22/12/2020

securenews.it

Argomento: Exprivia: si parla di noi

EAV: € 110
Utenti unici: 333

https://www.securenews.it/cybercrime-domenico-raguseo-direttore-cybersecurity-di-exprivia-attacchi-informatici-in-crescita-durante-la-pandemia-ecco-su-cosa-investire-per-essere-meno-vulnerabili/

Cybercrime, Domenico Raguseo (Direttore Cybersecurity di Exprivia): "Attacchi informatici in crescita durante la pandemia. Ecco su cosa investire per essere meno vulnerabili"

Cybercrime, Domenico Raguseo (Direttore Cybersecurity di Exprivia): “Attacchi informatici in crescita durante la pandemia. Ecco su cosa investire per essere meno vulnerabili”

L’Osservatorio Cybersecurity di Exprivia ha registrato nell’ultimo trimestre in Italia 148 attacchi, incidenti e violazioni della privacy. PA il settore più colpito

Sempre più pericoloso e difficile da combattere: è il cybercrime, la minaccia invisibile, ma tremendamente concreta che spaventa il mondo. Abbiamo approfondito l’argomento con Domenico Raguseo, Direttore Cybersecurity di Exprivia che ha recentemente diffuso il terzo rapporto sulle minacce informatiche nel 2020 in Italia elaborato dal suo Osservatorio sulla Cybersecurity.

Qual è la situazione dei crimini informatici in Italia? Durante l’anno, abbiamo osservato un numero di attacchi e incidenti crescente. Si è passati da 25 attacchi nel primo trimestre, a 119 attacchi nel secondo trimestre, a fronte di un numero di incidenti di 14 nel primo trimestre e 46 nel secondo. Anche il rapporto tra attacco e incidente è significatore di una aumentata attività: si passa dal 56% al 21% nel secondo trimestre, con la sensazione che gli attaccanti ci provino su grande scala (un attacco verso sorgenti multiple) senza un target specifico, mentre nel primo trimestre gli attacchi sembra fossero più mirati (un attacco verso un solo target). Nel terzo trimestre il trend sembra comunque confermato, con 107 attacchi e 25 incidenti. I valori assoluti sono leggermente inferiori – durante l’estate anche gli attaccanti si sono riposati – ma a settembre si ricomincia. Se giugno è stato il mese orribile, con 85 segnalazioni di attacchi e incidenti, il secondo mese peggiore dell’anno è settembre, con 70 segnalazioni. Anche il rapporto tra attacchi ed incidenti al 23% si mantiene costante rispetto ai dati del secondo trimestre. Non si tratta, però, solo di cybercrime. A questi dati, vanno aggiunte le violazioni della privacy segnalate dal Garante. Si registrano, infatti, ben 32 violazioni nei primi 9

mesi dell'anno. Pertanto, se il dato rappresenta il carburante dell'economia e, di conseguenza, l'oggetto del desiderio degli attaccanti, spesso chi è tenuto a gestire la sicurezza informatica non lo fa adeguatamente. Queste evidenze sono la conseguenza della veloce trasformazione digitale a cui abbiamo assistito in questi anni, e per cui la pandemia ha rappresentato solo una accelerazione.

Quali sono le principali tipologie di cyber-attacchi? La vulnerabilità maggiormente sfruttata dagli attaccanti è la mancanza di consapevolezza da parte della popolazione digitale sui rischi di un attacco. L'umanità ha avuto secoli per adattarsi alle minacce più comuni nel mondo fisico, ma solo una decina di anni per fare altrettanto nel mondo digitale. Utilizziamo il mondo digitale solo per trarne vantaggio, ma senza la cultura digitale che ci aiuta a comprenderne i rischi. La conseguenza è che la tecnica di attacco più comune è il phishing (e social engineering in genere) con 138 eventi registrati tra attacchi e incidenti nel 2020. Tale operazione avviene inviando mail fraudolente in cui si spingono gli utenti a rivelare informazioni personali quali password, dati delle carte di credito o dei conti correnti bancari, o si indirizzano gli utenti su un sito web fasullo. In alcuni casi un po' di attenzione sarebbe sufficiente per non cadere in tranelli. Senza il phishing gli attaccanti dovrebbero studiare tecniche di attacco più costose e la difesa avrebbe maggiore possibilità di focalizzare investimenti e attenzioni su vulnerabilità di hardware e software, magari anche di processo. Insomma, probabilmente il tema della cybersecurity non sarebbe sulle prime pagine dei giornali.

