Modul Keamanan Siber

ITERA

DAFTAR ISI

Keamanan Siber

Keamanan siber adalah serangkaian praktik, kebijakan, dan teknologi yang dirancang untuk melindungi perangkat komputer, jaringan, aplikasi, dan data dari berbagai ancaman digital yang dapat membahayakan baik itu individu maupun kelompok organisasi.

Jenis Ancaman Siber

- **Phising**
  Jenis Penipuan dimana penipu akan berperan sebagai orang terpercaya atau instansi besar dan akan mengirim tautan palsu atau email palsu dengan tujuan mencuri data atau mengambil material dari korban.
- **Malware**
  Malware adalah ancaman siber yang bentuknya adalah sebuah perangkat lunak, dimana contohnya seperti virus yang menyerang komputer atau smartphone yang bertujuan untuk merusak perangkat yang terkena virus tersebut. Pada kasus kali ini adalah virus dari aplikasi surat undangan yang sempat viral.
- **Penipuan E-commerce dan Carding**
  Penipuan yang terjadi saat transaksi belanja online, Carding adalah jenis kejahatan yang mencuri data kartu kredit atau debit untuk digunakan secara ilegal.
- **Pembobolan Data**
  Kebocoran data pribadi seperti informasi rekening atau data pribadi lainnya yang dapat digunakan untuk kejahatan lebih lanjut. Kasus ini bisa terjadi dari kelalaian dalam penyimpanan data oleh suatu organisasi atau lembaga.

Pencegahan dari Ancaman Siber

- **Amankan Akun Anda**
  1. Gunakan kata sandi yang kuat dan unik: Kombinasikan huruf besar, kecil, angka, dan simbol untuk setiap akun.
  2. Aktifkan autentikasi dua faktor (2FA): Lapisan keamanan tambahan ini melindungi akun Anda bahkan jika kata sandi Anda bocor.
  3. Ubah kata sandi secara berkala: Ganti kata sandi Anda secara teratur untuk meningkatkan keamanan.
- **Waspadai Penipuan dan Tautan Mencurigakan**
  1. Hati-hati dengan phishing: Jangan pernah mengklik tautan atau membuka lampiran dari email atau pesan dari pengirim yang tidak dikenal atau mencurigakan.
  2. Waspadai social engineering: Pelajari cara kerja taktik manipulasi yang digunakan penyerang untuk mendapatkan informasi sensitif dari Anda.

- **Lindungi Data dan Perangkat Anda**
    1. Perbarui perangkat lunak secara rutin: Pembaruan sistem operasi, aplikasi, dan browser penting untuk menambal kerentanan keamanan.
    2. Gunakan perangkat lunak keamanan: Pasang dan selalu perbarui antivirus dan firewall untuk mendeteksi dan memblokir ancaman.
    3. Lindungi informasi pribadi: Batasi informasi pribadi yang Anda bagikan secara online, termasuk lokasi, dan jangan bagikan data sensitif di ruang publik digital.
    4. Gunakan jaringan yang aman: Hindari melakukan transaksi penting atau masuk ke akun sensitif saat menggunakan Wi-Fi publik yang tidak aman.
    5. Cadangkan data Anda: Buat cadangan data penting Anda secara teratur dan simpan di lokasi yang berbeda untuk melindungi dari kehilangan data.
- **Edukasi Diri Anda**
    1. Tingkatkan kesadaran: Pahami risiko keamanan siber dan bagaimana cara menghindarinya.
    2. Bagikan pengetahuan: Edukasi anggota keluarga dan rekan kerja tentang praktik keamanan siber yang baik.

Apa yang harus dilakukan setelah kita secara tidak sadar menginstall apllikasi yang tidak jelas atau data kita terserbar?

