

Hacker, obiettivo piccole imprese. Più vulnerabili e disposte a tacere

La Provincia dell'8 febbraio 2022, Francesca Bonora, docente della nostra area formazione, parla dell'importanza della cyber security.

Hacker, obiettivo piccole imprese Più vulnerabili e disposte a tacere

Lecco

Molte aziende prese di mira hanno predisposto difese. L'idea di un progetto condiviso per ridurre i costi

Nessuno è immune: gli attacchi informatici possono colpire chiunque e qualsiasi azienda, anche di piccole dimensioni. Anzi, i dati disponibili confermano proprio questo trend: gli hacker non prendono più di mira solo o soprattutto le grandi realtà industriali ma "puntano" con sempre maggiore frequenza le Pmi, perché risultano più vulnerabili e, quindi, garantiscono ai malviventi una più alta probabilità di successo. Del resto, bloccando la rete dell'impresa la si può mettere agevolmente in ginocchio. È una consapevolezza, que-

Lecco Sondrio

Un corso gratuito con l'Api

Vista l'importanza del tema, che ancora non ha fatto breccia in tutte le Pmi del nostro territorio, Api Lecco Sondrio ha deciso di organizzare un corso sulla Cyber Security, che in due lezioni (2 e 9 marzo) darà ai partecipanti le informazioni più importanti sull'argomento. In un recente studio sulla cybersicurezza, circa la metà delle imprese intervistate ha dichiarato di aver subito un attacco significativo nell'ultimo anno, con conseguenze spesso importanti, come la perdita di contratti di fornitura a seguito dell'intrusione informatica. Più in generale, gli attacchi informatici alle aziende anche di piccole dimensioni stanno diventando una

costante e dunque è fondamentale aumentare la consapevolezza e la conoscenza sui temi della difesa informatica. Il corso di Api (gratuito) è volto a introdurre i concetti base inerenti alla sicurezza informatica, portando esempi e casi concreti. Si parlerà tra le altre cose degli strumenti del cyber attack (malware, exploit, phishing, spyware, spamming); di metodologie di analisi del rischio; analisi delle minacce e delle vulnerabilità; valutazione costi/benefici delle politiche di sicurezza; cosa fare in caso di attacco cyber, dalla gestione dell'emergenza alla relazione con le forze di polizia. Info: apilecco.it. C. Doz.

sta, che non molte aziende di piccole e medie dimensioni hanno. Serve dunque lavorare su questo aspetto e per farlo Api Lecco Sondrio ha organizzato una serie di attività formative tenute da Francesca Bonora, information security officer.

«Le Pmi generalmente non denunciano gli attacchi subito, a meno che la situazione non sia talmente grave da imporre loro di rivolgersi a terze parti o all'autorità giudiziaria - ha spiegato l'esperta -. Ma non è una "pecca" solo delle realtà medie e piccole: prima che la legge o regolamenti di settore imponessero diversamente, nemmeno grandi imprese e gruppi comunicavano volentieri di essere rimasti vittima di episodi di questo tipo».

Una lacuna che, però, va a vantaggio degli hacker. «Se la

comunità non è a conoscenza di determinati fenomeni non è indotta a mettere in campo azioni preventive. Invece il ransomware in particolare è molto diffuso ed è la tecnica che più frequentemente si conclude con successo».

Si tratta dell'invio (generalizzato o mirato nei confronti di una determinata azienda, an-

che di piccole dimensioni) di una comunicazione fasulla ma strutturata in modo tale da apparire affidabile, che induce a cliccare sui link i quali portano a pagine web o fanno scaricare file che contengono malware che viene inoculato nel sistema dell'utente. Questo genera una infezione generalizzata che può portare al blocco di tutta l'infrastruttura, compresi server e storage, cosa che dunque blocca l'attività lavorativa. Lo sblocco si potrà ottenere solo dietro pagamento di una determinata cifra in criptovaluta, non tracciabile.

«Nella situazione attuale - ha aggiunto Francesca Bonora - ci sono Pmi che stanno studiando come attrezzarsi, anche a fronte dei consistenti costi che le difese hanno, ma molte altre si stanno ancora chiedendo se sia il caso di porsi il problema e dunque sono intempestive ed esposte». Il pericolo, infatti, c'è per ogni tipo di im-

presa, da quelle che utilizzano l'e-commerce alle imprese manifatturiere la cui manutenzione degli impianti di produzione avviene con aziende che si collegano in remoto.

«I sistemi di difesa ci sono e permettono di limitare i rischi in modo importante. Si tratta di servizi costosissimi, per cui una soluzione di cui abbiamo discusso anche con Api potrebbe essere quella di fare "cartello", unendo le forze delle aziende per suddividere il costo, in modo tale da renderlo sostenibile anche per le piccole realtà». C. Doz.



Francesca Bonora

[Download](#)