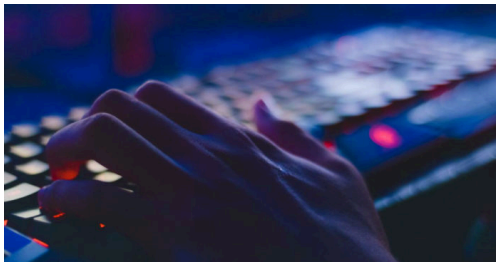
AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News



Tecnologia - *Cyber risk, Agcs: ransomware principale rischio per le aziende, ma emergono nuove minacce*

Roma - 26 ott 2022 (Prima Pagina News) **Il costo crescente degli attacchi ransomware influisce sulle aziende di tutte le dimensioni. Aumentano anche la gravità e la frequenza degli attacchi che compromettono le e-mail aziendali.**

Il ransomware rimane il principale rischio informatico per le aziende a livello globale, mentre gli incidenti che compromettono le e-mail aziendali sono in aumento e cresceranno ulteriormente nell'era del “deep fake”. Allo stesso tempo, secondo un nuovo report di Allianz Global Corporate & Specialty (AGCS), la guerra in Ucraina e le tensioni geopolitiche più ampie rappresentano una delle principali preoccupazioni, in quanto le ostilità potrebbero riversarsi nel cyber spazio e causare attacchi mirati contro aziende, infrastrutture o supply chain.L'analisi annuale di AGCS sul panorama del rischio informatico evidenzia anche le minacce emergenti poste dal crescente affidamento ai servizi cloud, da un panorama di responsabilità civile in evoluzione che comporta risarcimenti e sanzioni più elevati, nonché dall'impatto della carenza di professionisti della sicurezza informatica. Secondo il report, queste potenziali vulnerabilità fanno sì che oggi la resilienza della sicurezza informatica di un'azienda venga esaminata da un numero maggiore di soggetti rispetto al passato, compresi gli investitori globali, tanto che molte aziende la classificano come il loro principale rischio ambientale, sociale e di governance (ESG). “Gli scenari del rischio cyber non permettono di dormire sugli allori. I ransomware e le truffe di phishing sono più che mai attivi e a ciò si aggiunge la prospettiva di una guerra informatica ibrida”, afferma Scott Sayce, Global Head of Cyber di AGCS e Group Head del Cyber Centre of Competence. “La maggior parte delle aziende non sarà in grado di eludere una minaccia cyber. Tuttavia, è chiaro che le organizzazioni con una buona maturità in questo campo sono preparate per affrontare gli incidenti. Anche quando vengono attaccate, le perdite sono in genere meno gravi grazie a meccanismi di identificazione e risposta consolidati”. “Benchè si vedano notevoli progressi, la nostra esperienza dimostra che molte aziende devono ancora rafforzare i loro controlli, in particolare per quanto riguarda la formazione sulla sicurezza informatica, una migliore segmentazione della rete per gli ambienti critici e i piani di risposta agli incidenti e la governance della sicurezza. In qualità di assicuratori cyber, siamo disposti ad andare oltre il puro trasferimento del rischio, aiutando i clienti ad adattarsi ad un panorama di rischio in continua evoluzione e ad aumentare i loro livelli di protezione”.In tutto il mondo, la frequenza degli attacchi ransomware rimane elevata, così come i relativi costi degli indennizzi. Nel 2021 si è registrato un record di 623 milioni di attacchi, il doppio rispetto al 2020. Sebbene la frequenza si sia ridotta del 23% a livello mondiale durante la prima metà del 2022, il totale ad oggi supera già quello degli interi anni 2017, 2018 e 2019, mentre in Europa gli attacchi hanno subito un'impennata in questo periodo. Dal punto di vista di AGCS, il valore delle richieste di risarcimento per

