la tribuna di Treviso

Quotidiano Data 10-09-2023
Pagina 19
Foglio 1 / 2

Imprese nel mirino dei "pirati"

Unis&f lavora sul fronte delle cyber-sicurezza per Confindustria
«Molti attacchi nascono da comportamenti errati dei lavoratori»

Hacker, se i "complici" sono i dipendenti «Formazione specifica per salvare le aziende»

GUERRA SILENZIOSA

Il complice dell'hacker, seppur involontario, ce l'hai in azienda. «Molti degli attacchi informatici nascono da comportamenti dei singoli lavoratori che si approcciano in modo sbagliato o superficiale rispetto all'utilizzo degli strumenti informatici e ai relativi profili di sicurezza». Pasquale Costanzo è il direttore generale di Unis&f, la società di servizi e formazione del Sistema Confindustria che opera a Nordest. La raffica di attacchi alle imprese negli ultimi mesi diventa simile a un bollettino periodico, col rischio quasi di banalizzare quella che rappresenta una vera emergenza: i danni sono devastanti, milionari.

I PROGETTI DI FORMAZIONE

«Unis&f è in costante contatto con le aziende del territorio che, purtroppo, non hanno ancora una percezione adeguata al rischio del cyber crime – sottolinea Costanzo – Lo dimostra proprio il fatto che molti degli attacchi informatici nascono da comportamenti dei singoli lavoratori che si approcciano in modo sbagliato e/o superficiale rispetto all'utilizzo degli strumenti informatici e relativi profili di sicurezza. Ad esempio, la condivisione della propria password a favore di qualche collega o peggio a favore di uno stakeholder, così come la poca attenzione nel navigare su siti web poco attendibili per poi rilasciare i propri dati personali o aziendali oggi è ancora una prassi diffusa. Unis&f su questo tema dimostra molta attenzione, tanto che ha dato avvio al progetto Cyber security lab (Csl), un centro di competenza dedicato alla sicurezza informatica con il patrocinio di Clusit – Associazione italiana per la sicurezza informatica – e del Club bit, associazione di It Manager del territorio. Csl risponde all'esigenza di colmare la carenza di figure professionali specializzate in questo settore con attività di formazione mirate e simulazioni pratiche di incidenti, confermando che trasformazione digitale e operatività aziendale sono imprescindibili dalla cyber sicurezza».

L'ERRORE: SENTIRSI IMMUNI

Giorgio Sbaraglia, ingegnere, svolge attività di consulenza aziendale di formazione in materia di cyber security: è uno dei relatori del primo executive master in cyber security creato da Unis&f. «Le esigenze delle aziende del Trevigiano sono in linea con quelle del tessuto nazionale, la differenza sta nelle dimensioni delle aziende – spiega Sbaraglia – quelle più grandi hanno forse più "cultura" e più budget per queste attività. Il problema grosso è che le Pmi spesso fanno un ragionamento pericoloso, quello di pensare che a loro non accadrà mai un attacco informatico perché poco "allettanti". Spesso ci si immagina attacchi informatici sofisticati, complessi, e invece nella maggior parte dei casi vedo i pericoli arrivare dai computer aziendali o dai cellulari», spiega l'esperto informatico.

LE FRAGILITÀ

Il 90% degli hacker, sottolinea Sbaraglia, «fa leva sull'errore umano, basta un dipendente che fa clic sulla mail sbagliata per "aprire le porte" ai pirati. I web criminali hanno pazienza, entrano nei sistemi delle aziende e osservano a lungo le abitudini dei dipendenti. Oppure c'è un utilizzo "leggero" delle chiavette Usb, viatico per l'ingresso di malintenzionati. Tutte le aziende potrebbero difendersi adeguatamente con sistemi come un antispam avanzato, una casella per i dipendenti con doppia autenticazione. Non esistono aziende immuni dai cyber attacchi. L'unica soluzione è quella di investire nella sicurezza, e non sempre le imprese sono così lungimiranti da stanziare fondi per queste implementazioni». Ma i conti si fa presto a farli, secondo l'ingegnere: «Un buon intervento per alzare il livello di sicurezza può costare all'incirca 50 mila euro. Pensate a quanto invece può costare a un'azienda un attacco, in termini di danni ai clienti, di forniture non garantite, di reputazione. Se da un lato è molto difficile prevedere dove e quando possano avvenire gli attacchi, dall'altro si può puntare sulla prevenzione attraverso la formazione dei dipendenti, con la cultura d'impresa, lavorando sulla consapevolezza». —

FABIO POLONI

la tribuna di Treviso

Quotidiano
Data 10-09-2023
Pagina 19
Foglio 2 / 2

Pasquale Costanzo, direttore generale di Unis&f, società di servizi e formazione