

# HOW DO I KEEP MY ONLINE BANK ACCOUNT SAFE?

## DEFINISI

*Online/Internet banking* adalah layanan melakukan transaksi perbankan melalui jaringan internet. Merupakan kegiatan perbankan yang memanfaatkan teknologi internet sebagai media untuk melakukan transaksi dan mendapatkan informasi lainnya melalui *website* milik bank. Kegiatan ini menggunakan jaringan internet sebagai perantara atau penghubung antara nasabah dengan bank tanpa harus mendatangi kantor bank. Nasabah dapat menggunakan perangkat komputer *desktop*, *laptop*, *tablet*, atau *smartphone* yang terhubung ke jaringan internet sebagai penghubung antara perangkat nasabah dengan sistem bank.

## bagaimana kita dapat menjaga keamanan bank dari luar maupun dari dalam?

### Visibility

Visibilitas ke infrastruktur internal bank Anda hanyalah awal untuk mendapatkan kembali kendali atas ketakutan pelanggaran data Anda. Dengan mensegmentasi jaringan Anda di zona keamanan berdasarkan aset, pengguna, dan mitra yang memiliki profil keamanan serupa atau akses ke aset, orang IT memperoleh visibilitas yang lebih baik ke dalam interaksi dengan karyawan, dan dapat menggunakan teknologi inovatif tanpa meningkatkan tingkat risiko pada jaringan.

Keamanan bukan hanya tentang infrastruktur dan bank teknologi beroperasi. Ini tentang karyawan, mitra, dan segala sesuatu yang berhubungan dengan bisnis dan asetnya. Untuk membuat keputusan investasi yang tepat dalam keamanan dan masih menjalankan inisiatif strategis, perlu ada tingkat visibilitas di antara eksekutif bank dan profesional IT. Kedua pihak perlu mengajukan pertanyaan yang tepat untuk menjaga visibilitas jaringan mereka yang tepat untuk membuat keputusan yang tepat dalam berinvestasi dalam keamanan.

- Siapa yang memiliki akses ke data?
- Jenis informasi apa yang dapat mereka akses?
- Dari mana komunikasi itu berasal?
- Kapan orang mengakses informasi?
- Bagian mana dari infrastruktur yang rentan terhadap serangan?

Sangat penting untuk menemukan solusi yang memberikan tingkat transparansi tertinggi di berbagai tim yang terlibat dengan keamanan organisasi, menghilangkan silo intelijen ancaman dan informasi jaringan di sepanjang jalan.

Visibilitas memungkinkan Anda untuk mengetahui di mana infrastruktur Anda terpapar risiko cyber, dan kemudian mengurangi kerentanan Anda terhadap serangan jahat.

Seringkali orang jahat sama pintarnya, atau lebih pintar lagi, guru IT di perusahaan yang mereka serang. Mereka tidak memiliki lapisan peraturan dan perusahaan yang membebani lembaga keuangan, yang memungkinkan mereka menjadi lebih gesit. Namun, peretas dan penjahat dunia maya juga tidak disiplin. Banyak yang akan menempuh jalan dengan resistensi paling rendah, jadi cara terbaik bagi bank Anda untuk memajukan inisiatif strategisnya adalah dengan meminimalkan permukaan serangan Anda dan bukan menjadi sasaran empuk. Tingkatkan visibilitas Anda, baik secara internal maupun eksternal dan keamanan jaringan Anda akan dengan cepat menjadi lebih baik daripada pesaing Anda - dan Anda akan mengurangi risiko organisasi Anda menjadi korban serangan.

### **Be a head of the game**

Ledakan ancaman membuat banyak bank mencari lebih banyak solusi keamanan. Apa pun yang dapat dilakukan lembaga keuangan untuk tetap menjadi yang terdepan dalam permainan ini sangat bernilai; bahkan jika itu berarti melakukan tolak ukur terhadap rekan, mitra, dan pesaing Anda.

Jika Anda dapat mempelajari apa yang dilakukan pesaing, Anda dapat membandingkan strategi Anda dengan strategi mereka; melihat ancaman intelijen khusus untuk ekosistem perbankan, termasuk pelanggan, vendor perusahaan dan mitra, dan mencari celah di infrastruktur bank. Dengan membuat tolak ukur terhadap rekan-rekan Anda dan mempelajari strategi mereka, Anda dapat memindahkan postur keamanan jaringan institusi Anda dari yang responsif ke yang pencegahan.