Gli incidenti interni alle aziende rappresentano il 54% dei sinistri informatici



Non sono il problema principale in termini di danno economico, ma sicuramente gli incidenti informatici interni, legati ad errori dei dipendenti o guasti ai sistemi, sono estremamente insidiosi e soprattutto sono molto più diffusi di quanti immaginiamo.

Lo studio

Secondo un nuovo rapporto di Allianz Global Corporate & Specialty, dal titolo "***Managing The Impact Of Increasing Interconnectivity – Trends In Cyber Risk***" (Gestire l'impatto della crescente interconnettività – Tendenze nei rischi informatici), le criticità internet alle organizzazioni sono in aumento, anche se in termini finanziari non rappresentano

ancora un grande problema (e forse per questo se ne parla poco).

Gli incidenti interni accidentali, come gli errori dei dipendenti durante lo svolgimento di attività quotidiane, le interruzioni dell'IT o della piattaforma informatica, i problemi di migrazione di sistemi e software o la perdita di dati, **rappresentano oltre la metà dei sinistri informatici analizzati per numero (54%).**

Il peso degli incidenti interni

"*Le perdite derivanti da incidenti come gli attacchi DDoS (Distributed Denial of Service) o le campagne di phishing e ransomware rappresentano oggi la maggior parte del valore dei sinistri informatici*", ha affermato **Catharina Richter**, Global Head dell'Allianz Cyber Center of Competence, integrato in AGCS.

"*La criminalità informatica riempie i titoli dei giornali, tuttavia i guasti quotidiani dei sistemi, le interruzioni dell'IT e gli incidenti dovuti a errori umani possono causare problemi alle aziende, anche se il loro impatto finanziario non è, in media, altrettanto grave*".

Le perdite derivanti da incidenti esterni, come gli attacchi DDoS o le campagne di phishing e malware/ransomware, rappresentano infatti la maggior parte del valore dei sinistri analizzati (85%).

Ne consegue un ricorso crescente alle **cyber assicurazioni** da parte di queste organizzazioni.

Le cyber assicurazioni

Il numero dei sinistri cyber di cui la società è stata interessata è aumentato regolarmente negli ultimi anni, passando da 77 nel 2016, quando il cyber era una linea

assicurativa relativamente nuova, a 809 nel 2019.

Nel 2020 Allianz ha già registrato 770 indennizzi nei primi tre trimestri. Questo costante aumento di sinistri è stato trainato in parte dalla crescita del **mercato globale della cyber-assicurazione** che, secondo Munich Re, è attualmente stimato a **7 miliardi di dollari**.

Il rapporto evidenzia anche un **aumento nell'arco di cinque anni di oltre il 70% del costo medio**, dovuto alla criminalità informatica, fino a 13 milioni di dollari per azienda, e un aumento del 60% del numero medio di violazioni della sicurezza.

> *Gli incidenti interni alle aziende rappresentano il 54% dei sinistri informatici*

Black Friday: italiani pronti a condividere dati personali in cambio di sconti online. Cosa si rischia



Il prossimo 27 novembre sarà il giorno del ***Black Friday*** e per 24 ore si avrà la possibilità di acquistare prodotti a prezzi fortemente scontati.

In realtà diverse grandi catene di negozi hanno già avviato un piano di promozioni, online e negli store, molto accattivante, già dall'inizio del mese di novembre, mentre altre ancora saranno attivate nella settimana che partirà il prossimo 23 novembre, la "*Black week*".

Quindi non solamente una corsa agli acquisti in un solo giorno, come avviene negli Stati Uniti e in altri Paesi anglosassoni, ma una serie di grandi sconti su diversi prodotti spalmati su più giorni per rilanciare un settore duramente colpito dall'emergenza sanitaria in corso.

Black Friday, italiani pronti a

tutto per gli sconti

Secondo una nuova indagine Kaspersky, **l’82% degli utenti italiani è disposto a condividere le proprie informazioni personali con i rivenditori online in cambio di sconti consistenti**.

Considerando che anche le festività natalizie sono ormai alle porte, molti consumatori italiani cercano di approfittare di queste promozioni in rete per massimizzare i risparmi e allo stesso tempo senza rinunciare ai regali.

In poche parole, **nonostante i possibili rischi in termini di sicurezza informatica, meglio correre il rischio di qualche truffa, piuttosto che perdersi gli sconti**.

Solo il 27% degli italiani è consapevole del fatto che nel periodo natalizio o durante le giornate dedicate ai saldi online, le truffe siano più diffuse e ha dichiarato di non essere disposto a correre rischi in cambio di un grande affare.

