# RESUME

# KEAMANAN JARINGAN


**ACH WALDAN HIZAM FIKRI**

**E32230688**

**GOL : B**

**SEMESTER III**

**PROGRAM SETUDI TEKNIK KOMPUTER JURUSAN TEKNOLOGI INFORMASI**

**POLITEKNIK NEGRI JEMBER TAHUN 2024**

## Serangan Ransomware

Ransomware adalah jenis malware yang mengenkripsikan data korban dan menuntut tebusan untuk memullihkan akses. Serangan ini pertama kali muncul pada akhir 1980-an dengan munculnya “AIDS Trojan” atau “PC Cyborg,” tetapi baru beberapa tahun terakhir serangan ransomware menjadi ancaman global yang serius. Dengan perkembangan teknologi, ransomware telah berevolusi menjadi lebih canggih dan lebih sulit ditangani.

## Cara Kerja Ransomware

Ransomeware biasanya diserbarkan melalui metode seperti phishing, metode penyebaran lainnya termasuk exploit kit yang mengeksploitasi kerentanan dalam perangkat lunak, serangan Remote Desktop Protocol (RDP), dan pembaruan perangkat lunak palsu.

Setelah ransomware berhasil masuk ke system korban, ia akan memulai proses enkripsi file dengan ekstensi umum seperti docx, jpg, dan pdf menjadi target utama enkripsi. Setelah enkripsi selesai, pelaku akan menuntut tebusan dalam bentuk mata uang digital, sepertin Bitcoin, dengan janji memberikan kunci deskripsi setelah pembayaran dilakukan.

## Dampak Serangan Ransomware

Serangan ransomware dapat memiliki dampak yang sangat merugikan, baik secara finansial maupun non-finansial. Dampak yang paling jelas adalah hilangnya akses ke data penting yang bisa mengganggu operasi harian, menyebabkan kerugian finansial besar. Sebagai contoh, serangan ransomware pada perusahaan besar bisa mengakibatkan kerugian jutaan dolar dalam bentuk gangguan operasi, kehilangan pendapatan, dan biaya pemulihan.

Di samping dampak finansial, serangan ini juga dapat merusak reputasi organisasi, terutama jika data sensitif milik pelanggan turut terlibat. Kepercayaan pelanggan bisa menurun drastis, yang berpotensi menyebabkan penurunan bisnis jangka panjang.

Kasus terkenal seperti serangan WannaCry pada tahun 2017 dan serangan pada Colonial Pipeline pada tahun 2021 menunjukkan betapa parahnya dampak yang dapat ditimbulkan oleh ransomware. Serangan-serangan ini tidak hanya menyebabkan kerugian finansial, tetapi juga mempengaruhi layanan publik yang esensial.

## Pencegahan dan Perlindungan

Untuk mencegah infeksi ransomware, langkah-langkah keamanan yang solid sangat diperlukan. Beberapa langkah utama meliputi:

1. **Backup Data Secara Teratur**: Melakukan backup data yang teratur dan menyimpannya di lokasi yang terpisah dari jaringan utama adalah langkah penting untuk melindungi dari serangan ransomware.

2. **Pelatihan Karyawan**: Manusia sering kali menjadi titik lemah dalam keamanan siber. Memberikan pelatihan kepada karyawan tentang bagaimana mengenali dan menghindari ancaman seperti email phishing sangat penting.

3. **Keamanan Perangkat Lunak dan Jaringan:** Memastikan semua perangkat lunak diperbarui secara teratur untuk menutup celah keamanan yang bisa dieksploitasi oleh ransomware.

4. **Pembatasan Akses**: Mengimplementasikan prinsip "least privilege" di mana pengguna hanya diberikan akses ke data yang mereka perlukan untuk melakukan tugas mereka. Ini mengurangi risiko penyebaran ransomware jika terjadi infeksi.

5. **Monitoring dan Deteksi Awal**: Menggunakan alat monitoring jaringan yang canggih dapat membantu mendeteksi tanda-tanda awal infeksi ransomware, memungkinkan tindakan segera sebelum kerusakan lebih lanjut terjadi.

## Tanggapan Terhadap Serangan

Jika terkena serangan ransomware, langkah pertama yang harus diambil adalah memutus koneksi perangkat yang terinfeksi dari jaringan untuk mencegah penyebaran lebih lanjut. Selanjutnya, jika backup tersedia, data dapat dipulihkan tanpa perlu membayar tebusan.

Sangat tidak disarankan untuk membayar tebusan karena tidak ada jaminan bahwa pelaku akan memberikan kunci dekripsi, dan pembayaran ini hanya akan mendorong pelaku untuk melakukan serangan lebih lanjut. Sebaiknya, insiden ini dilaporkan kepada pihak berwenang, dan organisasi bekerja sama dengan pakar keamanan siber untuk memitigasi kerusakan dan memulihkan data.