ransomware in cui la compagnia è stata coinvolta insieme ad altri assicuratori, ha rappresentato ben oltre il 50% di tutti i costi dei sinistri cyber nel 2020 e 2021. La doppia e tripla estorsione è ormai la norma.“Il costo degli attacchi ransomware è aumentato perché i criminali hanno preso di mira aziende più grandi, infrastrutture critiche e supply chain. I criminali hanno affinato le loro tattiche per estorcere più denaro”, spiega Sayce. “Gli attacchi a doppia e tripla estorsione sono ormai la norma: oltre alla crittografia dei sistemi, i dati sensibili vengono sempre più spesso rubati e utilizzati come leva per le richieste di estorsione a partner commerciali, fornitori o clienti”. La gravità del ransomware rimarrà probabilmente una minaccia chiave per le aziende, alimentata dalla crescente sofisticazione dei criminali e dall'aumento dell'inflazione, che si riflette nell'aumento dei costi degli specialisti IT e di sicurezza informatica. Un numero sempre maggiore di piccole e medie imprese, che spesso non dispongono di controlli e risorse da destinare alla sicurezza informatica, viene preso di mira dai criminali, mentre le aziende più grandi investono maggiormente nella sicurezza. Gli estorsori utilizzano un'ampia gamma di tecniche di persecuzione, adattano le loro richieste di riscatto ad aziende specifiche e si avvalgono di negoziatori esperti per massimizzare i profitti. Truffe sofisticate Gli attacchi BEC (Business email compromise) continuano ad aumentare, favoriti dalla crescente digitalizzazione, disponibilità di dati, dal passaggio al lavoro da remoto e, sempre più spesso, dalla tecnologia “deep fake” e dalle conferenze virtuali. Secondo l’FBI, le truffe BEC hanno totalizzato 43 miliardi di $ a livello globale dal 2016 al 2021, con un'impennata del 65% solo tra luglio 2019 e dicembre 2021. Gli attacchi stanno diventando sempre più sofisticati e mirati: i criminali ora utilizzano piattaforme di riunioni virtuali per ingannare i dipendenti e indurli a trasferire fondi o condividere informazioni sensibili. Sempre più spesso, questi attacchi sono consentiti dall'intelligenza artificiale che permette di creare audio o video “deep fake” che imitano i dirigenti. L'anno scorso, un dipendente di una banca degli Emirati Arabi Uniti ha effettuato un trasferimento di 35 milioni di dollari dopo essere stato ingannato dalla voce clonata di un direttore d'azienda.La minaccia della guerra informatica La guerra in Ucraina e le più ampie tensioni geopolitiche sono un fattore importante che sta ridisegnando il panorama delle minacce informatiche, in quanto aumentano il rischio di spionaggio, sabotaggio e attacchi cyber distruttivi contro le aziende legate alla Russia e all'Ucraina, oltre che agli alleati e ai paesi limitrofi. Atti cyber sponsorizzati dallo Stato potrebbero potenzialmente prendere di mira infrastrutture critiche, supply chain o aziende.“Per il momento la guerra tra Russia e Ucraina non ha portato a un notevole aumento delle richieste di risarcimento per la cyberassicurazione, ma indica un potenziale aumento del rischio da parte degli Stati nazionali”, spiega Sayce. Sebbene gli atti di guerra siano tipicamente esclusi dai prodotti assicurativi tradizionali, il rischio di una guerra cibernetica ibrida ha accelerato gli sforzi del mercato assicurativo per affrontare la questione della guerra e degli attacchi cyber sponsorizzati da uno Stato sia nella formulazione dei testi di polizza sia nel fornire chiarezza di copertura ai clienti.Gli esperti di AGCS individuano una serie di altri trends evidenziati nel report Cyber: The changing threat landscape, tra cui: - Gli hacker si concentrano sulle supply chain vulnerabili: gli attacchi alla supply chain - che si tratti di infrastrutture critiche come la Colonial Pipeline o di servizi cloud - sono considerati un rischio significativo. Sempre più spesso, i criminali del ransomware utilizzano la minaccia di interruzione del servizio per spingere le aziende a pagare un

riscatto e le imprese manifatturiere sono particolarmente vulnerabili. - Outsourcing del cloud: le aziende continuano a trasferire i loro servizi e l'archiviazione dei dati nel cloud, nonostante le crescenti preoccupazioni sulla sicurezza e sull'aggregazione dei rischi. Affidandosi a un piccolo numero di fornitori di servizi cloud o di sicurezza informatica, si stanno creando grandi concentrazioni verso pochi punti deboli. È opinione comunemente errata che il fornitore di outsourcing o di cloud si assuma la piena responsabilità in caso di incidente. - La responsabilità di terzi, comprese multe e sanzioni, sta diventando sempre più rilevante con i progressi della tecnologia, le organizzazioni che raccolgono più informazioni e l'applicazione delle norme sulla privacy dei dati. Quasi tutti gli incidenti informatici, compreso il ransomware a doppia estorsione, possono portare a cause legali e a richieste di risarcimento da parte delle parti colpite. - La carenza di professionisti ostacola gli sforzi per migliorare la sicurezza informatica. Sebbene ci sia una crescente consapevolezza da parte dei consigli di amministrazione, il numero di posti di lavoro non occupati nel settore della sicurezza informatica in tutto il mondo è cresciuto del 350% negli ultimi otto anni, raggiungendo i 3.5 milioni, secondo le stime, il che significa che molte aziende faticano ad assumere, con un impatto sulla loro capacità di migliorare la propria posizione in materia di sicurezza informatica. - La sicurezza informatica è sempre più vista attraverso la lente ESG. Oggi la resilienza della sicurezza informatica delle aziende viene esaminata da un numero molto maggiore di stakeholder rispetto al passato. Sempre più spesso le considerazioni sulla sicurezza informatica vengono incorporate nei quadri di analisi del rischio ESG dei fornitori di dati, che analizzano le pratiche delle aziende per valutarne la preparazione alla criminalità informatica. Assicurarsi che i processi e le politiche informatiche di un'azienda siano compresi a livello di consiglio di amministrazione e che siano in atto processi di monitoraggio del rischio non è mai stato così importante. In risposta a un ambiente di rischio più complesso e all'aumento dei sinistri cyber, il settore assicurativo è passato a un processo di sottoscrizione più rigoroso nel tentativo di valutare meglio i profili di rischio informatico dei clienti e di incentivare le aziende a migliorare i controlli di sicurezza e di gestione del rischio. “La buona notizia è che stiamo assistendo a una discussione molto diversa sulla qualità del rischio cyber rispetto a qualche anno fa”, afferma Sayce. “Stiamo ottenendo informazioni molto più precise e apprezziamo il fatto che i clienti facciano il possibile per fornirci dati completi. Questo ci aiuta a fornire più valore e a offrire informazioni e consigli utili ai clienti, come ad esempio quali controlli sono più efficaci o dove migliorare ulteriormente la gestione del rischio e gli approcci di risposta. Il risultato netto dovrebbe essere un numero minore o meno significativo di eventi cyber per i nostri clienti e un numero minore di richieste di risarcimento per noi. Questa collaborazione contribuirà anche alla creazione di un mercato assicurativo informatico sostenibile a lungo termine che non si basa solo sulle coperture tradizionali ma anche, in misura crescente, sull'integrazione dei rischi informatici nei programmi captive e in altri concetti alternativi di trasferimento dei rischi".

(Prima Pagina News) Mercoledì 26 Ottobre 2022

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it