliere e Visualizzare le prestazioni del sistema di allarme in pochi secondi.
- Identificare le aree problematiche del sistema e le opportunità di variazioni, ad es. "Bad Actors" e/o allarmi fastidiosi.
- Analisi dettagliata per un'indagine dettagliata.
- Agire in modo mirato ed economico
- Monitorare i miglioramenti del sistema di allarme.
- Monitorare e ricevere informazioni costanti per l'ottimizzazione dei sistemi e dei processi, per raggiungere gli obiettivi di gestione degli allarmi.

AlarmWatch è uno strumento di analisi moderno, semplice ma sofisticato che consente ai manager di intraprendere prontamente azioni per identificare e risolvere problemi di manutenzione, ambito e priorità delle attività per la razionalizzazione degli allarmi, ridurre al minimo il rumore degli allarmi, ridurre il sovraccarico per gli operatori, migliorare le prestazioni e la sicurezza degli allarmi.

Dettagliate funzioni di Reporting, KPI e il confronto dei dati tengono traccia dei progressi e forniscono approfondimenti aziendali chiave per miglioramenti continui.

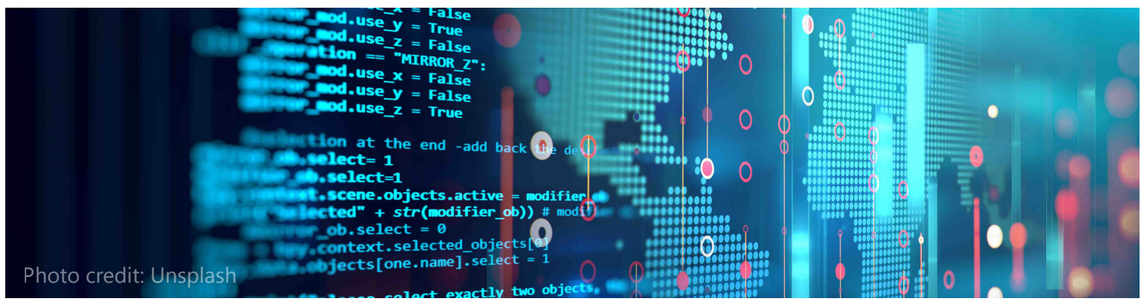


Photo credit: Unsplash

Il ritorno di attualità della qualità e della sicurezza dei dati: la Data governance come disciplina emergente

di ***Carlo Guastone - Sernet***

La governance e la qualità dei dati gestiti nelle aziende stanno assumendo crescente rilevanza per svariate motivazioni, per evidenti esigenze di disporre di informazioni corrette per favorire mirate decisioni di business, per ragioni di efficienza nello svolgimento dei processi interni senza dover impegnare tempi eccessivi nel reperimento e controllo delle informazioni trattate, e, fatto non secondario, per ragioni di compliance alle normative che sempre più richiamano la responsabilità del management aziendale nella "creazione" e "utilizzo" di informazioni che possono determinare, ad esempio, violazioni di sicurezza con possibili sanzioni (come nel caso di GDPR), o errori


Photo credit: Unsplash

nelle pratiche commerciali e negli adempimenti bilancistici. Questo scenario si può applicare a tutte le aziende di tutti i settori economici, ma è particolarmente rilevante per le aziende che appartengono a settori regolamentati come il settore bancario (Circolare Bankit 285/2013) e assicurativo (Regolamento IVASS N° 38 del 2018).

Tali settori hanno da sempre operato come apripista di mercato per svariate motivazioni, fra le quali la presenza di Normative internazionali, in particolare Basilea per il settore bancario e Solvency per il settore assicurativo, che nel tempo si sono focalizzate sull'impatto dei servizi informatici per il business, dall'IT risk management, alla sicurezza informatica, alla business continuity.

Non è casuale che il già citato Regolamento IVASS preveda due sezioni dedicate alla Cybersecurity e alla Data Governance.

Anche alcune Norme (come ISO 25012) e alcuni Framework internazionali (come Cobit19 dedicato all'IT Governance) trattano tematiche riconducibili rispettivamente alla "Qualità dei dati" e al "Data management".

La Norma ISO 25012 "appartiene" alla "famiglia" di Norme ISO 25000 dedicata allo sviluppo software e alla qualità di dati e identificata con la sigla SQuaRE (Systems and Software Quality Requirements and Evaluation).

La Norma ISO 25012 (Data quality model), pubblicata nel 2008 e aggiornata nel 2019, indica 15 requisiti da rispettare nei trattamenti informatici dei dati, descritti all'interno della Norma.