Il 18%, invece, ha dichiarato che farà gli acquisti di Natale solo da grandi brand per evitare problemi di sicurezza.

Gli utenti davvero consapevoli del fatto che per evitare problemi di sicurezza dovrebbe prestare maggiore attenzione durante gli acquisti online sono praticamente una piccola parte, soprattutto considerando che è proprio durante i periodi di festa che gli **attacchi phishing** si diffondono con maggiore forza.

Ad esempio, **appena un terzo degli italiani (36%) ha affermato di non essere disposto a fare acquisti attraverso siti web che sembrano illegittimi**, mentre **il 27% si dichiara consapevole dei potenziali rischi per la sicurezza** quando si acquista da brand sconosciuti che offrono grandi sconti.

Ma cosa si rischia in termini di sicurezza e privacy? I consigli

Le prossime settimane saranno cruciali per il mondo retail, perchè i brand lanceranno i saldi stagionali in anticipo rispetto a quanto previsto e sarà uno dei *Black Friday* più trafficati di sempre per i rivenditori online.

Anche i cyber truffatori si faranno trovare più pronti del solito per trarre vantaggio dagli acquisti di tutti gli utenti inconsapevoli dei rischi che si corrono.

Il retail phishing è aumentato del 233 % nel 2019, secondo dati Shopify, rivelando che i siti di e-commerce sono obiettivi primari per lo spoofing dei siti web durante le festività natalizie, poiché preparano diligentemente offerte e coupon.

Il phishing è una delle principali pratiche di cyber crime sfruttate per rubare dati sensibili e personali, semplicemente inviando mail fittizie molto appetibili, con lo scopo di far abboccare gli utenti, che rinviano a siti non sicuri. Nel testo della mail è contenuto un link o un banner, gli utenti apriranno uno o l'altro e gli hacker potranno intercettare e rubare i loro dati.

È fondamentale riflettere sul fatto che **non è assolutamente necessario condividere i propri dati personali per ogni acquisto, si tratta solo di un trucco per indurre gli utenti a rivelare le informazioni personali**.

Inoltre, **è necessario assicurarsi sempre che le offerte ricevute siano autentiche** prima di effettuare qualsiasi acquisto.

È sempre **più sicuro digitare manualmente l'indirizzo o selezionarlo dai preferiti piuttosto che cliccare su un link**.

Inoltre, è meglio utilizzare la barra degli indirizzi del browser per verificare che il sito web sia autentico e sicuro.

Quando si ricevono le mail in cui vengono offerti degli sconti sulle vendite controllare sempre il mittente e prima di fare clic su qualsiasi link, verificare che siano legittimi.

> *Black Friday: italiani pronti a condividere dati personali in cambio di sconti online. Cosa si rischia*

La cybersecurity e la gestione delle librerie Open Source nel percorso DevSecOps. Il caso d'uso Inail



Emerasoft e **Sonatype** presentano per la prima volta un evento

digitale live per raccontare e condividere con il pubblico come è possibile implementare al meglio la metodologia **DevSecOps** facendo della sicurezza parte integrante del processo di sviluppo e rilascio delle applicazioni.

Ospite d'eccellenza, per raccontare il caso d'uso **INAIL**, è **Adele Gambacorta**, Responsabile Ufficio Supporto al processo di produzione e Certificazione, Direzione centrale per l'organizzazione digitale.

Iscriviti al webinar

Webinar Emerasoft- Sonatype: Programma

L'evento, in programma il **26 novembre 2020 dalle 15:00 alle 16:30,** sarà sviluppato come una tavola rotonda a cui parteciperanno:

L'evento digitale ha l'obiettivo di condividere un vero e proprio progetto di **trasformazione digitale** che in Inail è nato dall'esigenza di miglioramento del processo di release e deploy management, per poi evolversi nella messa in sicurezza delle librerie Open Source, un vero e proprio punto di attenzione per tutte le Aziende che ambiscono al miglioramento della qualità dei propri servizi e relativa sicurezza, ma soprattutto una presa di coscienza del patrimonio open source detenuto in produzione e degli eventuali rischi a cui si è esposti.

- **Adele Gambacorta**, *Responsabile Ufficio Supporto al processo di produzione e Certificazione, Direzione centrale per l'organizzazione digitale*
- **Marco Pantano,** *DevSecOps consultant, responsabile del progetto DevSecOps di Inail e testimone oculare della progressiva crescita del progetto, parallela all'aumento della sensibilizzazione sul tema cybersecurity*

- **Fabrizio Corsaro**, *Customer Success Engineer at Sonatype*
- Modera: ***Riccardo Bernasconi**, Sales Director di Emerasoft*

Perché partecipare al webinar di Emerasoft – Sonatype

- Per conoscere da vicino una realtà come Inail che in contrasto con le proprie dimensioni, conserva un'attitudine all'innovazione e una elevata cultura della sicurezza applicativa.
- Per scoprire quanto è importante avere una Bill Of Material delle tue applicazioni, e che un'analisi statica del codice non è sufficiente a metterti al riparo da attacchi malevoli.
- È infine prevista una sessione Q&A.

