SANS SECURITY AWARENESS

Panduan Penerapan Kesadaran Keamanan–
Bekerja Aman di Rumah

Rangkuman Eksekutif

Karena Coronavirus, banyak organisasi mendapati diri mereka mengalihkan tenaga kerjanya untuk bekerja dari rumah. Hal ini cukup menantang karena banyak organisasi tidak punya kebijakan, teknologi, dan pelatihan untuk mengamankan tenaga kerja jarak jauh. Selain itu, banyak karyawan mungkin belum terbiasa atau kurang nyaman dengan ide bekerja dari rumah. Tujuan panduan ini adalah untuk memungkinkan Anda dengan cepat melatih orang-orang tersebut menjadi seaman mungkin. Jika memiliki pertanyaan tentang cara menggunakan panduan ini, hubungi kami di support@sans.org.

Karena tenaga kerja Anda kemungkinan besar sedang melalui tekanan dan perubahan yang besar, dan organisasi Anda juga memiliki keterbatasan waktu dan sumber daya, panduan strategis ini berfokus membuat pelatihan menjadi semudah mungkin. Kami menyarankan untuk fokus hanya pada risiko paling utama yang akan membawa dampak terbesar, yang kami gambarkan di bawah ini. Anggaplah ini sebagai titik awalnya. Jika ada risiko atau topik lain yang ingin Anda tambahkan, silakan Anda lakukan. Ketahuilah bahwa semakin banyak perilaku, proses, atau teknologi yang Anda wajibkan pada tenaga kerja, semakin kecil kemungkinan mereka dapat menerapkan semuanya.

Cara Menggunakan Panduan Ini

Kami sarankan Anda memulai dengan membaca materi dalam panduan ini dan meninjau tautan ke materi berbeda yang diberikan untuk memberi Anda gambaran tentang hal yang tersedia. Anda akan menyadari bahwa untuk setiap risiko, kami memberikan berbagai materi berbeda yang dapat Anda gunakan untuk berinteraksi dan melatih organisasi Anda. Hal ini membuat Anda bisa memilih pengandaian yang dirasa paling sesuai untuk kebutuhan dan budaya Anda. Setelah selesai membaca dokumen ini, baca Template Komunikasi dan Factsheet pendukung yang ada dalam kit ini untuk lebih memahami hal yang Anda sedang coba capai. Setelah Anda meninjau dokumentasi, ada dua grup inti yang perlu Anda koordinasi.

1. **Tim Keamanan**: Koordinasikan dengan tim keamanan Anda untuk lebih memahami jenis risiko utama yang berusaha Anda kelola. Dalam panduan ini, kami telah mengidentifikasi risiko yang menurut kami tertinggi dan paling sering terjadi perihal tenaga kerja yang bekerja di rumah, namun risiko Anda bisa saja berbeda. Sekadar peringatan, kesalahan umum yang dilakukan tim keamanan adalah mencoba mengelola semua risiko dan membebani orang dengan banyak kebijakan dan persyaratan. Cobalah membatasi risiko yang akan Anda hadapi sesedikit mungkin. Setelah Anda mengidentifikasi dan memprioritaskan risiko tersebut, konfirmasikan perilaku yang bisa mengatasi risiko tersebut. Seperti yang sudah disebutkan, jika organisasi Anda tidak mempunyai waktu

atau sumber daya untuk hal ini, maka manfaatkan hal yang kami dokumentasikan di bawah ini.

2. **Komunikasi**: Setelah Anda mengidentifikasi risiko manusia tertinggi dan perilaku kunci untuk mengelola risiko tersebut, maka bekerja samalah dengan tim komunikasi untuk berinteraksi dan melatih tenaga kerja Anda perihal perilaku tersebut. Program kesadaran keamanan paling efektif memiliki kemitraan yang kuat dengan tim komunikasinya. Bahkan jika memungkinkan, cobalah untuk memasukkan seseorang dari komunikasi ke dalam tim keamanan Anda. Ketika berkomunikasi dengan tenaga kerja, umpan efektif yang dapat Anda gunakan untuk berinteraksi dengan mereka adalah menekankan bahwa pelatihan ini tidak hanya mengamankan mereka dalam bekerja, tetapi juga memungkinkan mereka untuk menciptakan rumah Aman Dunia Maya yang melindungi mereka dan keluarga.

Pada akhirnya, dengan bekerja bersama dua grup ini, Anda berupaya membuat keamanan semudah mungkin untuk tenaga kerja Anda serta memotivasi mereka, dua elemen penting dalam perubahan perilaku. Kami sarankan Anda untuk juga mendirikan Dewan Penasehat berisi orang-orang penting yang tanggapan dan masukannya Anda perlukan untuk menjalankan program. Selain tim keamanan dan komunikasi, departemen lain yang mungkin Anda ingin ajak kerja sama dan koordinasikan antara lain adalah SDM dan Legal.

