Latar Belakang Toolkit Keamanan Siber GCA:
Kotak Peralatan
Lindungi Surat Elektronik dan Reputasi Anda

Surat elektronik digunakan secara luas sebagai inisiator atau awal mula untuk serangan siber. Surat elektronik adalah sarana yang mudah dan murah untuk menyebarkan ribuan surat elektronik dengan harapan si penerima tidak curiga dan kebanyakan orang tergoda untuk mengeklik tautan situs web yang rawan atau mengunduh lampiran berbahaya.

Tindakan ini dapat menyebabkan sistem komputer Anda terinfeksi dengan beberapa bentuk malware atau ransomware, yakni memberikan akses ke penjahat siber untuk mencuri data berharga atau mentransfer uang Anda ke akun si penipu. Situasi ini juga menjadi celah bagi penjahat siber untuk mengambil alih kendali sisem dan memanipulasi detail perbankan Anda, sehingga pelanggan melakukan pembayaran ke akun yang awalnya mereka kira itu adalah akun milik Anda.

Penggunaan surat elektronik phishing sangat efektif bagi penjahat siber - mereka dapat menjangkau ribuan calon korban dengan sangat cepat, tetapi agar mereka berhasil, surat elektronik harus tampak seolah-olah berasal dari sumber yang sah.

Ada beberapa cara yang mungkin dicoba oleh penjahat untuk melakukan tindakan berikut:

- **Spoofing Nama Tampilan**
  - Nama yang ditampilkan di 'kolom dari:' ***'Perusahaan'***
  - Alamat surat elektronik: *'<person@yahoo.com>'*
    - *Arahkan kursor pada nama tampilan untuk memeriksa alamat aktual sebelum melanjutkan.*
- **Spoofing Domain Serupa**
  - Nama yang ditampilkan di 'kolom dari:' ***'Perusahaan'***
  - Alamat surat elektronik: *'<person@c**0rn**pany.com>'*
    - *Periksa alamat surat elektronik dengan hati-hati sebelum melanjutkan.*
- **Spoofing Nama Domain**
  - Nama yang ditampilkan di 'kolom dari:' ***'Perusahaan'***
  - Alamat surat elektronik: *'<person**@company.com**>'*
    - *Gunakan DMARC untuk melindungi dari spoofing nama domain.*

Meskipun telah memeriksa dan memeriksa ulang, selalu lanjutkan dengan hati-hati dan gunakan cara alternatif untuk memeriksa keabsahan jika tidak yakin (yakni, hubungi pengirim untuk mengetahui apakah mereka benar-benar telah mengirim surat elektronik).

Dampak dari tidak memiliki pertahanan terhadap Spoofing Nama Domain berarti:

- Penyerang dapat berpura-pura menjadi Anda atau pemasok/pelanggan Anda untuk meminta pembayaran atau melakukan pemesanan.
- Penyerang juga dapat berpura-pura menjadi orang lain dari dalam organisasi Anda sendiri.

Mereka dapat melakukan:

- **CEO Fraud**, ketika surat elektronikl dikirim berpura-pura menjadi CEO atau staf senior yang berwenang. Mereka akan sering menginstruksikan kolega untuk segera melakukan pembayaran.
    - *Terapkan kebijakan bahwa ada baiknya untuk memeriksa ulang - bisnis keluarga sering beroperasi atas dasar kepercayaan dan jarang memeriksa; penyerang akan mengambil keuntungan dari keadaan ini.*
- **Pembobolan Surat Elektronik Bisnis (BEC)** terjadi ketika surat elektronik dikirim dari akun surat elektronik yang sudah disusupi – dikirim 'dari dalam organisasi' atau ketika surat elektronik tipuan menggunakan nama domain yang sah (spoofing nama domain). Ditujukan kepada pemasok atau pelanggan yang meminta pembayaran, tetapi mengubah detail bank. Karena penyerang berasal dari 'internal organisasi', mereka akan tampak lebih asli dan meyakinkan, dengan beberapa teknik autentikasi yang meratifikasi detail pengirim membuat mereka semakin sulit dikenali. Penyerang mungkin telah memantau komunikasi dan berada dalam sistem untuk sementara waktu, sehingga akan tampak sangat banyak tahu.
    - *Gunakan DMARC untuk membantu mencegah pembobolan awal, jika spoofing nama domain digunakan.*
    - *Gunakan kata sandi yang kuat dan mekanisme autentikasi multifaktor untuk mengurangi peluang pembobolan akun.*
    - *Periksa pengaturan akun surat elektronik Anda secara teratur untuk memastikan surat elektronik tidak diteruskan ke alamat surat elektronik yang tidak diketahui.*
    - *Memiliki kebijakan untuk memeriksa semua detail untuk pemasok dan pelanggan baru melalui setidaknya dua metode yang berbeda. Jika ada perubahan yang dilakukan, selalu periksa melalui metode alternatif yang diketahui (yakni, telepon melalui nomor/switchboard yang dikenal baik, tidak hanya apa yang mungkin terkandung dalam tanda tangan karena ini mungkin juga telah diubah).*

DMARC (Domain-based Message Authentication Reporting and Conformance)

Kebijakan DMARC memungkinkan pengirim menunjukkan bahwa pesan mereka dilindungi dan memberi tahu penerima apa yang harus dilakukan jika salah satu metode autentikasi lolos atau gagal.

DMARC

- Mencegah peniru 'berpura-pura menjadi Anda' dalam surat elektronik.
- Mencegah Anda menerima surat elektronik dari penipu.
- Memberikan wawasan tentang upaya spam, phish, atau spear-phish menggunakan domain surat elektronik organisasi Anda melalui pelaporan.
- Membangun kepercayaan dengan pelanggan dan rantai pasokan.

Namun

- Baik pengirim maupun penerima harus memiliki kebijakan DMARC dan verifikasi DMARC yang valid dan berlaku agar DMARC efektif
- Jika pelanggan dan pemasok menggunakan DMARC, ***keduanya*** DILINDUNGI dari spoofing domain surat elektronik – jika hanya salah satu yang menggunakannya, maka keduanya tidak dilindungi.
- Apa yang terjadi pada surat elektronik setelah diterima akan tergantung pada pengaturan kebijakan DMARC pengirim

Gunakan alat di Kotak Peralatan Lindungi Surat Elektronik dan Reputasi Anda untuk mengetahui lebih lanjut tentang DMARC dan mengonfigurasinya di domain surat elektronik Anda.

https://gcatoolkit.org/id/umkm/lindungi-surat-elektronik-dan-reputasi-anda/?_tk=implementasi-dmarc