Comunicato stampa

swisscom

Cybercriminalità: da dove vengono le minacce informatiche

L'ultima edizione del Cyber Security Threat Radar di Swisscom spiega come gli hacker hanno adattato i loro metodi a seguito della pandemia: indirizzano gli attacchi contro chi lavora in home office e usano la più recente tecnologia IA.

L'ondata di attacchi informatici non accenna a diminuire. Gli hacker continuano a prendere di mira le grandi aziende e le PMI. Con la pandemia, molti collaboratori sono passati alla modalità home office e costituiscono un nuovo bersaglio per gli hacker. Questi ultimi hanno adattato i propri metodi alla nuova situazione.

L'ultima edizione del Cyber Security Threat Radar lo dimostra: gli attacchi sono frequenti e non accennano a diminuire. È anche vero che alcune modalità di attacco, le più classiche, stanno diminuendo. In cambio, però, si riscontrano più frequentemente metodi intelligenti e spesso basati sull'IA. Per aziende e organizzazioni, questo comporta ancora di più la necessità di mantenere tutto sotto controllo: i metodi degli hacker si evolvono in continuazione.

Nuove condizioni, nuovi metodi di attacco

La workplace heterogeneity è ormai tra i rischi più significativi nell'ambito della sicurezza IT. Per i reparti IT e sicurezza, il rapidissimo passaggio alla modalità telelavoro ha comportato livelli di rischio mai visti negli ultimi anni. L'home office e i modelli di lavoro agile e in mobilità, come ad esempio «Bring your own Device» offrono grandi opportunità, ma rappresentano anche altrettante vulnerabilità. Gli hacker sanno bene come sfruttare questa situazione a proprio vantaggio.

Inoltre, ricorrono sempre più spesso ad attacchi che sfruttano l'intelligenza artificiale, i cosiddetti AI-based attack, che il Cyber Security Threat Radar identifica come minacce informatiche in aumento. Si manifestano, ad esempio, in casi di disinformazione mirata, come per le cosiddette deepfake. Tra queste ultime, ha acquisito una grande popolarità il canale di Tiktok «Deeptomcruise». Proponeva video che mostravano Tom Cruise facendo giochi di prestigio e giocando a golf. Il vero gioco di prestigio, però, stava nei video in sé. La star di Hollywood, infatti, non solo non aveva mai partecipato alle riprese, ma addirittura non sapeva niente di tutta questa vicenda. Si trattava di un falso quasi

perfetto, creato usando l'intelligenza artificiale. Questa tecnologia permette agli hacker di sfruttare le più diverse informazioni per creare un profilo falso, che però sembra autentico a tutti gli effetti. Il report descrive le contromisure che le aziende possono adottare per far fronte a questi e altri rischi.

Una bussola per orientarsi nel cybermondo

Nel Cyber Security Threat Radar, gli specialisti di Swisscom hanno analizzato lo stato attuale delle minacce informatiche in Svizzera. Il report spiega che cosa motiva gli hacker e come agiscono. Analizza e valuta tendenze e rischi e, combinando le conoscenze specialistiche di molti esperti, fornisce una visione d'insieme delle minacce informatiche e della loro evoluzione in Svizzera. Oltre a questo, spiega quali contromisure sono più efficaci per riconoscere gli attacchi con maggiore precisione e tempestività. Il Cyber Security Threat Radar funge da documento di riferimento e bussola per orientarsi in sicurezza nel cybermondo.

Berna, 16 aprile 2021

Ulteriori informazioni

www.swisscom.ch/security