Tecnologia - *I criminali informatici stanno alzando il tiro: come proteggere le aziende da attacchi noti ed emergenti*

Roma - 02 mag 2023 (Prima Notizia 24) **Emiliano Massa, Area Vice President Sales Southern Europe di Proofpoint.**

Tra i professionisti della sicurezza si è diffusa la sensazione che lo scorso anno abbia rappresentato una sorta di ritorno alla "normalità". Mentre il panico da pandemia si placava e le organizzazioni si trovavano sempre più a loro agio a operare in configurazioni ibride, aumentava pure la fiducia nella loro postura di sicurezza. Purtroppo, anche i criminali informatici si sentono a proprio agio in questa normalità. E con una superficie di attacco più ampia a cui mirare, hanno affinato le loro abilità, trovando modi sia familiari che nuovi per violare le difese ed esporre i dati. Lo State of the Phish Report 2023 di Proofpoint ha rilevato che gli attacchi via e-mail continuano a dominare il panorama delle minacce, con otto organizzazioni su dieci che lo scorso anno hanno subito almeno un attacco di phishing via e-mail, che nel 7% dei casi si è tramutato in una perdita finanziaria diretta. Sebbene i team di sicurezza possano fare ben poco per impedire che i criminali prendano di mira le loro organizzazioni, il fatto che le persone continuino a contribuire in modo significativo al successo di tali attacchi dovrebbe essere motivo di preoccupazione. La maggior parte di essi, infatti, continua a colpire gli utenti prima dei sistemi. Aumentare i livelli di conoscenza e comprensione Gli ultimi anni hanno rafforzato la consapevolezza dei CISO riguardo al rischio degli ambienti remoti e ibridi, e molti hanno reso prioritaria la protezione di queste configurazioni dopo la loro diffusione nel 2020. Oltre ai controlli innovativi e alle tecnologie, la formazione degli utenti ha costituito una pietra miliare di questa strategia di difesa. Quindi, la consapevolezza e la comprensione della sicurezza sono aumentate? Purtroppo, la risposta breve è no. Ancora una volta, la comprensione di base delle minacce informatiche più comuni risulta carente. Oltre un terzo degli intervistati del sondaggio State of the Phish a livello globale non si è detto in grado di definire il malware o il phishing, mentre solo il 40% sa cosa sia il ransomware. Purtroppo, non è difficile per trovare una spiegazione a questa situazione. Sebbene quasi tutte le organizzazioni dichiarino di avere un programma di formazione, solo il 56% a livello globale addestra tutti i membri del proprio team, con una percentuale che in Italia scende al 49%. Il risultato è che nella metà dei casi i dipendenti rimangono impreparati a rilevare e scoraggiare le minacce informatiche. Poiché il panorama delle minacce diventa sempre più sofisticato e incentrato sulle persone, questo problema deve essere affrontato rapidamente. La buona notizia è che, sebbene non sia sufficientemente completa, tre quarti delle organizzazioni svolgono una formazione formale di sensibilizzazione. Quindi, con il tempo già dedicato alla formazione, migliorare la comprensione è una questione di rivedere la strategia, piuttosto che implementare un programma da zero. Gli utenti devono capire come affrontare le sofisticate minacce moderne e cosa fare

quando ciò accade. Le simulazioni basate su esche reali sono un modo efficace per farlo, ma questo metodo di formazione è utilizzato solo dal 35% delle organizzazioni in tutto il mondo. Con budget sempre più ridotti, i team di sicurezza non possono fare tutto. Ma non si può mai lesinare sulla sicurezza informatica. Quindi, mentre il panorama delle minacce diventa sempre più pericoloso, è necessario un ripensamento per garantire che le nostre difese siano all'altezza del compito. Un'istantanea del panorama delle minacce A prima vista, nel panorama odierno delle minacce c'è ben poco che possa sorprendere un professionista esperto. Ma se il phishing, la compromissione delle e-mail aziendali (BEC), il ransomware e simili rimangono passatempi diffusi tra i criminali informatici, molti hanno ulteriormente potenziato i loro attacchi per infliggere il massimo danno. Quasi due terzi (64%) delle organizzazioni italiane hanno sperimentato il ransomware lo scorso anno, e il 44% ha subito un'infezione andata a buon fine. Peggio ancora, tra quelle che hanno pagato un riscatto, meno della metà (il 38%) ha riacquistato l'accesso ai propri dati al primo tentativo. Un altro nemico tristemente noto è il BEC. Tre quarti delle aziende mondiali hanno subito un tentativo di attacco lo scorso anno, con i Paesi non anglofoni particolarmente esposti. Evidentemente, gli attori delle minacce stanno migliorando le loro competenze linguistiche: gli attacchi BEC sono aumentati in tutti i paesi, Italia compresa, dove il 51% delle organizzazioni ha ammesso di averne subito uno nel corso dell'anno. Anche le minacce interne non sono destinate a scomparire presto e il COVID-19 ha ancora un ruolo importante da svolgere. Il lavoro remoto e ibrido ha aumentato il rischio di negligenza e aiutato i malintenzionati a nascondere le proprie azioni. L'anno scorso, il 39% delle organizzazioni italiane ha subito una perdita di dati a causa dell'azione di un insider, e il 42% di chi ha lasciato il lavoro ha ammesso di aver portato con sé dei dati. Nel frattempo, stanno aumentando le minacce via e-mail più complesse. L'anno scorso sono stati inviati centinaia di migliaia di messaggi di phishing con bypass dell'autenticazione a più fattori (MFA) e orientati al telefono (TOAD) al giorno, minacciando quasi tutte le organizzazioni intervistate. Dato che l'MFA è ancora considerato da molti un sistema di sicurezza per gli account e le reti altamente sensibili, qualsiasi metodo per eludere questa protezione offre ai criminali un nuovo vantaggio potenzialmente devastante. Tutto ciò si traduce in una storia già nota: gli attori delle minacce hanno il tempo e la tenacia per trovare nuovi modi volti ad aggirare le difese e i team di cybersecurity si sentono intrappolati in una corsa agli armamenti senza possibilità di vittoria. Vincere la corsa agli armamenti informatici Mentre miglioriamo le difese per far fronte all'evoluzione delle minacce, i criminali trovano nuovi e devastanti modi per aggirarle. Non è una novità. Ma se tenere il passo con il panorama delle minacce è d'obbligo, la difesa informatica non si limita a colmare le lacune che si presentano. Qualunque sia l'avversario, la comprensione e l'educazione dovrebbero sempre essere la base di una strategia di cybersecurity efficace. Quanto più i vostri utenti conoscono gli attacchi che devono affrontare, come li incontreranno e il loro ruolo nel tenerli a bada, tanto più saranno in grado di proteggere la vostra organizzazione e i suoi dati. Iniziate con l'identificare i soggetti più a rischio, sia per le scarse competenze informatiche che per l'elevata esposizione alle minacce, e indirizzate le vostre risorse dove sono più necessarie. Poi andate oltre con un programma di formazione sulla sicurezza in tutto il contesto, condotto regolarmente. Il risultato è una solida cultura della sicurezza sul posto di lavoro che motiva le persone a

costruire abitudini sostenibili e a metterle in pratica ogni giorno, e un’organizzazione molto più sicura, a prescindere dalle minacce che gli attori troveranno da lanciare.

(Prima Notizia 24) Martedì 02 Maggio 2023

Sede legale : Via Costantino Morin, 45 00195 Roma
E-mail: redazione@primanotizia24.it