GLOBAL CYBER ALLIANCE™

Buku Panduan Toolkit Keamanan Siber GCA untuk Usaha Kecil

Selamat datang

Kolega Yang Terhormat:

Internet adalah bagian yang sangat penting bagi sebagian besar bisnis perusahaan saat ini. Dalam bisnis Anda, menjamin keamanan ekosistem digital bisnis adalah hal yang sangat penting. Serangan siber dapat menimbulkan kerugian yang sangat besar, misalnya kerugian finansial, pencurian informasi sensitif, terganggunya rantai pasokan, dan banyak lagi.

Banyak hal penting dan tanggung jawab di tangan Anda, dan kami telah bekerja untuk menyediakan sumber daya yang benar-benar dapat Anda gunakan untuk memenuhi kebutuhan keamanan siber. Toolkit Keamanan Siber untuk Usaha Kecil Global Cyber Alliance (GCA) menyediakan alat gratis dan efektif untuk mengurangi risiko siber Anda. Alat-alat dipilih dengan cermat dan terorganisasi untuk memudahkan Anda menemukan dan menerapkan langkah-langkah penting yang akan membantu melindungi bisnis Anda dari ancaman siber. Kami memiliki video serta forum komunitas yang dapat Anda manfaatkan untuk menemukan dukungan dan melakukan tanya jawab dengan rekan dan pakar keamanan Anda. Toolkit ini dirancang untuk Anda, pelaku usaha kecil yang ingin mendapatkan keamanan siber layaknya perusahaan yang memiliki pakar keamanan siber serta anggaran yang besar.

Buku Panduan Keamanan Siber GCA untuk Usaha Kecil adalah sumber pelengkap toolkit yang akan memandu Anda selama penggunaannya. Anda dapat mengunduh buku panduan dalam versi utuh atau per bab, untuk mempelajari tindakan yang direkomendasikan dalam toolkit. Panduan ini memfasilitasi Anda untuk bekerja sesuai dengan kemampuan dalam mengambil tindakan dan dapat digunakan sebagai dokumen referensi yang praktis.

Sumber daya ini akan diperbarui secara berkala dengan masukan dari pengguna, pakar industri, dan mitra di seluruh dunia.

Kami harap toolkit dan buku panduan ini bermanfaat bagi Anda untuk mulai meningkatkan keamanan siber sekarang!

Salam,

Philip Reitinger
PRESIDEN DAN CEO

Daftar Isi

Bab Buku Panduan

Ketahui Aset Anda

Apa Permasalahan Yang Dibahas Di Kotak Peralatan Ini?

Mengetahui aset yang Anda miliki adalah langkah pertama untuk mewujudkan keamanan yang lebih baik, karena Anda tidak dapat melindungi aset jika tidak sadar bahwa Anda memilikinya. Perlu diketahui, banyak serangan siber dan pelanggaran data disebabkan oleh laptop dan perangkat lain yang hilang atau dicuri, akses tidak sah ke akun, dan kerentanan perangkat lunak yang tidak di-pacthing dengan baik. Dengan mengetahui komputer, perangkat, dan perangkat lunak (aset) yang Anda miliki, Anda akan lebih memahami potensi risiko yang mungkin ada, yang akan memungkinkan Anda untuk membuat keputusan secara sadar dan mengambil langkah-langkah untuk mengurangi risiko tersebut.

- Tahukah Anda jumlah laptop dan perangkat seluler yang bisnis Anda miliki, siapa yang dapat mengaksesnya, serta perangkat lunak dan aplikasi apa yang ada di dalamnya?
- Tahukah Anda sudah berapa lama komputer digunakan dan kapan terakhir Anda memperbarui kemanannya?
- Apakah Anda memiliki sistem atau perangkat yang terhubung ke nternet (seperti CCTV atau sistem otomasi gedung) yang juga terhubung ke jaringan bisnis Anda?

Aset ini dapat menjadi celah masuk bagi peretas ke dalam lingkungan bisnis Anda untuk mencuri atau merusak data Anda. Penting untuk mengetahui perangkat dan sistem apa yang Anda miliki.

Cara Menggunakan Kotak Peralatan

Gunakan alat di **Kotak Peralatan Ketahui Aset Anda** untuk membantu Anda mengidentifikasi semua perangkat Anda (termasuk desktop, laptop, ponsel pintar, dan printer) dan aplikasi (misalnya surat elektronik, perangkat lunak, peramban web, dan situs web) sehingga Anda dapat mengambil langkah-langkah untuk mengamankannya.

Inventaris ini berfungsi sebagai panduan dan daftar periksa saat Anda menyusun inventaris melalui alat lainnya di Kotak Peralatan. atau menghapus perlengkapan, akun, atau data penting baru.

Unduh alat dari situs web dan catat tanggal selesainya. Selain itu, ambil kesempatan ini untuk menjadwalkan peninjauan rutin agar memastikan semua informasi Anda sudah terbaru.

Apa Yang Dapat Anda Capai Melalui Kotak Peralatan Ini?

Setelah menyelesaikan kotak peralatan ini, Anda akan semakin memahami:

- **cara membuat inventaris data dan sistem**
- **perangkat dan aplikasi mana yang vital bagi operasi bisnis Anda**

Menavigasi Subkategori Kotak Peralatan dan Informasi Tambahan untuk Dipertimbangkan

1.1 Mengidentifikasi Perangkat

Saat membuat inventaris, penting untuk mempertimbangkan segala sesuatu di lingkungan Anda. Ini termasuk item seperti desktop, laptop, ponsel pintar, printer, CCTV, PoS, perangkat IoT, dan router.

Banyak perangkat IoT konsumen yang tidak memiliki atau minim keamanan bawaan, sehingga Anda perlu mempertimbangkan untuk tidak memakainya atau menghapusnya dari jaringan Anda.

Peralatan yang lebih lawas mungkin sudah habis garansinya atau tidak lagi terlindungi terhadap kerentanan baru, tetapi sangat vital bagi operasi bisnis. Ini harus diidentifikasi sebagai bagian dari inventaris Anda dan rencana yang dibuat untuk mengganti, meningkatkan, atau membatasi penggunaannya.

Bicara soal lingkungan TI, tidak sedikit perangkat seperti router, CCTV, dan printer luput dari perhatian. Padahal, segala yang berhubungan dengan nternet dan jaringan lokal perlu diperhatikan ketika Anda membuat inventaris, karena inilah yang berpotensi menjadi celah untuk menyusup ke dalam bisnis Anda.

Ketahui di mana data bisnis yang sensitif dan penting disimpan - apakah tersendiri, di perangkat yang terhubung jaringan, atau di cloud. Anda harus mendokumentasikan semua penyimpanan sebelum mempertimbangkan untuk menaikkan tingkat perlindungan perangkat Anda.

1.2 Mengidentifikasi Aplikasi

Identifikasi semua aplikasi Anda termasuk aplikasi bisnis, akun online tempat Anda menggunakan alamat surat elektronik bisnis, dan aplikasi lain yang Anda akses baik secara lokal maupun jarak jauh melalui perangkat Anda.

Penting untuk mepertimbangkan dan mencatat semua aplikasi dan akun yang sudah lama tidak Anda gunakan karena kemungkinan besar Anda tidak akan memperbarui perangkat lunaknya. Jika dirasa tidak bermanfaat, Anda dapat menghapus atau menutup akun tersebut. Akun online lama mungkin menyimpan beberapa informasi pribadi Anda, dan jika organisasi tempat Anda membuat akun tersebut diserang, data Anda mungkin dapat terpengaruh.

