BLOG AKAMAI

Seberapa Efektif Penerapan Segmentasi Anda untuk Memitigasi Risiko Serangan Siber?

oleh Carley Thornell, Cheryl Chiodi, Susan McReynolds, dan Helder Ferrão

Judul ini menjelaskan satu hal tentang pelaku serangan siber: Mereka tidak membeda-bedakan korban. Serangan ransomware ditujukan kepada organisasi berbagai ukuran di seluruh industri, yang mencakup beragam sektor penting seperti ecommerce, perawatan kesehatan, keuangan, dan energi. Tim keamanan dipaksa untuk mencari solusi yang bisa melindungi lingkungan, tanpa mengorbankan kinerja, inovasi, maupun keamanan dan kesejahteraan pelanggannya.

Memberikan pandangan spesifik tentang ancaman ransomware terhadap industri

Industri manakah yang paling berisiko menjadi target serangan siber? Seberapa efektif organisasi dalam sektor tersebut menerapkan solusi segmentasi untuk memitigasi risiko? Untuk menemukan jawabannya, Akamai baru menyelesaikan analisis data survei besar-besaran yang dilakukan oleh 1.200 profesional keamanan global untuk mendapatkan pandangan spesifik tentang ancaman ransomware modern terhadap industri modern serta kemajuan perusahaan dalam menerapkan sekaligus mengubah solusi segmentasi. Para profesional menyampaikan kelemahan dan rencana perbaikan utama.

Apa itu segmentasi?

Segmentasi adalah praktik menyegmentasikan suatu jaringan ke dalam beberapa jaringan kecil. Operator TI telah menggunakan metode seperti firewall internal, jaringan area lokal virtual, serta daftar kontrol akses untuk menyegmentasikan lingkungan dan aplikasi demi menurunkan risiko jaringan flat.

Belakangan ini, mikrosegmentasi dianggap sebagai dasar dari kerangka keamanan Zero Trust modern untuk memperkecil bidang serangan sekaligus meminimalkan kesulitan penerapan.

Poin penting dari 4 laporan tahap baru segmentasi

Hasil penelitian Akamai diringkas dalam empat laporan segmentasi mikro global (tautan di bawah) yang masing-masing mencakup industri kunci yang diserang oleh serangan siber: ecommerce, kesehatan, layanan keuangan, dan energi. Akamai menugaskan Vanson Bourne, pemimpin di bidang penelitian bisnis-ke-bisnis, untuk membuat ebook baru yang membahas pandangan tentang kondisi ancaman di zaman modern beserta dampak signifikannya terhadap strategi segmentasi komprehensif dalam risiko mitigasi.

Berikut beberapa poin penting dalam laporan:

- Ecommerce menjadi organisasi yang paling banyak menerima serangan ransomware, baik itu berhasil maupun gagal, dalam satu tahun terakhir: Rata-rata 167 serangan, dua kali lipat dari jumlah yang dicatatkan oleh sektor terbanyak kedua.

- Organisasi perawatan kesehatan dan ecommerce adalah industri yang cenderung akan mengalami kerugian finansial setelah mengalami serangan keamanan siber: 43% dan 42%, secara berurutan.
- Industri energi mengalami lonjakan serangan ransomware dari tahun ke tahun, dengan jumlah kasus kehilangan data yang juga ikut meroket.
- Organisasi layanan keuangan mengalami peningkatan serangan ransomware sebesar 50%.
- Di Eropa, Timur Tengah, dan Afrika (EMEA), pembuat keputusan keamanan TI dalam industri layanan keuangan makin menekankan pentingnya segmentasi jaringan. Namun, kawasan tersebut mencatatkan jumlah terendah untuk aset yang telah disegmentasi (7%).
- Ecommerce jarang menyegmentasikan server jika dibandingkan dengan industri lainnya: rata-rata hanya 12%, ketimbang 19% secara keseluruhan.
- Perawatan kesehatan sering mengalami masalah seputar pengeluaran dan peralatan berhak milik ketika menyegmentasikan jaringannya (41%, ketimbang 32% secara keseluruhan).
- Dari tahun 2021-2023, serangan ransomware terhadap organisasi perawatan kesehatan melonjak sebesar 162%.