Paket Unduhan Digital MGT433

SANS Institute menyediakan kursus pelatihan dua hari MGT433: Cara Membangun, Merawat, dan Mengukur Program Kesadaran Keamanan Berdampak Besar. Kelas intensif ini menyediakan semua teori, keterampilan, kerangka kerja, dan sumber daya untuk membangun program kesadaran berdampak besar yang memungkinkan Anda untuk efektif mengelola dan mengukur risiko manusia. Sebagai bagian dari panduan ini, kami memberikan akses gratis ke Paket Unduhan Digital kursus berisi template dan sumber daya perencanaan. Meskipun kemungkinan besar materi ini di luar kebutuhan kegiatan ini, materi ini mungkin berharga untuk organisasi yang lebih besar atau penerapan yang lebih kompleks.

Menanggapi Pertanyaan Tenaga Kerja

Selain berkomunikasi dan melatih tenaga kerja Anda, kami sangat menyarankan beberapa jenis teknologi atau forum tempat Anda dapat menjawab pertanyaan orang-orang, sebaiknya dalam waktu nyata. Hal ini dapat mencakup email alias khusus, saluran Skype atau obrolan Slack, atau beberapa jenis forum online seperti Yammer. Bisa juga dengan mengadakan webcast keamanan yang diulang beberapa kali seminggu agar orang dapat memilih waktu terbaik bagi mereka dan menonton acaranya langsung, bahkan mungkin mengajukan pertanyaan. Tujuannya adalah Anda ingin membuat keamanan semudah mungkin dilakukan dan membantu orang dengan pertanyaan mereka. Ini merupakan

peluang luar biasa untuk berinteraksi dengan tenaga kerja Anda dan memberi kesan ramah tentang keamanan, cobalah memanfaatkan hal ini. Untuk melakukannya secara efektif, kami menyarankan Anda untuk mendedikasikan sumber daya untuk menyederhanakan saluran ini dan menanggapi pertanyaan.

Materi Risiko & Pelatihan

Kami telah mengidentifikasi tiga risiko utama yang harus dikelola untuk tenaga kerja jarak jauh Anda. Ini merupakan titik awal dan yang kemungkinan besar hal-hal yang sangat bernilai untuk Anda. Setiap risiko berikut mempunyai tautan ke berbagai sumber daya untuk membantu membicarakan dan melatih topik tersebut. Kami menyediakan berbagai materi komunikasi agar Anda dapat memilih yang akan berdampak paling besar untuk budaya Anda. Selain itu, hampir semua materi tersedia dalam berbagai bahasa. Jika semua ini terlalu membebani dan waktu Anda sangat terbatas, kami menyarankan Anda untuk menerapkan dua materi berikut saja.

1. Factsheet Bekerja Dengan Aman dari Rumah (disertakan dalam Kit Penerapan Anda)
2. Video Menciptakan Rumah Aman Dunia Maya juga tersedia dalam bahasa lain di sini

Rekayasa Sosial

Salah satu risiko terbesar yang akan dihadapi pekerja jarak jauh, terutama pada masa perubahan dramatis lingkungan yang gawat ini, adalah serangan rekayasa sosial. Rekayasa Sosial adalah serangan psikologis saat penyerang menipu atau mengelabui korbannya agar melakukan kesalahan, yang akan menjadi lebih rentan dalam masa perubahan dan kebingungan. Kuncinya adalah melatih orang mengenai rekayasa sosial, cara mengenali indikator paling umum dari serangan rekayasa sosial, dan yang harus dilakukan saat menemukannya. Pastikan Anda tidak hanya berfokus pada serangan email phising, tetapi juga metode lain yang melibatkan panggilan telepon, pesan teks, media sosial, atau berita palsu. Anda dapat menemukan materi yang Anda butuhkan untuk melatih dan menyampaikan topik ini di folder Materi Pendukung Rekayasa Sosial. Selain itu, berikut dua video Kesadaran Keamanan SANS yang dapat Anda tautkan, sekali lagi dalam berbagai bahasa.

- Rekayasa Sosial (Bahasa Inggris) juga tersedia dalam bahasa lain di sini
- Phising (Bahasa Inggris) juga tersedia dalam bahasa lain di sini

Kata Sandi Kuat

Seperti yang disebutkan dalam Verizon DBIR tahunan, kata sandi lemah tetap menjadi salah satu pendorong utama dalam pelanggaran dalam skala global. Ada empat perilaku kunci untuk membantu mengelola risiko ini, tercantum di bawah. Anda dapat menemukan

materi yang dibutuhkan untuk melatih dan menyampaikan topik dan empat perilaku kunci ini dalam folder Kata Sandi kami.