- **Tindakan Darurat dan Isolasi**
    1. Langkah pertama adalah mengisolasi area yang terkena serangan untuk mencegah penyebaran lebih lanjut dan membatasi kerusakan:
    2. Identifikasi dan Konfirmasi: Pastikan bahwa benar-benar terjadi serangan siber. Cari tanda-tanda kompromi, seperti aktivitas mencurigakan, perubahan data yang tidak sah, atau pesan tebusan (ransomware).
    3. Isolasi Sistem Terdampak: Segera putuskan koneksi perangkat atau sistem yang terpengaruh (misalnya, mencabut kabel jaringan atau mematikan koneksi Wi-Fi) dari jaringan utama. Ini penting untuk menghentikan penyebaran serangan.
    4. Hentikan Operasional Sementara: Nonaktifkan server atau sistem yang terkena dampak jika diperlukan untuk analisis dan perbaikan tanpa gangguan.
    5. Ubah Kredensial: Segera ubah semua kata sandi (password) dan token autentikasi yang mungkin telah disusupi, terutama untuk akun administrator dan akun yang terhubung dengan sistem yang terkena dampak.

- **Pemulihan dan Perbaikan**
  Fokus utama adalah mengembalikan sistem ke keadaan normal dengan aman:
  1. Eradikasi Ancaman: Pastikan semua malware telah dihapus dan kerentanan yang dieksploitasi telah ditutup atau diperbaiki.
  2. Pemulihan Data: Pulihkan data dan sistem yang rusak atau terinfeksi menggunakan file backup terbaru dan bersih. Pastikan integritas data diverifikasi sebelum sistem dikembalikan ke operasi penuh.
  3. Perbaikan Kerentanan: Tinjau dan perbaiki semua kerentanan yang ditemukan. Ini termasuk memperbarui perangkat lunak (patching), memperkuat konfigurasi keamanan, dan mengubah kebijakan akses.
  4. Uji Coba Sistem: Lakukan uji coba menyeluruh setelah pemulihan untuk memastikan sistem berfungsi dengan baik, aman, dan tidak ada sisa ancaman.
- **Komunikasi dan Pelaporan**
  Transparansi dan kepatuhan hukum sangat penting dalam fase ini:
  1. Komunikasi Internal: Beri tahu semua karyawan, terutama tim manajemen dan tim teknis, tentang insiden tersebut dan batasan operasional yang mungkin berlaku.
  2. Pelaporan Pihak Berwenang: Laporkan serangan siber kepada pihak berwenang yang relevan, seperti kepolisian atau lembaga yang bertanggung jawab atas keamanan siber (di Indonesia, contohnya Badan Siber dan Sandi Negara/BSSN atau Kementerian Komunikasi dan Informatika/Kominfo jika terkait data pribadi).
  3. Berikan Pembaruan: Beri tahu pelanggan atau mitra yang mungkin terpengaruh tentang insiden tersebut, dampak yang ditimbulkan, dan langkah-langkah yang diambil untuk mengatasinya.

Phishing

Tujuan Pembelajaran

1. Mengerti apa itu phishing atau penipuan digital.
2. Mampu mengenali ciri-ciri pesan atau penipuan digital.
3. Tahu langkah aman saat menerima pesan mencurigakan.
4. Bisa membantu menyebarkan kesadaran di lingkungan sekitar.

Apa itu Phishing

Phishing (dibaca: fising) adalah penipuan lewat pesan digital , seperti :

- SMS , WhatsApp , Facebook , atau email
  Dimana berpura-pura berasal dari bank , pemerintahan , atau teman, dengan tujuan mengambil uang , data pribadi , atau akun kita.
  Contoh pesan :
  “Selamat! Anda mendapat bantuan dana desa Rp1.000.000. Klik link berikut untuk pencairan”
  https://selamat.anda.dapat.duit.com
- Mengaku menjadi pihak Bank
  Pelaku akan berpura pura menjadi pihak bank dan meminta kode OTP atau PIN ATM. dimana OTP dan PIN ATM tersebut digunakan untuk membobol rekening korban dan mengambil saldo yang ada di rekening.
- Tawaran Kerja Online
  Pelaku akan berpura pura menawarkan pekerjaan online dengan gaji besar tapi minta biaya pendaftaran terlebih dahulu.

Ciri-ciri Pesan Penipuan (Phishing).

Untuk mengenali ciri - ciri phishing dapat mengingat dengan rumus 3C : Cek Pengirim , Cek Isi , Cek Tautan.

