24/08/2020

ASSINEWS.it
il quotidiano assicurativo

EAV: € 487
Utenti unici: 1.100

Argomento: Exprivia: si parla di noi

Link alla pagina web

Cyber-attacchi su del 250%

I dati nel report dell'osservatorio di Exprivia relativi al secondo trimestre del 2020 Oltre il 60% degli eventi ha provocato il furto di dati Pagina a cura di Antonio LongoRispetto ai primi tre mesi del 2020, nel secondo trimestre dell'anno, in piena emergenza Covid- 19, si è registrato un incremento degli attacchi informatici di oltre il 250%. Da gennaio a marzo erano stati 47, da aprile a giugno sono stati 171, ben 86 solo a giugno, il mese in cui è stato rilevato il numero maggiore di attacchi, incidenti e violazioni della privacy a danno di aziende, privati e pubblica amministrazione. È quanto emerge dai dati contenuti nella seconda edizione del report elaborato dall'Osservatorio sulla cybersecurity di Exprivia. Crimini informatici e pandemia. Gli esperti di Exprivia, analizzando 40 fonti di informazione pubbliche, ritengono che l'emergenza abbia influito, in maniera decisiva, sulla sicurezza informatica a causa dell'incremento dello smart working, alla maggiore connessione ai social network e alla riapertura delle industrie subito dopo il lockdown.Dalla lettura del report si evince, infatti, che la maggior parte degli attacchi sono da collegare all'emergenza Coronavirus, oltre il 60% degli eventi ha provocato il furto dei dati con una crescita a tripla cifra rispetto al primo trimestre (+ 361%), superando in maniera significativa sia le violazioni della privacy (11% dei casi) che le perdite di denaro (7%).Inoltre, gli analisti evidenziano anche l'elevato rischio che riguarda i sistemi di videosorveglianza presi di mira dagli hacker. Termini come «Corona Antivirus» e simili sono stati utilizzati dai cyber criminali per introdurre software malevoli nei computer delle vittime, compromettendone il funzionamento.«Il cybercrime ha trovato terreno fertile soprattutto a causa di una diffusa mancanza di cultura digitale, anche nei singoli cittadini, e dell'inadeguatezza con cui aziende ed enti pubblici proteggono dati sensibili e sistemi informatici», osserva Domenico Raguseo, direttore Cybersecurity Exprivia, «prevediamo che nei prossimi mesi corrano un rischio elevato di attacchi anche i sistemi di videosorveglianza e i dispositivi IoT collegati a Internet che non vengono protetti adeguatamente, facilitando accessi illegittimi».Crescono gli attacchi «hacktivistici». I dati contenuti nel report sottolineano anche la crescita di un altro fenomeno nel corso del secondo trimestre (oltre il 700%), quello degli attacchi di matrice

«hacktivistica», ossia le pratiche di azione digitale in stile hacker spesso collegate a campagne internazionali su temi di grande attualità come «black-lives-matter» e «revenge-porn».Inoltre, si sono quadruplicate le truffe tramite tecniche di phishing e social engineering (+307% rispetto al primo trimestre, oltre il 37% dei casi), che ingannano l'utente facendo leva su messaggi «esca» via e-mail o su tecniche subdole tramite social network per carpire dati finanziari, ossia il numero di conto corrente o della carta di credito, oppure rubare i codici di accesso ai servizi a cui la persona è abbonata. Anche nel secondo trimestre resta ancora sconosciuta la modalità di attacco informatico in oltre il 30% dei casi (53 attacchi in più nel secondo trimestre), evidenziando la necessità di elaborare adeguati sistemi di protezione. Il 17% degli attacchi, invece, è avvenuto tramite malware, ossia software o programmi informatici malevoli, che hanno sfruttato il Coronavirus per attirare l'attenzione degli utenti.I settori più colpiti. Nel secondo trimestre dell'anno il 26% delle campagne criminali sono state indirizzate verso settori non classificabili mentre il 18% ha riguardato settori multipli; a seguire, tra gli ambiti individuati che hanno ricevuto più attacchi, quello della Pubblica amministrazione e del Cloud (circa il 10% ciascuno sul totale), le cui piattaforme, anche dopo il lockdown, continuano a risentire dello stress per il lavoro da remoto.I settori Finance ed Education rimangono ancora nella lista degli ambiti più vulnerabili, in particolare a giugno università e scuole impegnate con gli esami da remoto.Il decalogo per combattere i cybercriminali. Gli attacchi informatici, sempre più sofisticati, sono in continua evoluzione. Per combatterli, oltre alle soluzioni tecnologiche più avanzate, risulta fondamentale seguire alcuni semplici accorgimenti per proteggere i propri dati in modo efficace.Gli esperti di Cisco hanno, quindi, stilato una sorta di decalogo che riporta alcuni consigli su buone prassi da tenere a mente e mettere in pratica con attenzione.È quindi importante, innanzitutto, utilizzare dispositivi sempre aggiornati, infatti ad ogni aggiornamento dei sistemi la software house risolve i bug presenti nella versione precedente e, aggiornando il sistema operativo, il dispositivo che si utilizza è protetto dai più recenti virus informatici e malware.Il decalogo di Cisco punta l'attenzione anche sulle connessioni VPN: è buona norma collegarsi sempre ad una «virtual private network» se si debba scrivere o rispondere ad una e-mail dal proprio dispositivo utilizzando una rete esterna a quella aziendale.Gli esperti ricordano anche che il backup costituisce parte integrante della sicurezza, quindi bisogna assicurarsi che i dati che serviranno per lavorare da remoto siano archiviati sulla rete aziendale.I liberi professionisti dovrebbero, invece, effettuare un backup completo sia su un hard disk esterno sia su uno dei più comuni sistemi di backup su

