Cybercrime e vacanze, 5 consigli di sicurezza per un’estate sicura

Furto dei dati, violazione della privacy e perdite di denaro, dalla pubblica amministrazione alla finanza passando per la sanità. Se il 2020 è stato un annus horribilis per l’intero pianeta a causa della pandemia, nel 2021 stiamo vedendo che non è certo andata meglio nel mondo della sicurezza informatica a causa degli effetti collaterali della pandemia stessa. Tra la migrazione forzata del lavoro nelle case e l’emergenza vissuta negli ospedali, i criminali informatici hanno infatti avuto la vita più facile del solito. E a tendere il rischio è che, in assenza di contromisure adeguate, la forbice tra attacco e difesa possa allargarsi ulteriormente.

Adesso, in piena estate, il rischio aumenta. I criminali informatici infatti amano questi periodi, durante i quali le persone si svagano e calano la propria attenzione. E allora ecco i 5 consigli per non cadere vittima degli attacchi informatici durante le vacanze:

1. **Evita i Wi-Fi pubblici.** L’accesso wi-fi gratuito è allettante, ma può anche rappresentare una seria minaccia per la sicurezza. È possibile che gli hacker attendano ai bar o negli aeroporti, che i viaggiatori si connettano al wi-fi pubblico, in modo da poter colpire gli ingenui. Evita le reti wi-fi non criptate: deve essere sempre richiesto un protocollo di sicurezza prima di connettersi al web. Sii molto prudente quando usi il wi-fi gratuito – e, se devi usarlo, evita di accedere ad account personali o dati sensibili.

2. **Fai attenzione ai curiosi.** La persona seduta accanto a te sull'aereo o mentre aspetti l'imbarco potrebbe avere cattive intenzioni. Qualcuno può guardarti alle spalle mentre inserisci i dati della carta di credito o mentre ti registri sui social media. Procurati una protezione per la privacy dello schermo, che aiuta a nascondere il tuo dispositivo da occhi indiscreti.
3. **Controlla due volte i siti web su cui prenoti i viaggi.** Questi attacchi possono verificarsi anche prima che il viaggio inizi: assicurati che il sito web per le varie prenotazioni sia affidabile. I truffatori amano imitare i siti autentici e fingere di offrire vacanze di lusso o viaggi scontati, al fine di rubare le tue informazioni personali. Se un affare sembra troppo bello per essere vero, probabilmente lo è. Prima di andare avanti, fate una ricerca approfondita sull'azienda che offre l'affare. Usa una carta di credito per i pagamenti piuttosto che la tua carta di debito. Le carte di credito spesso hanno protezioni contro le frodi nel caso in cui tu cada vittima di un cyber crimine; mentre con una carta di debito, i tuoi soldi probabilmente li perderai.
4. **Diffida dei bancomat.** Evita di prelevare denaro da qualsiasi bancomat. Gli hacker, specialmente nelle zone turistiche, sono noti per inserire dei sistemi di furto delle credenziali delle carte di credito nei bancomat indipendenti. Usa i bancomat ufficiali della banca, preferibilmente quelli situati nell'atrio della tua banca di fiducia.
5. **Non condividere la tua posizione.** Condividere la tua posizione con i tuoi amici sui social media è divertente, ma è anche pericoloso. Evita di annunciare le date e il luogo delle tue vacanze sui social media e negli "out of office". Questo non è solo un invito a tutti i criminali "offline", ma fornisce anche indizi agli hacker per mettere in scena attacchi informatici.

https://www.key4biz.it/cybercrime-e-vacanze-5-consigli-di-sicurezza-per-unestate-sicura/371165/

I peggiori “hack” alle Smart home degli ultimi anni

Quando Adam e Heather Schreck si sono svegliati nel cuore della notte per un forte rumore proveniente dalla stanza del figlio, non era il solito pianto del loro bambino di 10 mesi. Precipitandosi nella sua stanza, i genitori si resero conto, con loro stupore e paura, che il rumore era la voce di un uomo adulto che gridava “Svegliati!” e che proveniva dalla loro baby monitor.

La parte peggiore? Non appena sono entrati nella stanza, la videocamera ha distolto lo sguardo dal bambino e dai genitori, in modo automatico. Per una baby monitor, programmata solo per sorvegliare il bambino, questa azione significava solo una cosa: la videocamera era stata hackerata e qualcuno ne aveva preso il controllo tramite Internet.

Questo incidente scioccante si è verificato nel 2014 ed è stato purtroppo solo il primo di molti attacchi alle smart home. Ora, nel 2021, gli hacker sono più sofisticati e pericolosi. Per capire l’impatto che possono avere sulle case moderne, ecco una carrellata dei più noti eventi che si sono verificati in tutto il mondo negli ultimi anni.

Il più grande hijack di sempre

Nel 2016, un vasto attacco informatico che ha sfruttato le vulnerabilità dei DVR e delle webcam smart ha messo in ginocchio gran parte delle reti Internet in Europa e negli Stati Uniti, poiché centinaia di migliaia di dispositivi sono stati compromessi attraverso ciò che gli esperti di sicurezza definiscono come un attacco DDoS (Distributed Denial of Service), utilizzando le botnet Mirai.

In parole povere, gli aggressori hanno hackerato i dispositivi connessi e li hanno usati per sopraffare i server di Dyn, una società che in precedenza controllava gran parte dell'infrastruttura del sistema dei nomi di dominio (DNS) di Internet, con il traffico. Il risultato? Siti web tra cui Twitter, The Guardian, Netflix, Reddit, CNN e molti altri in Europa e negli Stati Uniti sono stati bloccati per gran parte della giornata.

