Perché le aziende devono adottare pratiche di sicurezza informatica corrette per rafforzare la resilienza

James Tucker, Head of Field CISO, International di Zscaler

Introduzione

La resilienza informatica è una priorità di molte aziende che cercano di allinearsi alle nuove normative, come NIS2 e il regolamento DORA, in arrivo in tutta Europa. Tuttavia, per quante soluzioni si mettano in atto o per quanti sforzi si facciano, nessuna azienda può essere sempre resiliente al 100% dal punto di vista informatico. Ciò potrebbe essere dovuto al fatto che i dipendenti trovano il modo di aggirare i controlli di sicurezza per semplificare le loro attività quotidiane, o forse perché l'azienda ha un elevato livello di debito tecnico e si trova nell'impossibilità di creare un framework attorno all'intera infrastruttura legacy.

Indipendentemente dalla situazione in cui si trova un'azienda, l'obiettivo della dirigenza e dei team della sicurezza deve essere quello di mantenere il livello più elevato possibile di "cyber igiene", ovvero l'insieme delle buone pratiche da seguire per ridurre al minimo i rischi derivanti dall'utilizzo di sistemi informatici. Ma cosa si intende per "buona" igiene di sicurezza informatica e come possono le aziende evitare le insidie più comuni quando implementano un nuovo approccio alla cybersecurity?

La resilienza si basa su un solido framework

Attualmente, i due principali ostacoli a una buona igiene e resilienza informatica sono la mancanza di un framework di sicurezza coerente e la mancanza di trasparenza da parte dei team IT sui pericoli effettivi che un'azienda si trova ad affrontare quotidianamente. Molte aziende sono reattive ai problemi e dispongono di un mix di strategie e tecnologie che si sono accumulate nel corso degli anni. Per questo motivo possono "sentirsi" preparate ma, di solito, non sono consapevoli delle lacune del loro framework e non dispongono di metodi formali per testare la loro capacità di reazione e resilienza. Il CISO e il team della sicurezza sono visti come un organo interno all'IT e spesso non sono coinvolti nella pianificazione strategica dell'azienda. Questa situazione deve cambiare per far sì che le aziende siano in prima linea in termini di prontezza informatica: l'allineamento della funzione di sicurezza con gli obiettivi strategici dell'azienda non è più negoziabile.

In alternativa, un'organizzazione può disporre di un framework coerente, ma non comunicato in modo adeguato a causa di fattori interni, come le dimensioni dell'azienda o la territorialità. Ne conseguono complessità che fanno sì che alcune misure di sicurezza richiedano settimane per essere implementate o, peggio ancora, che i dipendenti fatichino a comprendere il ruolo che ricoprono nella resilienza informatica. Qualsiasi team della sicurezza dirà che i dipendenti sono spesso la più grande superficie di attacco per le aziende, con molte violazioni che derivano proprio da errori dei dipendenti. Ora, con tecnologie come l'intelligenza artificiale generativa che offrono agli hacker la possibilità di colpire individualmente migliaia di dipendenti in un breve periodo di tempo e in modo più personalizzato, questa superficie di attacco è destinata ad aumentare. Se i dipendenti non comprendono l'importanza di buone pratiche di sicurezza informatica, molto probabilmente ignoreranno i corsi di formazione informatica e continueranno ad abboccare alle esche, mettendo l'azienda a rischio di violazione delle normative.

Coinvolgimento dei dipendenti e semplificazione dei processi

La chiave per risolvere questo problema sta nella formazione contestuale e nell'equilibrio tra arte e scienza della formazione di sensibilizzazione alla sicurezza informatica. I team della cybersecurity devono rendere reali i potenziali pericoli ed essere più trasparenti su ciò che accade effettivamente all'interno dell'azienda: quali sono stati, ad esempio, alcuni dei recenti incidenti mancati? Quali paralleli si possono fare con le violazioni di alto profilo apparse sui media? Quindi, devono informare i dipendenti su come identificare e segnalare i problemi al membro del team IT competente. Anche la presenza di "champion" aziendali che promuovano la cybersecurity è importante per dimostrare che si tratta di un problema per tutti i dipendenti e che deve essere preso sul serio.

Un altro livello di sicurezza che le aziende dovrebbero implementare per limitare i potenziali errori dei dipendenti è l'adozione di un approccio Zero Trust a qualsiasi accesso interno o esterno. Ciò comporta la migrazione dal tradizionale accesso di rete instradato in cui, dopo l'autenticazione iniziale, gli utenti hanno una libertà virtualmente illimitata di muoversi all'interno dei sistemi di azienda, a un accesso più granulare, incentrato sull'identità, dove gli utenti autorizzati hanno un accesso controllato solo ai sistemi a cui hanno diritto. Le moderne implementazioni Zero Trust sono spesso accompagnate da funzionalità di deception e sandboxing, che attirano i criminali informatici in trappole e consentono agli analisti della sicurezza di identificare e mitigare rapidamente qualsiasi violazione del sistema prima che si verifichi un danno effettivo.

Infine, le migliori pratiche di sicurezza degli utenti possono essere positivamente rafforzate da una buona efficienza del sistema e da un'elevata produttività. Gli utenti che hanno a che fare con prestazioni insufficienti dei sistemi IT e devono gestire applicazioni mal progettate sono più propensi a compiere azioni incaute, facendo clic su un link di phishing o utilizzando software o dispositivi non approvati. Ecco perché una user experience soddisfacente dovrebbe essere alla base di qualsiasi strategia di sicurezza informatica, e non pensata in seguito. La sicurezza informatica deve facilitare le attività aziendali e non ostacolare il lavoro.

Conclusioni

La verità è che la conformità non dovrebbe mai essere facile. Se la conformità con le normative è semplice come spuntare un paio di caselle di sicurezza, quella legislazione non merita di esistere.

Per aderire alle normative più recenti, le aziende non devono limitarsi a comprendere la propria dotazione tecnica e a costruirvi intorno un framework di sicurezza, ma devono anche assicurarsi che tutti i membri dell'azienda ne comprendano l'importanza e il loro ruolo nel rafforzarlo. I team della sicurezza devono aiutare l'azienda nel suo complesso a capire che la cyber igiene equivale al concetto di un chirurgo che si lava le mani prima di un intervento. Può non sembrare un grande sforzo o importante come un intervento chirurgico di precisione, ma senza un ambiente pulito le probabilità di morte o di ulteriori problemi aumentano di dieci volte. Lo stesso vale per la cybersecurity.

La cyber igiene dovrebbe essere un imperativo per la dirigenza aziendale nel 2024 e i CISO dovrebbero essere al centro della strategia aziendale per allineare le funzioni di sicurezza e i risultati di business. In caso contrario, le aziende si troveranno rapidamente alla mercé dei legislatori, sia dal punto di vista finanziario che, in alcuni casi, con la minaccia di finire in carcere. Il prossimo livello di preparazione informatica richiede un quadro di sicurezza chiaro, un aumento della consapevolezza informatica dei dipendenti e risultati misurabili allineati agli obiettivi aziendali.

A proposito di Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange protegge migliaia di clienti da attacchi informatici e dalla perdita di dati collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata su SSE, è la più grande piattaforma di sicurezza cloud in line del mondo.

Per ulteriori informazioni:

Tania Acerbi e Monica Fecchio

Prima Pagina

Piazza Giuseppe Grandi 19 - 20129 Milano

e-mail: tania@primapagina.it

e-mail: monica@primapagina.it