BIBLIOTECA

Le minacce informatiche degli ambienti digitali

Introduzione

Salve,

le minacce informatiche degli ambienti digitali sono sempre più diffuse e riguardano tutti noi, che in un modo o nell'altro ci troviamo a lavorare, informarci o frequentare per puro svago gli ambienti digitali.

Questo è l'argomento della lezione di oggi, in cui proveremo a passare in rassegna le principali minacce informatiche, imparando a riconoscerle per essere poi in grado di difenderci da questi attacchi.

Attacchi informatici

Il miglior modo per imparare a difendersi dagli attacchi informatici è raggiungere una buona consapevolezza dei rischi in cui potremmo imbatterci, acquisendo le competenze minime necessarie che possano metterci nelle condizioni di riconoscere - e poter dunque prevenire - eventuali minacce.

È bene quindi definire quelle che sono in questo momento le tipologie di attacchi informatici più frequenti per comprendere la forma che assumono, le dinamiche attraverso cui colpiscono e gli accorgimenti di cui tener conto per evitarle.

Malware

Qualsiasi tipo di software dannoso o fonte di disturbo, creato per accedere segretamente a un dispositivo informatico senza che l'utente ne sia a conoscenza, viene chiamato **malware**, cioè software malevolo.

In genere i malware accedono ai dispositivi attraverso internet o file inviati come allegati alle email e, una volta installati, possono corromperli, sottrarre dati e informazioni e più in generale compiere operazioni volte a danneggiare un utente o un'organizzazione.

Pensiamo, ad esempio, ai malware fileless che vengono eseguiti direttamente nella memoria RAM del computer e non memorizzano alcun file sull'hard disk. Così facendo riescono a completare le loro azioni malevoli senza sollevare sospetti mentre rubano password, si appropriano di file sensibili o utilizzano il computer infetto per diffondersi su altri computer.

Come riconoscere un'infezione da malware

Tipicamente un malware non è in grado di danneggiare fisicamente i dispositivi. L'unico modo per capire che è presente un malware nei nostri dispositivi sono eventuali comportamenti anomali e sospetti, come:

- la lentezza di caricamento o il blocco del **sistema operativo** o delle app presenti sul nostro dispositivo
- l'aumento della velocità della ventola per sovraccarico di utilizzo di risorse
- l'antivirus che smette di funzionare e diventa impossibile da aggiornare
- la modifica della home page del browser senza alcuna autorizzazione
- oppure l'installazione di toolbar con estensioni sconosciute durante la **navigazione** web
- o, infine, lo schermo che si riempie di annunci pubblicitari o di finestre pop-up con avvisi difficili da rimuovere

Tutti questi segnali sono da tenere sotto controllo e ci devono fare insospettire.

Esistono, poi, alcune varianti di malware in grado di nascondersi in profondità nel sistema operativo infetto, passando inosservati anche ai software antivirus.

Può succedere anche che, in altri casi in cui i segnali sono più espliciti, all'improvviso appaia una schermata sul monitor del dispositivo infetto per informare la vittima di aver preso possesso dei suoi dati.

Come vedi, dunque, esistono varie tipologie di malware, distinte in base a come agiscono.

Tra i più noti ci sono gli spyware, gli adware, i trojan, i ransomware e molti altri ancora.

Andiamo aa analizzare qualcuno di questi più nello specifico.

Ransomware

Un particolare tipo di malware è il ransomware che, una volta installato in maniera fraudolenta su un dispositivo, è capace di rendere i dati contenuti nella sua memoria inaccessibili anche allo stesso proprietario.

In questo caso lo scopo di chi sviluppa e diffonde i ransomware è di chiedere un riscatto, in cambio del ripristino dei dati contenuti nel dispositivo infettato.

Di fatto il ransomware potrebbe essere visto come un "sequestro di dati informatici".

Spesso dietro gli attacchi ransomware si nascondono vere e proprie organizzazioni criminali che operano su larga scala infettando migliaia di dispositivi, come è accaduto nel 2017 con l'attacco ransomware WannaCry che ha infettato oltre 230.000 utenti, i quali hanno visto comparire sul proprio computer una schermata contenente un avviso di compromissione del sistema e una richiesta di riscatto in BitCoin.

Europol lo ha definito come il più grande attacco ransomware di sempre.

Phishing

Il phishing è un'altra delle truffe informatiche che si è diffusa sempre di più negli ultimi anni.

Lo scopo è raggirare l'utente per sottrarre informazioni personali.

Nella maggior parte dei casi un attacco phishing inizia con una email, che si presenta con caratteristiche del tutto simili a quelle di una comunicazione ufficiale da parte di una banca, di un istituto postale o di un gestore di servizi informatici.

