Latar Belakang Toolkit Keamanan Siber GCA:
Kotak Peralatan
Cegah Phishing dan Malware

Lebih dari 90% serangan siber dimulai dengan tautan phishing yang dikirim lewat surat elektronik (e-mail). Tujuan phishing adalah untuk mengelabui orang agar percaya bahwa mereka berurusan dengan pihak yang bertanggungjawab, sehingga informasi sensitif atau akses keuangan dapat direbut oleh penjahat siber.

Phishing adalah istilah yang umumnya terkait dengan komunikasi melalui surat elektronik, smishing (melalui pesan teks atau SMS), dan vishing (melalui telepon). Ada banyak jenis phishing, yaitu:

- **Phishing** (“memancing ikan”): Jenis ini umumnya tidak bertarget. Surat elektronik massal dikirim seolah-olah berasal dari organisasi terkemuka atau pihak yang bertanggungjawab. Komunikasi ini biasanya berhubungan dengan berita baru-baru ini, tahun pajak, atau tampak berasal dari organisasi umum yang digunakan oleh banyak orang dengan harapan bahwa beberapa penerima akan menanggapi.
- **Spear-Phishing** (“menombak ikan”): Jenis ini lebih bertarget. Surat elektronik dirancang sedemikian rupa sehingga tampak berasal dari orang atau organisasi yang dikenal oleh korban; sejumlah riset terhadap target yang dimaksud perlu dilakukan, sering kali dengan tujuan tertentu yang direncanakan.
- **Whaling** (Perburuan paus): Jenis ini sangat ditargetkan, biasanya terhadap tokoh-tokoh yang sangat senior dalam suatu organisasi. Pengintaian kemungkinan dilakukan dengan penjahat siber yang telah melacak gerakan dan mengumpulkan data selama berbulan-bulan sebelum bergerak. Tujuan yang sangat spesifik telah direncanakan.

Setelah berada di kotak masuk, penyerang akan berharap Anda mengklik tautan atau membuka lampiran yang akan memfasilitasi aktivitas yang dimaksudkan:

- **Malware**: Istilah umum yang digunakan untuk berbagai jenis perangkat lunak berbahaya:
    - **Virus**: Memperbanyak diri dan menyebar melalui inang. Jenis ini dapat menempel pada program atau file yang sah dan aktif ketika program berikutnya dijalankan.
    - **Worm**: Memperbanyak dan menyebarkan diri melalui koneksi jaringan. Misalnya, bersembunyi dalam lampiran lalu terkirim sebagai surat elektronik ke semua kontak di buku alamat surat elektronik Anda.
    - **Trojan**: Tidak memperbanyak diri; perangkat lunak berbahaya ini menyamar sebagai program sah yang bermanfaat (misalnya, lewat screensaver) sambil menyebabkan kerusakan di latar belakang.

Sebuah **backdoor** atau **pintu belakang** dapat dihasilkan (rute rahasia ke komputer untuk digunakan nanti), data mungkin dirusak, dan **perangkat mata-mata** (untuk melacak aktivitas Anda dan mengakses informasi pribadi) atau **ransomware** dapat diinstal (mengunci data Anda dan menuntut tebusan dibayar untuk mengambilnya).

Surat elektronik phishing TIDAK mudah dikenali, sebab:

- Terkadang tampak seperti dikirim olehseseorang yang Anda kenal.
- Alamat surat elektronik yang digunakan akan tampak sama persis dengan seseorang yang Anda kenal.
- Mereka mungkin meniru logo dan format surat elektronik dari organisasi terkenal.
- Mereka mungkin merujuk pada 'berita utama' baru-baru ini atau pekerjaan yang baru saja Anda selesaikan.
- Penyerang mungkin telah menelepon perusahaan Anda atau memeriksa secara daring untuk mempersonalisasi surat elektronik dan menambahkan 'legitimasi' lebih lanjut.

Penyerang akan melakukan apa pun yang mereka bisa untuk membuat surat elektronik mereka tampak asli dan menarik sehingga pengguna mengklik atau membukanya.

Konsekuensinya akan sangat buruk bagi individu dan usaha. Beberapa penelitian menunjukkan bahwa usaha kecil adalah usaha yang sangat berisiko terkena dampak phishing. Lebih dari 60% usaha kecil telah menderita serangan siber di tahun sebelumnya, penyebabnya dimulai oleh surat elektronik yang menjadi inisiator utama (atau vektor serangan) digunakan tanpa sengaja membuka tautan phishing.