Informasi, dukungan, dan panduan tambahan selama implementasi tersedia via **Kategori Ketahui Aset Anda** di Forum Komunitas GCA.

Tautan Ketahui Aset Anda:

Toolkit: Kotak Peralatan Ketahui Aset Anda

https://gcatoolkit.org/id/umkm/ketahui-aset-anda/

Forum Komunitas: Kategori Ketahui Aset Anda

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/know-what-you-have/8

Dukungan bahasa di forum

https://community.globalcyberalliance.org/t/language-support-on-the-forum-de-es-fr-id/900

Perbarui Ketahanan Anda

Apa Permasalahan Yang Dibahas Di Kotak Peralatan Ini?

Penjahat siber mencari kelemahan dan kekurangan (dikenal sebagai kerentanan) yang dapat digunakan untuk menyusup ke sistem atau menyebarkan perangkat lunak berbahaya. Pelaku bisa mendapatkan akses ke akun keuangan perusahaan Anda, data pelanggan Anda, dan banyak lagi. Anda dapat membantu melindungi hal penting ini dengan memperbarui pertahanan Anda (misalnya selalu memperbarui sistem, perangkat, dan data Anda). Produsen dan pengembang perangkat lunak secara berkala merilis pembaruan keamanan sistem operasi dan aplikasinya untuk mengatasi kelemahan atau kerentanan yang baru ditemukan. Perbaikan ini biasanya disebut sebagai patch, dan prosesnya dikenal sebagai patching.

Kotak Peralatan ini membahas kebutuhan untuk menerapkan patch ini secara tepat waktu, termasuk menyiapkan (juga disebut mengonfigurasi) sistem sehingga dapat diterapkan secara otomatis jika memungkinkan. Selain itu, penting untuk menyadari bahwa seiring waktu, banyak sistem ditambahkan ke, diadaptasi, atau dikonfigurasi sehingga memunculkan kelemahan baru yang dapat digunakan penjahat siber sebagai celah eksploitasi. Masalah lain yang perlu diperhatikan adalah apakah pemasok pihak ketiga memiliki akses ke data di dalam sistem Anda. Menyimpan rekaman terbaru sangat penting; ini memungkinkan Anda untuk mengelola pembaruan yang diperlukan untuk memastikan patch terbaru diterapkan ke sistem, perangkat, dan aplikasi Anda.

Cara Menggunakan Kotak Peralatan

Gunakan alat di **Kotak Peralatan Memperbarui Ketahanan Anda** untuk memastikan perangkat dan aplikasi Anda diatur dengan patch keamanan terbaru yang diterapkan dan dengan tingkat keamanan yang sesuai untuk jenis data yang berada di dalamnya. Jika Anda membuat inventaris di Kotak Peralatan Ketahui Aset Anda, gunakan ini sebagai panduan dan daftar periksa untuk memastikan semua perangkat Anda diperbarui dan diatur untuk menerima pembaruan keamanan secara otomatis.

Setelah Anda menyelesaikan Kotak Peralatan Memperbarui Pertahanan Anda, perbarui Daftar Periksa Keamanan Anda dan atur pengingat untuk mengulangi proses ini secara berkala sehingga menjadi rutin.

Apa Yang Dapat Anda Capai Melalui Kotak Peralatan Ini?

Setelah menyelesaikan kotak peralatan ini, Anda akan semakin memahami:

- **memeriksa apakah Anda menjalankan versi terbaru perangkat lunak di perangkat Anda**
- **mengatur perangkat Anda untuk menerima dan menerapkan pembaruan keamanan secara otomatis**
- **menerapkan pengaturan konfigurasi aman untuk perangkat seluler, peramban web, dan sistem operasi**

Menavigasi Subkategori Kotak Peralatan dan Informasi Tambahan untuk Dipertimbangkan

2.1 Memperbarui Perangkat dan Aplikasi

Ketika solusi, atau patch, dikembangkan dan dirilis untuk kerentanan yang umum, penting untuk semua pengguna sistem atau aplikasi tersebut menerapkan patch secepatnya, idealnya secara otomatis karena jika belum diterapkan, sangat berisiko mengalami pembobolan melalui kerentanan ini.

Periksa setiap perangkat dan aplikasi, dan konfigurasikan untuk diperbarui secara otomatis. Kami telah menyediakan daftar sistem dan aplikasi yang paling umum. Untuk aplikasi dan sistem yang tidak dicakup dalam kotak peralatan ini, periksa halaman petunjuk atau dukungan di situs webnya. Periksa setiap item dari daftar Anda kapan pun, dan pastikan untuk mengambil langkah ini tiap kali Anda menambahkan perangkat atau aplikasi baru ke bisnis Anda.

Sering kali pengaturan yang paling aman tidak disediakan sebagai pengaturan keamanan out-of-the-box default (dikenal sebagai konfigurasi) untuk perangkat atau aplikasi Anda, karena kemudahan penggunaan dan kenyamanan diprioritaskan daripada keamanan. Oleh karena itu, Anda harus memeriksa dan menerapkan konfigurasi keamanan yang direkomendasikan produsen untuk perangkat dan aplikasi Anda.

Semua perangkat yang tidak lagi didukung harus dihapus, karena berisiko terkena pembobolan yang bersumber dari kelemahan yang baru diketahui. Jika ini tidak memungkinkan, maka perangkat harus diisolasi dari perangkat lain dan digunakan secara terbatas pada fungsi bisnis tertentu saja.

Alat kotak peralatan ini menawarkan panduan konfigurasi agar sistem umum dapat pembaruan secara otomatis. Anda harus memeriksa panduan untuk semua perangkat dan sistem Anda agar memastikan semuanya sudah diatur dengan benar.

2.2 Mengenkripsi Data

Jika jaringan komputer Anda mengalami pelanggaran, kemungkinan besar peretas akan mencari jalan untuk mencuri informasi sensitif atau rahasia, yang dapat digunakan untuk keuntungan finansial atau politik pribadi mereka. Dengan mengenkripsi data yang disimpan di hard drive Anda, akan menyulitkan pelaku untuk menggunakan data ini karena perlu didekripsi sebelum dapat digunakan.

Enkripsi adalah proses konversi data dari formulir yang dapat dibaca (contohnya teks biasa), ke formulir yang dikodekan (contohnya teks tersandi). Pengodean ini dirancang agar tidak dapat dipahami kecuali oleh pihak-pihak yang memiliki "kunci" untuk membalikkan proses pengodean. Enkripsi memungkinkan penyimpanan dan transmisi data rahasia serta bukti bahwa itu berasal dari orang yang mengklaim telah mengirimnya.

Alat-alat ini memungkinkan Anda untuk mengenkripsi file yang tersimpan di hard drive Anda. Jika sistem operasi Anda tidak terdaftar di kotak peralatan ini, opsi lebih lanjut mungkin tersedia melalui produsen peralatan atau penawaran keamanan lain yang tersedia secara komersial.

2.3 Mengamankan Situs Web

Situs web Anda sangat penting bagi banyak bisnis dalam operasi bisnisnya. Penggunaannya dapat mencakup aliran informasi sensitif di seluruh rantai pasokan atau mungkin platform perdagangan utama tempat bisnis Anda bergantung. Jika peretas mendapatkan akses ke situs web, mereka dapat merusak atau mencuri data, mengubah isinya, menginfeksi situs web dengan malware, atau mengambil alih operasi. Semua ini dapat berdampak buruk pada kemampuan operasi organisasi Anda.

