TUGAS 1 CYBER SECURITY
COMMON CYBER THREAT

Disusun Oleh

Muh. Rifky
220205600005

JURUSAN PENDIDIKAN TEKNIK ELEKTRONIKA
PRODI TEKNIK ELEKTRONIKA-D4
FAKULTAS TEKNIK
UNIVERSITAS NEGERI MAKASSAR

2025

Soal:

Buatlah maksimal 1 halaman google docs terkait kasus malware yang ada di indonesia dan cara instansi / organisasi tersebut menangani

Jawab:

1. Serangan Ransomware pada PDNS (2024)
   a. Peristiwa
      Serangan ransomware pada Pusat Data Nasional Sementara (PDNS) menyebabkan gangguan layanan publik di ratusan instansi pemerintah karena data tidak dapat diakses.
   b. Penanganan
      Penanganan yang dilakukan pemerintah berfokus pada isolasi server yang terdampak untuk mencegah meluasnya serangan, aktivasi sistem cadangan atau *backup* data yang tersimpan di pusat pemulihan bencana, serta koordinasi dengan Badan Siber dan Sandi Negara (BSSN) dan Kementerian Komunikasi dan Informatika untuk mempercepat proses investigasi. Selain itu, penguatan infrastruktur keamanan dilakukan dengan menambah sistem deteksi intrusi, melakukan audit digital menyeluruh, serta memperbaiki protokol keamanan untuk mencegah kejadian serupa di masa mendatang.
2. Aktivitas Mencurigakan di Aplikasi KFCKU (2024)
   a. Peristiwa
      KFC Indonesia mendeteksi aktivitas mencurigakan yang berpotensi mengekspos data pelanggan, yang mengindikasikan adanya potensi serangan malware atau peretasan.
   b. Penanganan
      Penanganan yang dilakukan KFC adalah dengan menutup sementara akses ke aplikasi untuk meminimalisir risiko, melakukan investigasi internal untuk menemukan sumber celah keamanan, dan segera menambal kerentanan tersebut dengan *patching*. Perusahaan juga memberikan pemberitahuan resmi kepada pelanggan secara transparan agar mereka dapat lebih waspada. Sebagai tindak lanjut jangka panjang, KFC meningkatkan lapisan keamanan sistemnya dengan menerapkan autentikasi ganda atau *multi-factor authentication* (MFA) pada sistem internal agar akses tidak mudah ditembus peretas.
3. Serangan Malware pada BSI (2022)
   a. Peristiwa
      Bank Syariah Indonesia (BSI) pernah mengalami serangan ransomware yang mengganggu layanan bank tersebut.
   b. Penanganan
      Penanganan dilakukan dengan memanfaatkan pusat pemulihan bencana (*disaster recovery center*) untuk mengembalikan layanan secepat mungkin. Pihak bank juga melakukan analisis forensik digital guna melacak jejak pelaku serangan sekaligus memperbaiki celah keamanan yang dimanfaatkan peretas. Selain itu, data nasabah diperkuat dengan enkripsi berlapis agar tidak mudah diambil alih oleh pihak luar. Untuk mencegah kejadian serupa, BSI mengadakan pelatihan internal terkait kesadaran terhadap serangan *phishing* dan *social engineering*, karena faktor manusia seringkali menjadi pintu masuk utama malware.

4. Kasus Malware Trojan Activity (2021)
    a. Peristiwa

       Badan Siber dan Sandi Negara (BSSN) mencatat anomali malware Trojan activity sebagai jenis serangan siber terbanyak di Indonesia pada tahun 2021, yang berfokus pada pengumpulan informasi.
    b. Penanganan.

       Penanganan dilakukan melalui kampanye kesadaran keamanan digital yang menekankan pentingnya memperbarui sistem operasi dan perangkat lunak secara rutin. BSSN juga mendorong penggunaan sistem keamanan *endpoint* di instansi pemerintahan, memperkuat fungsi *firewall* serta monitoring jaringan secara real-time. Selain upaya teknis, edukasi publik menjadi langkah penting agar masyarakat lebih berhati-hati terhadap tautan, lampiran, maupun aplikasi mencurigakan yang sering menjadi sarana penyebaran Trojan.