{ Cyber.b1te }

SERANGAN SIBER & CARA MENGATASINYA

MEMAHAMI JENIS SERANGAN SIBER DAN LANGKAH PENCEGAHANNYA.

{ Cyber.b1te }

PENDAHULUAN

Di era digital, semakin banyak aktivitas yang dilakukan secara online, seperti berkomunikasi, bertransaksi, dan menyimpan data penting. Namun, kemajuan teknologi ini juga membawa risiko besar, terutama dalam hal keamanan data. Ancaman siber semakin meningkat dan menjadi salah satu masalah terbesar yang dihadapi individu maupun organisasi.

Dalam modul ini, kita akan membahas berbagai ancaman siber serta cara mencegah dan mengatasinya agar tetap aman saat beraktivitas di dunia digital.

- Phising
- Malware
- Man-in-the-middle Attack
- social Engieering

{ Cyber.b1te }

JENIS ANCAMAN SIBER

1. Phising

Phishing adalah metode penipuan di mana peretas berpura-pura menjadi pihak resmi, seperti bank atau perusahaan, untuk menipu korban agar memberikan informasi sensitif.

Ciri-ciri Phising

- Email atau pesan yang tampak resmi tetapi berasal dari alamat mencurigakan.
- Permintaan informasi pribadi secara mendesak (misalnya: "Akun Anda akan diblokir!").
- Tautan mencurigakan yang mengarahkan ke situs palsu.

Cara mencegah Phising

- Jangan klik tautan yang mencurigakan dalam email atau pesan.
- Periksa alamat pengirim dan pastikan berasal dari sumber terpercaya.
- Gunakan autentikasi dua faktor (2FA) untuk keamanan tambahan.

{ Cyber.b1te }

JENIS ANCAMAN SIBER

2. Malware - Perangkat Lunak Berbahaya

Malware adalah program berbahaya yang dirancang untuk mencuri data, menginfeksi sistem, atau mengendalikan perangkat tanpa izin.

Jenis-jenis Malware

- Virus – Merusak file dan menyebar ke sistem lain.
- Ransomware – Mengunci file korban dan meminta tebusan untuk membukanya.
- Spyware – Mengintai aktivitas pengguna tanpa izin.

Cara melindungi perangkat dari Malware

- Jangan mengunduh file dari sumber tidak terpercaya.
- Gunakan antivirus yang selalu diperbarui.
- Hindari membuka lampiran email mencurigakan.

{ Cyber.b1te }

JENIS ANCAMAN SIBER

3. Man-In-The-Middle Attack (MitM)

MitM adalah jenis serangan di mana peretas menyadap komunikasi antara dua pihak tanpa izin.

Bagaimana serangan ini terjadi?

- Peretas mencegat data yang dikirimkan antara korban dan server.
- Biasanya terjadi saat menggunakan Wi-Fi publik tanpa keamanan.
- Bisa juga terjadi pada situs web tanpa enkripsi (HTTP, bukan HTTPS).

Cara mencegah MitM

- Gunakan VPN saat menggunakan Wi-Fi publik.
- Pastikan situs web yang dikunjungi menggunakan HTTPS.
- Jangan login ke akun penting saat menggunakan jaringan umum.

{ Cyber.b1te }

JENIS ANCAMAN SIBER

4. Social Egineering - Manipulasi Psikologis

Tidak semua serangan siber dilakukan dengan teknologi canggih. Beberapa serangan memanfaatkan psikologi manusia, yang dikenal sebagai social engineering.

Jenis-jenis Social Engineering

- Pretexting – Pelaku berpura-pura menjadi orang terpercaya untuk mendapatkan informasi.
- Baiting – Korban diberikan iming-iming hadiah atau file menarik yang berisi malware
- Tailgating – Seseorang menyamar sebagai pegawai untuk masuk ke area terbatas.

Cara menghindari jebakan Social Engineering

- Jangan mudah percaya pada permintaan informasi pribadi.
- Selalu verifikasi identitas sebelum memberikan data.
- Waspadai pesan atau telepon yang menawarkan hadiah mencurigakan.

{ Cyber.b1te }

MENANGANI SERANGAN SIBER

Jika terkena serangan siber, penting untuk bertindak cepat agar dampaknya bisa diminimalkan.

JIKA TERKENA MALWARE/VIRUS

- ✅ Putuskan koneksi internet untuk mencegah penyebaran.
- ✅ Jalankan pemindaian antivirus dan hapus file yang terinfeksi.
- ✅ Jangan membayar tebusan jika terkena ransomware.

JIKA AKUN DIRETAS

- ✅ Segera ubah kata sandi dan aktifkan 2FA.
- ✅ Laporkan kejadian ke layanan terkait.
- ✅ Periksa perangkat lain yang mungkin masih login ke akun.

JIKA MENERIMA TAWARAN MENCURIGAKAN

- ✅ Jangan membagikan data pribadi ke sumber yang tidak jelas.
- ✅ Gunakan alat verifikasi untuk mengecek keaslian email atau situs.
- ✅ Jika ragu, tanyakan kepada pihak berwenang sebelum bertindak.

{ Cyber.b1te }

KESALAHAN UMUM YANG SERING TERJADI

1

PHISING EMAIL

Seorang pengguna menerima email dari "bank" yang meminta verifikasi akun. Tanpa sadar, ia memasukkan data login ke situs palsu dan kehilangan akses ke rekeningnya.

2

MALWARE DARI SOFTWARE BAJAKAN

Seorang pengguna mengunduh software gratis dari situs yang tidak terpercaya. Setelah diinstal, perangkatnya terinfeksi ransomware dan semua file terkunci.

3

DATA BOCOR DI WI-FI PUBLIK

Seorang pengguna login ke akun emailnya di Wi-Fi kafe tanpa VPN. Tanpa disadari, peretas di jaringan yang sama berhasil mencuri informasi loginnya.

✅ Pelajaran dari kasus ini:

- ✓ Waspadai email atau pesan mencurigakan.
- ✓ Jangan unduh file dari sumber yang tidak terpercaya.
- ✓ Gunakan VPN saat menggunakan Wi-Fi publik.

{ Cyber.b1te }

LANGKAH MENINGKATKAN KEAMANAN DIGITAL

01. Gunakan kata sandi yang kuat dan unik untuk setiap akun.

02. Aktifkan autentikasi dua faktor (2FA) untuk perlindungan tambah.

03. Jangan sembarangan membagikan informasi pribadi di internet

04. Selalu periksa sumber informasi sebelum mengklik tautan.

05. Pastikan semua perangkat memiliki perlindungan antivirus yang diperbarui.

{ Cyber.b1te }

KESIMPULAN

Mengenali berbagai jenis serangan adalah langkah awal untuk melindungi diri.

Keamanan digital adalah tanggung jawab bersama.

Ancaman siber bisa menyerang siapa saja, kapan saja.

Praktik keamanan yang baik dapat mencegah peretasan dan pencurian data

🛡️ Tetap waspada, tetap aman, dan selalu lindungi data pribadimu! 🚀