Di sini, Anda akan menemukan alat yang dapat Anda gunakan untuk menjalankan pemeriksaan rutin di situs web Anda (dikenal sebagai pemindaian) untuk mengidentifikasi potensi kelemahan dan kerentanan. Pastikan setiap masalah yang diidentifikasi mendapatkan tindakan yang sesuai dan dinilai oleh personel yang kompeten dalam bidang TI.

Subkategori kotak peralatan menyediakan instruksi dan alat untuk sistem yang umum digunakan. Untuk lainnya, cari bantuan via situs web vendor atau minta saran di Forum Komunitas GCA **Kategori Perbarui Pertahanan Anda** atau **Komunitas Usaha Kecil**.

Tautan Perbarui Ketahanan Anda:

Toolkit: Kotak Peralatan Perbarui Ketahanan Anda

https://gcatoolkit.org/id/umkm/perbarui-pertahanan-anda/

Forum Komunitas: Kategori Perbarui Ketahanan Anda

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/update-your-defences/9

Komunitas Usaha Kecil

https://community.globalcyberalliance.org/c/community-discussions/small-business-community/33

Kata Sandi yang Terlalu Mudah

Apa Permasalahan Yang Dibahas Di Kotak Peralatan Ini?

Kata sandi adalah garis pertahanan pertama dalam melindungi akun dan data Anda (seperti surat elektronik, rekaman personel, atau database klien).

Sayangnya, kata sandi sering menjadi target mudah bagi penjahat siber, dan pelanggaran data terkait peretasan sering terjadi karena kata sandi yang lemah. Penyerang memiliki banyak cara untuk mencoba dan mengakses kata sandi Anda, mulai dari menggunakan peretas kata sandi, yaitu program untuk menelusuri kombinasi yang umum digunakan hingga menggunakan nama pengguna dan kata sandi yang diperoleh dari akun korban pelanggaran yang sudah dicoba di situs populer lain. Teknik-teknik ini membutuhkan sedikit kemampuan teknis, bersifat cepat, sepenuhnya otomatis, dan tersedia bagi mereka yang tahu cara mencarinya di internet. Yang semakin memperparah keadaan adalah banyak usaha kecil dan skala menengah yang tidak memiliki kebijakan kata sandi, dan jika iya, mereka tidak memberlakukannya secara ketat.

Jadi, memiliki kata sandi yang kuat sangat penting untuk melindungi data Anda. Selain itu, Anda juga perlu melakukan langkah lebih lanjut dengan menerapkan autentikasi dua faktor atau multifaktor (2FA).

2FA membutuhkan beberapa kredensial, sehingga jauh lebih sulit bagi penyerang untuk mendapatkan akses ke akun Anda.

- Dengan 2FA, pengguna memerlukan:
- Sesuatu yang Anda tahu, seperti kata sandi;
- Dan sesuatu yang Anda miliki, seperti token (Google Authenticator, Authy, Okta, RSA, dll.) atau kode verifikasi yang dikirim ke ponsel Anda; atau
- Sesuatu yang dapat mengidentifikasi Anda, seperti sidik jari atau wajah (biometrik).

Kotak Peralatan ini membantu Anda membuat kata sandi yang lebih kuat dan unik untuk setiap akun Anda dan menunjukkan cara menyiapkan 2FA, yang keduanya merupakan langkah penting dalam melindungi akses ke akun dan data Anda.

Apa yang Dapat Anda Capai Melalui Kotak Peralatan Ini?

Setelah menyelesaikan kotak peralatan ini, Anda akan semakin memahami:

- **membuat kata sandi yang kuat**
- **menguji apakah akun Anda telah disusupi**
- **menyiapkan 2FA untuk akun online yang paling umum**

Cara Menggunakan Kotak Peralatan

Gunakan alat di **Kotak Peralatan Kata Sandi yang Terlalu Mudah** untuk memastikan kata sandi yang kuat dan 2FA diatur ke perangkat dan aplikasi Anda. Jika Anda membuat inventaris di Ketahui Aset Anda, gunakan ini sebagai panduan dan daftar periksa untuk memastikan bahwa Anda telah menerapkannya di semua akun Anda.

Setelah Anda menyelesaikan Kotak Peralatan Kaya Sandi yang Terlalu Mudah, perbarui Daftar Periksa Keamanan Anda dan atur pengingat untuk mengulangi proses ini secara berkala sehingga menjadi rutin.

Menavigasi Subkategori Kotak Peralatan dan Informasi Tambahan untuk Dipertimbangkan

3.1 Kata Sandi yang Kuat

Salah satu metode paling umum yang digunakan penjahat untuk mendapatkan akses ke akun, jaringan, dan informasi Anda adalah dengan cara masuk sebagai Anda. Sangat penting bagi Anda untuk:

- Menggunakan kata sandi (atau frasa sandi) yang unik dan kuat untuk setiap akun Anda.
- Menggunakan huruf, angka, dan karakter khusus untuk membuat kata sand yang kuat.
- Mengubah kata sandi Anda segera setelah mengalami pelanggaran.
- Menjaga kata sandi tetap rahasia dan aman.
- Jangan pernah menggunakan kata sandi lama yang sudah diganti.
- Jangan pernah mengklik tautan dalam surat elektronik yang memberi tahu Anda “sekarang saatnya untuk mengatur ulang kata sandi Anda;” selalu mengakses situs web akun melalui peramban web.
- Tidak masuk ke akun via Wi-Fi publik.

Menggunakan kata sandi yang sama di beberapa akun berarti bahwa jika penjahat mendapatkan salah satu kata sandi Anda, mereka mendapat celah yang sempurna untuk masuk ke semua akun yang menggunakan kata sandi itu. Detail nama pengguna dan kata sandi dapat dijual secara online oleh penjahat yang telah mencurinya dalam serangan siber dan digunakan kembali sampai kata sandi diubah. Kemajuan teknologi yang pesat berarti bahwa laptop modern yang murah dapat dengan cepat membuat pola melalui semua kombinasi untuk menghasilkan kata sandi sederhana yang pendek.

Anda harus memiliki kebijakan kata sandi yang dipahami dan dipatuhi oleh semua staf dan kontraktor yang memiliki akses ke sistem Anda. Beberapa sistem dan aplikasi mungkin memungkinkan Anda untuk menerapkan kata sandi minimum yang diperbolehkan sehingga tentunya ini patut untuk diperiksa di pengaturan keamanan.

Anda dapat menggunakan alat dalam Kata Sandi Yang Kuat untuk mempelajari lebih lanjut tentang kata sandi dan untuk memeriksa apakah alamat surat elektronik Anda telah dicuri dalam pelanggaran. Jika iya, segera ubah kata sandi Anda dan jangan pernah menggunakan kembali kata sandi itu.

Jangan lupa juga untuk memeriksa pengaturan kata sandi pada router, printer, dan peralatan lain yang terhubung ke jaringan Anda. Kata sandi tersebut bisa luput dari ingatan Anda dan biasanya berupa kata sandi default sederhana. Kerjakan inventaris yang Anda buat di Ketahui Aset Anda dan beri tanda centang saat Anda melakukannya!

3.2 Alat untuk 2FA

Autentikasi dua faktor (2FA) menyediakan lini pertahanan kedua yang penting di luar kata sandi untuk melindungi akun dari akses yang tidak sah. Ada sejumlah metode autentikasi yang dapat digunakan untuk 2FA. Ragamnya mulai dari kode unik yang dikirim melalui teks ke ponsel Anda, token perangkat keras yang Anda bawa, sidik jari, atau pengenalan wajah.

Alat untuk 2FA berisi sumber daya yang dapat diunduh yang menyediakan metode autentikasi yang disetujui oleh sebagian besar akun umum.

