Networking e Security: manca collaborazione



Tra il 2020 e il 2023, secondo IDC i progetti di trasformazione digitale riceveranno finanziamenti per un totale di 6,8 trilioni di dollari a livello globale. La trasformazione digitale è un termine che può essere applicato a una vasta gamma di progetti, ma per tutti questi progetti di trasformazione sarà necessario ripensare le architetture di rete e di sicurezza per supportare nuovi flussi di lavoro e gestire nuovi rischi. Ma una ricerca condotta da Censuswide per conto di Netskope ha rivelato una divisione potenzialmente dannosa tra i professionisti del networking e della sicurezza che potrebbe impedire alle organizzazioni di realizzare i vantaggi che sperano di ottenere dalla trasformazione digitale.

Il 54% dei CIO europei ritiene che la mancanza di collaborazione tra i team di specialisti impedisca alla propria organizzazione di realizzare i vantaggi della trasformazione digitale. In sostanza, ci stanno dicendo che se i team interni non sono in grado di collaborare in modo efficace, la spesa per la trasformazione digitale di $ 6,8 trilioni potrebbe essere sprecata e non riusciremo a ottenere architetture a prova di futuro come Secure Access Service Edge (SASE) basate sulla convergenza di networking e sicurezza.

Oltre ai CIO, la ricerca ha anche intervistato separatamente professionisti della rete e professionisti della sicurezza nel tentativo di comprendere le relazioni che ciascuno ha con l'altro. Se i CIO sono preoccupati per una collaborazione che ritengono inefficace tra i team, quanto in realtà stanno lavorando insieme questi due gruppi cruciali per la trasformazione digitale?

Le notizie non sono buone. Mentre il 45% dei team di sicurezza e networking europei siedono nello stesso gruppo più ampio e riferiscono allo stesso capo, il 43% dei partecipanti alla ricerca condotta in Europa ha dichiarato che “i team di sicurezza e networking non lavorano molto insieme”. Ancora più schiacciante, il 44% dei professionisti della rete e della sicurezza della region ha descritto la relazione tra i due team in termini fortemente negativi come “combattiva”, “disfunzionale”, “fredda” o “irrilevante”.

Qual è la radice di questi problemi? Ebbene, la ricerca mostra che non è che i due team stiano lavorando su obiettivi diversi. Entrambi i gruppi hanno selezionato le stesse tre priorità principali per il 2021; supportare una maggiore produttività per l’intera organizzazione, espandere l’infrastruttura per supportare la crescita aziendale e aumentare la visibilità e il controllo.

Né la questione risiede in una mancanza di opportunità per lavorare insieme. I progetti di trasformazione digitale sono perseguiti da professionisti del networking e della sicurezza (l’85% dei partecipanti alla ricerca sta attualmente lavorando a un progetto di digital transformation o ne ha appena completato uno) e più della metà di questi progetti coinvolge sia la trasformazione della rete che della sicurezza. Lo stesso numero (56%) ha uno sponsor sia all’interno dei team di networking che di sicurezza.

E non c’è problema con l’idea di collaborazione. L’82% di entrambi i gruppi intervistati ha affermato che la sicurezza fa parte della responsabilità del team di networking, rispondendo in particolare che “la sicurezza è integrata nell’architettura di rete”.

Quindi, qual è il problema?

Vent’anni fa la sicurezza rientrava nell’ambito del networking a livello organizzativo, ma da allora abbiamo assistito alla

graduale creazione di un team specializzato in security, che ha raggiunto il suo apice con la creazione del ruolo di CISO. Mentre inizialmente i CISO riferivano al CIO, non è passato molto tempo prima che la portata del rischio che stavano gestendo abbia consentito ai CISO di occupare un posto al tavolo del board, o almeno un'opportunità di relazionarsi con figure C-Level non tecniche. La nuova visibilità ottenuta dal CISO ha creato disaccordi con il CIO e i team di networking e abbiamo visto i team iniziare ad adottare approcci molto diversi per raggiungere gli obiettivi aziendali. Ma i CISO e i CIO non sono l'unico motivo di una divisione tra networking e sicurezza, né sono la ragione principale.

Il ruolo della sicurezza è trovare i problemi e orchestrare la loro risoluzione. E i problemi che si trovano sono molto spesso nelle architetture di rete. Questa è la natura del suo ruolo, ma crea un evidente attrito quando la sicurezza può essere vista come "chi" avanza critiche. Sebbene la sicurezza abbia una sua strategia, si basa sulla rete, sull'infrastruttura e sui team delle applicazioni per eseguire e raggiungere gli obiettivi di business. I team di sicurezza possono selezionare uno strumento, ma i team di neworking e dell'infrastruttura saranno quelli che lo implementeranno e lo eseguiranno.

