Minacce comuni che possono colpire un'azienda

Phishing:

Il phishing è un crimine che inganna le vittime inducendole a condividere informazioni sensibili quali password e numeri di carte di credito. Come nello sport della pesca ("fishing" in inglese), vi sono modi diversi di indurre la vittima ad abboccare all'amo, ma esiste una tattica di phishing più diffusa: la vittima riceve un'e-mail o un messaggio di testo che imita (o "falsifica") una persona o organizzazione di cui si fida, ad esempio un collega, un istituto bancario o un ufficio governativo. L'e-mail o il messaggio contiene informazioni volte a spaventare la vittima, con la richiesta di visitare un sito web e intraprendere azioni immediate per evitare conseguenze negative.

Se l'utente "abbocca all'amo" e fa clic sul link riportato nel messaggio, viene indirizzato sull'imitazione di un sito web legittimo. A questo punto, all'utente viene richiesto di accedere inserendo le proprie credenziali: nome utente e password. Se l'utente è abbastanza ingenuo da eseguire la richiesta, le informazioni inserite saranno trasmesse al criminale che potrà utilizzarle per rubare identità, intercettare accessi a conti bancari e vendere informazioni personali sul mercato nero.

Danni possibili: Furto d'identità, perdita finanziaria, accesso non autorizzato a sistemi o dati, costi di mitigazione.

Malware:

Malware o “software malevolo” è un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema. Ostili, invasivi e volutamente maligni, i malware cercano di invadere, danneggiare o disattivare computer, sistemi, reti, tablet e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo. Proprio come l'influenza, interferiscono con il loro normale funzionamento. Lo scopo dei malware è lucrare illecitamente a spese degli utenti. Sebbene i malware non possano danneggiare gli hardware fisici di un sistema o le attrezzature di rete (con un'eccezione — v. la sezione relativa a Google Android di seguito), possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.

Tra i malware è molto diffuso il **ransom malware**, o **ransomware:** un tipo di malware che blocca l'accesso ai sistemi o ai file personali degli utenti e chiede il pagamento di un riscatto per renderli nuovamente accessibili. Le prime varianti di ransomware risalgono alla fine degli anni '80, e i pagamenti dovevano essere effettuati tramite posta. Oggi, il pagamento del riscatto viene richiesto mediante criptovaluta o carta di credito.

Tipi comuni: virus, worm, trojan, ransomware, adware, spyware.

Danni possibili: Corruzione di dati, perdita di dati, interruzione delle operazioni aziendali, richieste di riscatto, costi di mitigazione.

Attacco DDos:

Un attacco di tipo Distributed Denial of Service (DDoS) è un'arma di sicurezza informatica che mira a interrompere le attività aziendali o estorcere denaro alle organizzazioni prese di mira. Le motivazioni di questi attacchi possono essere legate a ragioni di carattere politico, religioso, competitivo o di profitto finanziario. Un attacco DDoS è tecnicamente la versione distribuita del Denial of Service (DoS), che ha lo scopo di interrompere i servizi di un'azienda. I malintenzionati utilizzano enormi volumi di traffico per sovraccaricare i normali carichi di lavoro, server o interconnessioni di rete per renderli inutilizzabili. Se l'effetto degli attacchi DoS è quello di interrompere un servizio, gli attacchi distribuiti (DDoS) vengono invece eseguiti su scala molto più estesa, con il conseguente arresto di intere infrastrutture e servizi scalabili (servizi Cloud).

Danni possibili:

Downtime dei siti: Un DDoS che colpisce un server Web che espone la home page aziendale rende la pagina irraggiungibile ai clienti legittimi e può portare a una compromissione della reputazione del marchio e una perdita di fiducia.

Attivazione dello SLA: L'irraggiungibilità di un servizio da parte dei clienti può generare diversi problemi e rendere necessaria l'applicazione degli accordi sul livello del servizio, con un impatto economico sull'azienda.

Reazione a catena: Quando da un servizio dipende il funzionamento di diversi siti, eventuali problemi possono comportare la loro mancata disponibilità per un periodo di tempo più o meno lungo.

Costi di Mitigazione: possono sorgere costi significativi per investigare l'incidente, risolvere eventuali vulnerabilità, informare le vittime e ripristinare i sistemi compromessi.

SQL injection:

Gli attacchi SQL injection sono un tipo di attacco informatico in cui gli hacker mirano a iniettare, o inserire, il proprio codice in un sito web, in un'app o addirittura in un programma.Per cui, quando i criminali informatici trovano piccoli errori di script o imprecisioni nel codice sorgente dei sistemi di database basati su SQL, è come se trovassero una porta aperta perché sono in grado di scoprire vulnerabilità nei programmi, nei siti web e nelle app di aziende, banche o enti governative e di iniettare il proprio codice.

Nella maggior parte dei casi, un attacco SQL injection sfrutta una vulnerabilità che può manifestarsi se la connessione tra un'applicazione web e i database è configurata in modo errato. I codici iniettati in questo punto di connessione possono causare molti danni, come ad esempio bypassare la funzione di accesso e il relativo processo di autenticazione o spiare altri dati. Una volta che gli hacker hanno ottenuto l'accesso a un sistema di database basato su SQL tramite una piccola vulnerabilità, possono anche accedere facilmente ai database in cui sono conservati i dati veramente sensibili.

Danni possibili: Accesso non autorizzato, compromissione dei dati, costi di mitigazione.