Saat menerapkan alat dan panduan di Kotak Peralatan Kata Sandi Yang Terlalu Mudah, pertimbangkan juga izin apa yang dimiliki setiap pengguna saat mengakses aplikasi terkait bisnis. Pertimbangkan untuk membatasi akses hanya kepada orang yang memerlukannya dan sejauh yang diperlukan peran mereka.

3.3 Mengelola Kata Sandi

Pengelola kata sandi adalah cara untuk menjaga semua kata sandi Anda agar tetap aman tanpa perlu mengingat setiap kata sandi secara terpisah. Ini berarti bahwa Anda hanya perlu mengingat satu kata sandi setiap kali Anda ingin masuk ke salah satu akun yang kata sandinya disimpan di pengelola kata sandi. Pengelola kata sandi memang menawarkan lebih banyak kemudahan. Namun, ini juga berarti bahwa jika pengelola kata sandi dibobol, penyerang akan memiliki akses ke semua kata sandi.

Informasi, dukungan, dan panduan tambahan selama implementasi tersedia via **Kategori Kata Sandi Yang Terlalu Mudah** di Forum Komunitas GCA.

Tautan Kata Sandi Yang Terlalu Mudah:

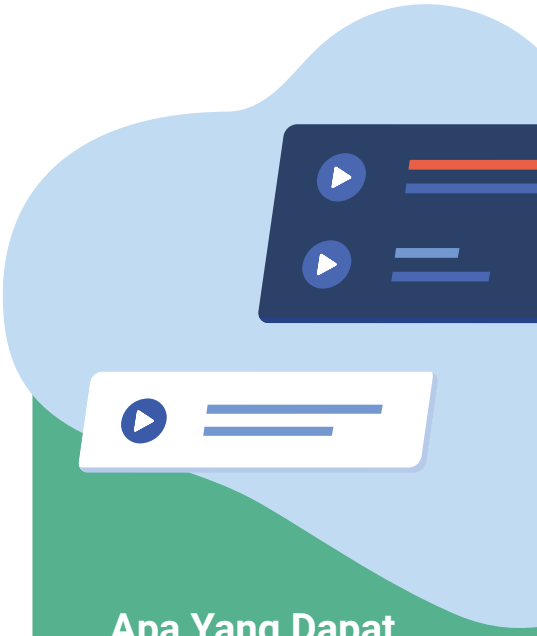
Toolkit: Kotak Peralatan Kata Sandi Yang Terlalu Mudah

https://gcatoolkit.org/id/umkm/lebih-dari-sekadar-kata-sandi-sederhana/

Forum Komunitas: Kategori Kata Sandi Yang Terlalu Mudah

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/beyond-simple-passwords/10

Mencegah Phishing dan Malware



Apa Permasalahan Yang Dibahas Di Kotak Peralatan Ini?

Setiap tahun banyak usaha kecil menjadi korban malware dan serangan phishing yang sangat merugikan. Ketika pengguna mengklik situs web yang terinfeksi malware atau membuka lampiran yang terinfeksi dalam surat elektronik phishing, akibatnya adalah file hilang atau diubah, pengubahan aplikasi, atau kelumpuhan fungsi sistem.

Malware adalah perangkat lunak yang dirancang untuk menyebabkan kerusakan pada dan/atau akses tidak sah ke perangkat atau jaringan. Surat elektronik phishing mengelabui pengguna agar percaya bahwa mereka berurusan dengan entitas yang dapat dipercaya sehingga penyerang dapat memperoleh akses tidak sah ke konten pribadi yang rahasia dan sensitif, atau uang. Penyerang akan melakukan apa pun yang mereka bisa untuk membuat surat elektronik mereka tampak asli dan menarik agar pengguna mengklik atau membukanya. Surat elektronik terlihat seperti berasal dari orang yang Anda kenal, pelaku meniru logo dan format surat elektronik dari organisasi ternama, atau mengirim surat elektronik yang mengacu pada tugas atau pekerjaan yang baru Anda selesaikan.

Diperkirakan sekitar lebih dari 90% serangan siber bermula dari surat elektronik phishing. Jika Anda mengklik tautan atau membuka lampiran dalam surat elektronik phishing, Anda mungkin memicu sejumlah aktivitas yang telah disiapkan oleh penyerang, misalnya mencuri data Anda, membuat rute rahasia (dikenal sebagai backdoor) ke komputer Anda untuk mengaksesnya nanti, menginstal jenis malware yang digunakan untuk mengakses data lalu meminta uang tebusan (dikenal sebagai ransomware), atau membuat Anda mengunduh jenis malware lain yang memungkinkan penyerang untuk melihat apa yang Anda ketik, seperti kata sandi atau nomor rekening (dikenal sebagai perangkat mata-mata).

Serangan phishing dan malware sangat merugikan bagi usaha kecil. Kerugiannya antara lain hilangnya atau rusaknya data, penurunan pendapatan selama serangan, biaya perbaikan atau penggantian peralatan yang tidak sedikit, biaya untuk memberi tahu konsumen atau klien tentang penyerangan, dan reputasi yang tercoreng serta kemungkinan perkara hukum.

Apa Yang Dapat Anda Capai Melalui Kotak Peralatan Ini?

Setelah menyelesaikan kotak peralatan ini, Anda akan semakin memahami:

- **cara perangkat lunak antivirus melindungi sistem dan data Anda**
- **cara menginstal perangkat lunak antivirus pada sistem Anda**
- **iklan digital dan risiko yang dapat muncul**
- **cara menginstal pemblokir iklan untuk mencegah iklan pop-up, video, dan konten lain yang tidak diinginkan**
- **apa itu DNS dan mengapa ini angat penting**
- **cara kerja keamanan DNS dan jenis serangan yang dimitigasi**
- **cara menginstal Quad9 di perangkat Android dan komputer**

Menavigasi Subkategori Kotak Peralatan dan Informasi Tambahan untuk Dipertimbangkan

Alat yang ditampilkan di sini telah dipilih secara cermat berdasarkan standar global yang diakui, dan tidak mewakili urutan atau prioritas rekomendasi khusus.

4.1 Antivirus

Penggunaan antivirus real time sangat penting karena pemeriksaan virus dilakukan secara real-time, dapat menghilangkan virus sebelum menimbulkan kerusakan, dan diperbarui jika perlindungan virus baru dikembangkan.

4.2 Pemblokir Iklan

Beberapa iklan online atau pesan yang muncul saat menjelajahi situs web berguna; namun, beberapa lainnya mungkin berisi kode berbahaya dan dapat menginfeksi komputer Anda dengan malware jika Anda mengkliknya. Pemblokir iklan dapat digunakan untuk mencegah iklan muncul di halaman web, menawarkan perlindungan tambahan saat menjelajah.

4.3 DNS Security

Keamanan DNS menggunakan Domain Name System (bisa diandaikan sebagai buku telepon di internet) untuk menerjemahkan nama situs web berbasis teks (nama domain) jenis pengguna di peramban ke dalam sekumpulan nomor (alamat IP) unik yang dipahami komputer.

Sebagian besar penyerang akan mencoba untuk menggunakan domain situs web yang mirip untuk mengecoh korban agar mereka merasa sedang membuka situs resmi. Nama situs webnya mungkin terlihat seperti asli, tetapi jika dicermati akan tampak perbedaannya.

Jadi, misalnya, URL situs web perusahaan yang resmi: “www. Mygreatwidgets.com,” sedangkan yang palsu: “www. rnygreatwidgets. com.”