Molti ritengono che l'attacco con la botnet Mirai sia stato il più grande attacco DDoS del suo genere, rappresentando un campanello d'allarme per le autorità del caso e per i produttori di dispositivi. Quindi, avere una protezione IoT per le smart home più forte e completa a livello di rete, non dovrebbe essere solo la priorità degli utenti.

Smart home: il sistema di riscaldamento che si è "congelato"

Un altro attacco DDoS (Distributed Denial of Service) che ha fatto notizia nel 2016 ha coinvolto due condomini a Lappeenranta, una città con una popolazione di circa 60.000 persone nella Finlandia orientale.

Questa volta, l'attacco ha preso di mira i sistemi che controllavano il riscaldamento centralizzato e la circolazione dell'acqua calda negli edifici. Forzando i sistemi di

riscaldamento a entrare in un ciclo di riavvio senza fine, gli hacker hanno bloccato il riscaldamento ai residenti, in un momento in cui le temperature in Finlandia erano sotto lo zero. Lo stesso sistema che è stato sviluppato per supportare l'automazione e ridurre le inefficienze e i disagi del riscaldamento a manutenzione manuale ha lasciato i residenti al freddo.

Per fortuna, una volta che i sistemi delle case smart interessate sono stati disconnessi da Internet, il riscaldamento ha ripreso a funzionare normalmente. Sembra una soluzione semplice, ma sarebbe come non voler guardare in faccia la realtà. Il vero problema risiede nell'atteggiamento delle persone nei confronti della sicurezza dei dispositivi intelligenti. Molte società immobiliari o proprietari privati, infatti, non vogliono investire in firewall di rete e la sicurezza in generale tende a essere permissiva.

Tuttavia, non è solo il riscaldamento smart che è vulnerabile agli attacchi. Anche i termostati di famosi brand sono stati vittime degli hacker. I malintenzionati possono prendere il controllo da remoto e alzare la temperatura quando si è lontani da casa, per esempio.

La scommessa IoT che non ha dato i suoi frutti

Sebbene non abbia tecnicamente influenzato una smart home, questo tipo di attacco potrebbe facilmente coinvolgere persone appassionate di acquari. Nel 2018, un casinò è stato hackerato tramite un termometro smart dell'acquario nella loro hall.

Secondo Nicole Eagan, CEO di Darktrace, società di sicurezza informatica, gli hacker hanno utilizzato il termometro connesso a Internet per entrare nella rete, e "hanno trovato il database high-roller e poi lo hanno ritrasmesso attraverso la rete, dal termostato fino al cloud."

Questo può benissimo accadere a una carta di credito e alle credenziali degli utenti. All'improvviso, rendere la casa più smart non sembra così attraente; però, esistono diversi modi grazie ai quali gli utenti possono potenziarne la sicurezza e difendersi dagli hacker. L'app mydlink di D-Link, ad esempio, consente agli utenti di controllare e monitorare i dispositivi collegati, come videocamere, smart plug o sensori, direttamente da uno smartphone o un tablet.

Non solo hack alle smart home, anche le Jeep

Le auto intelligenti, che tecnicamente non rientrano nella definizione di dispositivi dedicati alla smart home, sono sempre più connesse. Vale la pena, quindi, menzionare anche questo caso per aumentare la consapevolezza riguardante questi pericoli.

Nel 2015, alcuni ricercatori hanno dimostrato quanto fosse facile hackerare una Jeep Cherokee e prendere il controllo di tutto, dall'aria condizionata fino ai tergicristalli. Il test driver aveva notato che, senza toccare il cruscotto, le prese d'aria della Jeep Cherokee avevano iniziato a emettere aria fredda, alla massima potenza. Successivamente, la radio era passata a una stazione diversa, a tutto volume, e non era possibile spegnerla. I tergicristalli si erano accesi e il liquido ha offuscato il vetro. Sebbene il volante e i freni non abbiano subito interferenze, altre interruzioni sarebbero state sufficienti a causare un incidente.

Detto ciò, un hacker può tranquillamente distrarre il conducente con queste piccole cose, ma causare grandi pericoli. Finché un veicolo è connesso a Internet, per gli hacker è un potenziale gateway per entrare e trasformare un viaggio tranquillo in un incubo su ruote.

Come proteggersi al meglio?

Tutti sognano uno stile di vita smart e connesso, che semplifichi ogni cosa, eppure, come dimostra l'esperienza, gli hacker sono scaltri e disposti a sondare anche i dispositivi domestici intelligenti per individuare i più piccoli punti deboli.

Ogni persona, quando vuole configurare nuovi dispositivi nella smart home, può ridurre al minimo gli scenari sopra menzionati con semplici mosse. Ad esempio, per monitorare casa, soluzioni cloud come mydlink, forniscono una crittografia end-to-end tramite cloud che elimina il rischio di hack delle videocamere. Tale soluzione offre anche un ecosistema completo per la smart home che controlla e gestisce casa, con videocamere, smart plug e altri sensori.

Inoltre, vale sempre la pena aggiornare password e firmware per rinnovare continuamente la protezione dei dispositivi e modificare eventuali password predefinite. I dispositivi più vecchi spesso sono dotati di una password fornita dai produttori, che spesso è la stessa. Se non viene modificata, il dispositivo è estremamente vulnerabile ai cyber-attacchi.