Alcuni di questi requisiti relativi alla sicurezza delle informazioni, come integrità, disponibilità e riservatezza, sono previsti anche da altre Norme ISO dedicate alla sicurezza delle informazioni, alla business continuity e all'IT service management.

E' interessante, al riguardo, considerare che la adozione da parte delle aziende della Norma ISO 25012 può essere oggetto di un Attestato di conformità da parte di Enti di certificazione accreditati e, in questa logica, costituire la comprova di un corretto approccio di "Controllo Interno" in azienda, per quanto relativo ai dati di business sulla base dei quali sono prese decisioni e, fatto non marginale, per le implicazioni di compliance nei trattamenti di dati personali, come ad esempio il principio di "Accountability" richiamato nel Capitolo 5.2 di GDPR.

Il già citato Cobit, nella versione aggiornata nel 2019, ha inserito una specifica sezione dedicata a 10 processi di "Data Management", che rappresentano diversi aspetti da considerare nella progettazione, realizzazione e gestione di applicazioni: definizione di una strategia aziendale e delle responsabilità nella gestione dei dati, stesura di un dizionario dei dati, gestione dei metadati (aspetto rilevante del Regolamento e-Privacy di prossima pubblicazione), strategia di qualità da adottare, profilazione dei dati in termini di metodologie e strumentazione, assessment sulla qualità dei dati, adozione di un approccio di "cleaning" dei dati, identificazione del ciclo di vita del dato, archiviazione e "retention" dei dati, e infine "back up and restore".

Quali le implicazioni per le aziende? Da sempre il dato è stato il "driver" dell'automazione, non a caso l'informatica negli anni sessanta era identificata come "Data processing", e ora con la recente evoluzione delle tecnologie ICT, dalla già diffusa business intelligence, ai Big data, all'Iot, alla digitalizzazione dei processi e alla robotica, all'Intelligenza artificiale, la gestione del dato presenta una rilevanza ancor più fondamentale.

Si potrebbe dire "nulla di nuovo all'orizzonte", considerando che concetti come "modello dei dati", "dizionario dei dati" , "data administrator", erano già pratiche o ruoli di attualità negli anni settanta, epoca di diffusione dei servizi on line e dei data base nei sistemi informatici aziendali.

L'aspetto interessante da considerare è che l'avvento di Internet negli anni novanta non si è accompagnato ad una adeguata attenzione al "dato" da parte delle aziende, come se fosse "scontata" la sua integrità, disponibilità e riservatezza (requisiti fondanti della sicurezza delle informazioni, come già sottolineato).

Il ritorno di attenzione al "dato" è stato favorito negli anni duemila dagli adempimenti di Governance e Compliance richiesti, a vario titolo, alle aziende, che hanno trovato nella disponibilità di Norme e standard internazionali un concreto aiuto per indirizzare le soluzioni richieste.

In questo percorso che sta subendo una forte accelerazione a fronte della incessante evoluzione delle tecnologie e della cybersecurity, l'azienda dovrebbe considerare che l'Informatica non è solo hardware e software, ma anche l'insieme di metodologie che consentano alle organizzazioni di disporre di un patrimonio informativo affidabile, gestito secondo i principi di qualità, sicurezza, efficienza, efficacia e compliance.

Ne deriva, inevitabilmente, l'esigenza di una adeguata sensibilizzazione e formazione su tali tematiche da parte dei manager e professionisti aziendali coinvolti nella costruzione, gestione e utilizzo delle banche dati.

Photo credit: Unsplash

La necessita’ di tenere insieme tecnologia e fattore umano Impreparazione e overconfidence in cybersecurity

di ***Francesco Tieghi e Alessandro Pollini - ServiTecno***

Gli attacchi alla cybersecurity possono colpire qualunque azienda che faccia affidamento su applicazioni, dispositivi e sistemi collegati alla rete; sfruttando qualsiasi tipo di vulnerabilità: siano esse presenti nei software o nei dispositivi, oppure dipendenti dalla persona che li amministra e li utilizza.

E’ ormai un dato consolidato in tutte le ricerche condotte negli ultimi anni, da parte di soggetti come il ClusIT, l’Associazione Italiana per la Sicurezza Informatica, e l’ENISA, The European Union Agency for Cybersecurity, che le principali vulnerabilità rilevate sono riferite ai fattori umani implicati nella cybersecurity.

