Quattro passaggi per **gestire il rischio informatico negli istituti di istruzione superiore**

L'aumento vertiginoso degli attacchi ransomware e di altre violazioni della sicurezza informatica sta travolgendo gli istituti di istruzione superiore e, con essi, le compagnie di assicurazione informatica con cui stipulano contratti per proteggersi.

Come reagire ai rischi crescenti

Il settore dell'istruzione continua a essere intensamente colpito da ransomware e altri attacchi.[1] Gli istituti di istruzione superiore si trovano inoltre ad affrontare sfide informatiche specifiche, come i requisiti normativi specifici imposti da diversi stakeholder nel mondo accademico, amministrativo, della ricerca e dell'assistenza sanitaria.

Allo stesso tempo le richieste di riscatto dei ransomware, che nell'ultimo anno sono più che raddoppiate raggiungendo una media di 2,2 milioni di dollari per attacco [2], si ripercuotono sugli assicuratori informatici con lo stesso impatto di un disastro naturale. "Quando inizieremo a vedere condizioni più estreme, che si tratti di condizioni meteorologiche o di rischi, si assisterà a un concomitante incremento dei costi delle polizze future", afferma Stephen Singh, responsabile di fusioni, acquisizioni, cessioni, private equity e rischi informatici presso Zscaler.

Alla luce di questi fattori, i dirigenti degli istituti di istruzione superiore dovrebbero potenziare la sicurezza informatica dei propri istituti, gestire il rischio informatico e ridurre la probabilità che gli attacchi vadano a segno. Ecco quattro passaggi importanti da seguire:

1. Implementare pratiche di igiene e controlli adeguati

Un primo passo per potenziare la sicurezza informatica e migliorare il profilo di assicurabilità consiste nell'accertarsi che l'istituto segua le best practice del settore. Queste includono la sicurezza degli endpoint, l'autorizzazione a più fattori (MFA), l'applicazione delle patch ai sistemi esistenti, l'implementazione dei backup e la prevenzione della perdita di dati, oltre alla formazione di studenti e personale.

Numerosi studi dimostrano che molte organizzazioni non hanno adottato queste pratiche o le hanno implementate in modo improprio.

Secondo Singh "questo livello di efficacia è incredibilmente importante, soprattutto quando si cerca di misurare, gestire e sottoscrivere polizze sul rischio".

È importante documentare i controlli e le strategie messe in atto, sia per uso interno, sia per gli assicuratori informatici. "Non basta limitarsi a distribuire controlli e strategie", afferma Singh. "È importate stabilire un livello di attribuzione di tali misure pertinente per l'organizzazione e per coloro che potrebbero utilizzare queste informazioni a scopo di audit".

2. Adottare lo zero trust

In termini di difesa informatica, la maggior parte degli istituti ha creato "un guscio duro all'esterno, ma un interno molto morbido", sostiene Singh. "Una volta superato il guscio, gli utenti malintenzionati riescono ad andare ovunque".

Gli istituti dovrebbero invece adottare lo zero trust come framework di sicurezza. Lo zero trust, che Singh descrive come "un percorso, non un prodotto", è un approccio che verifica costantemente l'identità di ciascun utente mentre naviga sulla rete.

Lo zero trust assicura che gli utenti abbiano accesso solo ai sistemi e ai dati di cui hanno bisogno, riducendo notevolmente la probabilità che interi sistemi o archivi di dati vengano compromessi. "Una volta ridotta la superficie di attacco, prevenuto il movimento laterale e bloccata la perdita dei dati, si elimina un'enorme quantità di rischi dal sistema", afferma Singh.

Le architetture IT basate sullo zero trust forniscono inoltre dati e telemetria per monitorare costantemente i comportamenti sospetti e rispondere in modo automatico a seconda del rischio potenziale. L'intelligenza artificiale e il machine learning (AI/ML) stanno potenziando queste capacità e forniscono informazioni molto più approfondite su come gli istituti dovrebbero investire tempo e risorse.

3. Quantificare il rischio informatico

Il passo successivo richiede un cambiamento culturale nel modo in cui gli istituti concepiscono il rischio informatico. La quantificazione del rischio informatico, o CRQ (Cyber Risk Quantification), cambia le carte in tavola, valutando il rischio in termini finanziari. Gli istituti utilizzano valutazioni del rischio e analisi per prevedere il costo potenziale di una violazione, che spesso è nell'ordine di milioni o decine di milioni di dollari.

Sempre secondo il responsabile "questo livello di granularità consente di avere una visione molto più approfondita del livello reale di esposizione".