A chi è rivolto:

L'evento digitale è rivolto a tante figure manageriali come:

- CISO
- IT manager
- Quality Manager
- DevOps Manager

Come partecipare

Per partecipare all'evento digitale di Emerasoft e Sonatype clicca qui.

Iscriviti al webinar

> *La cybersecurity e la gestione delle librerie Open Source nel percorso DevSecOps. Il caso d'uso Inail*

Cybercrime, nel 2021 sempre più attacchi hacker a ospedali e sanità. Il report



Un 2020 senza pace per il settore sanitario. Non solo l'intero settore dovrà lottare contro l'emergenza da covid-19 ma anche contro criminali informatici che, attraverso attacchi hacker alla sanità, non daranno tregua a ospedali, strutture mediche e strutture che si occupano dello sviluppo della distribuzione del vaccino contro il virus.

Lo rivela il nuovo rapporto **Security Predictions 2021,** pubblicato da **FireEye**. Il trend, spiegano gli esperti di sicurezza, non diminuirà nel corso del 2021.

Attacchi hacker sanità: ransomware in aumento

Nel corso del 2020 è aumentato il ricorso a ransomware. Anche in questo caso, spiega il report, gli attacchi sono stati mirati alle strutture mediche nel corso della pandemia. Nel 2021 questo genere di minacce informatiche cresceranno ancora di più e più rapidamente, con un aumento delle tipologie e la frequenza degli attacchi.

In Germania, ricordano gli esperti, un decesso di un paziente è stato generato da un ransomware che, avendo bloccato i computer della struttura, ha obbligato i medici a spostare la persona malata in un altro ospedale e quest'ultima è deceduta durante il trasporto.

Cos'e' il ransomware?

Il ransomware è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, "ransom") da pagare per "liberarli".

La richiesta di pagamento, con le relative istruzioni, compare di solito in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All'utente viene minacciosamente comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.

Ci sono due tipi principali di ransomware:

• i cryptor (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);

• i blocker (che bloccano l'accesso al dispositivo infettato).

Come si diffonde?

Anche se in alcuni casi (non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che:

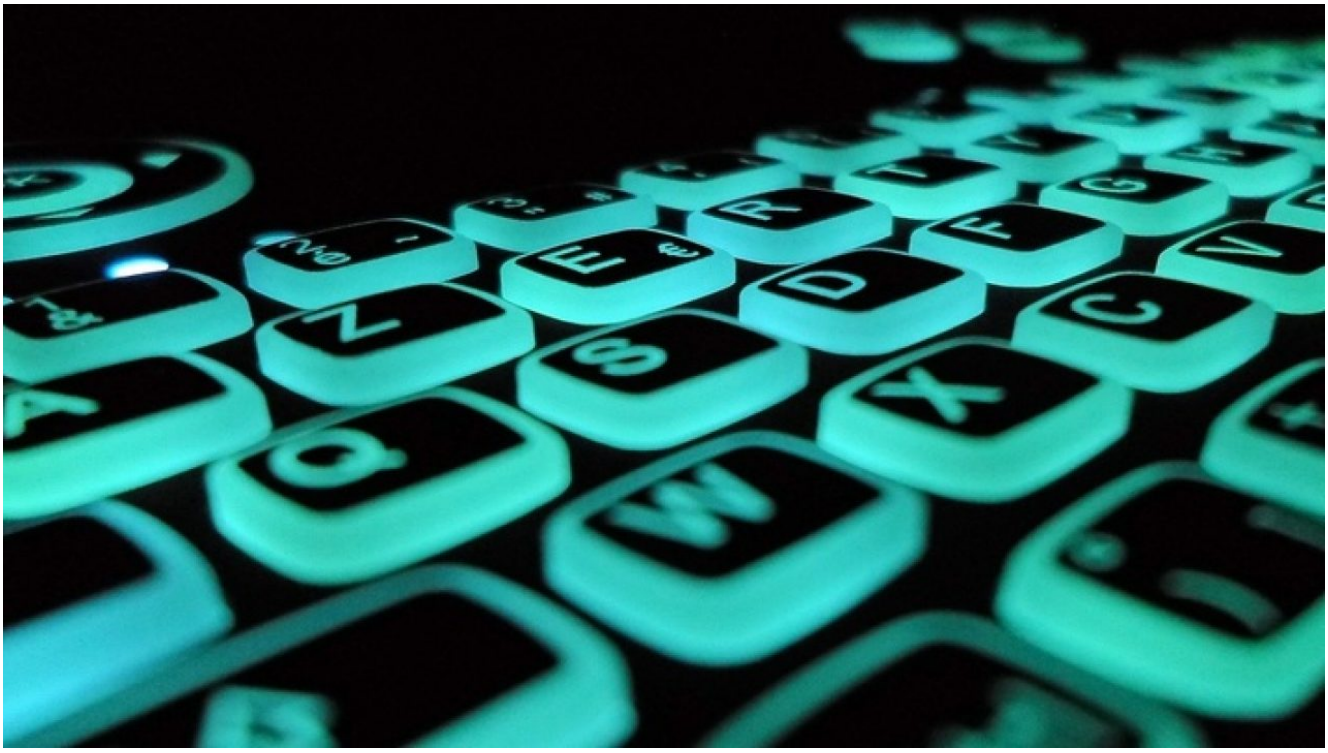
• sembrano apparentemente provenire da **soggetti conosciuti e affidabili** (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);