Perangkat Lunak Antivirus (AV):
Membantu melindungi dari infeksi; perangkat ini bekerja dengan memeriksa karakteristik yang terkait dengan virus yang diketahui (dikenal sebagai tanda tangan) dan jika diidentifikasi, memblokir virus dan membersihkan file. Strain virus baru terus dikembangkan oleh para penyerang untuk mencoba dan mengintai perangkat lunak AV. Ketika virus baru dirilis, butuh beberapa saat untuk mengidentifikasi karakteristik virus dan memblokirnya. Serangan dengan menggunakan virus baru yang belum ada atau belum dikembangkan penangkalnya dikenal sebagai serangan 'zero day'.
Perangkat lunak antivirus juga dapat melihat perilaku operator yang tidak biasa (dikenal sebagai heuristik); AV mempelajari pola perilaku Anda yang biasa dan menjadi curiga jika sesuatu yang tidak biasa terjadi (misalnya, masuk ke sistem pada waktu yang tidak biasa).

Penting untuk selalu memperbarui perangkat lunak antivirus. Virus baru terus dikembangkan.

- *Pastikan perangkat lunak antivirus waktu nyata diinstal di semua komputer dan perangkat bergerak.*
- *Lakukan pemindaian berkala dan rutin pada semua sistem Anda.*

Pemfilteran Nama Domain (Pemfilteran DNS)

Syarat dan ketentuan berlaku saat menyiapkan situs web baru untuk memastikan situs web tersebut digunakan untuk tujuan yang sah - penjahat siber mengabaikan hal ini dan niat yang sebenarnya sulit diidentifikasi hingga situs web benar-benar beroperasi.

- Diperkirakan bahwa dari 200.000+ domain baru yang terdaftar setiap hari di seluruh dunia, hingga 70% diduga ditujukan untuk aktivitas berbahaya.
    - https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

Banyak perusahaan keamanan siber spesialis memantau penggunaan situs web bersama informasi lain untuk mengidentifikasi mereka yang beroperasi secara mencurigakan. Intelijen Ancaman dihasilkan dan, setelah dianalisis, digunakan untuk mengonfirmasi maksud berbahaya. Pemfilteran Nama Domain akan menggunakan Intelijen Ancaman ini (dari berbagai sumber) untuk memblokir akses ke situs web berbahaya, sehingga dapat mencegah bahaya yang dimaksudkan terjadi.

- **Quad9** adalah layanan Pemfilteran DNS yang dikembangkan oleh Global Cyber Alliance yang bermitra dengan IBM dan Packet Clearing House. Memiliki 19 umpan intelijen ancaman yang berbeda dan diketahui memblokir akses ke situs web berbahaya secara hampir waktu nyata (*real time*). Bekerja dengan menolak untuk mengonversi dan merutekan lalu lintas ke alamat IP yang terkait dengan nama domain situs web yang diketik di peramban. Juga dapat memblokir alamat IP perangkat IoT atau komputer Anda dapat diatur (tanpa sepengetahuan Anda) untuk terhubung secara otomatis.

Pemfilteran Nama Domain hanya dapat memblokir situs web setelah ambang batas aktivitas berbahaya diidentifikasi.

DNS: Layanan Nama Domain

- Layanan Nama Domain (DNS) mirip dengan buku telepon di Internet.
- Nama atau domain situs web yang unik, dalam format teks yang akan kita pahami (yakni, globalcyberalliance.org), diterjemahkan oleh Server Nama Domain ke dalam deretan angka unik (alamat IP - 192.124.249.5) yang dapat dipahami komputer.
- Situs web dan domain baru terus dibuat dan didaftarkan oleh Pencatat Nama Domain yang mengalokasikan dan mencatat alamat IP yang sesuai (GoDaddy merupakan salah satu contoh Pencatat Nama Domain).

Pendaftar harus memastikan bahwa situs web masing-masing memiliki nama domain dan alamat IP unik. Sebagian besar penipu akan mencoba untuk menggunakan domain situs web yang mirip untuk mengecoh korban agar mereka merasa sedang membuka situs resmi. Situs web semacam ini mungkin terlihat memiliki nama situs web asli, tetapi dengan memeriksanya lebih dekat dapat terlihat perbedaannya (misalnya, 'rn' dapat digunakan sebagai pengganti 'm' di alamat situs web).

Pemblokir Iklan

Beberapa iklan atau pesan yang muncul ketika menjelajah internet dirasa bermanfaat; namun, banyak yang tidak diinginkan, dan banyak juga yang mengandung kode berbahaya. Pemblokir iklan dapat digunakan untuk mencegah iklan muncul di halaman web saat menjelajah internet. Mereka menawarkan lini pertahanan lebih lanjut untuk melawan serangan.

Gunakan alat di Kotak Peralatan Cegah Phishing dan Malware untuk membantu melindungi Anda agar tidak menjadi korban phishing dan malware.

https://gcatoolkit.org/id/umkm/mencegah-phishing-dan-malware/?_tk=antivirus-id