

Argomento: Exprivia: si parla di noi

Cyber-attacchi su del 250%

PAGINA A CURA DI ANTONIO LONGO

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 Rispetto 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



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. © Riproduzione riservata.