In particolare si tratta di vulnerabilità legate alla consapevolezza dei collaboratori su policy e buone pratiche di comportamento, alla distrazione, all’accesso in mobilità alle informazioni aziendali, alla presenza di dispositivi mobili personali. Questi dati confermano che tecnologia, organizzazione e consapevolezza individuale devono procedere assieme se vogliamo garantire sicurezza informatica e il fattore umano non può rimanere il principale fattore di rischio e, allo stesso tempo, il fattore più trascurato.

Negli ultimi cinque anni tutti i maggiori attacchi in settori anche molto eterogenei hanno sfruttato la fragilità racchiuse nei comportamenti individuali. Social engineering, phishing, malware nascosti nei plug-in dei browser web, scambio di informazioni sensibili attraverso canali come chat di messaggistica o email private, password scritte sui biglietti: sono tutte pratiche che aprono autostrade per i malintenzionati.

Molte persone hanno le competenze per scaricare un plug-in; poche per capirne la pericolosità: così si diventa “porte di accesso” per i cyber attack.

È un problema di cultura ed è un problema di design. Per quanto riguarda la cultura, quella della sicurezza informatica è bassa in tutta Italia.

Spesso non fanno eccezione neppure realtà del settore IT, per le quali si può cadere nel paradosso dell’overconfidence, ossia un eccesso di fiducia nelle proprie competenze che porta a sottovalutare la probabilità di essere vittima di un attacco informatico.

Le ricerche dimostrano che questa probabilità è alta, ma sopratutto è probabile che moltissime aziende siano già state coinvolte in un attacco, che siano parte di una botnet, o che abbiano una porta di accesso pronta all’uso.

Il problema di design invece è dato dal fatto che non ci sono gli strumenti adeguati che permettano di gestire dati e processi in sicurezza e con facilità. O, almeno, con una facilità compatibile ai ritmi di lavoro.

Quando si parla di ergonomia cognitiva per la digitalizzazione si intende la progettazione di strumenti che si adattino ai limiti, ai bisogni e alle capacità della persona e non adattare la mente alla “forma” di quegli strumenti. In cybersecurity ciò si traduce in due traguardi.

Il primo è lo sviluppo di strumenti informatici sicuri e facili da impiegare; il secondo è la costruzione di una cultura del rischio informatico che raggiunga il livello e la dignità della cultura del rischio di sicurezza in altri settori, come i trasporti e l’aeronautica.

Abbiamo bisogno di audit di sicurezza informatica, abbiamo bisogno di formazione e alfabetizzazione sul rischio digitale, abbiamo bisogno di automatismi che instaurino comportamenti virtuosi.

E’ un processo che richiederà anni, ma possiamo, però, iniziare da un approccio olistico alla cyber security capendo che la sicurezza informatica riguarda un sistema socio-tecnico: è fatto da hardware e umanità.

Se manca un pezzo manca la sicurezza.