Anche acquisire familiarità con i controlli di sicurezza sul router e configurarlo per regolare l'esposizione a Internet è una considerazione importante. Ad esempio, disabilitare semplicemente l'accesso remoto sul router può impedire a un hacker di prenderne il controllo. E, naturalmente, un'adeguata protezione antivirus e antimalware su tutti i computer e laptop di casa, è di grande aiuto.

Anche informarsi su come funzionano i dispostivi già in possesso può essere un aiuto prezioso per migliorare la sicurezza smart home, correggendo eventuali impostazioni sbagliate o pericolose. Infine, prima di acquistare un nuovo dispositivo, ogni persona dovrebbe capire che tipo di funzionalità e dettagli sono inclusi. Qualità e sicurezza

dovrebbero essere le prime caratteristiche da considerare prima di un acquisto.

https://www.key4biz.it/i-peggiori-hack-alle-smart-home-degli-ultimi-anni/371083/

Cybercrime, i 15 ransomware più popolari del 2021

Nella prima metà del 2021 gli **attacchi ransomware** hanno segnato ancora un aumento rispetto all'anno passato. Anche se di poco, 304,7 milioni di attacchi nel primo semestre 2021 contro i 304,6 dell'interno 2020, è facile prevedere un ulteriore sostanzioso incremento di queste attività criminali entro la fine dell'anno in corso.

Nel primo trimestre del 2021, i ricercatori di sicurezza di Unit 42 hanno rilevato 113 diverse famiglie di ransomware e in base ai dati statistici, solo le prime 15 coprono il 52,3% del totale dei casi. Questo dimostra la diversità di questa minaccia e sottolinea quanto sia difficile estendere la copertura di rilevamento dei ransomware con una profilazione statica. Tra tutti, il 6,7% dei campioni di ransomware è rappresentato da Virlock, attivo dal 2014, dotato del maggior numero di varianti a causa del suo comportamento di tipo file-infector.

Un numero più elevato di varianti di malware non implica necessariamente una maggiore prevalenza. Alcune famiglie di ransomware non creano ogni volta varianti diverse, ma il

rapporto di infezione per campione è alto, il che significa che gli attaccanti hanno usato lo stesso malware per un gran numero di vittime. Il secondo grafico mostra un risultato completamente diverso dal primo e deriva dal solo conteggio dei campioni di ransomware relativi a casi di infezione di più di cinque da parte dello stesso malware. Le prime tre famiglie sono Ryuk (31,7%), Sodinokibi (20%) e Maze (15%).

Classificando le famiglie di ransomware con questo filtro si ottiene una visione diversa di quelli dominanti. In questo caso le famiglie più attive sono Ryuk, Sodinokibi e Maze, seguite daMespinoza, Babuk, Egregor, NetWalker, MedusaLocker, Dharma e TorrentLocker.

Le e-mail sono ancora il metodo più efficiente per colpire con un ransomware. Il processo di consegna del malware tramite un URL può includere varie tecniche, ad esempio, i link possono essere pubblicati su forum o gruppi di chat, inviati da applicazioni IM, offerti tramite falsi freeware da scaricare, o allegati nelle e-mail. Il ransomware di hosting web può anche essere scaricato e installato con successo attraverso una catena di infezione multilivello tra diversi tipi di file. Ad esempio, AlumniLocker viene prima consegnato come un PDF di phishing, conduce al download di un archivio ZIP che contiene un downloader LNK che scarica ed esegue uno script PowerShell offuscato per installare infine il ransomware.

Per quanto riguarda le tipologie di file rilevate nel e la loro prevalenza, L’’EXE a 32 bit è il più comune. Altri tipi di file sono spesso utilizzati come primo stadio di infezione o downloader, come archivi, documenti e script. La maggior parte dei ransomware viene consegnata via e-mail con un allegato; il ransomware è compresso nei file archiviati con o senza protezione password. “Resume” o “portfolio document” sono esempi di nomi di file di archivio, che contiene uno o

più parti di malware con icone di file di documenti falsi. Abbiamo inoltre osservato che Mailto (AKA NetWalker) tende a consegnare il ransomware in uno script PowerShell altamente offuscato. I documenti di exploit sono utilizzati raramente per consegnare il ransomware, un esempio è un exploit RTF che ha portato a scaricare e installare il ransomware Makop da remoto.

https://www.key4biz.it/cybercrime-i-15-ransomware-piu-popolari-del-2021/370907/

Campagne di estorsione su larga scala, in Italia la media del riscatto è di 950 euro

Sono state individuate numerose **campagne di estorsione su larga scala, ancora in corso,** che sfruttano le credenziali degli utenti rese pubbliche a seguito di violazioni di dati o fughe di notizie avvenute negli ultimi anni.

Secondo i ricercatori di **Bitdefender**, gli attacchi sono **diffusi in tutto il mondo**, con un numero insolitamente alto di email di spam che hanno raggiunto gli utenti in Romania (oltre 400.000 email), **Italia** e Paesi Bassi. I messaggi provengono da più indirizzi IP in Europa, Asia, Africa e Americhe. Sembra che siano stati distribuiti su larga scala attraverso una botnet di spam di grandi dimensioni controllata dallo stesso gruppo di hacker che ha organizzato la campagna.

Caratteristiche dell’estorsione via email

Gli spammer inondano le caselle di posta attraverso attacchi di phishing “spray and pray” nella speranza di ingannare il maggior numero possibile di vittime. Le caratteristiche specifiche di queste truffe a scopo di estorsione non sono nuove.