• contengono **allegati** da aprire (spesso "con urgenza"), oppure **link e banner** da cliccare (per verificare informazioni o ricevere importanti avvisi), ovviamente collegati a software malevoli.

Per approfondire

https://www.key4biz.it/cybercrime-nel-2021-sempre-piu-attacchi-hacker-a-ospedali-e-sanita-il-report/331343/

IoT anello debole della cybersecurity, la Ue corre ai ripari



La filiera dell'IoT è diventata l'anello debole della cybersecurity, tanto da lasciare le aziende potenzialmente esposte a cyberattacchi di ogni tipo a causa di vulnerabilità di ci peraltro non sono nemmeno consapevoli. Ransomware sempre più in agguato; vulnerabilità nascose in dispositivi medicali come pacemaker e microinfusori dell'insulina; crescente diffusione di dispositivi in rete nei veicoli connessi e nei sistemi di trasporto; tutto il mondo della smart home, con tutti i device elettronici di casa che, senza adeguate protezioni, rischiano di trasformarsi in porte aperte per gli hacker.

IoT cybersecurity: linee guida dell'Enisa

E' per contrastare questi rischi sempre più diffusi che l'Unione Europea ha da poco realizzato le nuove linee guida dell'ENISA (European Union Agency for Cybersecurity) in materia di sicurezza ed IoT, per contribuire a proteggere le vulnerabilità legate al nuovo mondo degli oggetti connessi.

Una delle raccomandazioni chiave è che la sicurezza sia

integrata a tutti i livelli delle organizzazioni, fra cui l'egineering, il management, il marketing così che eventuali rischi siano identificabili in tutti gli ambiti aziendali.

Security by design

Un'altra raccomandazione dell'Enisa è che si adotti la "*security by design*" a tutti i livelli del processo di sviluppo dell'IoT.

Un altro aspetto importante per contrastare eventuali problemi di sicurezza è la comunicazione fra le diverse fasi di sviluppo di nuove soluzioni di prodotto, per evitare vuoti e buchi neri di comunicazione o carenza di coordinazione fra fornitori di componenti, produttori e IoT vendor.

Detto questo, non tutte le responsabilità dovranno essere date ai produttori IoT.

Anche clienti e i fruitori delle applicazioni dovranno dire la lro per migliorare i livelli di affidabilità delle soluzioni.

Secondo l'ENISA, sono 10 i principali trend del cybercrime

1. L'area o meglio la superficie di potenziali cyberattacchi continua ad espandersi con l'avvicinarsi di una nuova fase della trasformazione digitale.
2. Ci sarà una nuova normalità sociale ed economica dopo la pandemia COVID-19 ancora più dipendente da un cyberspazio sicuro e affidabile.
3. L'utilizzo di piattaforme di social media in attacchi mirati è una tendenza seria e raggiunge diversi domini e tipi di minacce.
4. Attacchi mirati e persistenti su dati di alto valore (ad es. Proprietà intellettuale e segreti di stato) vengono pianificati ed eseguiti meticolosamente da attori

