Latar Belakang Toolkit Keamanan Siber GCA:
Kotak Peralatan
Cadangkan dan Pulihkan

Mencadangkan data sangatlah penting. Sebab kini semakin banyak informasi yang disimpan secara daring, baik untuk kepentingan bisnis maupun personal. Sehingga, pencadangan data sangat penting untuk Kelangsungan Bisnis.
Ada berbagai kemungkinan yang menyebabkan akses ke data Anda hilang. Dalam hal ini, kami mempertimbangkan factor kehilangan atau kerusakan data karena serangan siber, tetapi mencadangkan jdata uga akan memfasilitasi pemulihan karena penyebab seperti kegagalan hard disk, pencurian peralatan, kesalahan atau kelalaian manusia, kerusakan yang tidak disengaja, bahkan bencana banjir.

Ketergantungan yang tinggi pada komputer dan dunia daring membuat dampak kehilangan data, atau pemadaman sistem menjadi sangat serius pada produktivitas dan profitabilitas organisasi. Bahkan, hilangnya foto berharga di komputer pribadi, akan dapat menimbulkan keresahan dan kesedihan pada keluarga.

Mari berpikir sejenak, apa yang akan terjadi jika Anda:

- Tidak dapat menerapkan/menggunakan sistem TI Anda selama sehari penuh?
- Kehilangan proposal penting yang bisa memenangkan kontrak besar berikutnya?
- File pelanggan tidak dapat diakses lagi atau file tersebut rusak?
- Diperingatkan bahwa Anda hanya dapat mengakses informasi jika membayar uang tebusan?

Memiliki cadangan yang sangat penting untuk dapat melakukan pekerjaan sehari-hari!

Ransomware:
Ransomware adalah jenis malware yang memblokir akses ke sistem, perangkat, atau file sampai permintaan tebusan dibayarkan - biasanya dalam cryptocurrency (yaitu, bitcoin), yang cukup sulit dilacak dibandingkan transfer mata uang biasa.
Aksi semacam ini semakin populer dan melatari sejumlah serangan dengan profil tinggi. Contoh serangan ransomware meliputi:

- WannaCry: WannaCry memanfaatkan kerentanan di Sistem Operasi Windows pada tahun 2017 - NHS, Renault, dan FedEx terpengaruh.
- Petya (2016) dan NotPetya (2017): Petya menyebar, tersembunyi dalam PDF yang dilampirkan di surat elektronik (misalnya, CV berbahaya yang dikirim ke departemen SDM), dan berevolusi menjadi NotPetya yang memanfaatkan bagian kerentanan yang sama seperti pada serangan Wannacry.

- Pada awal 2020, TravelEx, sebuah perusahaan valuta asing global, menjadi korban serangan ransomware yang membuatnya luring selama lebih dari dua minggu dan menyebabkan kekacauan bagi jutaan pelaku perjalanan.

Meskipun jalan pintas dapat ditempuh dengan membayar tebusan, namun tindakan ini TIDAK disarankan.

Perlindungan Terhadap Ransomware:

- **Pastikan semua sistem sudah diperbarui** – disiplin siber yang baik, penambalan, pembaruan otomatis, dan perangkat lunak Antivirus waktu nyata akan membantu mencegah menjadi korban serangan ransomware.
- **Cegah pesan phishing/spam** dengan mengaktifkan filter yang sesuai dan mengedukasi pengguna untuk tidak mengeklik tautan atau membuka lampiran dari sumber yang tidak tepercaya.
- **Pencadangan reguler dan eksternal** akan membantu pemulihan jika Anda menjadi korban serangan ransomware (atau malware/penyebab kehilangan/kerusakan data lainnya).

Ada berbagai cara untuk mencadangkan:

- **Pencadangan luring** mengacu pada penyimpanan data secara lokal dan luring, seperti penyimpanan di hard drive eksternal, drive USB, kartu memori, atau perangkat lainnya. Perangkat tersebut harus dilepaskan dan disimpan terpisah dari perangkat itu sendiri.
- **Pencadangan daring** atau pencadangan cloud membuat salinan data penting dan menyimpannya di luar lokasi kerja di server yang aman 'di cloud.'

Pertimbangkan 'dampak kerugian' dari data yang Anda simpan; kembangkan kebijakan pencadangan yang memperhitungkan hal ini. Enkripsi harus diterapkan untuk melindungi informasi sensitif.

- Terapkan pendekatan (kebijakan) yang sesuai untuk mencadangkan data Anda, setelah mengategorikan berbagai jenis data yang Anda simpan.
- Pertimbangkan data penting dan sensitif - seberapa rutin harus dicadangkan dan bagaimana/di mana data tersebut harus disimpan?

Gunakan alat di Kotak Peralatan Cadangkan dan Pulihkan untuk mengonfigurasi pencadangan di semua sistem. Gunakan drive/perangkat eksternal untuk melakukan pencadangan luring.

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