I criminali inviano alla vittima una email in cui specificano che le credenziali di accesso al suo account online sono state acquistate sul web e utilizzate per installare un software dannoso e uno spyware sul suo dispositivo. Usano tattiche per intimidire e per indurre un forte senso di panico nei destinatari, **minacciando di esporre ad amici e familiari un video che contiene scene d’intimità delle vittime mentre guardano siti per adulti online.**

Nel testo dell’email, i truffatori affermano che utilizzare una soluzione di sicurezza sarebbe inutile, infatti l’hacker scrive: “Il mio virus aggiorna continuamente le firme (è basato su driver), e quindi rimane invisibile al software antivirus”. “Avrai perciò capito perché ho agito inosservato fino a questa email…”.

Anche se nell’email l’hacker afferma chiaramente di avere accesso alla webcam, al microfono e ad altri software sul dispositivo della vittima, in realtà si tratta di un bluff.

Le email sono scritte con la lingua del Paese di riferimento **e gli importi di pagamento richiesti sono diversi,** a seconda di dove si trovano i destinatari:

- Italia – 950 Euro
- Paesi Bassi – 1350 Euro
- Brazil – 309 Dollari
- Francia – 650 Dollari
- Romania – 1250 Dollari

- Stati Uniti – 1500 Dollari

In maniera simile alle precedenti campagne di estorsione segnalate dagli esperti di sicurezza i criminali delineano una serie di regole. I messaggi specificano che le “offerte” non sono negoziabili e richiedono il pagamento entro 48 ore in criptovaluta (Bitcoin). Agli utenti viene specificato di non rispondere all’email e di non contattare la polizia o i fornitori di soluzioni di sicurezza.

I criminali informatici hanno utilizzato più indirizzi bitcoin per ricevere il pagamento dalle vittime, e alcuni di loro hanno rivelato di aver ricevuto **diverse transazioni per un ammontare di migliaia di dollari**.

I trasferimenti di dati sul dark web alimentano campagne di spam e a scopo di estorsione

Le violazioni e le fughe di dati si verificano ogni giorno, esponendo indirizzi email e informazioni più sensibili come password in chiaro, numeri della previdenza sociale e dettagli delle carte di credito.

Le informazioni rubate o sottratte vengono trasferite sul dark web dove i criminali informatici e i truffatori pagano una cifra irrisoria per consultare i dati e usarli per rubare le identità o compromettere gli account online ed estorcere denaro alle vittime di phishing.

Tuttavia, i criminali informatici possono comunque ricattare le vittime anche con pochi dati a disposizione. **L'estorsione, si è trasformata in un business altamente redditizio nell'era digitale** per i criminali informatici che possono raggiungere milioni di individui in un paio di clic senza necessariamente avere prove compromettenti su di loro.

https://www.key4biz.it/campagne-di-estorsione-su-larga-scala-in-italia-la-media-del-riscatto-e-di-950-euro/370878/

Sanità, in Italia il settore resta il più colpito da malware e ransomware

Nel nostro Paese nel 2020 sono stati 20.777 i malware unici e 2.063 i ransomware unici che hanno colpito le strutture

sanitarie italiane, rendendo di fatto il settore sanitario il più bersagliato in Italia per quantità di malware e ransomware unici è stato quello della sanità. A seguire il banking e la PA.

Il dato, che emerge dall'ultimo report di Trend Micro Research, prende in considerazione il numero totale di programmi maligni pensati appositamente per un determinato settore e non il numero totale di volte che sono stati utilizzati per un attacco, numero che ovviamente risulterebbe maggiore.

Attacchi malware unici in Italia per settore

Un settore già sotto pressione a causa della criticità e sensibilità dei dati custoditi e che ha dovuto fare i conti con una situazione resa ancora più difficile dal momento sanitario globale. L'esigenza di dover garantire al massimo le prestazioni e l'erogazione dei servizi in un periodo di pandemia ha infatti attratto ancora di più i cybercriminali e costretto le strutture sanitarie ad alzare maggiormente le proprie difese.

A seguire, i settori più bersagliati sono stati il banking e il tech per quanto riguarda i malware unici e la PA e i trasporti per i ransomware unici. I numeri alti di malware e ransomware unici indicano che nel 2020 i cybercriminali hanno scelto determinati settori e costruito attacchi su misura, caratterizzati da un'alta targettizzazione e profilazione degli obiettivi.

Attacchi ransomware unici in Italia per settore

Italia terzo Paese al mondo per attacchi malware

La multinazionale di sicurezza informatica, ad aprile 2021, aveva svelato un altro triste primato. Il nostro Paese si posizionava al terzo posto della classifica mondiale dei Paesi maggiormente presi di mira dai malware. A gennaio era il quinto Paese più colpito, a febbraio e marzo il quarto, mentre ad aprile la terza nazione maggiormente afflitta dal fenomeno malware.

La top five dei Paesi più attaccati è guidata da Stati Uniti (31.056.221) e Giappone (30.363.541). Dopo l'Italia in terza posizione, seguono India (4.411.584) e Australia (4.387.315).

