Studio sull'impatto della segmentazione

Settore pubblico

La segmentazione sta emergendo come una potente difesa nel mondo della cybersecurity. Scopri come le organizzazioni del settore pubblico stanno riducendo l'impatto dei ransomware, aumentando la visibilità, rispondendo agli attacchi zero-day, garantendo la privacy e ottemperando ai requisiti di conformità.

Nel settore pubblico, il ransomware non è solo un'interruzione operativa, ma erode anche la fiducia nelle organizzazioni governative, espone informazioni sensibili e, nel peggiore dei casi, costituisce una minaccia per la sicurezza nazionale.

La posta in gioco non potrebbe essere più alta. Nello **studio sull'impatto della segmentazione di Akamai nel 2025**, condotto da Phronesis Partners, l'89% delle organizzazioni del settore pubblico (Federal Civil, Federal DoD e SLED) ha subito attacchi ransomware negli ultimi due anni con il tasso di esposizione più elevato di qualsiasi settore. Oltre alle perdite finanziarie, questi attacchi minacciano i servizi pubblici essenziali, mettendo a rischio le comunità e i cittadini.

Per proteggere la sicurezza locale e nazionale, molte organizzazioni stanno adottando la segmentazione, come delineato dal **NIST**, come parte essenziale della propria strategia di sicurezza e molte altre organizzazioni intendono seguire questo approccio in futuro.

Lo studio di Akamai è stato condotto su 128 responsabili del settore pubblico negli Stati Uniti; in Europa, Medio Oriente e Africa (EMEA); nell'America Latina (LATAM); e in Asia-Pacifico (APAC).

La segmentazione consente di contenere i ransomware più velocemente

Negli enti federali, statali e locali, la segmentazione svolge un ruolo importante nella protezione dei dati governativi. Oltre ai servizi finanziari, il settore pubblico presenta i tassi di implementazione più elevati. Quasi la metà delle organizzazioni del settore pubblico (48%) ha adottato la segmentazione basata sulle identità, mentre il 43% ha adottato la **microsegmentazione**.

La maggior parte delle organizzazioni implementa la segmentazione per isolare le risorse ad alto rischio (74%), contenere i ransomware (66%) e garantire la conformità alle normative (62%).

Il settore pubblico utilizza la segmentazione con un ritmo più elevato rispetto ad altri settori oggetto dell'indagine, soprattutto in relazione alle seguenti risorse:

- Applicazioni business-critical (91%, al primo posto di tutti i settori di questa categoria)
- Server (82%, anche la più alta percentuale del settore)
- Endpoint (82%)

Anche l'impatto tangibile della segmentazione è più elevato nel settore pubblico. Le organizzazioni hanno riportato una riduzione del 46% nel tempo necessario per arrestare un attacco ransomware.

La segmentazione influisce anche sulla conformità. Sebbene la maggior parte delle organizzazioni ritenga che la segmentazione non sia necessaria per la conformità alle normative, il 78% di esse ritiene che ciò aumenti le probabilità di approvazione delle richieste di rimborso.

Risultati principali

L'**89%** delle organizzazioni del settore pubblico ha subito attacchi ransomware negli ultimi due anni

La microsegmentazione consente di contenere i ransomware più velocemente del **46%**

Il **91%** delle organizzazioni del settore pubblico implementa la segmentazione per le applicazioni business-critical

Le tre principali risorse interessate dalla segmentazione:

1. Applicazioni business-critical (91%)
2. Server (82%)
3. Endpoint (82%)

Akamai

La segmentazione è il futuro della sicurezza IT

La segmentazione non sostituisce la sicurezza esistente. Al contrario, le organizzazioni la stanno integrando in strategie più ampie che includono già firewall di rete, accesso remoto/VPN e sicurezza di cloud/CNAPP.

Anche nell'ambito di una strategia più ampia, la segmentazione comporta delle sfide, in particolare relative a costi e complessità, sebbene la resistenza organizzativa possa rallentarne l'adozione. Tuttavia, i vantaggi apportati superano gli ostacoli. La segmentazione limita la diffusione di **ransomware** e minacce interne, protegge i dati sensibili e può ridurre l'impatto delle violazioni, il che la rende uno strumento essenziale per la mitigazione dei rischi.

Il risultato: quasi la metà delle organizzazioni del settore pubblico sta pianificando di **implementare la microsegmentazione** nei prossimi due anni e l'80% degli utenti attuali intende aumentare i propri investimenti in questa tecnologia. Per i responsabili decisionali, questo approccio indica un chiaro caso di utilizzo: investire nella segmentazione oggi rafforza il sistema di sicurezza, riduce i potenziali tempi di downtime e protegge sia le informazioni sensibili che la fiducia pubblica.

Supportare il percorso verso la segmentazione

Con i ransomware e la pressione normativa che aumentano le difficoltà dei team addetti alla sicurezza, un numero sempre maggiore di organizzazioni del settore pubblico sta adottando la segmentazione per:

- Ridurre i tempi necessari per contenere le minacce
- Proteggere le risorse business-critical
- Aumentare le richieste di risarcimento informatiche accolte

Tuttavia, l'implementazione non è sempre facile, soprattutto nel settore pubblico, in cui sono in gioco informazioni sensibili e le interruzioni operative non devono succedere.

Ecco perché il 73% delle organizzazioni del settore pubblico utilizza un'organizzazione di terze parti per le operazioni di sicurezza: il più alto tasso di qualsiasi settore, ad eccezione dei servizi finanziari.

Metodologia di ricerca

Questo rapporto è basato sulle informazioni ricavate da una ricerca proprietaria condotta da Phronesis Partners per Akamai nel 2025, nell'ambito della quale sono stati intervistati 128 responsabili della sicurezza e delle tecnologie, che rappresentano il settore pubblico, inclusi Federal Civil, Federal DoD e SLED (State, Local, Education), allo scopo di offrire una panoramica su come le organizzazioni si stanno approcciando alla segmentazione e come si evolvono per migliorare il loro livello di microsegmentazione. Il campione sottoposto al sondaggio spazia in diverse aree geografiche e dimensioni delle organizzazioni, fornendo una visione dettagliata sulle pratiche attuali, sulle sfide da affrontare e sulle priorità emergenti.

Per leggere il rapporto completo e scoprire le best practice da adottare per la segmentazione, puoi scaricare lo studio sull'impatto della segmentazione nel 2025.

Desideri discutere dei problemi legati alla segmentazione e di come Akamai può aiutarti? **Richiedi una demo** di Akamai Guardicore Segmentation.

Per ulteriori informazioni su come eliminare i rischi nella rete grazie ad un'innovativa tecnologia di segmentazione, visita il sito **akamai.com/guardicore**.

Akamai

Akamai è l'azienda di cybersecurity e cloud computing che abilita e protegge il business online. Le nostre soluzioni di sicurezza leader del settore, l'innovativa intelligence sulle minacce e il team presente su scala globale forniscono una difesa approfondita in grado di proteggere applicazioni e dati critici ovunque. Le soluzioni complete di cloud computing offerte da Akamai assicurano performance elevate e notevoli risparmi grazie alla piattaforma più distribuita al mondo. Le maggiori aziende internazionali si affidano ad Akamai per ottenere la protezione, la scalabilità e le competenze leader del settore di cui hanno bisogno per far crescere le loro attività senza rischi. Per ulteriori informazioni, visita il sito akamai.com o akamai.com/blog e segui Akamai Technologies su X e LinkedIn. Data di pubblicazione: 04/26.