Firewall DNS, salah satu jenis keamanan DNS, dapat membantu mencegah virus dan serangan phishing. Firewall ini memeriksa apakah ada kode berbahaya yang disimpan di alamat IP situs web yang diminta, dan jika ada, akan memblokir aksesnya. Pengguna dapat menerapkan layanan pemfilteran DNS pada sistem mereka menggunakan alat dalam subkategori ini untuk membantu mencegah akses ke situs web berbahaya yang paling umum.

Subkategori kotak peralatan menyediakan alat untuk sistem yang umum digunakan. Ajukan pertanyaan atau cari dukungan lebih lanjut di Forum Komunitas GCA Community **Kategori Mencegah Phishing dan Malware** atau **Komunitas Usaha Kecil**.

Tautan Mencegah Phishing dan Malware:

Toolkit: Kotak Peralatan Mencegah Phishing dan Malware

https://gcatoolkit.org/id/umkm/mencegah-phishing-dan-malware/

Forum Komunitas: Mencegah Phishing dan Kategori Malware

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/prevent-phishing-and-viruses/11

Komunitas Usaha Kecil

https://community.globalcyberalliance.org/c/community-discussions/small-business-community/33

Pencadangan dan Pemulihan

Apa Permasalahan Yang Dibahas Di Kotak Peralatan Ini?

Data yang hilang atau rusak dapat disebabkan oleh serangan siber (misalnya ransomware) atau karena kegagalan peralatan, pencurian, kesalahan manusia, kerusakan yang tidak disengaja, kebakaran, atau banjir. Terlepas dari penyebabnya, dampak dari hilangnya data atau waktu henti peralatan bisa sangat merugikan bagi produktivitas dan pendapatan bisnis Anda.

Cadangan adalah salinan data, disimpan di lokasi yang berbeda dari data asli, dan dapat membantu Anda pulih dari serangan atau kehilangan data. Mencadangkan secara rutin dan membuat cadangan offline akan membantu Anda lebih cepat pulih dari kehilangan atau kerusakan data. Keduanya penting karena cadangan online diatur untuk secara otomatis mencadangkan di seluruh jaringan, sedangkan cadangan offline memerlukan perangkat eksternal yang dapat dilepas-pasang (misalnya USB atau hard drive) untuk penyimpanan secara fisik di tempat lain (yang juga membantu melindungi pencadangan data yang sudah rusak secara tidak sengaja).

Cara Menggunakan Kotak Peralatan

Gunakan alat di **Kotak Peralatan Pencadangan dan Pemulihan** untuk memastikan sistem dicadangkan secara rutin pada tingkat dan frekuensi yang sesuai untuk jenis data yang ada di dalamnya.

Apa yang harus Anda cadangkan? Itu bergantung pada informasi yang Anda miliki dan risiko kehilangan informasi tersebut. Jika Anda membuat inventaris di kotak peralatan Ketahui Aset Anda, gunakan itu sebagai panduan dan daftar periksa untuk Anda perbarui kapan pun.

Setelah Anda menyelesaikan Kotak Peralatan Pencadangan dan Pemulihan, perbarui Daftar Periksa Keamanan dan atur pengingat untuk meninjau secara berkala agar memastikan kebijakan tetap sesuai dengan bisnis.

Apa Yang Dapat Anda Capai Melalui Kotak Peralatan Ini?

Setelah menyelesaikan kotak peralatan ini, Anda akan semakin memahami:

- **alasan pentingnya pencadangan bagi bisnis Anda, terutama pemulihan dari serangan ransomware**
- **cara mengaktifkan cadangan penuh di mesin Windows atau Mac**

Menavigasi Subkategori Kotak Peralatan dan Informasi Tambahan untuk Dipertimbangkan

Ransomware adalah salah satu metode serangan yang menjadi masalah serius bagi usaha kecil. Ransomware adalah jenis perangkat lunak berbahaya yang menginfeksi komputer dan memblokir akses ke data Anda. Pelaku meminta uang tebusan, terkadang dalam bentuk cryptocurrency, (misalnya bitcoin yang lebih sukar dilacak dibanding transfer tradisional) dengan janji bahwa data akan dipulihkan setelah tebusan diterima. Penting bagi Anda untuk memiliki cadangan data untuk mengakses informasi jika sewaktu-waktu Anda menjadi korban ransomware.

5.1 Mencadangkan Sistem Operasi

Memiliki kebijakan pencadangan yang solid mencakup pencadangan online maupun offline dapat membantu Anda untuk lebih cepat pulih dari kehilangan dan kerusakan data.

- Berbagai himpunan data yang Anda miliki harus dikategorikan di dalam inventaris (lihat Kotak Peralatan Ketahui Aset Anda untuk bantuan mem buat inventaris).
- Pertimbangkan penggunaan enkripsi untuk informasi sensitif (lihat Kotak Peralatan Memperbarui Pertahanan Anda untuk informasi selengkapnya tentang enkripsi).
- Terapkan pendekatan yang bijaksana untuk mencadangkan setiap him punan data setelah mempertimbangkan setiap “dampak kerugiannya”. Kerugiannya dapat berupa reputasi, finansial, atau hukum.

Dalam subkategori Pencadangan Sistem Operasi, Anda akan menemukan petunjuk pencadangan pada sistem operasi umum. Jika milik Anda tidak tercantum, cari bantuan via situs web penyedia Anda atau ajukan pertanyaan di **Kategori Pencadangan dan Pemulihan** di Forum Komunitas GCA.

Pastikan juga bahwa Anda memiliki rencana pemulihan bencana, yang membantu memungkinkan pemulihan sistem penting setelah bencana (baik bencana yang tidak disengaja atau bencana alam). Anda juga dapat meningkatkan keamanan dengan menyusun rencana agar dapat mempersingkat waktu pemulihan dan meminimalkan kerusakan pada sistem dan melindungi data dari potensi ancaman. Templat dan panduan untuk membuat rencana banyak disediakan secara online. Pastikan Anda terus memperbaruinya, lakukan simulasi untuk menjalankan rencana, dan pastikan semua orang tahu cara mengimplementasikannya.

Tautan Pencadangan dan Pemulihan:

Toolkit: Kotak Peralatan Pencadangan dan Pemulihan

https://gcatoolkit.org/id/umkm/pencadangan-dan-pemulihan/

Forum Komunitas: Kategori Pencadangan dan Pemulihan

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/back-up-and-recover/16

Proteksi Surat Elektronik dan Reputasi

Apa Permasalahan Yang Dibahas Di Kotak Peralatan Ini?

Surat elektronik sering digunakan sebagai titik awal serangan siber. Surat elektronik adalah sarana yang mudah dan murah untuk menyebarkan ribuan surat elektronik dengan harapan si penerima tidak curiga dan beberapa diantaranya terkecoh untuk mengklik tautan situs web atau mengunduh lampiran berbahaya.

Salah satu teknik yang digunakan penjahat siber adalah membuat surat elektronik tampak seolah-olah dikirim dari sumber yang sah, seperti lembaga keuangan, klien, mitra bisnis, atau organisasi lain yang sudah dikenal. Salah satu teknik ini dikenal sebagai spoofing domain surat elektronik, yaitu surat elektronik "palsu" yang digunakan sama persis dengan yang asli, sehingga membuatnya tampak benar-benar dikirim dari organisasi itu dan nyaris tidak membuat si penerima curiga.

Jika domain surat elektronik perusahaan Anda (bagian dari alamat surat elektronik Anda setelah "@") dipalsukan, ini akan menimbulkan kerugian yang besar bagi Anda, pelanggan Anda, dan rantai pasokan. Jika penerima surat elektronik melakukan tindakan yang diinstruksikan di surat elektronik karena percaya bahwa Andalah pengirimnya, ini dapat mengakibatkan sistem komputer mereka terinfeksi malware atau ransomware. Ini juga menjadi celah bagi penjahat untuk mengambil alih kendali dan memanipulasi detail perbankan Anda, sehingga pelanggan melakukan pembayaran ke akun yang awalnya mereka kira itu adalah milik Anda.