Per lo studio la famiglia di malware più rilevata ad aprile in Italia, in generale e a livello business, è stata quella di **DOWNAD**, mentre i consumatori sono stati colpiti maggiormente da **COINMINER**, famiglia di malware specializzata nel nascondersi all'interno del sistema per sfruttare le risorse computazionali e produrre criptovaluta.

https://www.key4biz.it/sanita-in-italia-il-settore-resta-il-piu-colpito-da-malware-e-ransomware/370107/

Polizze assicurative contro attacchi informatici, +50% nell’ultimo anno

Per il Rapporto **Clusit 2021** gli attacchi informatici sono aumentati del 12% a livello globale. Nel 2020, anno di pandemia, lockdown e smart working, la sicurezza informatica è stata messa a dura prova, toccando il numero più alto mai registrato di attacchi.

I danni globali sono arrivati a toccare cifre impressionanti, paragonabili per ordine di grandezza al PIL italiano. Ipotizzando una tendenza di crescita costante degli attacchi, pari al 15% circa, nel 2024 si stima che le perdite per l’Italia possano arrivare all’astronomica cifra di 20-25 miliardi di euro.

Per questo motivo nell’ultimo anno si è visto un aumento sostanziale delle polizze assicurative contro gli attacchi informatici. Per ASSITECA, gruppo italiano attivo nella gestione dei rischi d’impresa e nel brokeraggio assicurativo, “*prima della pandemia le aziende clienti che avevano sottoscritto una polizza sul cyber risk erano circa il 3% del nostro portafoglio, oggi sono più del 15%. Le richieste di copertura che ci sono pervenute nell’arco degli ultimi 12 mesi, da Nord a Sud dalle piccole come dalle grandi imprese, sono cresciute di oltre il 50%*”.

Ridurre i danni e prevenire i rischi, grazie a piani di business continuity e con la messa a punto di specifici piani

di cybersecurity deve essere, quindi, una priorità per le aziende di qualsiasi grandezza e settore. Nonostante tutte le difficoltà economiche del periodo, lo scorso anno la spesa per la sicurezza informatica è cresciuta del 4%, segno di una maggiore consapevolezza dei rischi e della necessità di attuare finalmente una piena digitalizzazione anche come leva di sviluppo.

Anche se gli investimenti in ICT security potrebbero sembrare tanti (nel 2020 sono stati pari a 145 miliardi di dollari a livello globale, di cui 1,5 in Italia) sono nulla se si considera che i danni generati solo dal cyber crime nel 2020 hanno toccato i 945 miliardi di dollari. Per ogni dollaro investito in sicurezza, quindi, se ne contano 7 di perdita.

https://www.key4biz.it/polizze-assicurative-contro-attacchi-informatici-50-nellultimo-anno/369735/

Industria 4.0, allarme ransomware per sistemi di controllo industriali (ICS). Il report

In tutto il mondo, Italia compresa, le industrie sono a rischio di subire blocchi della produzione e furti di dati sensibili a causa di attacchi ransomware. Il dato emerge da “2020 Report on Threats Affecting ICS”, l’ultima ricerca Trend Micro.

I sistemi di controllo industriali (ICS) sono elementi cruciali all'interno di industrie, fabbriche e impianti e sono utilizzati per il monitoraggio dei processi industriali nelle reti IT-OT. Un ransomware che riesce a penetrare questi sistemi è in grado di bloccare le operazioni per giorni e di entrare in possesso di dati critici, come progetti, programmi, invenzioni e brevetti.

La ricerca svela che i ransomware più pericolosi per le industrie, e che insieme hanno raggiunto più della metà delle infezioni nel 2020, sono Ryuk (20% di attacchi), Nefilim (14,6%), Sodinokibi (13,5%) e LockBit (10,4%).

Il report inoltre rivela:

- I cybercriminali utilizzano gli endpoint ICS per il mining di criptovalute, sfruttando sistemi operativi senza patch che sono ancora vulnerabili a EternalBlue
- Alcune varianti di Conficker si stanno diffondendo all'interno di endpoint ICS che utilizzano nuovi sistemi operativi, attraverso attacchi di "forza bruta" ai privilegi degli amministratori
- Alcuni vecchi malware come Autorun, Gamarue e Palevo, sono ancora presenti nelle reti IT-OT e si diffondono attraverso i dispositivi rimovibili

Lo studio pone l'accento sull'urgenza di una cooperazione più stretta tra i team IT e OT, per identificare i sistemi chiave e le dipendenze, come ad esempio la compatibilità con i sistemi operativi e i requisiti di up-time, con l'obiettivo di sviluppare strategie di security più efficaci.

Come difendere i sistemi dai ransomware

- Implementare un patching veloce è vitale. Nel caso non sia possibile, si può considerare la segmentazione della

rete o il virtual patching

- Affrontare i ransomware in seguito a un’intrusione mitigando le cause dell’infezione alla radice, attraverso software di application control e strumenti di rilevamento e risposta, per pulire le reti in base agli indicatori di compromissione
- Limitare le condivisioni di rete e rinforzare l’utilizzo di combinazioni username/password forti, per prevenire gli accessi non autorizzati attraverso la forzatura di credenziali
- Utilizzare un IDS o un IPS per sondare i comportamenti normali di rete e identificare attività sospette
- Scansionare gli endpoint ICS in ambienti air gap, utilizzando strumenti indipendenti
- Stabilire punti di scansione malware all’interno dei dispositivi USB, e verificare gli strumenti utilizzati per trasferire dati tra endpoint in ambienti air gap
- Applicare il principio del privilegio minimo agli amministratori e agli operatori delle reti OT

https://www.key4biz.it/industria-4-0-allarme-ransomware-per-sistemi-di-controllo-industriali-ics-il-report/369035/

Come proteggere smartphone e tablet durante le vacanze estive? 10 consigli sulla sicurezza

Finalmente, dopo lockdown e chiusure locali a causa della pandemia, possiamo partire e goderci delle meritate ferie. Per godersi al meglio le proprie vacanze, occorre però mettere al sicuro smartphone, tablet, pc e i dati personali, in modo da non perdere l'accesso ai vari account o conti bancari. Qui di seguito alcuni consigli da adottare non solo prima di partire ma anche quando si è in vacanza.