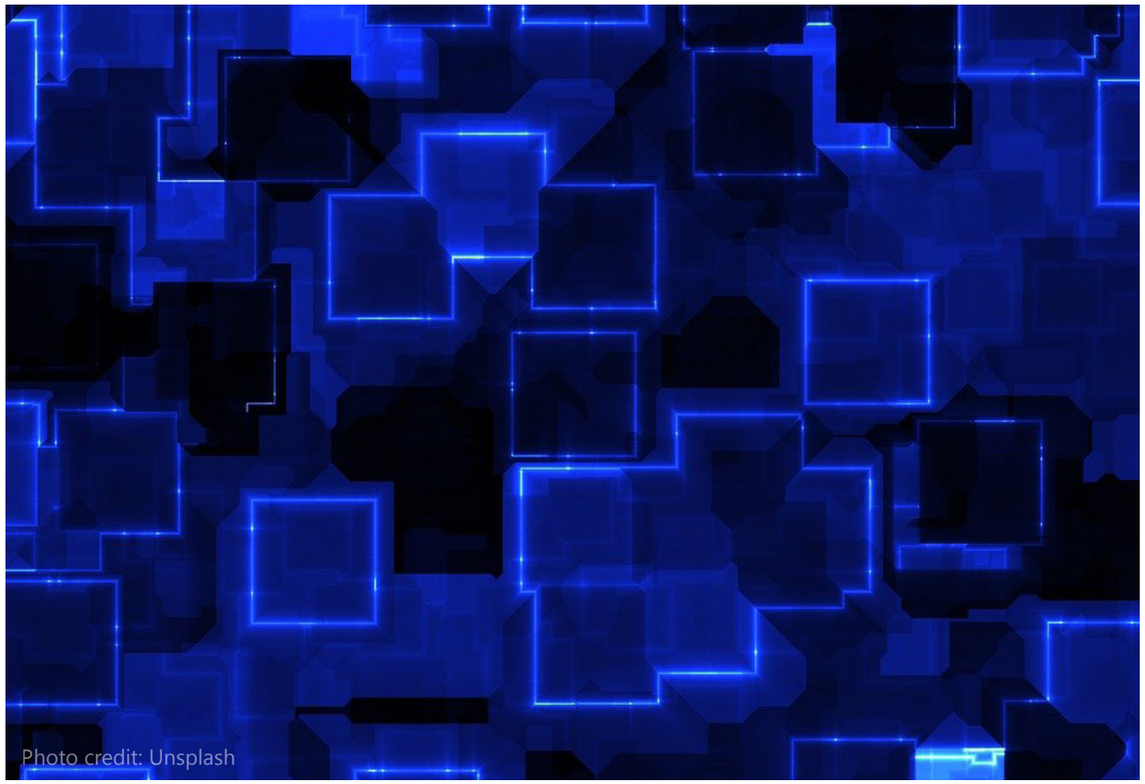


Photo credit: Unsplash

Previsioni sulle minacce per il 2021. Attenzione a privacy, estorsioni e vaccini

di **Kaspersky Lab**

La pandemia ha indubbiamente modificato il nostro stile di vita. Le misure di distanziamento sociale hanno spostato sul web molte attività della vita quotidiana come il lavoro, lo studio, gli acquisti e perfino l'entertainment. Questo ha comportato, inevitabilmente, un ampliamento delle superfici di attacco e nuove opportunità per i cyber criminali.
Solo in Italia, nel 2020, è stata registrata una crescita del 280% degli attacchi di forza bruta sui protocolli RDP (Remote Desktop Protocol) per un totale di 174 miliardi di file dannosi mascherati da applicazioni di comunicazione aziendale.
A causa della pandemia di Covid19 il settore sanitario e la tecnologia sono stati protagonisti indiscussi del 2020. Il notevole aumento del livello di criticità delle infrastrutture mediche, unita all'aumento di una digitalizzazione trasversale, hanno contribuito a rendere il settore sanitario ancora più vulnerabile.
L'utilizzo di tematiche che riguardano il settore sanitario come esca continuerà anche il prossimo anno e rimarrà rilevante almeno fino alla fine della pandemia.
Il motivo principale del crescente interesse degli attaccanti per la ricerca medica è stato lo sviluppo di un vaccino contro il COVID-19. Nel 2021, l'impegno dei criminali per rubare i dati relativi alla ricerca sul coronavirus continuerà.
Finché le organizzazioni sanitarie cercheranno di combattere il virus, qualsiasi azienda che rivendichi un successo significativo nello sviluppo di un vaccino diventerà una potenziale vittima di attacchi mirati.
Anche il furto di cartelle cliniche diventerà parte integrante degli attacchi mirati, poiché la condivisione di informazioni accurate sui pazienti renderà i messaggi falsi molto più credibili. Nel dark web questi dati vengono già venduti ad un prezzo irrisorio: da 0,84 centesimi a 25 euro.
Tuttavia, l'attenzione alla sicurezza digitale negli ospedali offre la speranza che nel 2021 ci possa essere una maggiore collaborazione tra esperti di sicurezza e organizzazioni e sistemi sanitari.
Il 2020 è stato anche l'anno in cui il settore dell'istruzione ha subito una svolta decisiva: 1,5 miliardi di studenti hanno dovuto seguire le lezioni a distanza con educatori costretti a districarsi nel tentativo di padroneggiare nuovi strumenti e, al contempo, mantenere un livello di istruzione alto.
Per molti, questo passaggio all'apprendimento da remoto, è stato improvviso esponendo molti studenti ed educatori ai rischi informatici.
Infatti, da gennaio a giugno 2020, il numero totale di utenti vittima di minacce diffuse sfruttando le popolari piattaforme di apprendimento online e applicazioni di videoconferenza, è stato di 168.550 - un aumento del 20.455% rispetto allo stesso periodo del 2019. Gli esperti di Kaspersky hanno scoperto che questo numero ha continuato a crescere nella seconda parte dell'anno e a gennaio 2021 ha raggiunto i 270.171 utenti con un aumento del 60% rispetto alla prima metà del 2020.
Il processo di digitalizzazione del settore dell'istruzione a cui abbiamo assistito nel 2020 è destinato a continuare anche il prossimo anno.
Da un lato trarremo enormi benefici dalla possibilità di sfruttare nuovi strumenti.
Dall'altro lato però questo però comporterà anche la nascita di nuove minacce per la privacy.
Sarà quindi necessario prestare attenzione e puntare alla formazione degli utenti in tema di cybersecurity.
Guardando al settore finanziario, nel 2021 è probabile che molti cybercriminali prenderanno di mira con maggiore frequenza i Bitcoin, mentre altri criminali informatici chiederanno pagamenti in criptovalute alternative, come Monero, che consentono maggiore privacy.
Aumenteranno anche le pratiche di estorsione sia tramite attacchi DDoS che ransomware, con questi ultimi che si rafforzeranno e utilizzeranno exploit avanzati per colpire le vittime.
Infine, non possiamo non guardare al settore industriale.
Nel 2020 alcuni gruppi criminali hanno esaminato attentamente le caratteristiche delle organizzazioni industriali ottenendo l'accesso a grandi quantità di informazioni sulle loro reti.
Questo trend dovrebbe continuare anche nel 2021.
In particolare, gli attacchi ransomware contro i sistemi ICS diventeranno più mirati e, di conseguenza, ancora più sofisticati grazie alle tattiche APT.
Si tratta di una minaccia significativa, poiché le reti industriali sono diventate più vulnerabili a causa dei limiti imposti sulla presenza dei dipendenti sul luogo di lavoro, unitamente all'aumento del numero di persone che accedono alle reti da remoto.