A partire da queste informazioni, gli istituti determinano in che misura gli investimenti in diverse strategie di sicurezza informatica possano contribuire a ridurre eventuali perdite. Secondo Singh "ognuna di queste strategie rappresenta un modo per abbattere i costi in base all'ammontare della potenziale perdita finanziaria mitigabile attraverso i controlli implementati".

Concentrandosi sulle questioni finanziarie anziché sulla tecnologia, il CRQ consente ai leader degli istituti di discutere le strategie con una prospettiva incentrata sul business. Singh sostiene che "è fondamentale rendere il dialogo più comprensibile per i dirigenti e il consiglio di amministrazione". "Riequilibrare la strategia di investimento in base ai rischi informatici diventa un tema molto più semplice da affrontare con la dirigenza".

In queste valutazioni basate sui dati, i dirigenti senior determinano la quantità di rischio finanziario che l'istituto è disposto ad accettare e lo mitigano con investimenti in controlli di sicurezza informatica o attraverso il ricorso ad assicuratori informatici.

Il 65% delle organizzazioni non ha ancora un piano di resilienza informatica o di risposta agli incidenti per reagire agli attacchi, attacchi che i responsabili degli istituti dovrebbero considerare come inevitabili.

"La considerazione della perdita finanziaria porterà a fare la scelta migliore. "Più si mitiga il rischio, più si riducono i rischi da accettare e quelli da trasferire alle compagnie assicurative", afferma Singh. "Questo porta inoltre a polizze assicurative informatiche più favorevoli, perché si riesce a parlare la stessa lingua".

4. Collaborare con gli assicuratori informatici

Gli assicuratori informatici fanno molto di più che sottoscrivere polizze per le coperture di violazioni e attacchi. Oggi, molti di loro offrono un'ampia gamma di servizi, tra cui la valutazione e la progettazione dei rischi, la risposta agli incidenti e servizi gestiti. Alcuni offrono addirittura servizi legali e di pubbliche relazioni, in caso di violazione.

Preparati al peggio, ma pianifica per il meglio

Innanzitutto, è fondamentale essere realisti riguardo alle minacce. Singh ricorda che il 65% delle organizzazioni non ha ancora un piano di resilienza informatica o di risposta agli incidenti per reagire agli attacchi, attacchi che i responsabili degli istituti dovrebbero considerare come inevitabili.

"Tutti dovrebbero dare per scontato che la compromissione dei sistemi sia già avvenuta o avverrà in un prossimo futuro, in modo da avere un piano di azione", afferma Singh. "Le minacce, i rischi, le vulnerabilità, le violazioni e le estorsioni non hanno mai registrato un'evoluzione tanto rapida. Per questo motivo è importate stabilire quale modello adottare, in modo che le risorse finanziarie abbiano il ritorno sull'investimento più elevato in relazione all'ambiente dell'organizzazione".

Note finali:
1. https://news.sophos.com/en-us/2023/07/20/the-state-of-ransomware-in-education-2023/
2. https://www.zdnet.com/article/ransomware-payments-heres-how-much-falling-victim-will-now-cost-you/

Questo articolo è stato scritto e prodotto dal Center for Digital Education Content Studio, con informazioni e contributi di Zscaler.

Prodotto da:

CENTER FOR DIGITAL EDUCATION

Il Center for Digital Education è un istituto nazionale di ricerca e consulenza specializzato in tendenze, politiche e finanziamenti tecnologici per l'istruzione primaria e superiore. Il Center fornisce al settore dell'istruzione e ai suoi leader supporto decisionale e approfondimenti utili per incorporare efficacemente le nuove tecnologie del XXI secolo.

www.centerdigitaled.com

Con il patrocinio di:

zscaler™ aws

Zscaler, partner software di livello Avanzato di AWS, è la più grande piattaforma di cloud security inline del mondo. Zscaler Zero Trust Exchange agisce come un centralino, collegando in modo sicuro gli utenti direttamente alle app e ai workload (mai alla rete) da qualsiasi posizione e da qualsiasi dispositivo, offrendo una sicurezza zero trust all'avanguardia nel settore. Zscaler riduce i rischi aziendali, migliora la produttività degli utenti e usa informazioni approfondite, aziendali e informatiche basate sull'AI e all'avanguardia per trasformare i dati in conoscenza. In più, il monitoraggio proattivo dell'esperienza digitale mantiene gli utenti produttivi, riducendo al contempo le chiamate al supporto tecnico. Zscaler elimina inoltre i costi, la complessità e i rischi di sicurezza associati alle VPN, ai firewall e ai prodotti singoli tradizionali.

www.zscaler.it