Proteggete la vostra azienda da attacchi ransomware

Secondo l'Official Annual Cybercrime Report del 2019, ogni 14 secondi un'impresa subisce un attacco ransomware. Con i dipendenti che lavorano da casa senza firewall aziendale, il rischio è ancora più elevato.

Di cosa si tratta?

Il ransomware è un software dannoso che impedisce all'utente di accedere a un sistema o a un dispositivo informatico fino al pagamento di una somma in denaro. Il malware trova e codifica dati preziosi e blocca l'accesso al sistema operativo da parte dell'utente, richiede poi un pagamento - solitamente sotto forma di bitcoin o altra criptovaluta - per rivelare la chiave di codifica.

Non vi è alcuna garanzia che, una volta pagato l'importo richiesto, la vittima ottenga nuovamente accesso al proprio dispositivo e ai dati in esso contenuti.

Backup e aggiornamento

Usate diverse soluzioni di backup e accertatevi che almeno una sia sempre disponibile offline. Ricordate: i servizi di sincronizzazione cloud come Dropbox o Google Drive possono sincronizzarsi dopo la codifica dei dati, rendendo inutile il backup.

Aggiornate regolarmente il software antivirus aziendale e optate per un provider che offra degli add-on in grado di rilevare la codifica dei dati e fare automaticamente delle copie dei file a rischio.

Scegliete una password sicura e modificatela periodicamente. Ricordate che gli attacchi Brute Force rappresentano il 31% di tutti i casi riscontrati.

L'elemento umano

Formate i dipendenti affinché siano in grado di riconoscere e segnalare e-mail sospette; il ransomware può diffondersi facilmente da e-mail di spam e phishing.

Usate sistemi di scansione dei contenuti e filtri e-mail per una protezione aggiuntiva. Questi strumenti possono rilevare link dannosi ed eliminare e-mail pericolose prima che raggiungano i dipendenti.

Predisponete un protocollo di sicurezza standardizzato a livello aziendale, che coinvolga dai dipendenti all'alta dirigenza.

Sviluppate un piano di emergenza che comprenda la risposta a eventuali attacchi. Inserite linee guida tecniche, ma anche strategie per limitare le conseguenze legali e sulla reputazione.

Verificate con la vostra compagnia di assicurazione che la polizza da voi sottoscritta copra i costi associati ad attacchi ransomware.

Create una strategia PR per spiegare la situazione a clienti, investitori e alla stampa in caso di attacco.

Per ulteriori consigli di sicurezza informatica per il vostro impianto visitate il www.euautomation.com