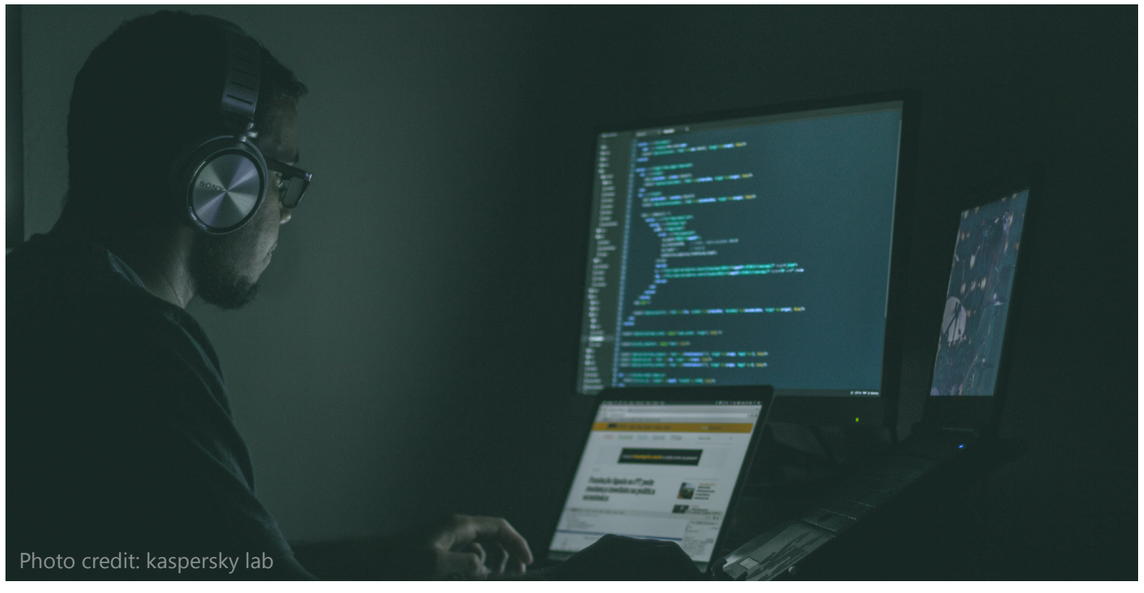


Photo credit: kaspersky lab

Tik tok e minori: Houston abbiamo un problema

Con i suoi video divertenti, creativi e di breve durata Tik Tok si è da subito fatto strada come un social di successo tra i più giovani. Quali, però, i rischi in cui incorrono?

---

di ***Valentina Arena - Ikran Services***

Le perplessità. Sotto il profilo della privacy e del trattamento dei dati non mancano le perplessità sull'utilizzo della piattaforma, che ha anche generato delle conseguenze negative sul piano psicologico e comportamentale dei più piccoli. Proviamo a ripercorrerle brevemente:

