La security secondo Matteo

La realtà parla chiaro: molte aziende considerano ancora la sicurezza informatica come un costo e non un investimento. Una falsa credenza, che richiede un cambio culturale.

Matteo è il titolare di un'azienda attiva in Ticino nel settore manifatturiero. La sua storia è importante e significativa, iniziata negli anni del boom economico dal padre, quasi per gioco. A quel tempo il modello imprenditoriale non seguiva la regola "studia, apprendi che poi qualcuno in futuro ti pagherà per ciò che hai imparato". Tutt'altro. Il modello che ha reso famosa e virtuosa la sua azienda, ereditata in seguito dal figlio Matteo, fondava le sue radici in un concetto tanto semplice quanto disarmante, che di continuo veniva ripetuto in azienda come un mantra ai suoi collaboratori: "le persone non si rivolgeranno a noi perché siamo bravi, lo faranno solo se saremo bravi a risolvere i loro problemi". Pensando ai tempi moderni, in cui numerose start up faticano a instradare sul mercato le loro trovate imprenditoriali, verrebbe da pensare che l'approccio market-oriented, rispetto a quello fantasy-oriented, continui a mantenere il suo pragmatismo agli occhi dei nuovi clienti. Il tempo passa e Matteo ha preso le redini dell'azienda, senza conoscere le reali difficoltà che il padre ha dovuto superare, quando internet non esisteva e la gestione della sicurezza informatica era un privilegio di poche aziende strutturate, che potevano permettersi un tecnico più o meno preparato all'utilizzo e alla gestione dei programmi (a quel tempo) primitivi per la protezione dei dati.

Amarcord. Musica d'altri tempi, soprattutto per una piccola media impresa come quella di Matteo, che oggi impiega decine e decine di collaboratori in svariati settori, con la crescente necessità di avvalersi di prodotti e servizi per la sicurezza moderni, affidabili, robusti e sicuri. Siamo alla fine degli anni Novanta e il suo business cresce in continuazione, al punto che i rudimenti informatici installati fino a quel momento per la protezione dei dati e dell'infrastruttura aziendale non sono più sufficienti. In termini pratici, l'azienda non può più fare a meno dei programmi antivirus e dei sistemi di protezione perimetrale (firewall),

che all'epoca spopolavano sul mercato, atti a impedire infiltrazioni abusive da parte di malintenzionati. In questo modo Matteo riesce a superare indenne il primo decennio degli anni duemila, senza subire alcun attacco informatico, pur continuando a integrare in azienda nuovi dispositivi elettronici, stampanti multifunzione, computer portatili e apparecchi specifici per la validazione della qualità dei prodotti venduti.

Con loro arrivano anche i primi tecnici informatici dedicati alla manutenzione dell'infrastruttura informatica, con il compito di garantire l'interoperabilità dei dati, la sicurezza delle informazioni e la compatibilità di comunicazione tra i diversi dispositivi in uso nei vari reparti. Di questo passo, in pochi anni è venuto a crearsi in azienda un mare magnum tecnologico, che solo pochi tecnici erano in grado di conoscere fino in fondo ogni volta che si verificava un problema. La percezione che Matteo aveva a quel tempo della sicurezza informatica era tale da considerare questo modus operandi normale e privo di anomalie; anzi, si fidava ciecamente dei suoi informatici, ai quali delegava completamente tutta la gestione della sicurezza informatica e le rispettive decisioni strategiche, senza immaginare che questo atteggiamento ingenuo e poco strutturato lo avrebbe portato presto al collasso. Per i tecnici era fondamentale impedire l'accesso alla rete interna aziendale, convinti che antivirus e firewall, se ben aggiornati, fossero sufficienti. La loro concezione di sicurezza non contemplava a quel tempo il fatto che i singoli dispositivi interni collegati alla rete e usati dai vari collaboratori, dovessero anch'essi far parte di una strategia condivisa e centralizzata per la sicurezza delle informazioni aziendali.

In breve tempo, però, qualcosa ha cambiato improvvisamente e drasticamente le loro false credenze. È bastata la prima grande ondata di attacchi informatici, resilienti e mirati a sfruttare le ingenuità operative dei singoli collaboratori durante le attività professionali, per materializzare in azienda una realtà a cui non avevano mai pensato. Sia Matteo che i suoi tecnici erano convinti di essere al riparo da ogni tipo di attacco, e che i loro dati sensibili fossero al sicuro da occhi indiscreti. Falso. Nessuno aveva mai considerato con la dovuta attenzione l'ipotesi che le vecchie stampanti multifunzione in uso nei vari reparti e i computer portatili dei collaboratori fossero anch'essi collegati alla rete Internet, e, se pur protetti da una banale password di accesso, erano privi di protezione, controllo e rivelazione di eventuali virus acquisiti a livello di 'Bios', magari attraverso la lettura di un'e-mail ingannevole, aperta ingenuamente e frettolosamente durante il lavoro.

