Latar Belakang Toolkit Keamanan Siber GCA:
Kotak Peralatan
Ketahui Aset Anda

Sangat penting untuk mengenali apa yang Anda miliki, sebab Anda tidak dapat melindungi apa yang tidak Anda kenali. Dengan mengenali apa yang Anda miliki, Anda akan mampu:

- Memahami potensi risiko dan memungkinkan Anda melakukan sesuatu untuk melindunginya
- Mengetahui bahwa Anda tidak akan bisa menghilangkan seluruh risiko, tetapi Anda dapat menguranginya
- Memiliki disiplin dan kesadaran siber yang tinggi dapat mengurangi hingga 80% dari ancaman siber

Keamanan siber adalah sebuah proses, jadi mulailah berlatih untuk menerapkannya dalam rutinitas Anda sehari-hari.

Daftar Periksa
Ketahui Aset Anda

<u>Membuat inventaris:</u>

- Apa saja perangkat dan akun Teknologi Informasi (TI) Anda?
  - *Perangkat - desktop, server, laptop, smartphone, tablet, POS, IoT, CCTV...*
  - *Aplikasi - Microsoft Office, Adobe, aplikasi POS, Chrome...*
  - *Akun daring - surat elektronik, akun belanja daring, iCloud, Facebook, perbankan, kartu kredit...*

- Apa saja yang dapat diakses via Internet atau lewat jaringan internal Anda?
  - *Perangkat Internet-of-Things (IoT) seperti TV Pintar yang juga menggunakan jaringan internal Anda, tetapi dapat dikontrol melalui Internet, memiliki risiko siber*
  - *Perangkat lama yang tidak terpakai dan tidak diperbarui, tetapi masih aktif atau menyala, mungkin rentan terhadap serangan*
  - *Perangkat apa pun yang masih menggunakan kata sandi bawaan yang belum Anda ubah juga rentan mengalami pembobolan (misalnya, sistem CCTV dengan kata sandi admin/kata sandi admin sederhana atau router versi lama)*
  - *Akun daring lama yang tidak Anda gunakan tetapi masih menyimpan data Anda akan mudah disusupi dan membuat sistem Anda (dan perangkat terhubung lainnya) berisiko*

    - *Perangkat lunak di komputer yang tidak dipakai, tetapi belum dihapus, dapat menjadi target serangan siber*
- Tingkat akses apa yang diperlukan untuk memastikan kelancaran usaha?
    - Apakah akses telah dihapus untuk mereka yang tidak lagi membutuhkan akses? Contohnya:
        - *Hubungan yang sudah berakhir dengan kontraktor pihak ketiga*
        - *Pemasok yang sudah tidak lagi bekerjasama*
        - *Karyawan berhenti dari organisasi, beralih peran, atau sedang mengambil cuti yang lama*
    - Apakah sistem dan aplikasi yang tidak lagi relevan atau tidak lagi digunakan sudah dihapus?
    - Batasi jumlah pengguna dengan hak istimewa admin. Akses di level admin hanya boleh diberikan untuk administrator saja, bukan untuk pengguna harian.

- Batasi akses ke sistem dan aplikasi untuk berpotensi mengurangi kerusakan dari:
    - Ancaman internal baik yang disengaja maupun tidak disengaja. Penyebabnya:
        - *Tindakan yang disengaja oleh karyawan yang tidak puas atau kecewa*
        - *Karyawan yang diperas untuk memberikan akses ke informasi rahasia*
        - *Dampak dan konsekuensi dari membuka tautan phishing di e-mail*
        - *Penghapusan data yang tidak disengaja atau kerusakan data*

Saat melakukan inventaris, pertimbangkan juga apakah persyaratan kata sandi yang kuat dapat diterapkan dan Autentikasi Dua Faktor (2FA) telah diaktifkan. (2FA adalah lapisan perlindungan tambahan untuk kata sandi Anda.)

- Buatlah jaringan terpisah dan batasi hak akses (tiga level: admin/pengguna/tidak ada akses) sehingga informasi sensitif semakin sulit diakses dan sistem kunci tidak berada di jaringan yang sama dengan perangkat yang kurang aman, yang berpotensi mengurangi dampak serangan. Penyebabnya:
    - Banyaknya perangkat IoT konsumen yang tidak dilengkapi keamanan internal atau sangat minim keamanannya
    - Peralatan lama yang garansinya sudah habis dan sistemnya tidak lagi dilindungi dari kerentanan baru
    - Pihak ketiga dengan hak akses jaringan menawarkan rute bagi penyerang
        - *Jika pihak ketiga memiliki akses ke jaringan Anda, apakah mereka memiliki kebijakan untuk menerapkan perubahan kata sandi saat personel utama berhenti kerja?*

- Pastikan Anda memperbarui inventaris secara teratur, termasuk setiap kali Anda menambahkan atau menghapus perlengkapan, akun, atau data penting yang baru.

Gunakan alat di Kotak Peralatan 'Ketahui Aset Anda' untuk membantu Anda mengembangkan sistem alternatif yang sesuai untuk Anda.

https://gcatoolkit.org/id/umkm/ketahui-aset-anda/?_tk=mengidentifikasi-perangkat