cloud.Attenzione anche alle reti Wi-Fi pubbliche, certamente comode ma anche pericolose in quanto il rischio è che alla rete si connetta un hacker o un dispositivo già infetto in grado di raggiungere il proprio computer.Particolare attenzione va naturalmente prestata alle comunicazioni ricevute, le campagne di attacco sono in continua evoluzione e il social engineering è uno strumento spesso utilizzato per indurre le potenziali vittime a cliccare su un nuovo link o ad aprire un allegato apparentemente innocuo. E ancora, gli esperti di Cisco ricordano che le policy delle aziende precisano che tutte le comunicazioni di lavoro devono avvenire tramite gli account aziendali e sono davvero tanti i casi in cui le persone hanno causato danni all'azienda per cui lavorano soltanto perché hanno usato l'account email privato per comunicare.Tradizionale raccomandazione riguarda i dati sensibili, bisogna fare molta attenzione ai messaggi che chiedono informazioni quali dati bancari e password di accesso, è necessario controllare sempre il mittente e il dominio dell'email che è stata ricevuta.Inoltre, è meglio utilizzare, ove possibile, un'autenticazione a più fattori, in grado di bloccare l'accesso in caso una password venga compromessa da un attacco di phishing o quando un malintenzionato tenta di accedere a un sistema non consentito.Nel mirino anche i router domesticiA settembre del 2019 gli attacchi per compromettere i log in dei router sono stati 23 milioni, a dicembre sono diventati 249 milioni, a marzo di quest'anno si sono attestati sui 194 milioni. I cyber criminali stanno compromettendo il funzionamento anche dei router domestici per compiere altri attacchi. Il dato emerge dall'ultimo report Trend Micro dal titolo «Worm War: The Botnet Battle for IoT Territory».In base alle evidenze che scaturiscono dalla lettura del report vi è anche un altro indicatore che riguarda i dispositivi che tentano di aprire sessioni con altri dispositivi collegati tramite Internet of Things.Il protocollo di rete è utilizzato, infatti, per fornire all'utente sessioni di login remote ma non è protetto da crittografia, è quindi preferito dagli aggressori come mezzo per sondare le credenziali dell'utente. Si consideri che, secondo i dati aggiornati a metà marzo 2020, 16.000 device hanno tentato di aprire sessioni con altri dispositivi IoT in una sola settimana. Il trend è preoccupante in quanto i criminali informatici sono in competizione per compromettere il maggior numero possibile di router, in modo da poterli utilizzare per compiere attacchi o per coprire frodi e furti di dati. In particolare, i cybercriminali disinstallano ogni malware che trovano sul router per avere il completo controllo sul dispositivo, la conseguenza maggiore per l'utente, oltre a un calo di prestazioni, è che se il router continua a essere utilizzato per attacchi l'indirizzo IP può essere «bannato» da internet per sospetta attività criminale.©

Riproduzione riservataFonte: