IL WEB NON COLLEGA SOLO MACCHINE, COLLEGA PERSONE

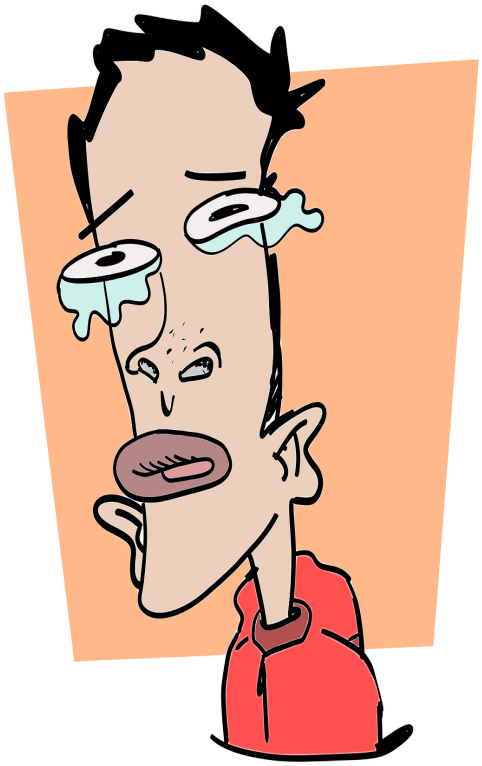
MIGLIAIA DI ATTACCHI INFORMATICI OGNI GIORNO MINANO LA TUA SICUREZZA DIGITALE

Affrontare con superficialità il problema comporta gravi conseguenze.

Esercitando la mia professione, mi sono reso conto di come la maggior parte dei miei clienti ignorino il concetto di sicurezza informatica.

Quando propongo di investire in sicurezza la risposta tipica è la seguente: "*Cosa mai potranno rubare? Non ho nulla di importante*". Purtoppo i cyber criminali contano proprio sul fatto che abbassiate la guardia.

Oltre il 70% degli attacchi informatici avvengono a causa di un errore umano; per questo motivo trascurare la formazione del personale è un grave errore. C'è inoltre da considerare che questi attacchi avvengono sempre su larga scala, per cui se non ne sei mai stato afflitto è solo fortuna.



Gli obiettivi principali di un attacco informatico sono il furto d'identità, il furto di dati, la sottrazione di credenziali, la sospesione temporanea della rete o del server, il sabotaggio dei sistemi informatici e l'utilizzo del dispositivo colpito per condurre un ulteriore attacco.

Le conseguenze di un attacco informatico possono comportare la perdita di fatturato, un danno alla reputazione, la perdita di clienti, il pagamento di una sanzione e in alcuni casi il risarcimento dei danni o la chiusura dell'attività.

La protezione al 100% non esiste: per questo, la prevenzione è la migliore strategia per la tua sicurezza digitale.

RANSOMWARE

Si tratta di un software che infetta il computer il quale, una volta effettuato l'avvio del sistema operativo, mostra una richiesta di riscatto per ripristinare tutti i file che sono stati criptati. Purtroppo, non solo quelli del computer, ma anche quelli su periferiche esterne collegate al momento dell'attacco e le risorse di rete accessibili saranno stati resi inaccessibili.

Si tratta di un attacco devastante, poiché i dati sono persi irrimediabilmente e non c'è modo di recuperarli, se non da un backup. Lo scopo dell'attacco è persuadere l'utente ad effettuare il pagamento a cui ovviamente non segue l'invio della password di decriptazione. Oltre alla perdita dei dati sarà necessario reinstallare da zero il sistema operativo e gli applicativi.

LE CHIAVETTE USB

Qualsiasi dispositivo tecnologico può essere infettato da una chiavetta USB, per questo motivo è importante che l'antivirus abbia attiva la funzione di controllo dei dispositivi rimovibili.

IL BACKUP

Non sempre è possibile riparare a un disastro informatico: perciò, oltre a cercare di prevenirlo, è molto importante poter contare sulla disponibilità di un backup.

Purtoppo capita spesso che il backup non sia stato implementato in modo corretto e che al momento del bisogno non se ne disponga.

Per essere efficace, il backup deve essere svolto su un dispositivo adeguato e su più livelli, impostato per essere eseguito automaticamente e sopratutto controllato periodicamente.

AGGIORNAMENTI

Molto spesso gli aggiornamenti del sistema operativo e delle APP non vengono effettuati. Uno dei motivi per cui questo accade è la mancanza di tempo.

Gli aggiornamenti, però, servono ad installare patch di sicurezza, che eliminano vulnerabilità note, e grazie ad essi spesso è possibile evitare alcuni attacchi.

POLICY

Le password di accesso ai dispositivi informatici non dovrebbero essere troppo semplici da indovinare, inoltre dovrebbero essere soggette a scadenza, integrate con un ulteriore livello di sicurezza a doppio fattore quando possibile ed essere idonee ad un utilizzo esecutivo (e non amministrativo) del dispositivo sul quale sono state implementate.

PHISHING

Sei stato vittima di un attacco di phishing se hai ricevuto una e-mail o un messaggio contenente un link sul quale un mittente che finge di essere qualcun altro (tipicamente un corriere, un fornitore che chiede il saldo di una fattura, la banca, il gestore del tuo sito web che ti chiede di rinnovare il dominio etc.) ti invita a cliccare.

Capita non di rado che in questi messaggi siano presenti degli allegati i quali, se aperti, possono infettare il sistema con un virus. Si tratta in ogni caso di una truffa che ha il fine di rubare i tuoi dati e sfortunatamente c'è sempre qualcuno che abbocca.

Potrebbe essere utile frequentare un corso di informatica di base per imparare come riconoscere e gestire questo tipo d'attacco.

IL GIORNALINO INFORMATICO
A CURA DI GIAMPAOLO LABOUREUR