



Menjaga bisnis Anda tetap aman saat kerja jarak jauh diperlukan

Direktur Keamanan Informasi Alcatel-Lucent Enterprise, Sebastien Roche, berbagi pandangan tentang pendekatan ALE terhadap keamanan dan kelangsungan bisnis di masa sulit ini.

Realita baru #WFH

Munculnya krisis kesehatan internasional baru-baru ini dan peraturan untuk tinggal di rumah yang diterapkan secara global membuat perusahaan yang sebelumnya tidak menawarkan pilihan bekerja dari rumah (#WFH), kini menghadapi tantangan untuk mengubah organisasi mereka guna memastikan bisnis tetap berjalan dan aman.

Di tahun 2008, Alcatel-Lucent Enterprise memprakarsai strategi bekerja dari rumah yang dilakukan oleh lebih dari 50% dari 2.000 karyawan yang bekerja di 50 kantor di seluruh dunia. Ada lebih dari setengah karyawan ALE yang bekerja dari rumah. Hal tersebut menjadi bukti bahwa kami telah memiliki jaringan dan arsitektur TI yang diperlukan untuk mendukung kerja jarak jauh. Tantangan yang sebenarnya adalah bagaimana cara kami untuk bertransisi dari 50% pekerja online menjadi 100%.

Siap beraksi

Dalam tiga tahun sebelum pandemi terjadi, ALE telah memulai transformasi ekstensif di bidang TI. ALE menggunakan arsitektur jaringan WAN Berdasarkan Layanan, yang memberikan keamanan *cloud* untuk secara proaktif memblokir utas, mengidentifikasi potensi serangan, dan memastikan akses yang aman bagi karyawan.

Transformasi ini mencakup:

- Keamanan di *cloud* dengan titik akses virtual
- Pelacakan secara *real-time*
- Mengidentifikasi pola perilaku yang tidak biasa untuk mendeteksi ancaman





Persiapan = Respon yang tangkas dalam situasi krisis

Keputusan untuk mulai bekerja jarak jauh pada hari Senin dibuat pada hari Jumat sore sebelumnya. Karyawan diberi instruksi untuk membawa pulang laptop mereka. Pekerjaan di hari Senin pagi dimulai seperti biasa, tanpa gangguan, karena karyawan memulai hari mereka dari kantor jarak jauh. Transformasi jaringan yang sebelumnya dilakukan memastikan konektivitas jarak jauh yang aman di mana pun karyawan berada.

Tantangan akses

Salah satu tantangan utama yang kami hadapi adalah terkait profil pengguna, termasuk tim dukungan teknis dan R&D. Mereka memiliki kebutuhan khusus untuk mengakses server dan platform pengembangan tertentu, yang tidak diizinkan oleh solusi akses jarak jauh kami. Profil pengguna karyawan ini melewati solusi akses pribadi yang berbeda dari tim lainnya.

Ketika upaya untuk mentransisikan semua karyawan ke #WFH dimulai, kami menyesuaikan infrastruktur untuk meningkatkan bandwidth agar dapat mendukung peningkatan jumlah koneksi jarak jauh yang dibutuhkan oleh karyawan yang bekerja dari rumah.

Keamanan menjadi kuncinya

Keamanan dan perlindungan data perusahaan sangat penting dalam masa-masa yang tak menentu. Banyak organisasi yang menangani data sensitif, seperti organisasi sektor publik, kementerian, kota, dan kota kecil mengalami dampaknya.

Bahkan sebelum adanya #WFH di ALE, kami telah menggunakan infrastruktur terdistribusi dan aman, serta solusi koneksi pribadi yang sepenuhnya berbasis *cloud* untuk semua karyawan, guna memastikan akses jarak jauh yang aman ke jaringan. Kami mempertahankan solusi VPN lama untuk sebagian kecil tim yang memiliki kebutuhan khusus, seperti menyambungkan perangkat telepon IP di kantor jarak jauh mereka. Kami juga memberi karyawan PC profesional yang mampu mengelola pengunduhan dan pembaruan perangkat lunak secara otomatis.

Menutup celah pelanggaran keamanan

Nyatanya, selama periode kerja jarak jauh yang ekstensif ini, telah terjadi peningkatan panggilan dan email masuk terkait masalah email yang mencurigakan, dan permintaan pembaruan kata sandi. Kami juga melihat lonjakan serangan *phishing* serta serangan yang ditargetkan pada perangkat lunak yang rentan.

Meskipun penggunaan proxy melindungi ALE dari masalah utama keamanan siber, kami masih melihat pelanggaran baru setiap hari, dari email, unduhan, atau dari versi perangkat lunak/OS yang tidak diperbarui.

Jaga agar komunikasi tetap berjalan

Selama masa sulit ini kami terus menjalin hubungan virtual dengan tim ALE. Kami berkomunikasi secara rutin, berbagi kiat dan praktik terbaik, serta memastikan bahwa tim kami siap mendukung semua karyawan.