Kotak Peralatan Proteksi Surat Elektronik dan Reputasi Anda menyediakan panduan dan alat untuk melindungi dari jenis ancaman ini, termasuk membimbing Anda melalui penggunaanstandar surat elektronik yang dikenal sebagai DMARC (Domain-based Authentication, Reporting, and Conformance). DMARC adalah cara efektif untuk menghentikan pengirim spam dan phisher dari penggunaan domain perusahaan untuk melakukan serangan siber berbahaya. DMARC adalah cara untuk memverifikasi pengirim surat elektronik apakah memiliki izin untuk menggunakan domain surat elektronik Anda dan mengirim surat elektronik.

Penyerang juga mungkin membuat situs web "tiruan". Misalnya, domain asli "BestBusiness .com" dapat ditiru dengan mendaftarkan "BestBusness .com" atau "BestBusiness .net" untuk mengelabui pelanggan atau pengguna agar mengunjungi situs webnya.

Apa Yang Dapat Anda Capai Melalui Kotak Peralatan Ini?

Setelah menyelesaikan kotak peralatan ini, Anda akan semakin memahami:

- **apa itu DMARC, mengapa ini sangat penting, dan serangan apa yang dimitigasi**
- **Panduan Penyiapan DMARC**
- **cara memeriksa domain surat elektronik milik Anda untuk mengetahui apakah DMARC diaktifkan**

Jika surat elektronik atau domain situs web Anda dipalsukan, ini dapat mencoreng reputasi dan merek Anda, serta membahayakan pelanggan Anda. Menggunakan alat di Proteksi Surat Elektronik dan Reputasi membantu Anda mengidentifikasi dan mencegah peniruan identitas.

Cara Menggunakan Kotak Peralatan

Gunakan alat di **Kotak Peralatan Proteksi Surat Elektronik dan Reputasi** untuk memastikan perusahaan Anda terlindungi dari spoofing domain surat elektronik melalui implementasi DMARC dan identifikasi kemungkinan peniruan domain situs web.

Perbarui Daftar Periksa Anda setelah selesai dan ajak pelanggan dan rantai pasokan yang memiliki dan menggunakan domain sendiri untuk melakukan hal serupa, karena keefektifan DMARC bergantung pada pengirim dan penerima yang sama-sama mengimplementasikan DMARC.

Menavigasi Subkategori Kotak Peralatan dan Informasi Tambahan untuk Dipertimbangkan

6.1 Mengimplementasikan DMARC

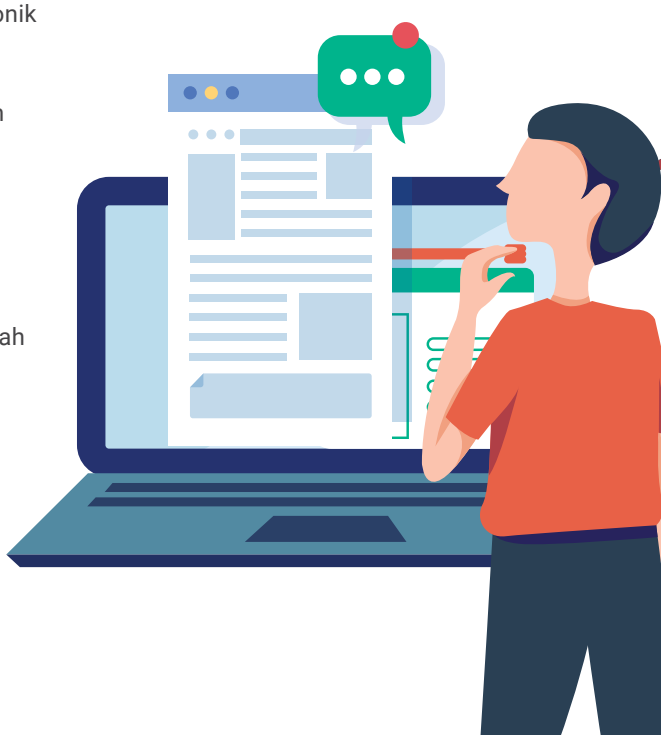
Gunakan alat dalam subkategori ini untuk mengetahui selengkapnya tentang DMARC, periksa apakah domain surat elektronik Anda dilindungi oleh DMARC, dan jika iya, di tingkat apa.

6.2 Memahami Laporan DMARC

Setelah kebijakan DMARC diatur ke domain surat elektronik Anda, Anda akan mulai menerima laporan yang menunjukkan bagaimana domain surat elektronik Anda digunakan. Ini dapat menyulitkan interupsi dalam format mentahnya.

Alat dalam subkategori Memahami Laporan DMARC membantu memberikan interpretasi dan identifikasi aktivitas penipuan yang lebih cepat. Laporan ini dapat menjadi pertimbangan yang kuat untuk menaikkan tingkat kebijakan dari “tidak ada”, ke “karantina”, dan ke tingkat yang tertinggi “tolak”. Penting juga untuk mempertimbangkan organisasi surat elektronik atau layanan apa pun yang berwenang untuk mengirim surat elektronik atas nama Anda, seperti layanan pemasaran surat elektronik, dan pastikan apakah mereka telah mengimplementasikan DMARC.

Anda akan mendapatkaan manfaat penuh dari DMARC hanya ketika domain Anda berada di tingkat “tolak”.



6.3 Perlindungan Merek Dagang

Penipu dapat mendaftarkan domain yang terlihat sangat mirip dengan domain milik Anda dengan harapan orang akan mengkliknya. Gunakan alat di sini untuk membantu mengidentifikasi domain yang mencoba meniru domain Anda, serta domain yang berisi phishing atau konten berbahaya yang menargetkan domain Anda.

Untuk dukungan lebih lanjut saat mengimplementasikan DMARC, baca **Forum DMARC** atau **Kategori Proteksi Surat Elektronik dan Reputasi Anda** di Forum Komunitas GCA.

Tautan Proteksi Surat Elektronik dan Reputasi:

Toolkit: Kotak Peralatan Proteksi Surat Elektronik dan Reputasi

https://gcatoolkit.org/id/umkm/lindungi-surat-elektronik-dan-reputasi-anda/

Forum Komunitas: Forum DMARC

https://community.globalcyberalliance.org/c/dmarc/5

Kategori Proteksi Surat Elektronik dan Reputasi

https://community.globalcyberalliance.org/c/cybersecurity-toolbox/protect-your-email-and-reputation/13

Glosarium Istilah

Glosarium beberapa istilah yang umum digunakan berkaitan dengan keamanan siber. Beberapa istilah ini telah dimasukkan dalam bab Buku Panduan Toolkit Keamanan Siber GCA untuk Usaha Kecil, sementara yang lain disediakan untuk informasi tambahan jika Anda ingin menjelajahi lebih banyak sendiri.

akun Umumnya mengacu pada akses ke sistem komputer atau layanan online, biasanya memerlukan kata sandi untuk masuk.

pelanggar Seseorang, sekelompok, organisasi, atau pemerintah yang melakukan atau berniat untuk melakukan aktivitas yang merusak.

antivirus Perangkat lunak yang dirancang untuk mendeteksi, menghentikan, dan menghapus virus dan jenis perangkat lunak berbahaya lainnya.

aplikas Program yang dirancang untuk melakukan tugas tertentu. Aplikasi sering mengacu pada program yang diunduh ke perangkat bergerak.