Come risolvere la questione?

All'interno della più ampia comunità IT, i professionisti della rete e della sicurezza non sono gli unici ad avere frizioni. Vediamo molti degli stessi problemi tra i team di sviluppo, i team operativi IT, tra chi si occupa di applicazioni e di infrastruttura, quindi possiamo cercare di capire come questi altri ruoli IT stiano risolvendo le loro divisioni.

DevOps è stato creato per riunire un team interfunzionale con tutte le competenze e le persone necessarie per creare, distribuire ed eseguire un prodotto o un software, ed è

abbastanza consolidato che riunire i team in questo modo abbia portato vantaggi significativi. Ora stiamo iniziando a vedere che queste lezioni sono state apprese anche dal team di sicurezza. Stiamo iniziando a vedere SecOps (sicurezza + operazioni IT) e DevSecOps (dove la sicurezza delle applicazioni e dell'infrastruttura è progettata sin dall'inizio) come team interfunzionali impegnati a unificare le priorità e intrecciare la sicurezza nei flussi di lavoro di sviluppo e operativi.

Negli ultimi anni abbiamo anche assistito alla formazione di "tiger team" specializzati e agili all'interno delle organizzazioni, incaricati di affrontare specifiche sfide aziendali. Questo approccio di team interfunzionale è stato adottato da molti team di vendita e marketing, il che ha spesso portato l'IT verso lo stesso modello con cui lavoriamo per supportare l'attività aziendale. Nell'ultimo anno il COVID-19 ha dato a molti l'opportunità di ripensare le linee organizzative, utilizzando i Tiger Team per affrontare le sfide legate all'abilitazione e alla sicurezza dei lavoratori remoti. In questi team, ai partecipanti è stata assegnata la missione di abilitare il lavoro a distanza il più rapidamente e umanamente possibile e non rimanere bloccati da infinite approvazioni per questioni come il budget. I team sono stati autorizzati dalla leadership senior per realizzare ciò che propongono e in questo abbiamo visto i silos tradizionali rompersi momentaneamente.

Questi team interfunzionali sono senza dubbio il modo migliore per correggere il divario che vediamo tra networking e security. Una delle manifestazioni quotidiane più irritanti del conflitto di rete e sicurezza è dato da NOC e SOC (centri operativi di networking e di security) che si scagliano ticket l'uno contro l'altro. Questi ticket rimbalzano avanti e indietro senza alcuna volontà di collaborare per affrontare la causa principale del problema. La convergenza di NOC e SOC in un unico centro operativo di sicurezza e rete (SNOC) è un

grande passo avanti nella giusta direzione.

Team dedicati, interfunzionali e basati sulle competenze riducono la necessità di compromessi che abbassano gli standard e la responsabilizzazione da parte della leadership è la chiave del successo. I team dovrebbero concentrarsi sui risultati piuttosto che sull'attività, creando ownership su obiettivi condivisi e risultati chiave. Un esempio di OKR (objectives and key results) potrebbe essere "Migliorare la consapevolezza della sicurezza del mio personale ottenendo una riduzione del 20% del numero di dipendenti che cadono preda di tentativi di phishing simulati". Sebbene sia ancora importante far sì che il lavoro sia visibile all'interno e all'esterno del team, queste strutture ristabiliscono naturalmente la relazione tra networking e sicurezza.

È stato permesso che la relazione disfunzionale tra networking e security sfuggisse al controllo, ma la posta in gioco è troppo alta per continuare a farlo. La collaborazione è fondamentale se un'organizzazione vuole ottimizzare la sicurezza e la gestione del rischio, nonché l'esperienza utente e la produttività. In definitiva, **senza un rapporto di lavoro costruttivo ed efficace, le ingenti somme investite nella trasformazione digitale rischiano di andare sprecate**. C'è un precedente per sistemare le cose ed è ora che i due team si riuniscano per perseguire obiettivi comuni. Unire i team di networking e sicurezza con una collaborazione efficace e strutture rimodellate consentirà alle imprese di intraprendere le trasformazioni di rete e sicurezza che sono essenziali per il successo della trasformazione digitale.

Per consultare la ricerca:

https://www.netskope.com/lp-digital-transformation-needs-a-more-perfect-union/

A cura di **Mike Anderson,** *Chief Digital and Information Officer, Netskope*

https://www.ictsecuritymagazine.com/articoli/networking-e-security-manca-collaborazione/