Preso atto di questa realtà, Matteo ordina ai suoi tecnici di eseguire una distinta dettagliata di tutti i dispositivi elettronici usati in azienda, vecchi e nuovi, nessuno escluso. Voleva disporre di una mappa precisa sullo stato dell'arte di tutto ciò che poteva essere collegato alla rete e da cui potevano transitare i dati aziendali, e quindi potenzialmente attaccabile dall'esterno.

Un lavoro immane per la trascuratezza accumulata nel tempo, ma assolutamente necessario per rimediare, in tempi brevi, a una situazione fuori controllo, soprattutto dopo l'applicazione del nuovo regolamento europeo sulla protezione dei dati (Gdpr). Ne aveva sentito parlare, ma dopo aver preso conoscenza della distinta fatta dai suoi informatici, aveva capito che in caso di attacco informatico la sua azienda non era per nulla protetta.

Il grosso problema non era tanto nella sicurezza perimetrale dell'azienda, di fatto già ampiamente garantita da molteplici antivirus e tunnel di sicurezza cifrati, bensì nelle vecchie stampanti multifunzione e nei computer portatili, non più allo stato dell'arte con quella che oggi viene comunemente chiamata end-point-security.

Serviva un cambio culturale nella gestione della sicurezza informatica aziendale, e Matteo doveva intervenire in fretta, senza però interrompere le attività produttive della sua azienda, e senza mettere in condizione di disagio i propri collaboratori. Ecco perché ha deciso di ridisegnare completamente la rete informatica aziendale, integrando nuovi dispositivi multifunzione ad accesso centralizzato, progettati per garantire un maggior controllo delle minacce cyber e una gestione centralizzata della sicurezza delle informazioni, comprese le ruotine impiegate dal 'Bios' per il controllo delle funzioni di accesso all'hardware delle singole periferiche. La sicurezza informatica dei computer aziendali, delle stampanti e dei dispositivi usati per il controllo delle merci, dovevano essere gestiti con un nuovo paradigma, maggiormente orientato ai sistemi moderni di protezione delle informazioni, integrando anche sistemi innovativi per la protezione visiva dei dati durante il loro utilizzo. Tutti questi cambiamenti, avvenuti con il prezioso accompagnamento di un'azienda leader come Hp, hanno garantito a Matteo e ai suoi collaboratori un incremento strategico della sicurezza informatica durante le attività professionali quotidiane. I vantaggi sono stati molteplici.

> «Serviva un cambio culturale nella gestione della sicurezza informatica aziendale, e Matteo doveva intervenire in fretta, senza però interrompere le attività produttive della sua azienda, e senza mettere in condizione di disagio i propri collaboratori»

I tecnici informatici hanno colto questa occasione per incrementare le loro competenze, e Matteo può avvalersi tutt'ora di strumenti adeguati e moderni per la manutenzione continua e controllata della sicurezza delle informazioni. In una società digitale sempre più interconnessa, affidarsi ad aziende con grande esperienza nel settore della sicurezza offre molteplici vantaggi. Per esempio, la mappa infrastrutturale interattiva che Matteo ha ottenuto dopo questo cambiamento, è usatissima in azienda come guida per gli aggiornamenti tecnici, per la verifica continua dello stato operativo dei singoli dispositivi, ma anche come strumento di alfabetizzazione per migliorare la consapevolezza dei singoli collaboratori quando usano i dispositivi elettronici aziendali.

Alessandro Trivilini

Informazioni di contatto:
HP Svizzera
Alan Boffi
+41 79 438 6556
www.hp.com/ch

Social Engineering

Sala Beatrice - Hotel Dante, Lugano 11 dicembre 2018
Più che un corso, è un evento di grande interesse, su un argomento ancora spesso troppo confuso e sottovalutato.
Insieme a esperti di Cyber Security, vi sarà l'opportunità di scoprire come si progetta e si esegue una campagna di Social Engineering simulata per la propria azienda.
Come si misurano e si presentano i risultati? E come nella realtà questi attacchi possono andare a buon fine prendendo il controllo di un'intera azienda? Ci sarà la possibilità di scoprire insieme come si misura la vulnerabilità umana utilizzando le stesse metodologie di un criminale informatico.
Per informazioni e iscrizioni:
www.ated.ch/social_engineering.jsp