Prima della partenza

Una volta deciso l'itinerario del viaggio, è bene dedicare del tempo a preparare i dispositivi che si porteranno in vacanza.

1. **Aggiornare le password**

Regola valida per tutti gli account online per proteggersi da qualsiasi potenziale attacco di "credential stuffing". Scegliere password uniche e robuste, e abilitare l'autenticazione a più fattori (MFA) o a due fattori (2FA) dove è disponibile

2. **Abilitare i codici di accesso e i PIN su tutti i dispositivi mobile**

Una protezione in più per salvaguardare i dati nel caso in cui il dispositivo sia lasciato incustodito o venga smarrito

3. **Installare gli aggiornamenti di sicurezza in sospeso**

Gli aggiornamenti vanno eseguiti sul proprio smartphone, tablet o laptop in modo da avere i propri dispositivi in linea con gli ultimi aggiornamenti

4. **Installare una soluzione di sicurezza in locale**

Meglio con una protezione anti-malware per proteggersi da attacchi dannosi mentre si naviga sul web

5. **Effettuare il backup dei dati**

In caso di furto o violazione del dispositivo sarà più facile e veloce recuperare i propri dati

6. **Installare una VPN su tutti i dispositivi**

Una mossa per garantire che i propri dati siano al sicuro se ci si connette a una rete Wi-Fi pubblica, si fanno acquisti online o si accede al proprio conto bancario

7. **Disabilitare la connettività automatica Bluetooth**

Sul proprio smartphone per evitare che estranei si colleghino al dispositivo in spazi pubblici

In vacanza

8. **Evitare di connettersi a reti Wi-Fi pubbliche gratuite**

In modo particolare in ristoranti, aeroporti, bar o alberghi. Se necessario, scegliere reti protette da password e usare una VPN per evitare intrusioni

9. **Resistere all'impulso di pubblicare sui social media le proprie attività e posizione.**

Questo per evitare che chiunque possa introdursi in casa o possa usare le informazioni per truffare amici e familiari

10. **Lasciare i dispositivi intelligenti in luoghi sicuri**

Ad esempio come hard disk esterni, computer portatili e USB in una cassaforte in hotel per evitare perdite di dati e violazioni dei dispositivi mentre si è fuori.

https://www.key4biz.it/come-proteggere-smartphone-e-tablet-durante-le-vacanze-estive-10-consigli-sulla-sicurezza/369012/

Il cyber-attacco alla Regione Lazio? Bisogna investire subito in nuove competenze e tecnologie

Il recente attacco informatico al CED della Regione Lazio sollecita molte considerazioni di sistema e di dettaglio. Vediamone alcune.

Il fenomeno globale: norme e comportamenti

Da molti anni la crescita esponenziale degli attacchi *cyber*, dall'avvio globale di Internet negli anni '90, è all'attenzione dei tecnici e degli esperti.

Nella sola Europa, almeno dal 2010, le strategie e i piani nazionali di difesa si sono attestati per far fronte anche congiuntamente all'attacco crescente alla confidenza e sicurezza degli utenti nell'utilizzo dei diversi servizi telematici. Il moltiplicarsi delle piattaforme *social*, dell'*e-business*, dell'*e-banking*, dell'*e-commerce*, delle piattaforme *cloud*, della IoT, ecc. hanno sollecitato le norme in materia di sicurezza *cyber* nell'on line: la direttiva NIS del 2016, operativa dal 2018 ad esempio, e il controllo del cosiddetto perimetro di sicurezza nazionale per l'Italia, dal 2019.

Per la NIS, è prevista la *compliance* di *risk assessment* e *risk evaluation*, con riferimento a norme (di fatto minime) come le ISO e ad 'adeguate' misure di difesa.

Per il perimetro di sicurezza nazionale, la certificazione di reti, prodotti, servizi e processi digitali interni ed esterni al sistema. La considerazione globale è che all'accrescersi dello spazio e dei servizi telematici è corrisposta nel tempo, in maniera esponenziale la quantità e la qualità degli attacchi, in particolare ma non solo nei settori delle infrastrutture critiche: il settore finanziario, la sanità, l'energia, i trasporti, l'ambiente, ecc.

Scopi, impatti, cybercriminalità

Per comprendere i rischi, vanno approfonditi gli scopi, gli impatti, gli autori degli attacchi.

Partiamo da questi ultimi. Trattare l'attacco come hackeraggio generico, oscura le tipologie dei cybercriminali: anzitutto la filiera delle aziende cybercriminali che vendono attacchi incaricati da entità diverse; i piccoli criminali *cyber* che studiano la tematica degli attacchi mediante veri e propri corsi online; e anche, le entità del cyberterrorismo di stati nemici come rilevato dal Dipartimento della sicurezza nazionale statunitense (il *Department of homeland security* e il NIST).