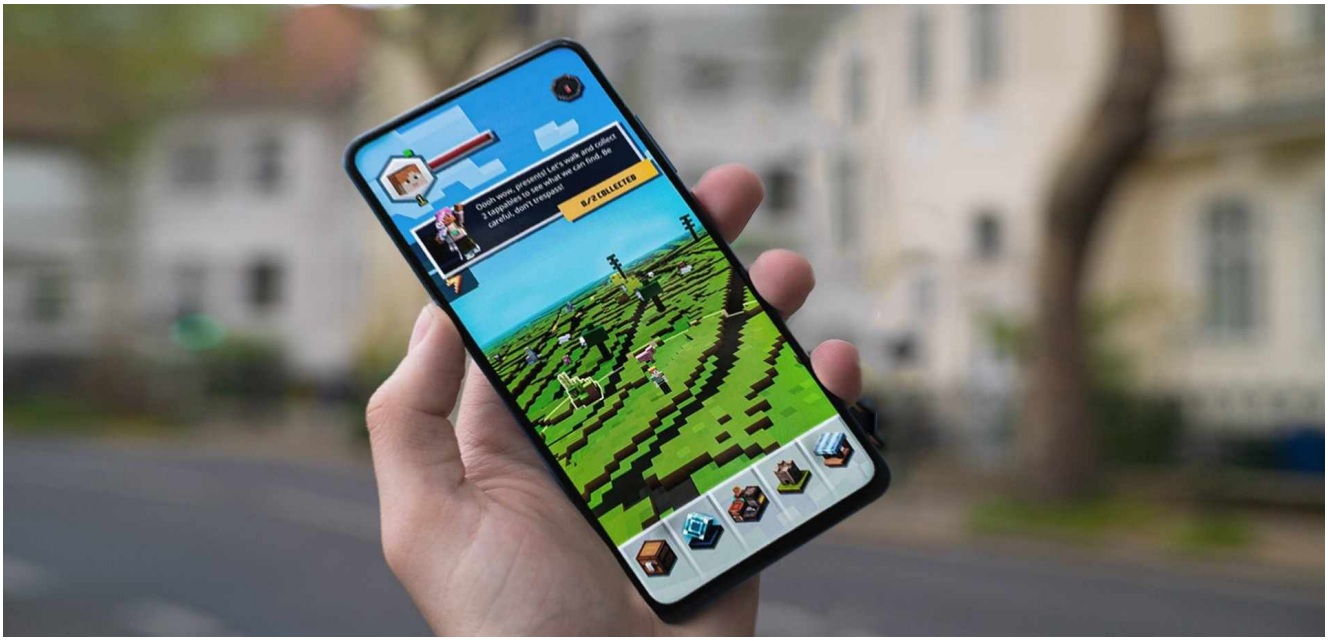
sponsorizzati dallo stato

5. Gli attacchi distribuiti in modo massiccio con una breve durata e un ampio impatto vengono utilizzati con molteplici obiettivi come il furto di credenziali.
6. La motivazione alla base della maggior parte degli attacchi informatici resta ancora quella finanziaria.
7. Il ransomware rimane sempre diffuso con conseguenze costose per molte organizzazioni.
8. Ancora molti incidenti di sicurezza informatica passano inosservati o richiedono molto tempo per essere rilevati.
9. Con una maggiore automazione della sicurezza, le organizzazioni investiranno di più nella preparazione utilizzando la Cyber □□Threat Intelligence
10. Il numero di vittime di phishing continua a crescere poiché sfrutta la dimensione umana che è l'anello più debole.

Per saperne di più: IoT

IoT anello debole della cybersecurity, la Ue corre ai ripari

App dannose su Google Play, truffati 5 milioni di utenti del gioco Minecraft



Più di 5 milioni di utenti del popolare videogioco “***Minecraft***” sono stati vittime inconsapevoli di diverse applicazioni mobili hackerate.

Sette le app dannose individuate dall’indagine Avast che hanno coinvolto milioni di *gamers* in tutto il mondo e offerte in download su **Google Play**.

Si tratta di frodi perpetrate attraverso la tecnica detta “***fleeceware***“, dove si offrono nuove skin, sfondi colorati o modifiche per il gioco, ma addebitando in maniera illecita agli utenti fino a centinaia di euro al mese.

Il team di ricercatori ha reso di noto di aver segnalato queste app a Google, ma al momento sembra siano tutte ancora attive.

Queste le fake app individuate dal Rapporto:

- ***Skins, Mods, Maps for Minecraft PE***, scaricata oltre 1 milione di volte, addebitava 30 dollari a settimana;
- ***Skins for Roblox***, scaricata oltre 1 milione di volte, addebitava 30 dollari a settimana;
- ***Live Wallpapers HD & 3D Background***, scaricata oltre 100.000 volte, addebitava 90 dollari l’anno;
- ***MasterCraft for Minecraft***, scaricata oltre 1 milione di

volte, addebitava 30 dollari a settimana;
- ***Master for Minecraft***, scaricata oltre 1 milione di volte, addebitava 30 dollari a settimana;
- ***Boys and Girls Skins***, scaricata oltre 1 milione di volte, addebitava 30 dollari a settimana;
- ***Maps Skins and Mods for Minecraft***, scaricata oltre 100.000 volte, addebitava 30 dollari a settimana.