- difficoltà/impossibilità di verificare l'effettiva età degli utenti ed estrema facilità con la quale il divieto di iscriversi per i minori sotto i 13 anni risulta aggirabile;
- poca trasparenza e chiarezza nelle informazioni rese agli utenti e uso di impostazioni predefinite non rispettose della privacy: le informative ad oggi presenti sono sin troppo complicate per noi adulti figuriamoci per i ragazzini;
- trasferimento dei dati all'estero: anche se la sede principale della piattaforma è a Dublino vi è la certezza che gran parte dei server della stessa siano ubicati in Cina. Tale circostanza comporterebbe un trasferimento di informazioni ultrasensibili verso un Paese poco avvezzo alla tutela dei dati personali. Per questo, tempo addietro, è stata avviata una formale richiesta di indagine da parte di un senatore statunitense, il quale ha ritenuto che la app costituisca un rischio per la sicurezza nazionale, perché sarebbe usata per "censurare contenuti e mettere a tacere l'aperta discussione su argomenti ritenuti sensibili dal governo cinese e dal Partito comunista, qui l'articolo dell'Ansa. https://www.ansa.it/sito/notizie/tecnologia/software_app/2019/10/10/usa-tiktok-rischia-indagine-per-censura_85257a7c-0719-4652-a02b-b70e2af242ca.html

Il caso

Un recente caso di cronaca ha richiamato l'intervento del Garante. Anche se ancora la dinamica dei fatti non è stata del tutto accertata, la questione origina dalla morte di una ragazza di dieci anni di Palermo: impiccatasi nel bagno di casa con la cinta di un accappatoio, mentre stava partecipando a una blackout challenge.
Si tratta di una prova di resistenza che consiste nel mostrare la propria capacità di resistere maggior tempo possibile con una cintura stretta attorno al proprio collo.