aset Seseorang, struktur, fasilitas, informasi, dan catatan, sistem dan sumber daya teknologi informasi, materi, proses, hubungan, atau reputasi yang memiliki nilai. Apa pun yang berguna yang berkontribusi pada keberhasilan sesuatu, seperti misi organisasi; aset adalah hal-hal yang bernilai atau properti yang nilainya dapat ditetapkan.

serangan Upaya untuk mendapatkan akses tidak sah ke layanan sistem, sumber daya, atau informasi, atau upaya untuk membahayakan integritas sistem. Tindakan yang disengaja untuk mencoba melewati satu atau lebih layanan keamanan atau kontrol sistem informasi.

ciri khas serangan Ciri khas atau pola jelas yang dapat ditelusuri atau dicocokkan dengan serangan yang diidentifikasi sebelumnya.

faset serangan Serangkaian cara yang dipat digunakan oleh pelanggar untuk memasuki sistem dan berpotensi menyebabkan kerusakan. Karakteristik sistem informasi yang memungkinkan pelanggar untuk mencari celah, menyerang, atau mempertahankan keberadaan di sistem informasi.

penyerang Pelaku yang berusaha mengeksploitasi sistem komputer dengan maksud untuk maksud untuk mengubah, menghancurkan, mencuri atau melumpuhkan informasi mereka, dan kemudian mengeksploitasi hasilnya.

autentikasi Proses untuk memverifikasi bahwa seseorang adalah orang yang sama saat mencoba untuk mengakses komputer atau layanan online. Ini juga merupakan sumber dan integritas data, pengguna, proses, atau perangkat.

back door Cara terselubung bagi penjahat siber untuk mendapatkan askes tidak sah ke sistem komputer

cadangan Komputer atau perangkat yang terhubung ke nternet, berisi kode berbahaya secara rahasia, yang melakukan aktivitas di bawah perintah atau kendali administrator jarak jauh.

mencadangkan Membuat salinan data yang disimpan di komputer atau server untuk mengurangi dampak potensi kegagalan atau kehilangan.

bot Komputer atau perangkat yang terhubung ke nternet, berisi kode berbahaya secara rahasia, yang melakukan aktivitas di bawah perintah atau kendali administrator jarak jauh.

Glosarium Istilah

botnet Jaringan perangkat yang terinfeksi (bot), terhubung ke nternet, digunakan untuk melakukan serangan siber terkoordinasi tanpa sepengetahuan pemiliknya.

pelanggaran Insiden ketika data, sistem komputer, atau jaringan diakses atau dipengaruhi tanpa otorisasi.

serangan brutal Menggunakan kekuatan komputasi untuk secara otomatis memasukkan sejumlah besar kombinasi nilai, biasanya untuk menemukan kata sandi dan mendapatkan akses.

bug Kesalahan, kecacatan, atau ketidaksempurnaan yang tidak diduga dan relatif kecil dalam sistem atau perangkat informasi.

konfigurasi Pengaturan komponen perangkat lunak dan perangkat keras dari sistem atau perangkat komputer.

mengonfigurasi Proses pengaturan perangkat lunak atau perangkat untuk komputer, sistem, atau tugas tertentu.

serangan siber Upaya berbahaya untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer, jaringan atau perangkat, melalui sarana siber.

insiden siber Pelanggaran aturan keamanan yang umumnya menyasar sistem atau layanan; upaya untuk mendapatkan akses tidak sah ke sistem dan/atau data, penggunaan sistem yang tidak sah untuk pemrosesan atau penyimpanan data, perubahan pada perangkat lunak atau perangkat keras firmware sistem tanpa persetujuan pemilik sistem, gangguan berbahaya dan/atau penyangkalan layanan.

keamanan siber Perlindungan perangkat, layanan, dan jaringan — dan informasi yang ada di dalamnya — dari pencurian atau kerusakan.

mata uang kripto Uang digital. Mata uang kripto disimpan dalam dompet digital (online, di komputer Anda atau di perangkat keras lainnya). Mata uang kripto biasanya tidak didukung oleh pemerintah mana pun, jadi tidak memiliki perlindungan yang sama dengan uang yang disimpan di bank.

serangan berbasis kamus Salah satu jenis serangan brutal, yaitu penyerang menggunakan kata-kata kamus, frasa, atau kata sandi umum yang diketahui sebagai tebakannya.

jejak digital 'Jejak' informasi digital yang berasal dari aktivitas online pengguna di masa lampau.

Serangan DoS (denial of service) Serangan dengan cara menolak akses pengguna yang sah ke layanan komputer (atau sumber daya), biasanya dengan membebani layanan dengan permintaan.

perangkat Perangkat keras komputer yang dirancang untuk fungsi tertentu - misalnya laptop, ponsel, atau printer.

DMARC Singkatan dari Domain-based Message Authentication, Reporting and Conformance. DMARC adalah mekanisme yang memungkinkan pengirim dan penerima untuk memantau dan meningkatkan perlindungan domain mereka dari surat elektronik penipuan.

spoofing domain surat elektronik Teknik yang digunakan oleh penjahat siber di mana alamat surat elektronik "palsu" yang digunakan persis dengan yang asli, sehingga membuatnya seolah-olah dikirim oleh organisasi tersebut.

enkripsi Mengonversi data menjadi formulir yang sulit dipahami oleh orang yang tidak berwenang.

firewall Perangkat keras/perangkat lunak atau program perangkat lunak yang membatasi lalu lintas jaringan sesuai dengan seperangkat aturan aksesnya dan tidak diizinkan atau diautorisasi.

peretas Seseorang yang melanggar keamanan komputer karena alasan yang jahat atau demi keuntungan pribadi.

perangkat keras Komputer, komponennya, dan alat yang terkait dengannya. Perangkat keras mencakup disk drive, sirkuit terintegrasi, monitor, kabel, modem, speaker, dan printer.

ancaman internal Seseorang atau sekelompok orang dengan akses dan/atau pengetahuan internal perusahaan, organisasi, atau perusahaan yang dapat menimbulkan potensi risiko melalui pelanggaran kebijakan keamanan dengan maksud untuk menimbulkan bahaya.

Internet of things (IoT) Mengacu pada kemampuan objek (bukan komputer dan perangkat) untuk terhubung ke nternet. Contohnya termasuk ketel, kulkas, dan televisi.

intrusi Tindakan melewati mekanisme keamanan sebuah sistem informasi atau jaringan tanpa izin.

sistem deteksi intrusi (IDS) Program atau perangkat yang digunakan untuk mendeteksi bahwa penyerang sedang atau telah berupaya mengakses sumber daya komputer tanpa izin.

sistem pencegahan intrusi (IPS) Sistem pendeteksi intrusi yang juga memblokir akses tanpa otorisasi saat terdeteksi.

pencatat input tombol Perangkat lunak atau perangkat keras yang melacak input tombol dan aktivitas keyboard, biasanya secara diam-diam, untuk memonitor tindakan pengguna sistem informasi.

malvertising Penggunaan iklan online sebagai metode pengiriman malware.

malware (perangkat lunak berbahaya) istilah yang meliputi virus, trojan, worm, atau kode atau konten apa pun yang dapat berdampak merugikan bagi organisasi atau individu. Perangkat lunak yang dibuat untuk menerobos dan merusak atau melumpuhkan komputer.

mitigasi Aplikasi satu atau lebih dari satu langkah untuk mengurangi kemungkinan kejadian yang tidak diinginkan dan/atau meminimalkan konsekuensinya.

jaringan Dua komputer atau lebih yang saling terhubung untuk berbagi sumber daya.

ancaman (pihak) luar Seseorang atau sekelompok orang di luar organisasi yang tidak berwenang untuk mengakses aset organisasi tersebut dan menghadirkan potensi risiko terhadap organisasi dan asetnya.

kata sandi Sederet karakter (huruf, angka, dan simbol lainnya) yang digunakan untuk mengautentikasi sebuah identitas atau untuk memverifikasi otorisasi akses.

pembobol kata sandi Program yang dirancang untuk menebak kata sandi, sering kali dengan mengutak-atik kombinasi yang sering digunakan atau menggunakan nama pengguna dan kata sandi yang didapatkan dari akun yang disusupi.

pengelola kata sandi Program yang memungkinkan pengguna untuk membuat, menyimpan, dan mengelola kata sandi di satu lokasi yang aman.

penerapan patch Menerapkan pembaruan pada firmware atau perangkat lunak untuk meningkatkan keamanan dan/atau menyempurnakan fungsi.

pentest (pengujian penetrasi) Pengujian resmi sebuah sistem atau jaringan komputer guna mencari kelemahan untuk diperbaiki.