Daftar periksa ALE untuk kerja jarak jauh yang aman

- Jangan mengizinkan atau menganjurkan penggunaan perangkat pribadi (PC) untuk melakukan komunikasi dan pertukaran data profesional
- Aktifkan akses pribadi yang aman untuk karyawan
- Otomatisasi Pembaruan perangkat lunak di seluruh jaringan perusahaan
- Perhatikan permintaan email yang mencurigakan
- Gunakan perangkat lunak bersertifikat. Audit dan sertifikasi akan memberikan autentikasi keamanan perangkat lunak.
- Sederhanakan proses pengambilan keputusan. Dalam situasi darurat, CISO atau CIO perlu membuat keputusan dengan cepat untuk mengatasi masalah guna memastikan kesinambungan layanan

Brosur

Menjaga bisnis Anda tetap aman saat kerja jarak jauh diperlukan



Enam rekomendasi ALE untuk konektivitas jarak jauh yang aman



1. Otomatisasi pengingat perubahan kata sandi

Bantu karyawan mengubah kata sandi perusahaan sebelum kadaluwarsa. Sebelum kadaluwarsa, karyawan akan menerima email setiap hari yang meminta mereka untuk mengubah kata sandi.

2. Aktifkan pencadangan data di *cloud*

Izinkan dan anjurkan karyawan untuk menyimpan data secara teratur guna menghindari kerugian jika terjadi masalah dengan laptopnya. Aktifkan ruang penyimpanan cadangan data dan tawarkan bantuan jarak jauh melalui Layanan Bantuan TI atau spesialis TI jika diperlukan.

3. Ingatkan karyawan tentang praktik terbaik perlindungan perangkat

Jaga laptop Anda tetap dalam kondisi prima:

- Matikan laptop di penghujung hari (hindari mode *sleep*/penguncian)
- Jauhkan laptop dari sumber panas (seperti matahari atau pemanas)
- Jangan makan atau minum di samping laptop
- Amankan kabel dari jangkauan anak-anak dan hewan peliharaan

4. Utamakan keamanan

Berikan edukasi kepada tim tentang risiko dan praktik keamanan terbaik

- Anjurkan karyawan untuk berpikir dua kali sebelum mengklik tautan di email, meski email tersebut tampaknya dikirim oleh seseorang yang dikenal
- Tawarkan tindak lanjut TI jika ada keraguan
- Sediakan alat pelaporan untuk kasus email yang mencurigakan

- Gunakan gamifikasi untuk menciptakan budaya yang mengutamakan keamanan: ALE menggunakan gamifikasi untuk mendorong karyawan agar dapat mendeteksi dan melaporkan email yang mencurigakan

5. Komunikasi

Saat terisolasi, karyawan akan rentan terhadap serangan siber. Temukan cara agar tim Anda dapat tetap terhubung:

- Atur pembaruan rutin, rapat virtual, acara, ruang kolaborasi, dan waktu besenang-senang
- Dorong karyawan untuk terhubung dengan tim secara teratur
- Kirim email rutin untuk memberi tahu karyawan bahwa tim TI siap membantu dan ingatkan mereka tentang praktik terbaik keamanan secara teratur

6. Dorong kebiasaan konektivitas yang sehat

Risiko kerja jarak jauh adalah konektivitas terus-menerus dan rapat tanpa bertatap muka selama jam kerja 12 jam. Himbau karyawan untuk meluangkan waktu beristirahat dari depan layar, dan menghabiskan waktu bersama keluarga atau di luar ruangan.



Alcatel-Lucent Rainbow™ untuk kolaborasi yang terhubung

Rainbow: platform kolaborasi cloud untuk melakukan obrolan, panggilan video dan audio, serta untuk berbagi layar dan dokumen yang membuat karyawan ALE tetap terhubung. Selama masa #WFH, platform ini telah digunakan secara luas oleh semua karyawan untuk berkolaborasi dengan rekan kerja.

Selain itu, mitra dan pelanggan kami juga telah menggunakan Rainbow sebagai pilihan solusi kolaborasi. Rainbow memenuhi persyaratan keamanan di sektor publik, pertahanan, pelayanan kesehatan, dan sektor spesifik lainnya serta mematuhi peraturan keamanan yang ketat termasuk: GDPR, ISO 27001, HDS, dan lain-lain.



Brosur

Menjaga bisnis Anda tetap aman saat kerja jarak jauh diperlukan



Mendukung komunitas kami

Sebagai bagian dari kampanye Kelangsungan Bisnis, ALE telah menawarkan ratusan ribu lisensi gratis untuk membantu perusahaan, kota, dan pemerintah mempertahankan kesinambungan layanan. Selain itu, untuk mengatasi lonjakan permintaan, serta lonjakan jumlah pengguna, kami telah memperluas kapasitas *cloud hosting*.

Untuk mengetahui praktik terbaik keamanan siber lainnya, lihat [rekomendasi Badan Keamanan Siber UE](#).

www.al-enterprise.com Nama dan logo Alcatel-Lucent merupakan merek dagang Nokia yang digunakan di bawah lisensi oleh ALE. Untuk melihat merek dagang yang digunakan perusahaan yang terafiliasi ALE Holding, kunjungi: www.al-enterprise.com/en/legal/trademarks-copyright. Semua merek dagang lainnya adalah properti dari masing-masing pemiliknya. Informasi yang ditampilkan dapat diubah tanpa pemberitahuan. ALE Holding maupun semua afiliasinya tidak bertanggung jawab terhadap kesalahan informasi yang tercantum dalam teks ini. © Copyright 2023 ALE International, ALE USA Inc. Hak cipta dilindungi undang-undang di semua negara. DID20060201ID (Maret 2023)