Zero-day exploits:

Il software presenta spesso vulnerabilità della sicurezza che gli hacker possono sfruttare per scatenare il caos. Gli sviluppatori di software sono sempre alla ricerca di vulnerabilità da "correggere" sviluppando una soluzione da rilasciare in un nuovo aggiornamento. A volte tuttavia gli hacker o i malintenzionati individuano la vulnerabilità prima degli sviluppatori di software. Mentre la vulnerabilità è ancora esposta, gli autori di attacchi possono scrivere e implementare un codice per sfruttarla. Questa tecnica è nota come codice exploit.

Il codice exploit permette di attaccare gli utenti del software, che diventano vittime, ad esempio, di furti di identità o di altre forme di cybercrimine. Dopo aver identificato una vulnerabilità zero-day, gli autori di un attacco devono trovare un modo per raggiungere il sistema vulnerabile. A questo scopo, si servono spesso di un'email di ingegneria sociale, ovvero un'e-mail o un altro tipo di messaggio che si ritiene inviato da un contatto noto o legittimo, ma che in realtà proviene dall'autore dell'attacco. Lo scopo del messaggio è convincere un utente a eseguire un'azione come aprire un file o visitare un sito Web dannoso. Il risultato di questa azione è il download del malware dell'autore dell'attacco, che si infiltra nei file dell'utente e ruba i dati riservati.

Quando una vulnerabilità diventa nota, gli sviluppatori creano una patch per cercare di fermare l'attacco, ma spesso le vulnerabilità della sicurezza non vengono scoperte subito. A volte passano giorni, settimane o addirittura mesi prima che gli sviluppatori identifichino la vulnerabilità all'origine dell'attacco. E anche dopo il rilascio di una patch zero-day, non tutti gli utenti la implementano in tempi brevi. Negli ultimi anni, gli hacker sono diventati più veloci a sfruttare le vulnerabilità non appena scoperte.

Gli exploit sono in vendita sul Dark Web a cifre esorbitanti. Dopo che un exploit è stato individuato e corretto, non costituisce più una minaccia zero-day.

Gli attacchi zero-day sono pericolosi soprattutto perché gli unici a esserne a conoscenza sono proprio gli autori degli attacchi. Dopo essersi infiltrati in una rete, i criminali possono attaccare immediatamente o restare in attesa del momento più vantaggioso per farlo.

Danni possibili: Accesso non autorizzato, compromissione dei dati, distribuzione di malware, costi di mitigazione.

MITM (Man in the Middle):

L'attacco Man-in-the-Middle (MITM) è un attacco informatico in cui un criminale informatico intercetta i dati inviati tra due aziende o persone. Lo scopo dell'intercettazione è quello di rubare, "origliare" o modificare i dati per scopi malevoli, come l'estorsione di denaro. Gli attacchi MITM dipendono dalla manipolazione di reti esistenti o dalla creazione di reti dannose controllate dal criminale informatico. Il criminale informatico intercetta il traffico e lo lascia passare, raccogliendo informazioni, oppure lo dirotta altrove. I criminali informatici agiscono essenzialmente come "intermediari" tra chi invia le informazioni e chi le riceve, da cui il nome "attacco Man-in-the-Middle" (o uomo-che-sta-in-mezzo). Questi attacchi sono sorprendentemente diffusi, soprattutto nelle reti Wi-Fi pubbliche. LaWi-Fi pubblica è spesso non protetta, quindi non è possibile sapere chi sta monitorando o intercettando il traffico web, dato che chiunque può accedervi.

Danni possibili:

Furto di informazioni e interferenza nei dati: Uno degli obiettivi principali di molti attacchi MITM è la cattura di credenziali di accesso. Questo può includere nomi utente e password, PIN, risposte a domande di sicurezza e altre credenziali che possono essere utilizzate per accedere a conti e risorse. L'attaccante può anche modificare le informazioni in transito tra le due parti e l'ascolto delle comunicazioni (eavesdropping) può rivelare informazioni sensibili come dettagli finanziari, piani aziendali, dati personali e altro, che possono poi essere utilizzati per fini fraudolenti o venduti sul mercato nero.

Distribuzione di Malware: Durante un attacco MITM, l'attaccante potrebbe inserire malware o altri software malevoli nei dati in transito, che vengono poi scaricati e eseguiti dalla vittima.

Frodi Finanziarie: Se un attacco MITM è rivolto verso una transazione finanziaria, l'attaccante può reindirizzare i fondi, alterare l'importo di una transazione o intercettare dettagli della carta di credito.

Danni alla Reputazione: Se un attacco MITM viene eseguito contro un'organizzazione e ciò diventa di dominio pubblico, la reputazione dell'organizzazione potrebbe subire danni, portando a perdite finanziarie o di fiducia da parte dei clienti.

Costi di Mitigazione: Una volta scoperto un attacco MITM, possono sorgere costi significativi per investigare l'incidente, risolvere eventuali vulnerabilità, informare le vittime e ripristinare i sistemi compromessi.

Insider threats:

L'insider threat si verifica quando qualcuno legato all'azienda, sfrutta i propri privilegi di accesso per compromettere sistemi e informazioni sensibili dell'azienda stessa. Non deve trattarsi necessariamente di un dipendente; anche fornitori, collaboratori esterni, e partner aziendali possono costituire una minaccia interna. In base alle intenzioni di chi ne è responsabile, l'insider threat può essere involontario, o doloso. L'impiegato che, per negligenza, cade vittima di un attacco phishing, è un esempio di minaccia interna involontaria. Chi invece sottrae o distrugge dati aziendali sensibili, o pratica attività di spionaggio, rientra ovviamente nell'insider threat doloso. La causa principale dell'insider threat sono le persone. Le minacce possono provenire da qualsiasi livello e da chiunque abbia accesso ai dati aziendali, tanto da costituire il 25% di tutti gli incidenti di sicurezza informatica.

Danni possibili: Furto di dati, sabotaggio, fuga di notizie.