- Frasa sandi (catatan, baik, gunakan kata sandi berbeda kerumitan kata sandi dan masa kedaluwarsa sandi sudah tidak berlaku).
- Kata sandi unik untuk semua akun.
- Pengelola Sandi
- MFA (Multi-Factor Authentication) (Autentikasi Multi-Faktor). Disebut juga Autentikasi Dua Faktor atau Verifikasi Dua Langkah

Sistem yang Diperbarui

Risiko ketiga adalah memastikan teknologi apa pun yang digunakan tenaga kerja Anda berjalan dengan versi terkini dari sistem operasi, aplikasi dan aplikasi seluler. Untuk orang-orang yang menggunakan perangkat pribadi, hal ini mungkin memerlukan pembaruan otomatis. Anda dapat menemukan materi yang dibutuhkan untuk melatih dan menyampaikan topik ini dalam folder Malware atau Menciptakan Rumah Aman Dunia Maya.

Topik lain untuk dipertimbangkan

- **Wi-Fi**: Mengamankan jalur akses Wi-Fi Anda. Hal ini dibahas dalam materi Menciptakan Rumah Aman Dunia Maya. Selain itu, harap pertimbangkan video ini tentang Video Menciptakan Rumah Aman Dunia Maya (Bahasa Inggris) juga tersedia dalam bahasa lain di sini.

- **VPN**: Yang dimaksud dengan VPN dan alasan Anda harus menggunakannya. Kami menyarankan buletin OUCH tentang VPN.

- **Bekerja dari Jarak Jauh**: Ini ditujukan pada individu yang bekerja dari jauh tetapi TIDAK bekerja dari rumah, seperti di kafe, bandara, atau hotel. Pertimbangkan untuk menggunakan Video pelatihan Bekerja dari Jarak Jauh (Bahasa Inggris) kami juga tersedia dalam bahasa lain di sini.

- **Anak-Anak/Tamu**: Untuk menyampaikan ide bahwa keluarga/tamu tidak boleh mengakses perangkat terkait pekerjaan, pertimbangkan untuk menggunakan Video pelatihan Bekerja dari Jarak Jauh (Bahasa Inggris) juga tersedia dalam bahasa lain di sini.

- **Deteksi/Tanggapan**: Apakah Anda ingin orang melapor jika mereka merasa ada insiden selama bekerja di rumah? Jika ya, apa yang Anda ingin mereka laporkan dan kapan? Hal ini dibahas di materi Diretas kami.

Buletin OUCH

Selain itu, pertimbangkan untuk menggunakan buletin OUCH yang tersedia untuk publik guna mendukung program Anda, yang masing-masing diterjemahkan dalam lebih dari dua puluh bahasa. Berikut ini buletin OUCH yang menurut kami paling baik mendukung kegiatan Bekerja Aman di Rumah. Anda dapat menemukan semua buletin di Arsip Buletin Kesadaran Keamanan OUCH online.

RANGKUMAN

Four Steps to Staying Secure (Empat Langkah agar Tetap Aman)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Membuat Rumah Aman Dunia Maya)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

REKAYASA SOSIAL

Social Engineering (Rekayasa Sosial)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging/Smishing (Pesan/Smishing)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Penipuan Terpersonalisasi)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Penipuan CEO)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks/Scams (Serangan/Penipuan Panggilan Telepon)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Hentikan Phising Itu)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Menipu Anda Lewat Media Sosial)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

KATA SANDI

Making Passwords Simple (Mempermudah Kata Sandi)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login(2FA) (Kunci Login Anda(2FA))
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

TAMBAHAN

Yes, You Are a Target (Ya, Anda Adalah Target)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Perangkat Rumah Pintar)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Tips Cepat

Tips dan trik yang dapat Anda bagikan dengan mudah untuk menyerap format.

