Latar Belakang:
Bank Nexus adalah salah satu bank besar di Indonesia yang menyediakan berbagai layanan perbankan untuk nasabah individu dan korporat. Pada tahun lalu, Bank Nexus mengalami serangan ransomware yang signifikan yang mengakibatkan gangguan operasional besar dan kerugian finansial yang cukup besar. Kasus ini bertujuan untuk menganalisis insiden tersebut, mengidentifikasi kerentanan, dan memberikan rekomendasi untuk mencegah kejadian serupa di masa depan.

Tujuan Analisis:

Analisis ini bertujuan untuk mengevaluasi insiden ransomware yang dialami oleh Bank Nexus, mengidentifikasi titik lemah dalam sistem keamanan mereka, dan memberikan rekomendasi untuk meningkatkan postur keamanan siber bank guna mencegah serangan serupa di masa depan.

Existing Security Posture

Langkah-Langkah Keamanan yang Saat Ini Diterapkan:

1. Firewall dan IDS/IPS:
    - Penggunaan firewall untuk melindungi jaringan dari akses yang tidak sah.
    - Sistem deteksi dan pencegahan intrusi (IDS/IPS) untuk memonitor dan menghentikan aktivitas mencurigakan.
2. Antivirus dan Anti-Malware:
    - Solusi antivirus dan anti-malware di semua endpoint dan server untuk mendeteksi dan menghapus perangkat lunak berbahaya.
3. Data Backup:
    - Pencadangan data secara rutin, tetapi belum ada strategi pencadangan yang robust dan terpisah secara fisik dari jaringan utama.

Kerentanan yang Tersisa:

- Phishing Susceptibility: Karyawan yang belum cukup terlatih dalam mengenali email phishing.
- Backup Strategy: Pencadangan data yang belum terenkripsi dan tidak terisolasi dari jaringan utama, sehingga masih rentan terhadap serangan ransomware.
- Patch Management: Sistem yang tidak diperbarui secara rutin, meninggalkan celah keamanan yang dapat dieksploitasi.

- Low Employee Discipline and Oversight: Kedisiplinan karyawan yang rendah dan kurangnya pengawasan yang ketat mengakibatkan peningkatan risiko terjadinya insiden keamanan.