Gli scopi sono molteplici e si possono riassumere in due obiettivi: ricavi economici di varia natura: ad esempio la vendita di account vati, bancari e telefonici, ad esempio, disponibili a pacchetti nel *dark web* o richieste di riscatto come negli attacchi cyber di tipo *ransom* che criptano i dati rendendone impossibile l'uso; e, anche finalità conoscitive di sistema: politica, affari, militari, ecc.

E, veniamo agli impatti: non solo la criptazione ma anche il rallentamento o il blocco dei servizi nei DOS, l'esfiltrazione dei dati, la corruzione o la distruzione dei dati e o dei servizi, come il caso noto della distruzione del sistema energetico ucraino, o il nucleare, e, caso poco discusso ma di piena preoccupazione da anni all'estero, lo spionaggio

industriale, politico, istituzionale, militare che in molti casi si avvale di *malware* spesso non individuato per anni.

Le modalità degli attacchi

Alla preparazione informatico-cibernetica dei cybercriminali non corrisponde la possibilità concreta di difesa nei sistemi paese.

Prima di venire a ciò, chiediamoci come avviene un attacco: le cause sono dovute a vulnerabilità di duplice natura.

Le vulnerabilità comportamentali sono dovute a fragilità da parte degli utenti nelle istituzioni, nelle aziende nei sistemi associativi (si vedano attacchi al settore degli ordini professionali: ingegneri, notai, commercialisti, ecc.).

Il fenomeno del *phishing* si è raffinato: non solo allegati malevoli, dirottamento a siti ammalorati, risposte a *mail* nocive, ecc.

Ma i difetti comportamentali riguardano ovviamente anche le malconfigurazioni del sistema tecnologico.

Vulnerabilità diverse invece risiedono nei *bug*, nei prodotti informatici: sistemi operativi e app, e nelle infrastrutture digitali, *cloud* e piattaforme varie. Queste sono in parte censite *ex post* dal NIST americano e dai *vendor* che propongono aggiornamenti e *patch* rimediali.

Gli attaccanti non si limitano a inoculare il malware: l’attacco si snoda attraverso una ricerca nei social, negli OSINT, per conoscere il target dell’attacco. Poi, provvedono ad armare l’attacco con una sequenza di azioni talora ricorsive, utili entrare nei sistemi, analizzarli e inoculare malware funzionale agli scopi ovvero ai danni logici immaginati.

Le difese

Come difendersi. A parte il back-up corretto e il *mirroring*, ad oggi due sono i principali set di strumenti: software di monitoraggio che dovrebbero segnalare comportamenti anomali del sistema ovvero degli *asset*, indicatori di compromissione e/o di attacco, IoC e IoA, e le soluzioni tecnologiche di difesa, IDS, IPS, *antimalware*, antivirus, antispam, honeypot.

Questi sistemi, tuttavia, riconoscono solo fenomeni noti le cui firme siano registrate nei *software* di difesa.I cosiddetti *zero day* includono non solo soluzioni tecnologiche d'attacco del tutto innovative ma anche soluzioni tecnologiche malefiche in tipologie di malware e attacchi già largamente riscontrati come nel caso dei *ransomware*.

Un secondo limite generale sta nell'assenza di correlazione e integrazione delle tipologie dei dati relativi a quanto rilevato dai sistemi di monitoraggio e difesa.

Ho più volte ricordato che l'analisi, l'interpretazione e la rappresentazione/*knowledge* di dati correlati è in grado di offrire informazioni di sistema pregiate, necessarie e utili in chiave preventiva e, in futuro, predittiva.

Senza questa conoscenza condivisa, sarà impossibile fronteggiare in maniera solida il gravissimo crescendo degli attacchi e dei danni.

Il prezzo e gli investimenti

Ultima considerazione. La *cybersecurity* costa ma in genere, anche in Italia, non si valuta correttamente il rischio operativo economico ma ci si limita alla *compliance* superficiale pure utilmente richiesta dalla norma.

Le conclusioni da trarre sono le seguenti: occorre innalzare l'alfabetizzazione digitale della sicurezza a livelli

crescenti negli utenti in genere, negli impiegati, nei dirigenti, negli addetti. Occorre rivedere concretamente le *policy* della sicurezza *by design*, sviluppare concretamente con ricerca e sviluppo potenziati la competenza in *cybersecurity*, investire consapevolmente nella sicurezza in tutti i processi di digitalizzazione.

Troppe applicazioni o soluzioni estemporanee nell'uso di servizi e transazioni digitali vengono adottate, presi dal fascino dell'innovazione digitale: app su app, piattaforme su piattaforme, competizioni tra giganti high tech che non possono garantire da soli sicurezza e il business economico imponente che regge la trasformazione digitale in corso. Il *cybercrime* è conscio delle fragilità di sistema e si specializza sistematicamente nelle tipologie e tecnologie innovative degli attacchi.

Non esistono, ad oggi, soluzioni di sicurezza efficaci. Le misure da adottare sono multiple, come detto: *awareness*, competenze tecnologiche infrastrutturali di sistema non improvvisate, acquisizione, condivisione e analisi dei dati relativi a *threat intelligence*, *infosharing* e reportistica degli eventi e degli incidenti. Servono modellistiche architetturali dei dati, tassonomie e ontologie non di facciata: i temi dell'analitica dei dati sono complessi e la reportistica internazionale lo conferma. Il cammino è lungo e impervio e gli strumenti non sono solo le norme e le istituzioni di strutture vecchie e nuove.