Cek	Yang perlu di perhatikan
Pengirim	Nomor/akun tidak dikenal , bukan dari nomor resmi.Kadang pakai nama mirip instansi seperti “BANK BRI ASLI”
Isi pesan	Menjanjikan hadiah,bantuan,atau ancaman blokir akun.Kadang pakai bahasa tergesa-gesa seperti “Segera klik link ini!”
Tautan	Mengarah ke situs aneh (misalnya : selamat.anda.dapat.duit.com bukan situs resmi seperti bri.co.id

Dampak Jika Tertipu

Beberapa dampak atau hal - hal yang dapat terjadi jika berhasil tertipu :

- Uang hilang di rekening / e-wallet
- Akun sosial media diambil alih lalu digunakan untuk menipu orang lain
- Data pribadi disalahgunakan untuk menipu atau mendaftar ke situs ilegal
- Perangkat dapat rusak karena terkena virus.

Cara Mencegah

Langkah-langkah mudah untuk mencegah yang dapat dilakukan oleh siapa pun:

1. Jangan klik link atau lampiran dari orang tidak dikenal.
2. Jangan berikan PIN, OTP , atau kata sandi ke siapa pun (termasuk yang mengaku dari bank / pemerintah)
3. Gunakan verifikasi dua langkah di akun-akun penting untuk mengamankan akun dari pembobolan.
4. Pastikan situs resmi yang biasanya berakhiran .go.id , .co.id atau sumber terpercaya lainnya.

Contoh Kasus Nyata

Berikut beberapa kasus yang pernah didapati di dunia nyata.

1. Kasus ibu sari
   Bu sari menerima pesan WhatsApp dari nomor tak dikenal yang mengaku dari "Kementerian Sosial".
   Pesannya :
   "Selamat, ibu sari terdaftar sebagai penerima bantuan langsung tunai Rp.900.000. Silahkan klik link berikut untuk pencairan:
   👉bansos-gratis2025.netlify.app

   Bu sari membuka link itu dan mengisi nama , NIK , nomor rekening , dan OTP dari SMS bank. Keesokan harinya, saldo rekening bu sari hilang sebesar Rp.10 Juta.

   Ciri-ciri phising yang terlihat :
   - Domain situs bukan resmi
   - Ada janji bantuan cepat dan desakan waktu
   - Diminta kode OTP dan data pribadi.

2. Kasus Yanto
   Yanto melihat iklan di facebook yang berisi :
   "Lowongan kerja online dari rumah! Gaji Rp.300.000 per hari. Cukup isi data dan bayar biaya pendaftaran sebesar Rp50.000.

   Yanto tergiur, mengisi data pribadinya, lalu mentransfer uang "pendaftaran". Setelah itu,nomor pengirim tidak bisa dihubungi lagi.

   Ciri-ciri phishing yang terlibat:
   - Ada permintaan transfer uang terlebih dahulu
   - Tawaran terlalu bagus untuk dipercaya

Penutup

Phishing atau penipuan digital kini banyak menyasar ke masyarakat desa melalui pesan WhatsApp, SMS, dan media sosial.Agar tidak tertipu, kita perlu selalu waspada terhadap pesan yang menawarkan hadiah, bantuan, atau meminta data pribadi.Jangan pernah membagikan kode OTP, PIN, atau kata sandi kepada siapa pun dan pastikan informasi hanya sumber resmi. Jika ragu , tanyakan dulu kepada perangkat desa atau keluarga sebelum bertindak. Dengan saling mengingatkan dan berhati-hati , kita bisa menjaga desa agar aman dari penipuan digital.

KEAMANAN DATA PRIBADI

TUJUAN PEMBELAJARAN

1. Memahami apa itu data pribadi
2. Mengenali modus penipuan
3. Melakukan tindakan pencegahan
4. Bereaksi dengan tepat

I. Bagian I: Memahami Apa Itu Data Pribadi

Penjelasan yang Ada: Data dibagi 3 Level (Kunci Brankas, Surat Berharga, Data Penunjang).