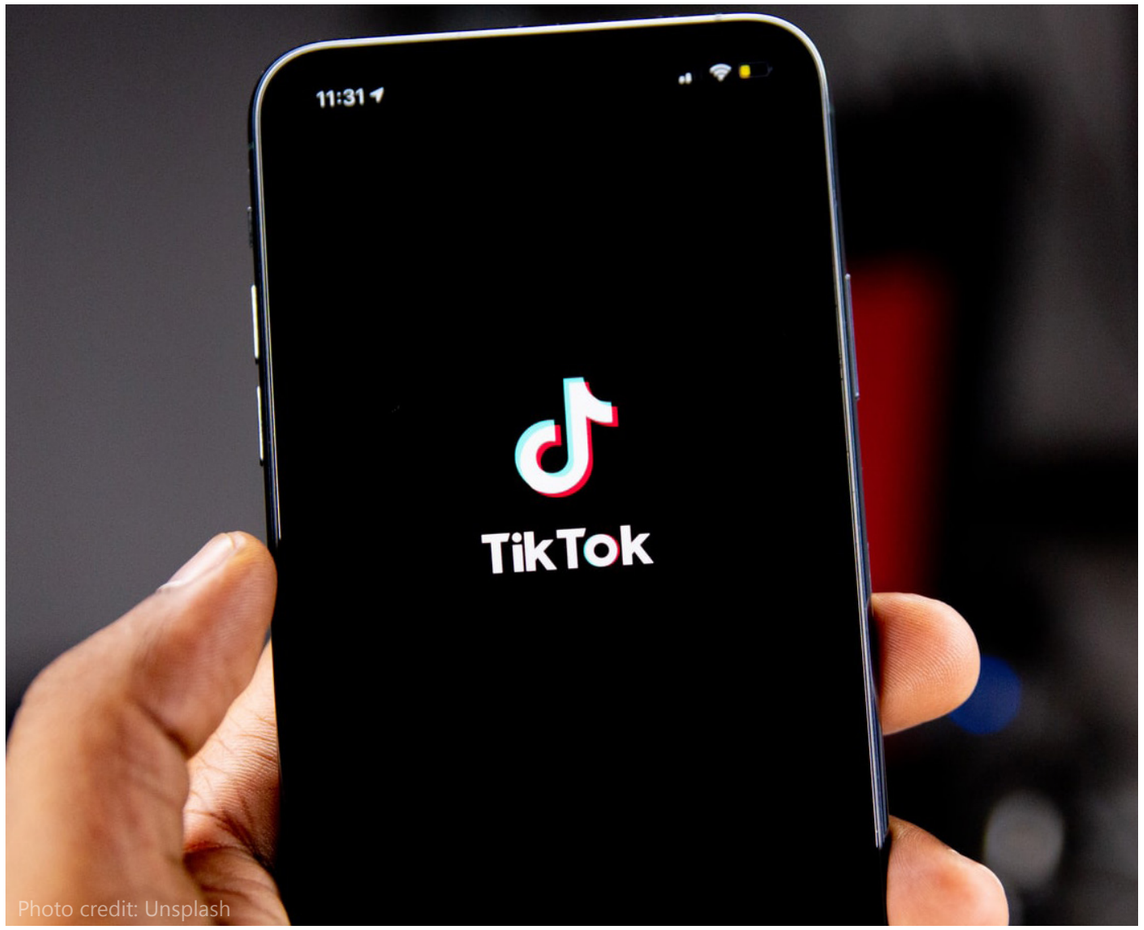


Photo credit: Unsplash

Le tappe del Garante Italiano e la reazione del Social
Il **22 gennaio 2021** il Garante, riprendendo una contestazione già avanzata a dicembre, è corso ai ripari disponendo nei confronti di Tik Tok la misura della limitazione provvisoria del trattamento.

Con provvedimento ha vietato l'ulteriore trattamento dei dati degli utenti che si trovano sul territorio italiano e per i quali non vi sia assoluta certezza dell'età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico;

Il **27 gennaio 2021** l'Autorità ha inoltre aperto un fascicolo su Facebook e Instagram - entrambi utilizzati dalla ragazza di Palermo - con l'intento di comprendere come sia stato possibile, per una minore di 10 anni, iscriversi alle due piattaforme. Nello specifico, ha chiesto ai social di fornire precise indicazioni sulle modalità di iscrizione e sulle eventuali misure adottate per verificare l'età dell'utente (leggi qui: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9527301)

Il **3 febbraio 2021** Tik Tok, in risposta al provvedimento, ha manifestato l'intenzione di:

- fermare, all'ingresso, gli utenti con meno di 13 anni;
- introdurre sistemi di intelligenza artificiale per la verifica dell'età;
- lanciare una campagna informativa per sensibilizzare genitori e figli.

Pertanto, il **9 febbraio 2021** tutti gli utenti italiani saranno bloccati e dovranno indicare di nuovo la data di nascita prima di continuare ad utilizzare l'app. Se verrà identificato un under 13, il suo profilo sarà rimosso.

Leggi la determinazione: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533424

Il commento. Se non hai l'età i social possono attendere

Sono dell'idea che vietare in assoluto agli adolescenti l'utilizzo dei social - qualunque essi siano - oltre a dimostrarsi praticamente impossibile in quanto nativi digitali, possa determinare per gli stessi un effetto ancor più devastante: il loro isolamento.

Non dimentichiamoci che per i più piccoli queste piattaforme, ormai, costituiscono la loro unica rete di relazioni.

Unitamente a ciò, ritengo che non si debba cadere nell'errore di considerare i genitori gli unici responsabili dell'accaduto ed insorgere nei loro confronti al grido di "shame, shame, shame".

Il problema è molto più ampio e riguarda ognuno di noi, nessuno escluso. La realtà è una sola: stiamo normalizzando ciò che ordinario non è.

Fermiamoci un attimo a pensare a quanto sia determinante anche il comportamento di chi, come me non è genitore, a quante volte, senza dar loro la possibilità di scegliere, abbiamo postato foto o video di figli di amici, fratelli, nipotini, cuginetti solo perché presi dall'irrefrenabile voglia di condividere con il resto del mondo la nostra felicità e la loro bellezza; a quante volte (non) abbiamo segnalato ai responsabili delle piattaforme tali anomalie quando, a postare questi contenuti, erano i nostri amici virtuali; a quanti cuoricini e like abbiamo dispensato a neonati e bambini inconsapevoli.

Prima di puntare il dito, dovremmo tutti riflettere e, nel nostro piccolo, porre un freno a tutto questo.

Come istituzione, nell'ottica di sensibilizzare la popolazione sul tema - anche se forse un po' in ritardo - il Garante per la protezione dei dati personali sta facendo la sua parte e realizzato, con Telefono Azzurro, questo spot: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9537523