Dallo studio emerge un andamento che sembra marciare parallelo a quello della pandemia di Coronavirus, come si spiega questo fenomeno? La pandemia ha costretto aziende, istituzioni e popolazione ad accelerare il processo di digitalizzazione di servizi e abitudini. Questo ha fatto sì che servizi erogati e utilizzati nel mondo fisico siano stati traslati nel mondo digitale (pensiamo ad esempio alla scuola a distanza, ma anche al rapporto tra medico e paziente, alla necessità di acquistare on-line beni ordinari, ecc.). La velocità con cui questa trasformazione è avvenuta, l'aumento del perimetro di un potenziale attacco, il fatto che servizi digitali siano diventati sempre più critici, hanno fatto sì che gli attaccanti abbiano avuto vita più facile.

Quali sono i settori che sono risultati maggiormente vulnerabili? Tradizionalmente il settore finanziario è quello maggiormente preso di mira dagli attaccanti, il cui interesse è trarre profitto; e quindi, accedere direttamente al denaro è il modo più immediato per ottenerlo, senza intermediari, senza chiedere riscatti. A causa della pandemia, la pubblica amministrazione è il settore maggiormente impattato dalla

trasformazione digitale. Di conseguenza, attacchi e incidenti verso la pubblica amministrazione nei mesi di luglio, agosto e settembre hanno superato quelli del settore finanziario. In terza posizione si classificano gli attacchi verso target multipli. Ad esempio, campagne di phishing non indirizzate a un settore specifico, nella speranza che qualcuno abbocchi semplicemente puntando alla folla.

È possibile fare un confronto con il resto d'Europa e a livello globale? Ritengo che i dati siano compatibili con quelli osservati a livello globale. Il fenomeno è parallelo all'impennata della digitalizzazione, quindi si registrano più eventi criminali nelle economie dove il cambiamento è in fase avanzata e in quei paesi dove il processo di trasformazione è più veloce.

Exprivia è impegnata nel diffondere la cultura della sicurezza informatica, ma quali sono nel concreto le azioni da mettere in campo per proteggersi e rendersi meno vulnerabili? In cosa dovrebbero investire le imprese? Sicuramente è una priorità investire in consapevolezza. Tale investimento consiste nell'implementare i controlli di sicurezza fondamentali, con particolare riferimento a quelli che hanno a che fare con la protezione dell'endpoint, salvaguardia della migrazione verso il cloud dei servizi, gestione delle vulnerabilità e monitoraggio degli eventi generati dai dispositivi di sicurezza. L'endpoint rappresenta il punto di ingresso dell'infrastruttura, tanto più se l'accesso viene fatto non all'interno di un perimetro definito, ma remotamente (ad esempio da casa). Di contro, gli attaccanti possono sviluppare malware diversi in continuazione. La conseguenza è che i sistemi di protezione devono essere pronti a identificare anomalie più che a verificare la presenza di qualche agente malevolo. Anche la migrazione al cloud rappresenta un rischio, in quanto mette in discussione i principi con cui le reti sono state segmentate. Difficile portare in cloud delle policies che si basano su informazioni tipiche della segmentazione fisica. È necessario, perciò, cominciare a pensare a tecnologie di microsegmentazione che diano la possibilità di taggare tutte le risorse e sviluppare policies sui tag, piuttosto che su elementi fisici. La portabilità verso il cloud di simili policies è pertanto più semplificata. Se gli endpoint sono il punto di ingresso, le vulnerabilità sono la porta di ingresso per gli attaccanti. I vulnerability assessment e penetration test non possono essere attività saltuarie, ma devono essere inserite in processi continui in cui le vulnerabilità vengono scoperte e gestite (quando non risolte). Infine, è importante investire nel monitoraggio degli eventi generati da dispositivi di sicurezza tramite l'implementazione di processi di gestione della sicurezza delle informazioni (SIEM). Non è sufficiente avere un antivirus, un Intrusion Prevention System, un Intrusion Detection System o un firewall (e così via)

per essere sicuri: dobbiamo assicurarci che gli eventi che questi dispositivi generano siano opportunamente gestiti. Gli attacchi sono costruiti nel tempo e accorgersi che qualcosa di anomalo sta accadendo, attivando le funzioni atte alla risposta, potrebbe talvolta eliminare i danni di un incidente.