- Langkah paling efektif yang dapat Anda ambil untuk mengamankan jaringan nirkabel di rumah adalah dengan mengubah kata sandi admin default, mengaktifkan enkripsi WPA2, dan menggunakan sandi kuat untuk jaringan nirkabel Anda.
- Perhatikan semua perangkat yang terhubung ke jaringan rumah Anda, termasuk monitor bayi, konsol game, TV, alat rumah tangga, atau bahkan mobil Anda. Pastikan semua perangkat tersebut dilindungi kata sandi yang kuat dan/atau menggunakan versi terkini sistem operasi mereka.
- Salah satu cara paling efektif untuk melindungi komputer Anda di rumah adalah dengan memastikan sistem operasi dan aplikasi Anda tertambal dan terbarui. Aktifkan pembaruan otomatis jika memungkinkan.
- Pada akhirnya, akal sehat adalah perlindungan terbaik Anda. Jika email, panggilan telepon, atau pesan online terkesan janggal, mencurigakan, atau tak masuk akal, mungkin itu adalah serangan.
- Pastikan Anda menggunakan kata sandi yang kuat dan unik untuk setiap akun. Tidak bisa mengingat semua kata sandi/frasa sandi? Coba gunakan pengelola sandi untuk mengelola semua kata sandi dengan aman.
- Verifikasi dua langkah adalah salah satu langkah terbaik untuk mengamankan akun mana pun. Verifikasi dua langkah adalah ketika Anda memerlukan kata sandi dan kode

yang dikirim ke atau dibuat oleh perangkat seluler Anda. Contoh layanan yang mendukung verifikasi dua langkah adalah Gmail, Dropbox, dan Twitter.

- Phising adalah ketika penyerang berusaha mengelabui Anda untuk mengeklik tautan berbahaya atau membuka lampiran dalam email. Waspadai email atau pesan online mana pun yang menciptakan kesan mendesak, mempunyai ejaan yang buruk, atau menyapa Anda sebagai "Pelanggan Yang Terhormat."

Metrik

Metrik perilaku cukup sulit untuk situasi ini karena lebih sulit mengukur cara manusia berperilaku di rumah. Selain itu, beberapa perilaku ini tidak berstandar pekerjaan (seperti mengamankan perangkat Wi-Fi mereka). Namun, Anda dapat mengukur interaksi. Kami mendapati bahwa topik pribadi atau emosional seperti ini bisa sangat interaktif, menarik lebih banyak minat dibanding topik lainnya. Karena itulah, metrik seperti ini mungkin berguna.

- **Interaksi**: Seberapa sering orang bertanya, memposting ide, atau meminta bantuan di saluran keamanan atau forum mana pun yang Anda adakan?
- **Simulasi**: Adakan sejenis simulasi rekayasa sosial, seperti serangan berbasis phising, pesan, atau panggilan telepon.

Untuk daftar metrik yang lebih komprehensif, unduh Matrix Metrik Kesadaran Keamanan interaktif dari Paket Unduhan Digital MGT433.

Lisensi

Penulis Kit Penerapan

Lance Spitzner telah berpengalaman lebih dari 20 tahun dalam penelitian ancaman siber, arsitektur dan kesadaran keamanan dan pelatihan. Beliau membantu mencanangkan bidang penipuan dan kecerdasan siber dengan karyanya, honeynets dan merupakan penemu Honeynet Project. Sebagai instruktur SANS, beliau mengembangkan kursus MGT433: Kesadaran Keamanan dan MGT521: Budaya Keamanan. Selain itu, Lance telah menerbitkan tiga buku keamanan, melakukan konsultasi di lebih dari 25 negara, dan membantu lebih dari 350 organisasi dalam membangun program kesadaran dan budaya keamanan untuk mengelola risiko manusianya. Lance adalah pembawa acara, pencuit aktif (@lspitzner) dan bekerja di berbagai proyek keamanan masyarakat. Sebelum keamanan informasi, Mr. Spitzner mengabdi sebagai tentara di Rapid Deployment Force dan memperoleh gelar S1 di University of Illinois

Tentang SANS Institute

SANS Institute didirikan tahun 1989 sebagai organisasi penelitian dan pendidikan kooperatif. SANS merupakan penyedia yang paling dipercaya, dan sejauh ini, paling besar dalam bidang pelatihan dan sertifikasi keamanan siber untuk profesional di institusi pemerintahan dan komersial di seluruh dunia. Para instruktur SANS yang terkenal mengajar lebih dari 60 kursus di lebih dari 200 acara pelatihan keamanan siber baik langsung maupun online. GIAC, afiliasi dari SANS Institute, mengesahkan kualifikasi praktisi lewat lebih dari 35 sertifikasi dalam keamanan siber secara teknis dan langsung. The SANS Technology Institute, sebuah anak perusahaan terakreditasi wilayah, menawarkan gelar master di bidang keamanan siber. SANS menawarkan berbagai sumber daya gratis untuk komunitas InfoSec, termasuk proyek konsensus, laporan penelitian, dan buletin. SANS juga mengoperasikan sistem peringatan dini Internet: The Internet Storm Center. Di pusat SANS terdapat banyak praktisi keamanan, mewakili berbagai organisasi global dari perusahaan sampai universitas, yang bekerja sama untuk membantu seluruh masyarakat keamanan informasi. (https://www.sans.org)