

Cambia la rete, cambia la sicurezza e così anche i team dell'IT



Che tu sia un esperto di reti o di sicurezza, un CIO, un CISO o un'altra figura chiave dell'IT, starai certamente impostando – o pianificando – la trasformazione della rete e della sicurezza. Lo testimonia una ricerca* (condotta in ottobre 2021) da cui è emerso come **il 99,5% delle aziende europee con oltre 5.000 dipendenti** stia proprio affrontando questo cambiamento. Più della metà è già pronta alla trasformazione, alcune aziende ci stanno già lavorando o la prevedono per quest'anno, mentre il 79% ha già ottenuto, come risultato, un buon risparmio sui costi. Ciò che non è possibile affermare con uguale certezza è in che modo questa trasformazione verrà affrontata: poichè la stessa ricerca ha dimostrato che i responsabili dell'IT sono piuttosto divisi sull'approccio da adottare.

L'unificazione delle discipline

Una delle principali domande cui la ricerca ha cercato di rispondere è stata: “chi si occupa della trasformazione della rete e della sicurezza?”. I dati hanno mostrato che quasi un terzo dei CIO europei semplificano il compito di esecuzione del progetto facendo convergere i team (networking e security). Sebbene tale iniziativa rappresenti un enorme cambiamento organizzativo, è anche molto sensata. I CIO che attualmente pianificano tale convergenza spiegano di ritenerla necessaria perché l'utilizzo del cloud rende oggi inutile la separazione dei team.

L'aggregazione dei team consentirebbe di ridurre i problemi anticipati dal 28% dei responsabili dell'IT, secondo i quali i

team di rete e sicurezza andrebbero a contendersi la titolarità dei progetti. Da un'altra ricerca, svolta all'inizio del 2021, era emerso che il 54% dei CIO europei ritiene che la mancanza di collaborazione tra i team di specialisti impedisca all'azienda di cogliere appieno i vantaggi della trasformazione digitale. Nello stesso report il 44% degli esperti di rete e sicurezza europei aveva descritto la relazione fra i due team in termini fortemente negativi, usando aggettivi come "agguerrita", "disfunzionale", "gelida" o "irrilevante". Quindi, la fusione fra i team di rete e sicurezza è un modo proattivo di evitare inefficienza e dispute.

Il 28% delle aziende secondo la nuova indagine ha già spostato la propria sicurezza nel cloud almeno in parte, riportando anche di aver effettuato modifiche alla struttura o allo staff del team di rete, mentre il 26% ha apportato le stesse modifiche al proprio team di sicurezza.

La scelta delle tecnologie e la divisione degli incarichi

Secure Access Service Edge (SASE), Secure Service Edge (SSE) e Zero Trust Network Access (ZTNA) sono tre degli acronimi in gioco quando si parla di trasformazione in termini di rete e sicurezza. L'architettura SASE è un framework che consente di ripensare la sicurezza e le reti, per soddisfare i requisiti e proteggere dai rischi le aziende cloud native. All'interno di un'architettura SASE, l'SSE consolida le tecnologie di sicurezza. Lo ZTNA è un modello di accesso che, per determinare i permessi, richiede una visibilità granulare e contestuale degli utenti, delle applicazioni e dei dati.

Per quei team di rete e sicurezza che restano separati, i responsabili dell'IT stanno cercando la via per la collaborazione per gestire il grande progetto della trasformazione. La titolarità di SASE, SSE e ZTNA non è sempre

contraddistinta dalla coerenza, poiché alcuni CIO e CISO credono faccia parte delle responsabilità del team di rete, mentre altri di quelle del team di sicurezza.

Nello specifico, il 28% dei CIO ha affermato che dell'architettura SASE erano titolari i team di rete e solo il 18% la assegnava ai team di sicurezza, mentre per il 31% la titolarità era condivisa. Sorprendentemente, la componente SSE (comunemente indicante gli elementi della SASE gestiti dal team di sicurezza) spettava solo per il 18% ai team di sicurezza, per il 30% ai team di rete e per il 33% risultava condiviso. Anche lo Zero Trust Network Access (ZTNA) è risultato essere assegnato principalmente ai team di rete (37% rete, 21% sicurezza, 23% condiviso), mentre resta ancora irrisolta la vecchia questione del secure web gateway – il 23% dei CIO crede che l'SWG spetti ai team di sicurezza, il 28% lo assegna ai team di rete e solo il 27% afferma che viene condiviso.

Due diversi responsabili

La ricerca ha indagato anche nelle linee di riporto, al fine di identificare in che modo CIO e CISO lavorano insieme ai team. Il 67% dei team di IT europei deve relazionarsi sia con CIO che con CISO, in modo diretto o tramite gerarchie indirette. Tuttavia, il 27% delle aziende intervistate ha affermato di non avere alcun CISO al proprio interno (la percentuale più elevata riguarda la Germania con il 31%, quella più bassa il Regno Unito con il 22%).

Talento & reclutamento

Poiché i media citano costantemente la questione dei talenti e del reclutamento nel settore della cyber sicurezza, la ricerca ha indagato su questo argomento anche tra i CIO. Il 28% delle aziende sta ampliando – o pianifica di farlo – il proprio team di sicurezza, per avere a disposizione maggiori competenze necessarie all'uso del cloud. Il 46% ha affermato di essere

già in difficoltà a trovare candidati idonei, oppure prevede difficoltà in futuro.

Quando è stato chiesto ai CIO dove cercano oggi i tecnici per il team di sicurezza del futuro, il 44% ha indicato di volere candidati aventi già competenze ed esperienza in cloud / SaaS / IaaS, sebbene la seconda risposta più comune delinei una strategia di reclutamento totalmente diversa, che punta sulla creatività per vincere le sfide. In effetti, il 38% dei responsabili dell'IT cerca candidati senza cyber competenze o al di fuori del mercato dell'IT, per poi formarli o conferire loro una nuova qualifica. Il 31% delle aziende afferma di voler passare la sfida del reclutamento ai fornitori, affermando che esternalizzerebbero il loro team di sicurezza, mentre il 30% intende acquisire e formare appositamente il personale attingendo dal team di rete, dall'helpdesk o da altri team interni.

Stiamo attraversando un periodo di enormi svolte in termini di sicurezza e rete. I responsabili IT europei stanno affrontando questa sfida con creatività, dimostrando di non aver paura dei grandi cambiamenti in atto. In alcune aree specifiche, i vendor possono essere di supporto: offrendo esempi di best practice e case study dei clienti che hanno per primi adottato la trasformazione, garantendo dettagliate valutazioni TCO che definiscono l'impatto e il risultato positivo delle tecnologie attraverso gli ambiti di rete e sicurezza.

Per maggiori approfondimenti sulla ricerca, consultare <https://resources.netskope.com/ebooks/navigating-change-the-operational-impact-of-network-and-security-transformation>

***Informazioni sulla ricerca**

La ricerca è stata condotta nell'ottobre 2021 da Censuswide per conto di Netskope, intervistando 700 professionisti dell'IT in Germania e nel Regno Unito. Tutti i partecipanti erano CIO, CISO o direttori IT di aziende con più di 5.000 utenti IT.

A cura di **Neil Thacker**, CISO EMEA, Netskope

<https://www.ictsecuritymagazine.com/notizie/cambia-la-rete-cambia-la-sicurezza-e-cosi-anche-i-team-dellit/>