La tecnica "*fleeceware*" è una categoria relativamente nuova di cybercrime ed è sfruttata per offrire agli utenti un servizio molto accattivante, di solito per un breve periodo di prova gratuito di pochi giorni.

Il problema arriva dopo, quando l'app inizia automaticamente e senza dare nell'occhio ad addebitare al malcapitato utente costi eccessivi, fino a 30 dollari a settimana.

Nel caso in cui si sospetti di aver installato un'app del genere, è suggerito dalla ricerca, non è sufficiente disinstallarla ma è necessario annullare l'abbonamento direttamente nel Google Play Store.

https://www.key4biz.it/app-dannose-su-google-play-truffati-5-milioni-di-utenti-del-gioco-minecraft/331037/

Cyber crime, cosa ci riserva il futuro?



L’ultimo rapporto FortiGuard Labs, partendo da un’attenta osservazione degli sviluppi significativi nel panorama delle minacce informatiche nel 2020 a livello globale, comprendendone dinamiche e trend, riporta delle previsioni molto verosimili sui nuovi strumenti e strategie che potrebbero essere disponibili ai criminal hacker nel breve e nel lungo termine.

Tale scenario, come si evince dal documento “Cyber Threat Predictions for 2021”, risulta principalmente influenzato dalle evoluzioni implementative che subiranno i malware e gli attacchi informatici in genere alla luce delle nuove potenzialità offerte dal 5G, dal quantum computing e dall’intelligenza artificiale (AI) e machine learning (ML), tutte opportunità sfruttabili anche dal cyber crime.

Ecco alcuni spunti interessanti che aziende ed organizzazioni dovrebbero prendere seriamente in considerazione.

Evoluzione del malware e dell’ingegneria sociale

Gli smart worker con le loro risorse domestiche, continueranno a rappresentare, per i criminali informatici, degli obiettivi sensibili da utilizzare come teste di ponte preferenziali per sferrare attacchi, attentamente coordinati, alle reti aziendali. Il malware avanzato del prossimo futuro potrebbe anche essere in grado di carpire dati sensibili e ricavare preferenze e abitudini delle vittime attraverso gli Edge Access Trojan (EAT) ovvero una nuova entità spyware distribuita e capace d’intercettazioni e compromissioni più invasive.

In tal senso non fa eccezione nemmeno il mercato degli strumenti cyber estorsivi con le famiglie dei ransomware che continueranno a evolversi e a colpire i sistemi di tecnologia operativa (OT) e in particolare le infrastrutture critiche che, coinvolgendo maggiormente i sistemi IT e estendendo la superfice di attacco, mettono a rischio ancor più dati, dispositivi e spesso, in base ai settori, anche vite umane.

Anche i dispositivi IoT e i sistemi domestici, che interagiscono con gli utenti, non saranno più dei semplici bersagli, ma rappresenteranno loro stessi dei canali di attacco più insidiosi, rendendo più efficace anche il social engineering.

Gli attacchi swarm-based e il 5G

La trasformazione digitale in atto in questi anni ha esteso, e in modo particolare durante questa fase emergenziale, ciò che tradizionalmente viene definito perimetro di rete con nuovi ambienti cloud, smart e IoT ciascuno dei quali, portando con sé dei rischi intrinseci che vanno ad aggiungersi a quelli preesistenti, hanno finito con l’esporre maggiormente la

superfice di rete estesa potenzialmente attaccabile. Di conseguenza, il cyber crime sta evolvendo le proprie strategie offensive contro questi ambienti cercando di sfruttare la velocità e la scalabilità offerte dal 5G, aprendo delle opportunità per minacce più avanzate e il dispiegamento di attacchi swarm-based. I criminali informatici, in tal senso, stanno compiendo notevoli progressi per compromettere e dirottare i dispositivi abilitati per il 5G anche se con tecnologie che richiedono comunque una certa potenza di elaborazione per abilitare i singoli swarmbot e condividere in modo efficiente le informazioni.

Innovazioni nelle prestazioni di elaborazione a scopo di lucro

Il rapporto stilato prevede anche l'evolversi di altri tipi di attacchi che, attraverso l'amplificazione delle prestazioni di elaborazione e di connettività, avranno l'unico scopo di accrescere i profitti illeciti dei criminal hacker coinvolgendo e sfruttando nuovi ambiti per migliorare l'efficienza del cryptomining, estendere su larga scala il bacino dei target e scardinare gli algoritmi di crittografia asimmetrica.