Informasi yang Dapat Mengidentifikasi Pribadi/Informasi Identifikasi Pribadi (PII) Informasi yang memungkinkan identitas seseorang disimpulkan secara langsung maupun tidak langsung.

pharming Serangan terhadap infrastruktur jaringan yang mengakibatkan pengguna dialihkan ke situs web yang tidak sah meskipun pengguna sudah memasukkan alamat yang benar.

phishing Surat elektronik massal tanpa target yang dikirim ke banyak orang untuk meminta informasi sensitif (misalnya informasi perbankan) atau mengajak mereka untuk mengunjungi situs web palsu. Sebuah bentuk rekayasa sosial secara digital untuk mengelabui orang-orang agar memasukkan informasi sensitif.

teks polos Informasi yang tidak dienkripsi.

server proxy Server yang bertindak sebagai perantara antara pengguna dan server lainnya, memvalidasi permintaan pengguna.

ransomware Perangkat lunak berbahaya yang membuat data atau sistem tidak dapat digunakan sebelum korban melakukan pembayaran.

pemulihan Aktivitas setelah insiden atau peristiwa untuk memulihkan layanan dan operasi penting dalam jangka waktu pendek dan menengah, dan seluruh kemampuan dalam jangka waktu yang lebih panjang.

ketangkasan Kemampuan beradaptasi pada kondisi yang berubah-ubah dan bersiap, bertahan dari, dan pulih dengan cepat dari gangguan.

pemulihan Pemulihan data setelah terjadinya kegagalan komputer atau hilangnya data.

penilaian risiko Proses identifikasi, analisis, dan evaluasi risiko serta konsekuensi dengan potensi berbahaya yang bertujuan untuk menunjukkan prioritas, mengembangkan atau membandingkan sejumlah tindakan, dan sebagai landasan untuk pengambilan keputusan.

Glosarium Istilah

manajemen peristiwa dan informasi keamanan (security information and event management/SIEM) Proses pengumpulan, penyortiran, dan pengaitan informasi jaringan untuk mendeteksi aktivitas yang mencurigakan.

smishing Phishing lewat SMS - pesan teks massal yang dikirim kepada pengguna yang meminta informasi sensitif (misalnya informasi perbankan) atau meminta mereka untuk mengunjungi situs web palsu.

penciri Pola yang berbeda dan dapat dikenali. Ada beberapa jenis penciri: penciri serangan, penciri digital, penciri elektronik.

rekayasa sosial Memanipulasi orang agar melakukan tindakan tertentu atau membocorkan informasi yang dapat dimanfaatkan penyerang.

perangkat lunak Program untuk memerintahkan pengoperasian komputer atau pemrosesan data elektronik.

spam Penyalahgunaan sistem pengiriman pesan elektronik untuk mengirim pesan secara massal tanpa diminta dan tanpa pandang bulu.

spear-phishing Bentuk phishing yang lebih bertarget, lewat surat elektronik yang dirancang seolah berasal dari orang yang dikenal/dipercayai si penerima pesan.

spoofing Pemalsuan alamat pengiriman transmisi untuk mendapatkan akses masuk ilegal [tanpa otorisasi] ke dalam sebuah sistem aman. Spoofing memiliki berbagai bentuk, seperti meniru, menyamar, membonceng, dan menyusup.

perangkat mata-mata Malware yang mengirim informasi tentang aktivitas pengguna komputer kepada pihak ketiga.

rantai pasokan Sebuah sistem organisasi, orang-orang, aktivitas, informasi, dan sumber daya, untuk membuat dan memindahkan produk termasuk komponen produk dan/atau layanan dari pemasok kepada pelanggannya.

sistem Secara umum mengacu pada sistem pada satu atau lebih dari satu komputer atau perangkat yang memasukkan, menghasilkan, mengolah, dan menyimpan informasi data.

administrator sistem (admin) Orang yang menginstal, mengonfigurasi, memecahkan masalah, dan memelihara konfigurasi server (perangkat keras dan perangkat lunak) untuk memastikan kerahasiaan, integritas, dan ketersediannya terjaga; admin juga mengelola akun, firewall, dan patch; bertanggung jawab atas kontrol akses, kata sandi, pembuatan akun, dan administrasi.

ancaman Sesuatu yang membahayakan sistem atau organisasi.

pengancam Sebuah program komputer yang dibuat menyerupai perangkat lunak yang sah tetapi memiliki fungsi tersembunyi yang digunakan untuk meretas komputer korban. Ini adalah sejenis malware.

trojan (kuda trojan) Sebuah program komputer yang dibuat menyerupai perangkat lunak yang sah tetapi memiliki fungsi tersembunyi yang digunakan untuk meretas komputer korban. Ini adalah sejenis malware.

autentikasi dua faktor (2FA) Penggunaan dua komponen yang berbeda untuk memverifikasi identitas yang diklaim pengguna. Ini juga dikenal dengan sebutan autentikasi multi-faktor.

virtual private network (VPN) Jaringan terenkripsi yang sering kali dibuat untuk membuat koneksi aman bagi pengguna jarak jauh, misalnya dalam organisasi yang memiliki kantor-kantor di berbagai lokasi.

virus Program komputer yang dapat mereplikasi sendiri, menginfeksi komputer tanpa izin atau sepengetahuan pengguna, lalu menyebarkannya ke komputer lain. Ini adalah sejenis malware.

kerentanan Sebuah kelemahan, atau kecacatan, dalam sebuah perangkat lunak, sistem, atau proses. Penyerang dapat memanfaatkan kerentanan untuk mendapatkan akses tanpa otorisasi ke sebuah sistem.

whaling Serangan phishing dengan target yang sudah direncanakan (terlihat sebagai surat elektronik yang sah) yang ditujukan kepada eksekutif senior.

worm Program mandiri yang mampu menyebar dan mereplikasi sendiri, menggunakan mekanisme jaringan untuk menyebarkan diri. Ini adalah sejenis malware.

Definisi disusun berdasarkan sumber daya yang dibuat oleh:

British Standards Institute

www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

National Cyber Security Centre (NCSC -UK)

www.ncsc.gov.uk/information/ncsc-glossary

National Initiative for Cybersecurity Careers and Studies (NICCS-US)

https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

Sumber Daya Tambahan:

Glosarium Australian Cyber Security Centre

www.cyber.gov.au/acsc/view-all-content/glossary

Global Knowledge

www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

SANS Institute Glossary of Security Terms

www.sans.org/security-resources/glossary-of-terms/