Penjelasan Lebih Lanjut (Mengapa Demikian?):

- **Mengapa "Nama Gadis Ibu Kandung" Jadi Kunci Ajaib? (Data Level 2)**
    - **Latar Belakang:** Ini adalah "pertanyaan keamanan" (security question) yang sudah dipakai puluhan tahun oleh bank di seluruh dunia.
    - **Logikanya Dulu:** Bank mengira ini adalah data "statis" (tidak berubah) dan "privat" (hanya diketahui keluarga inti).
    - **Kelemahannya Sekarang:** Di era digital, data ini tidak privat lagi. Data ini sering ada di dokumen publik (seperti akta kelahiran) dan kadang diumbar di media sosial (saat hari ibu, dll). Namun, karena sistem perbankan lambat berubah, data ini *masih* dianggap sebagai kunci cadangan terkuat. Inilah mengapa penipu sangat mengincarnya. Ini adalah "kunci pas" untuk membuktikan identitas Anda di telepon.
- **Bagaimana "Data Penunjang" (Level 3) Bekerja? Konsep "Puzzle Profiling"**
    - Penipu itu seperti sedang menyusun puzzle gambar wajah Anda.
    - Satu kepingan (misal, tanggal lahir Anda dari postingan Facebook) tidak berbahaya.
    - Kepingan kedua (misal, alamat Anda dari kiriman paket di status WA) juga sepele.
    - Kepingan ketiga (misal, nama lengkap Anda) juga biasa.
    - **Bahayanya:** Ketika 3 kepingan ini digabung, penipu mendapatkan "informasi" (profil). Dia bisa menebak password Anda (Budi10Oktober1980), atau menelepon Anda dengan pura-pura jadi teman lama ("Halo, ini saya teman SD-mu di Desa A..."), atau bahkan mencari tahu nama ibu Anda dari data kependudukan yang mungkin bocor.

2. Bagian 2: Mengenali Modus Penipuan

Penjelasan yang Ada: Modus .apk, Modus Hadiah, Modus Kecelakaan, Modus Petugas Bank. Psikologinya Panik & Serakah.

Penjelasan Lebih Lanjut (Teknik di Balik Modus):

- **Detail Teknis Modus .apk: Ancaman Ganda**
  - Bukan hanya **Membaca SMS OTP**, aplikasi .apk modern punya kemampuan kedua yang lebih jahat: **"Screen Overlay" (Layar Tampilan Palsu).**
  - *Cara Kerjanya:* Anda membuka aplikasi m-banking Anda yang ASLI. Si aplikasi jahat .apk ini mendeteksinya, lalu dia *secepat kilat* menampilkan **layar login palsu** di atas aplikasi asli Anda.
  - Terlihat sama persis. Anda memasukkan Username dan Password Anda di layar palsu itu. Data Anda langsung terkirim ke penipu. Setelah itu, layar palsu itu menghilang, dan Anda kembali ke aplikasi asli (Anda mengira salah ketik). Padahal, data Anda sudah dicuri.
- **Istilah Sebenarnya: "Rekayasa Sosial" (Social Engineering)**
  - Anda bisa jelaskan ke warga: "Bapak/Ibu, semua modus tadi itu namanya 'Rekayasa Sosial'. Ini adalah **ilmu tipu-tipu**. Penipu zaman sekarang itu bukan meretas komputer, tapi **meretas pikiran manusia.**"
  - Mereka menggunakan **Asas Otoritas** (pura-pura jadi polisi, petugas bank) agar kita takut dan patuh.
  - Mereka menggunakan **Asas Keterdesakan** (pura-pura "Anak kecelakaan!", "Blokir dalam 10 menit!") agar kita tidak sempat berpikir jernih.
  - Intinya: Mereka membuat kita panik agar logika kita mati.

3. Bagian 3: Melakukan Tindakan Pencegahan

Penjelasan yang Ada: Password kuat (Frasa Sandi), Gembok Ganda (2FA), Jaga Medsos (Alun-alun).

Penjelasan Lebih Lanjut (Menaikkan Level Keamanan):