Che fare: dobbiamo investire, subito, in nuove competenze e tecnologie.

https://www.key4biz.it/il-cyber-attacco-alla-regione-lazio-bisogna-investire-subito-in-nuove-competenze-e-tecnologie/371161/

La cybersecurity in Italia? Continuiamo così…facciamoci del male!

Da giorni la notizia di cui dibattono tutti gli esperti di cybersecurity (e anche i non) è quella dell'attacco al CED (Centro Elaborazione Dati) della Regione Lazio, in cui sono stati criptati i dati mettendolo così fuori uso. Non è la prima volta che un attacco cyber colpisce un'istituzione, eppure abbiamo assistito ad un eccesso di informazioni confuse e talvolta deliranti, che hanno creato audience ma che non hanno certo fornito chiarezza sulla questione.

A distanza di tre giorni, rimane il fatto che **l'approccio a tali situazioni resta inadeguato**. A quanto si apprende da una recente dichiarazione dell'assessore regionale alla Sanità, risulta essere criptato anche il backup dei dati.

Gli errori ignorati

Una domanda nasce spontanea: **non si è appreso nulla dagli errori del passato**? Che poi non sono nemmeno così lontani nel tempo. Era settembre 2020 quando un ransomware travolse l'Università di Roma Tor Vergata criptando tutti i dati, rallentando ricerche preziose e l'amministrazione dell'ateneo. Era novembre 2018 quando un'intrusione informatica nel data center Telecom di Pomezia aveva provocato il blackout della rete telematica giudiziaria.

E gli esempi potrebbero continuare.

Il punto però non è, come ormai è noto nel mondo della security, che l'attacco è dietro l'angolo per chiunque, la

differenza sta nel cercare di contrastarlo al meglio e di predisporre le misure di recupero, perché **nessuno è inviolabile**.

Nel caso dell'ateneo romano, l'attacco aveva criptato anche i dischi del backup, costringendo l'amministrazione ad un lungo e faticoso lavoro di recupero per ricostruire la situazione digitale a partire dal cartaceo (laddove c'era). Certamente, ogni responsabile della sicurezza informatica di ogni istituzione sarà stato a conoscenza di tale incidente. Dopo aver tirato un sospiro di sollievo, come fa un soldato quando il fuoco nemico lo risparmia, avrà di sicuro fatto un controllo approfondito della sua situazione, assicurandosi che, qualora un attacco ransomware fosse capitato in futuro alla sua organizzazione, i suoi dischi di backup sarebbero stati fisicamente isolati dal resto del sistema. Avrebbe così minimizzato i danni evitando le settimane di ritardo alla piena normalità che hanno funestato nell'autunno scorso la quotidiana attività del personale di Tor Vergata.

Infatti…

Ora, non me ne vogliano i tanti amici informatici e ingegneri, **questo non è un problema di preparazione tecnica del personale. Questo è un problema di carente cultura della sicurezza informatica**. Non serve conoscere il più recente protocollo quantistico per la distribuzione di chiavi o lo stato dell'arte per la fattorizzazione di interi o la crittografia a curve ellittiche (io personalmente non ne so molto: ho solo citato tre esempi di temi tecnici di attualità che mi ha suggerito un amico fidato).

Un nuovo mindset

Il punto chiave è che deve cambiare l'approccio, o meglio il *mindset* con cui si affronta il tema della cybersecurity. Perché prima di tutto, qualunque strada si decida di intraprendere, bisogna essere disposti a fare i conti con il

passato e trarre il dovuto insegnamento (*lesson learned*, in inglese). È chiaro che questo non sta avvenendo, dal momento che **ci stiamo abituando ad uno schema perdente**: si subisce un attacco, spesso peraltro per un'inadeguata gestione della sicurezza all'interno dell'Istituzione o dell'organizzazione; puntualmente arrivano le interviste a politici ed esperti su quanto avvenuto; si rilancia la possibile soluzione del momento; si prosegue indisturbati in attesa del prossimo evento, mentre i responsabili pensano "a noi questo non succederà mai".

Questo schema, si sa, è infruttuoso, ma si ripete inalterato ormai da anni.

Non ci sono pallottole d'argento

Certamente l'istituzione di un'Agenzia la cybersicurezza nazionale è un'iniziativa importante per il nostro Paese, ma non può essere vista come la panacea. Quando si guarda a ciò che accade in altri paesi, infatti, ci si accorge che pur avendo da tempo centri e strutture di alto livello per la sicurezza informatica, i problemi ci sono comunque. L'attacco ransomware a Colonial Pipeline, uno dei più grandi oleodotti degli Stati Uniti, con conseguente pagamento del riscatto, è il classico esempio di come sia **inutile armarsi di muscoli e pensare di andare in guerra, tipo guerrieri della notte**, quando poi basta il furto di una singola password per creare un problema enorme.

No culture, no cybersecurity!

Come ho ampiamente sottolineato in un mio libro, molto apprezzato all'estero (forse perché in inglese e probabilmente anche per una diversa sensibilità sul tema culturale) se non si lavora sulla **costruzione di una vera cybersecurity culture** non ci saranno strutture stellari e super-eroi a contrastare la situazione.

Cominciamo a **lavorare sulle competenze che servono per costruirla**, quelle accertate e sperimentate sul campo e non solo dichiarate con titoli altisonanti.

Altrimenti non rimane che commentare con Nanni Moretti: “Continuiamo così. Facciamoci del male”

[embedded content]
https://www.key4biz.it/la-cybersecurity-in-italia-continuiamo-cosi-facciamoci-del-male/371156/