Nella email viene chiesto all'utente di intervenire per modificare la propria username, password e codici di accesso al sito, oppure i dati delle carte di credito o altri dati sensibili, rimandando a un sito web attraverso un link.

Una volta aperto il link, l'utente viene portato su sito apparentemente simile al sito ufficiale, ma che in realtà è una copia fittizia, situata su un server controllato da chi vuole sottrarre le informazioni personali inserite dalla vittima.

Una volta ottenuti i dati sensibili degli utenti, questi vengono usati per sottrarre denaro dai conti correnti, fare acquisti con le carte di credito e appropriarsi di informazioni preziose contenute negli account personali o aziendali.

Attacchi DDos

Oltre ad agire direttamente sul singolo utente, gli attacchi possono riguardare anche interi sistemi informatici.

Tra questi tipi di attacchi particolari, uno dei più diffusi è il cosiddetto attacco DDos - acronimo dell'espressione inglese Distributed Denial of Service - traducibile in lingua italiana come "Interruzione distribuita del servizio".

Questo tipo di attacco informatico consiste nel tempestare il sito che ospita il servizio di un'azienda di richieste di accesso, fino a sovraccaricarlo per mandarlo in tilt, con l'obiettivo di renderlo irraggiungibile agli utenti e quindi creando un danno all'azienda che offre quel determinato servizio.

Nella maggior parte dei casi, gli attacchi DDos vengono rivolti verso reti di distribuzione e data center, ma può anche essere indirizzato verso un server di posta elettronica.

Le motivazioni che muovono un attacco DDoS possono essere le più svariate e vanno dal cosiddetto hackeraggio dimostrativo per ragioni vandaliche fino all'estorsione, in cui la minaccia di un attacco DDoS serve a intimorire le aziende al fine di estorcere loro denaro.

Come rimuovere i malware

Bene, adesso abbiamo imparato a riconoscere i segnali di un attacco malware e anche, nello specifico, come si comportano i più comuni. Ma nel caso in cui ci dovessimo trovare in questa spiacevole situazione, come dobbiamo comportarci?

Non è semplice rimuovere un malware da un sistema infetto, anche perché come abbiamo visto ci sono casi in cui l'eventuale infezione non produce alcuna attività malevola visibile.

Per eliminare ogni possibile codice malevolo da un dispositivo è quindi opportuno affidarsi a un programma antimalware. Ne esistono vari, uno ad esempio è Malwarebytes, disponibile in versione Windows, Mac e Android.

Non è detto però che possa semplicemente bastare il solo antimalware. I criminal hacker, infatti, investono molto tempo e risorse economiche per sviluppare varianti di malware sempre più evolute e in grado di

aggirare i sistemi di sicurezza aziendale. È quindi utile attivare più livelli di sicurezza per proteggersi da questi attacchi.

Come prima cosa, dunque, attiviamo l'anti-maleware e, terminata la pulizia "fisica" del malware, è opportuno cambiare le password del computer, dello smartphone o del tablet, quella della casella di posta elettronica, dei vari account social, dei siti utilizzati per lo shopping online e, ovviamente, quella dei servizi di home banking e di pagamento online.

In ambito aziendale, inoltre, è opportuno adottare alcune semplici regole di sicurezza informatica utili a mettere in sicurezza il patrimonio informativo.

Innanzitutto, è importantissima la formazione dei propri dipendenti, mirata a metterli in condizioni di saper riconoscere e difendersi dagli attacchi informatici.

In quest'ottica, tutte le aziende dovrebbero prevedere dei piani di formazione continua in materia di sicurezza informatica, che aiutino i dipendenti a districarsi tra i differenti vettori di attacco e mettendoli in condizioni di distinguere, ad esempio, tra una comunicazione ufficiale di un fornitore o di un Dirigente e un'e-mail di phishing con oggetto "Invio Fattura elettronica".

È molto importante adottare anche una policy di patching aziendale che consente ai responsabili dei reparti IT di accorgersi per tempo di un eventuale problema e di gestirlo di conseguenza per rinforzare i punti deboli del sistema, senza limitarsi al loro semplice aggiornamento.

Bisogna poi ricordarsi di installare sempre le patch di sicurezza rilasciate per i sistemi operativi o per le principali applicazioni utilizzate quotidianamente sui server e sugli endpoint aziendali. Questo perché, abbiamo ormai capito, è abbastanza semplice per i cyber criminali identificare dispositivi e software privi di patch su una rete aziendale e, una volta individuati, sfruttare le loro vulnerabilità per comprometterli.

Conclusioni

Bene, anche per questa lezione è tutto.

Abbiamo illustrato i principali attacchi informatici, abbiamo visto come riconoscerli e quali azioni di base possiamo fare per prevenirli e neutralizzarli.

Grazie per l'attenzione e buon proseguimento!