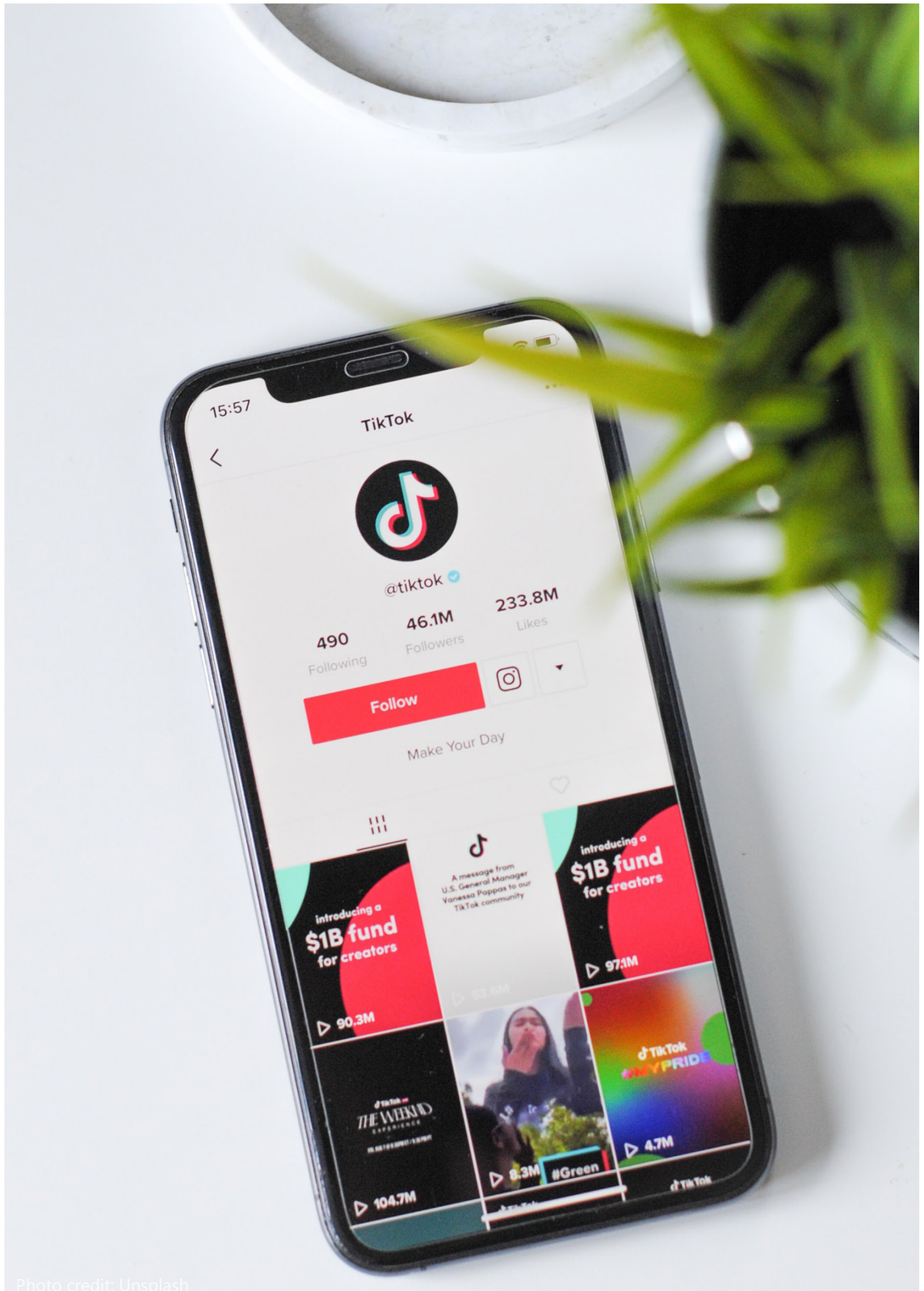
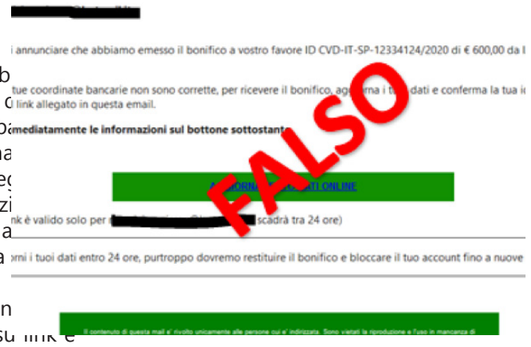


Photo credit: Unsplash

ATTENZIONE: INPS, NUOVA ONDATA DI PHISHING

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



"Siamo lieti di annunciare che abbiamo emesso il b
a vostro favore ID CVD – IT –SP – 12334124/2020 d
600,00 da I.N.P.S. - purtroppo le tue coordinate b
non sono corrette per ricevere il bonifico - aggiorna
dati e conferma la tua identità accedendo al link alle
questa email - Aggiorna immediatamente le informazi
bottone sottostante " È questo il contenuto di e-mail, a
di phishing, inviate in queste ore a ignari utenti con la
di sottrarre fraudolentemente dati sensibili.
Trattandosi di e-mail dal contenuto inaffidabile e ingan
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

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

Anno 2 / Numero 3
2021

CYBER
MAGAZINE

ASSINTEL CYBER SECURITY

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT