MINACCE INFORMATICHE CHE POSSONO COLPIRE UN AZIENDA

Nel campo delle minacce informatiche, sono molti i rischi che un'azienda può affrontare. Gli attacchi più comuni che subiscono le aziende sono principalmente 4, ovvero il phishing, malware, attacchi DDoS e furto di dati.

PISHING: è tecnica la quale scopo è ottenere vari informazioni sugli utenti, come nome utente, password e altre cose. Tuttavia non fa tutto in autonomia, anzi è proprio la stessa vittima a fornirglieli, in quanto spingono la vittima a cliccare qualcosa come per esempio email false, ovvero email che come mittente riportano istituti o servizi famosi e quindi credibili, e che solitamente chiedono di cliccare su un link per eseguire un'operazione nel minor tempo possibile, altrimenti un servizio che utilizzano potrebbe essere cancellato, per esempio un conto in banca. Una volta cliccato il link il gioco è fatto, e le informazioni della vittima arrivano direttamente agli attaccanti. Oltre i link, possono essere anche allegati dannosi, che una volta aperti possono compromettere la sicurezza della rete. In alcuni casi, una mail di pishing può arrivare personalizzata proprio per utente specifico grazie ad informazioni sia private (e quindi rubate), sia pubbliche. I danni che può causare sono:

- Violazione della privacy: furto di identità per effettuare altre truffe
- Violazione dati aziendali: rivelazione di dati sensibili aziendali che ne compromettono la sicurezza
- Perdite finanziarie: un'azienda può avere perdite in quanto a causa degli attacchi, deve sospendere alcune operazioni
- Reputazione: i clienti dopo aver sentito che la rete di un'azienda è stata compromessa, potrebbero virare altrove su altre aziende.

MALWARE: sono dei software progettati per danneggiare, infettare, rubare informazioni o ottenere accesso non autorizzato a un sistema informatico. Si dividono in diverse categorie:

- Virus: si replicano inserendosi in altri programmi o file eseguibili, danneggiano e alterano dati o il computer stesso.
- Worm: sono programmi che si propagano attraverso le reti e possono diffondersi rapidamente tra i dispositivi connessi.
- Trojan: possono essere utilizzati per rubare informazioni sensibili, ottenere accesso non autorizzato ai sistemi o installare altri tipi di malware.
- Ransomware: bloccano un sistema, e poi richiedono un riscatto per lo sblocco
- Spyware: è progettato per spiare le attività dell'utente senza il loro consenso, raccogliendo informazioni sensibili.
- Adware: L'adware mostra annunci indesiderati sul computer attraverso pubblicità false.
- Rootkit: sono programmi progettati per nascondere l'attività del malware o garantirne la persistenza nel sistema, rendendo difficile la loro rilevazione e rimozione.

ATTACCHI DDOS: Un attacco DDoS, o Distributed Denial of Service (Nega del Servizio Distribuito), è un tipo di attacco informatico che mira a rendere inaccessibili i servizi online, come siti web, server, reti o applicazioni, aumentando il traffico dati e creando un sovraccarico. Possono essere lanciati da una singola fonte e vengono utilizzati per inviare grandi quantità di traffico verso il bersaglio. Inoltre, possono coinvolgere una vasta gamma di risorse di rete, tra cui larghezza di banda, capacità di elaborazione del server e risorse di archiviazione. Gli obiettivi degli attacchi DDoS possono variare, ma spesso includono siti web di grandi dimensioni, servizi online, infrastrutture di rete critiche e aziende. Gli attacchi possono essere motivati da una varietà di ragioni, tra cui motivi finanziari, politici, ideologici o di rivalsa. I danni che possono causare gli attacchi DDoS possono causare interruzioni significative nei servizi online, provocando perdite finanziarie, danni alla reputazione aziendale e disagi agli utenti finali. Le organizzazioni possono subire costi elevati per ripristinare i servizi e implementare misure di mitigazione per prevenire futuri attacchi.