La potenza di elaborazione assumerà un valore sempre più prezioso qualora si volessero scalare attacchi futuri basati sul machine learning e l'intelligenza artificiale in grado di gestire enormi quantità di dati e consentire anche un maggiore rendimento del mining.

Anche la connettività dei sistemi satellitari e delle telecomunicazioni in generale potrebbe essere una ulteriore arma interessante per i criminali informatici. Una compromissione delle stazioni base e la successiva diffusione di malware attraverso le reti satellitari potrebbero dare agli aggressori la possibilità di prendere di mira milioni di utenti connessi su larga scala e infliggere attacchi DDoS

devastanti.

Dal punto di vista della sicurezza informatica, infine, il quantum computing è candidato a generare un nuovo rischio. Anche se non alla portata di tutti, l'enorme potenza di calcolo dei computer quantistici, infatti, potrebbe rendere risolvibili alcuni algoritmi di crittografia asimmetrica. Di conseguenza, le organizzazioni dovrebbero quanto prima adottare delle strategie di agilità crittografica elaborando algoritmi crittografici più resistenti.

Le future armi di difesa

Sicuramente l'evoluzione dell'intelligenza artificiale, potenziando le future tecnologie capaci di prevedere e reagire con nodi di apprendimento locali (machine learning), sarà fondamentale per la difesa contro queste tipologie di attacchi in continua evoluzione e con velocità di propagazione sempre più performanti.

Con questo tipo di approccio sarà possibile, fornendo ai sistemi d'intelligenza artificiale informazioni sulle tattiche, tecniche e procedure (TTP) degli attori delle minacce e dettagliate mappe sinottiche, rilevare i modelli di attacco e intervenire in modo proattivo offuscando gli obiettivi sensibili.

Purtroppo è solo questione di tempo ed è ragionevole pensare che molte di queste tendenze del crimine informatico diventeranno gradualmente realtà, anche tramite risorse mercificate e rese disponibili nei marketplace underground.

Pertanto, come dicono gli stessi ricercatori, sarà necessaria un'attenta combinazione di tecnologie, di persone, di formazione e di partnership per proteggersi dal cyber crime del futuro.

Cyber crime, cosa ci riserva il futuro?

L’insostenibile insicurezza del software. Videointervista a Serafini (ENTRUST) e a Bucci (N.I.D.O.)

“L’insostenibile insicurezza del software. Moduli hardware (HSM) e blockchain per la protezione dei dati e garanzia di compliance” è il titolo del webinar che si terrà il 19 novembre 2020 dalle ore 10-30 – 11:30.
Alcuni dei temi del webinar, come l’insicurezza del software per la gestione delle chiavi crittografiche e la sua valida alternativa (i moduli hardware), e l’utilizzo della blockchain per l’erogazione delle identità digitali, sono stati discussi durante la videointervista a **Claudio Serafini**, Sales Engineering Manager Southern Europe – **ENTRUST** e a **Osvaldo Bucci**, Direttore Commerciale, Divisione Digital Security – **N.I.D.O. SpA**.

[embedded content]
I temi saranno illustrati in modo approfondito durante il webinar, in cui sarà spiegato:

- qual è la migliore tecnologia per gestire la rete di trasporto di bonifici istantanei, ossia la modalità di pagamento che consente di ricevere l’importo in meno di 10 secondi, a qualsiasi ora e ogni giorno della settimana.
- E come è possibile con la blockchain dar vita sia a una firma elettronica avanzata, da usare nel **B2B** e **B2C**, sia a **eID**, **identità auto-sovrane** ed **eDelivery**”

I 4 relatori del webinar



WEBINAR

19 novembre 2020 | 10:30 – 11:30

Il form per iscriversi al webinar

Registrati

> *L'insostenibile insicurezza del software. Videointervista a Serafini (ENTRUST) e a Bucci (N.I.D.O.)*

Deepfake: come possono difendersi le aziende?

Nov 11, 2020 Manuela Santini Approfondimenti, Minacce,

Scenario, Women for Security 0

L’utilizzo di app basate su algoritmi di AI per la manipolazione di immagini, video e audio è in aumento. Eppure, non sempre le aziende che sviluppano tali app tengono conto dei rischi a cui potrebbero essere esposti gli utenti. Uno dei maggiori pericoli deriva dall’utilizzo delle app per creare falsi di altissimo livello, noti come “**deepfake**”.

Sostituire i visi delle persone in video ed immagini (face swapping) e manipolare contenuti audio (audio deepfake) è oggi alla portata di tutti: con qualche click e secondo di attesa, è possibile realizzare video falsi di buona qualità, magari pensando ad un semplice scherzo tra amici. Ma le conseguenze possono essere ben più gravi.



