GUIDA ALLA NUOVE PROCEDURE CONCORSUALI

La sicurezza in rete

I rischi informatici negli ambienti digitali

La crescente centralità economica e sociale degli ambienti digitali li ha resi nel tempo luoghi sempre meno sicuri, appetibili per chi voglia trarne profitto mosso da cattive intenzioni. Oggi, la navigazione su internet, l'utilizzo dei servizi online e, più in generale, ogni ambiente digitale, rappresentano un varco potenziale per chiunque sia intenzionato a voler compromettere la nostra sicurezza.

Introduzione agli ambienti digitali

Per ambienti digitali si intendono tutti quegli spazi immateriali - generati mediante l'uso dell'informatica - e accessibili attraverso l'intermediazione di dispositivi digitali, come computer, smartphone, tablet, consolle per i videogiochi o altri strumenti elettronici. L'evoluzione tecnologica rende gli ambienti digitali ogni giorno più persistenti, più frequentati da una moltitudine di persone e sempre meno "virtuali", nel senso che la linea di demarcazione tra ambienti fisici e ambienti digitali tende sempre più a sfumare. Quasi non ci facciamo più caso, ma parlare in tempo reale con i nostri colleghi in videoconferenza, organizzare un incontro attraverso i social network, raggiungere un locale guidati da una mappa sullo smartphone dà la dimensione di quanto "reale" e "virtuale" siano sempre più sovrapposti e integrati l'uno con l'altro.

Sicurezza informatica

In questo contesto di estrema complessità, le misure orientate alla sicurezza informatica degli utenti che frequentano gli ambienti digitali rivestono un ruolo essenziale per garantire lo sviluppo socio-economico della comunità. La sicurezza informatica, intesa come l'insieme dei mezzi e delle tecnologie volte alla protezione dei sistemi informatici, diventa parte integrante dell'infrastruttura su cui si basano gli ambienti digitali, consentendo agli utenti di scambiare informazioni e fruire contenuti senza il timore di imbattersi in potenziali pericoli.

Approccio integrato alla sicurezza informatica

Spesso tuttavia, nonostante le garanzie offerte dalle misure tecnologiche ed informatiche, i sistemi informatici subiscono attacchi a causa della vulnerabilità dovuta al fattore umano, imputabile ad elementi come la disattenzione, l'incompetenza, la disinformazione e più in generale all'assenza di competenze digitali volte a rendere gli utenti più consapevoli dei pericoli presenti in rete. Spesso infatti il fattore umano rappresenta l'anello più vulnerabile della catena della cybersecurity.

Ed è proprio partendo da questa considerazione che la maggior parte degli attacchi informatici sono progettati per colpire innanzitutto l'utente finale, attraverso email ingannevoli o file infetti da virus. Conoscere le diverse tipologie di attacco, quindi, è il primo passo per imparare a difendersi, evitando di cadere in situazioni spiacevoli che possono portare alla perdita di dati o al furto della nostra identità digitale.

Le minacce informatiche degli ambienti digitali

Il modo migliore per contrastare gli attacchi informatici è rendere gli utenti consapevoli dei rischi in cui potrebbero imbattersi, mettendoli nelle condizioni di riconoscere - e così poter prevenire - eventuali minacce (si parla in questo caso di prevenzione della vulnerabilità). 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 tenere 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 i file allegati alle email e, una volta auto-installatisi, possono sottrarre dati e informazioni, o, più in generale, compiere operazioni volte a danneggiare un utente o un'organizzazione. Esistono varie sottocategorie di malware, distinte in base a come agiscono. Tra i più noti ci sono:

- gli spyware (software malevolo che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso)
- gli adware (software indesiderato che mostra messaggi pubblicitari senza il consenso dell'utente che lo ha istallato)
- i trojan (software che permette a terzi di usare le funzioni del dispositivo all'insaputa dell'utente)
- e molti altri ancora

Di seguito approfondiremo ransomware, phishing e furto d'identità, che negli ultimi anni hanno assunto particolare rilevanza a causa della frequenza e della portata dei danni che possono causare.

Ransomware

Con ransomware si fa riferimento a un particolare tipo di malware 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.

Phishing

Il phishing è una delle truffe informatiche che più si è diffusa negli ultimi anni. Lo scopo è aggirare 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, la password e i 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 della 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, appropriarsi di informazioni preziose contenute negli account personali o rubare l'identità digitale del malcapitato.

I furti di identità online

La diffusione dei social network, che portano naturalmente gli utenti a condividere online informazioni sul proprio conto come dati anagrafici, foto e luoghi frequentati, unita alla grande disponibilità di dati personali presenti sui siti web, sta contribuendo all'aumento di una particolare tipologia di crimine informatico: i furti di identità online.

Come avvengono

Per furto d'identità online - noto anche con il nome inglese Identity fraud - si intende la pratica di sottrazione malevola di dati personali, codici bancari e informazioni sensibili da parte di cybercriminali che poi vengono utilizzati:

- per commettere reati
- per spiare la vittima senza essere scoperti
- per creare identità fasulle sui social network

Il furto d'identità online può avvenire principalmente attraverso due modalità:

- tramite il furto delle credenziali di accesso
- oppure tramite la creazione di una falsa identità

Nel primo caso il furto può avvenire attraverso la pratica di phishing, cioè facendo leva su debolezza o impreparazione dell'utente, per metterlo nella condizione di compiere azioni in grado di fornire al malintenzionato le informazioni di cui ha bisogno per effettuare la violazione. Opure forzando un sistema informatico che contiene di dati dell'utente sottraendoli in blocco.

Mentre nel secondo caso, la creazione di una falsa identità si verifica attraverso la creazione su un social network di un profilo utente del tutto simile a quello della vittima, attingendo online le informazioni che servono come il nome, il cognome, la data di nascita, le foto del profilo, eccetera.

In Italia il furto d'identità online è un vero e proprio reato. Secondo il Codice penale, infatti, questa pratica scorretta può rientrare nell'Articolo 494, configurandosi come reato di "sostituzione di persona", o nell'Articolo 640 ,come reato di "frode informatica".

Come difendersi

Per qualunque utente prevenire il furto di identità è davvero molto complesso. Infatti, le attività di hacking dei database contenenti informazioni personali e la creazione di profili fasulli sui vari social network hanno in comune l'impossibilità da parte del derubato di venire a sapere in maniera immediata del furto. Oltre ad adottare le regole di base di buona condotta in ogni ambiente digitale, come:

- utilizzare password complesse
- prestare attenzione alle mail sospette
- o, connettersi ai propri account da connessioni reputate sicure

non ci sono specifiche misure preventive per difendersi dai furti di identità online. Qualora ci si dovesse accorgere di essere stati vittima di un furto d'identità online è importante intervenire con prontezza, segnalando alla piattaforma social il profilo falso in modo che venga bloccato. Oppure rivolgendosi alla Polizia postale per sporgere denuncia.

La costante evoluzione dei rischi informatici

Le minacce informatiche evolvono di pari passo con la tecnologia. Gli hacker - cioè i criminali informatici capaci di violare un sistema informatico per rubarne o manometterne i dati - elaborano tecniche sempre diverse e più raffinate per aggirare le difese dei sistemi di sicurezza. Così come avviene per i software, che si aggiornano con grande frequenza per rinforzare di volta in volta le proprie difese chiudendo le falle di sicurezza, anche gli utenti per difendersi devono stare al passo, mettendosi al corrente dei pericoli in cui potrebbero imbattersi al fine di evitarli. Per questa ragione il rafforzamento delle competenze digitali è un asset fondamentale per garantire la sicurezza informatica dei sistemi tecnologici.