Segmentasi mengurangi bidang ancaman

Temuan paling signifikan adalah fakta bahwa industri yang mengalami serangan dapat pulih

11-13 jam lebih cepat (tergantung jenis industrinya) dengan menerapkan segmentasi di seluruh area bisnis yang penting, seperti aplikasi, pengontrol domain, titik akhir, server, dan lainnya. Manfaat signifikan dan terukur lainnya adalah: identifikasi penyusupan serta penahanan serangan yang lebih cepat.

Mengungkap tren industri dan regional

Laporan menyoroti tren industri yang sedang populer.

- Perawatan kesehatan dan ecommerce unggul sebagai industri yang sering terancam oleh serangan siber.
- Selain itu, survei menyatakan bahwa profesional keamanan dalam industri layanan keuangan merasa lebih yakin dengan tingkat keamanan siber mereka dibandingkan profesional dalam sektor lainnya.
- Laporan mencatat bahwa 24% organisasi energi tidak menerima serangan siber dalam setahun terakhir, padahal rata-rata serangan terhadap industri lainnya adalah 5%. Namun, serangan yang berhasil menyusupi industri energi dapat berdampak lebih parah bagi masyarakat.

Setelah meneliti setiap industri, laporan memberikan wawasan tentang aktivitas dan dampak serangan dari sisi regional.

- Organisasi ecommerce di Amerika Latin (LATAM) lebih banyak yang memprioritaskan mikrosegmentasi (42%), ketimbang organisasi di Asia-Pasifik (APAC; 35%), Amerika Serikat (34%), dan EMEA (26%).
- Serangan ransomware yang menargetkan ecommerce jauh lebih sering terjadi kepada organisasi di Amerika Serikat (rata-rata 312 kali dalam 12 bulan) ketimbang di EMEA (91 kali), APAC (119 kali), atau LATAM (68 kali).
- Selain itu, layanan keuangan menjadi sektor dengan jumlah rata-rata serangan tertinggi di APAC (73 kali). Rata-rata serangan di Amerika Serikat adalah 59 kali.

- Responden APAC di ecommerce umumnya menderita kerugian finansial dari serangan ransomware, di mana lebih dari separuh (51%) mengalami kerugian, dibandingkan rata-rata keseluruhan kawasan lainnya yang hanya 42%.

Poin utama dari serangan siber adalah kapan, bukan jika

Menurut Richard Meeus, Director of Security Technology and Strategy, EMEA, di Akamai, “Organisasi harus memberlakukan semua serangan sebagai penyusupan. Bukannya dramatis, tapi dengan demikian, bisnis dapat berfokus pada inti bisnis mereka. Organisasi harus menyegmentasikan jaringan agar sulit diterobos oleh calon pelaku serangan yang ingin mencuri data berharga.

“Layaknya kapal selam, kebocoran di salah satu ruangan tidak akan membuat kapal tenggelam, karena kebocoran bisa diatasi dengan menutup sekat ruangan. Sayangnya, poin utama dari serangan siber adalah kapan, bukan jika. Alangkah baiknya jika kita dapat mencegah kebocoran daripada harus memperbaiki kerusakan, atau bahkan tenggelam.”

Seiring dengan serangan ransomware yang makin marak dan berdampak, segmentasi juga kian condong menjadi pusat strategi Zero Trust perusahaan. Laporan status global baru tentang mikrosegmentasi memberikan pandangan inovatif yang berpusat pada industri seputar topik keamanan krusial.

Pelajari selengkapnya

Baca selengkapnya di laporan spesifik industri yang berdampak berikut ini:

- Layanan keuangan
- Perawatan kesehatan
- Ecommerce
- Energi

Baca selengkapnya