Il revenge porn ha trovato un nuovo alleato in applicazioni come DeepNude, che permettono di spogliare le donne e poi

condividerne la nuova immagine. I danni reputazionali, psicologici e più in generale gli impatti sulla vita privata delle persone oggetto di tali foto non sono spesso presi in considerazione da chi sviluppa e utilizza le app. Ad essere colpiti sono spesso singoli individui, in particolare le donne, ma anche le aziende possono pagarne il prezzo perché immagini e video manipolati possono essere sfruttati per carpire segreti industriali, cambiare politiche aziendali o arrecare un danno di immagine a un'azienda.

Come difendersi da tutto ciò?

Per le aziende la strategia di difesa non può che basarsi su un *processo di gestione del rischio.* Tecnologie di deep learning dovrebbero essere progettate e utilizzate con prudenza da parte delle aziende, prestando attenzione ad esigenze di business come anche ai rischi per i diritti e le libertà degli utenti.

Per difendersi dai deepfake esistono specifiche tecniche basate sull'intelligenza artificiale: dall'**inserimento di pixel di disturbo** in grado di impedire la manipolazione dei video, all'analisi di fotogrammi specifici allo scopo di **rilevare eventuali distorsioni dell'immagine** frutto di manipolazione, fino all'**analisi dello spettro acustico** alla ricerca di frequenze non compatibili con il parlato naturale di una persona.

Tuttavia, come spesso accade, con la nascita di tecnologie capaci di contrastare una minaccia, la minaccia stessa tende ad evolvere. È perciò fondamentale garantire un'adeguata **formazione e sensibilizzazione del personale aziendale** su come gestire informazioni riservate e/o privilegiate.

Un contributo importante in tal senso può provenire da soluzioni di people engagement che permettano ai dipendenti di sentirsi parte attiva della propria organizzazione ed elemento fondamentale nella gestione della sicurezza delle informazioni

in azienda. Le attività di formazione e sensibilizzazione dovrebbero coinvolgere chiunque utilizzi sistemi di social network o piattaforme di instant messaging (es. whatsapp, telegram, etc.), le quali rappresentano oggi i principali veicoli di trasmissione dei deepfake.

Il messaggio deve essere chiaro: caricando un'immagine, un audio o un video in un'app, si rischia di perderne il controllo. Occorre quindi verificare la fonte dei contenuti multimediali che si ricevono e al minimo dubbio sulla loro autenticità evitare di condividerli.

Condividi l'articolo

Attacco a Campari: il riscatto chiesto da un account Facebook
CyberArk usa l'AI per individuare i permessi eccessivi sul cloud

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/11/11/deepfake-come-possono-difendersi-le-aziende/?utm_source=rss&utm_medium=rss&utm_campaign=deepfake-come-possono-difendersi-le-aziende

---

Ue blocca export di prodotti

di cybersorveglianza a regimi totalitari



L’Unione Europea ha varato un pacchetto di norme che riguardano il blocco dell’export di prodotti di cybersorveglianza verso regimi repressivi in paesi totalitari extra europei.

Lo scrive *Euractiv*, precisando che Parlamento e Consiglio Ue hanno trovato un accordo dopo quattro anni di negoziati, anche se la decisione finale sul blocco delle esportazioni di tecnologie di cybersorveglianza, come ad esempio quelle di riconoscimento facciale, spetterà agli stati membri.

Lunedì, i negoziatori del Parlamento e del Consiglio hanno convenuto che i beni di sorveglianza informatica che consentono la *“sorveglianza segreta delle persone fisiche mediante il monitoraggio, l’estrazione, la raccolta o l’analisi dei dati, compresi i dati biometrici”* dovrebbero

rientrare nelle nuove restrizioni all’esportazione.

La Germania cambia idea

L’accordo chiude un negoziato di quattro anni su termini delle restrizioni all’export per i prodotti di cybersorveglianza, apparentemente prolungato per le resistenze tedesche che rappresenta circa il 50%-60% dell’export europeodi cosiddetti dispositivi duali.

La posizone della Germania si sarebbe ammorbidita dopo la conclusione del cosiddetto scandalo FiniFisher. Nel 2018 è emerso che la società tedesca **FiniFisher** avrebbe venduto prodotti al governo turco senza permesso. Prodotti che sarebbero serviti a sorvegliare i membri dell’opposizione nel 2017, nascosti all’interno dei loro smartphone.

Per saperne di più: UE

> *Ue blocca export di prodotti di cybersorveglianza a regimi totalitari*