- **Kebersihan Password: "Satu Akun, Satu Password Kuat"**
  - **Masalah:** Banyak orang pakai 1 password (misal `Budi12345`) untuk Facebook, Email, dan M-Banking.
  - **Bahayanya:** Jika akun Facebook-nya (yang keamanannya lemah) diretas, penipu akan otomatis mencoba password yang sama di Email dan M-Banking Anda. Ini disebut **"Credential Stuffing"**.
  - **Solusi Praktis:** Gunakan "Frasa Sandi" yang sudah kita pelajari, lalu tambahkan nama layanannya.
    - Contoh: Frasa dasar: `SayaPunya5AyamKate`
    - Password Facebook: `SayaPunya5AyamKate-FB`
    - Password Google: `SayaPunya5AyamKate-GMAIL`
  - Ini tetap mudah diingat, tapi gemboknya beda-beda.
- **Detail "Gembok Ganda" (2FA): Jenis-jenisnya**
  - **Level 1 (Bagus): 2FA via SMS.** Ini yang paling umum. Kode dikirim ke nomor HP kita.
  - **Kelemahan:** Bisa dibajak oleh modus `.apk` yang membaca SMS.
  - **Level 2 (Lebih Bagus): 2FA via Aplikasi Authenticator** (Contoh: Google Authenticator).
  - **Penjelasan Sederhana:** "Ini adalah aplikasi di HP kita yang membuat kode 6 angka baru setiap 30 detik. Kode ini tidak dikirim lewat SMS, jadi tidak bisa diintip oleh penipu `.apk`. Ini jauh lebih aman." (Ini bisa jadi materi untuk workshop lanjutan).
- **Detail Medsos: Konsep "Jejak Digital" (Digital Footprint)**
  - Analogi "Alun-alun" itu bagus. Tambahkan ini: "Apapun yang Bapak/Ibu posting di alun-alun itu, akan **tercatat selamanya**, seperti ada yang mencatat di buku besar, walaupun postingannya sudah dihapus."
  - Penipu bisa "menggali" (stalking) postingan kita 5 tahun lalu untuk mencari tahu: "Siapa nama hewan peliharaan pertama?" atau "Apa nama SD Anda?". Pertanyaan-pertanyaan ini sering dijadikan pertanyaan keamanan untuk mereset password.

4. Bagian 4: Bereaksi Dengan Tepat

Penjelasan yang Ada: Jangan Panik, Jangan Klik. Skenario reaksi untuk telepon, WA, dan OTP.

Penjelasan Lebih Lanjut (Tindakan Darurat & Lanjutan):

- **Aturan Emas Verifikasi: "Gunakan Saluran Kedua"**
  - Ini adalah prinsip utama saat bereaksi.
  - **Jika penipu menghubungi Anda lewat WA** (misal, mengaku teman pinjam uang) -> Anda harus verifikasi lewat **Telepon** ke nomor aslinya.
  - **Jika penipu menghubungi Anda lewat Telepon** (misal, mengaku dari bank) -> Anda harus verifikasi dengan **Datang Langsung** ke kantor bank terdekat.
  - **Intinya:** Jangan pernah percaya pada saluran komunikasi yang *digunakan oleh penipu*. Selalu pindah saluran untuk mengecek.
- **SKENARIO DARURAT: "Saya SUDAH TERLANJUR Klik Link .apk! Harus Bagaimana?"**
  - Ini adalah pertanyaan paling penting yang mungkin ditanyakan warga. Mereka butuh **Pertolongan Pertama Pada Kecelakaan Digital**.
  - **Langkah 1 (Putus Koneksi):** Segera **MATIKAN DATA INTERNET** dan **WIFI** di HP tersebut. Ini memutus koneksi penipu ke HP kita.
  - **Langkah 2 (Amankan Uang):** Gunakan **HP LAIN** (pinjam HP tetangga/keluarga). **Telepon Call Center resmi Bank** Anda. Minta **BLOKIR SEMUA REKENING** dan kartu ATM Anda saat itu juga. Jelaskan Anda baru saja meng-klik .apk.
  - **Langkah 3 (Amankan Akun):** Masih dari HP LAIN, buka akun media sosial dan email Anda, ganti semua passwordnya.
  - **Langkah 4 (Bersihkan HP):** Tindakan terbaik adalah **"FACTORY RESET"** atau **"Setel Ulang Pabrik"** HP yang terinfeksi. Ini akan menghapus semua data, termasuk aplikasi jahatnya. Bawa ke orang yang mengerti (konter HP) jika tidak bisa sendiri.
- **Tindakan Lanjutan: Melapor Kemana?**
  - Bukan hanya diblokir, tapi laporkan agar rekening dan nomor penipu ditindak.
  - **Lapor Rekening Penipu:** ke situs resmi Kominfo: cekrekening.id
  - **Lapor Nomor HP Penipu:** ke situs resmi Kominfo: aduannomor.id
  - **Lapor ke Polisi:** Buat laporan resmi sebagai bukti jika terjadi kerugian besar.