# TUGAS KELOMPOK

**KASUS CYBERCRIME**

**KOMPUTER DAN MASYARAKAT**

Dosen Pengampu:

Sattriedi Wahyu Binabar, M.Kom



**Disusun Oleh:**

1. Achmad Rhiza Khulaify 21.230.0071
2. Aliffiyan Azizul Rifqi 21.230.0072
3. Lilis Royani 21.230.0078
4. Nadya Sakina Amalia 21.230.0082
5. Faradia Nur Karimah 21.230.0099

**INSTITUT WIDYA PRATAMA PEKALONGAN**

# 2024

1. Pencurian Data Bank Syariah Indonesia (BSI) oleh Ransomware

Pada tanggal 8 Mei 2023, Bank Syariah Indonesia (BSI) mengalami serangan ransomware yang diduga dilakukan oleh kelompok peretas LockBit 3.0, yang mengakibatkan gangguan signifikan pada layanan perbankan, termasuk mobile banking dan ATM. Serangan ini menyebabkan kebocoran data sensitif, dengan total data yang dicuri mencapai 1,5 TB, mencakup informasi pribadi 15 juta pengguna seperti nama, nomor ponsel, alamat, saldo rekening, dan riwayat transaksi. Meskipun manajemen BSI awalnya menyatakan bahwa gangguan disebabkan oleh pemeliharaan sistem, para ahli keamanan siber mengindikasikan bahwa serangan tersebut lebih serius dan dapat mengganggu operasional bank secara keseluruhan. Dalam merespons insiden ini, BSI berusaha melakukan pemulihan sistem dan menjaga keamanan dana nasabah, sambil meminta nasabah untuk tetap waspada terhadap penipuan digital. Penyerang menggunakan teknik penetrasi melalui perangkat keamanan dengan pengaturan default yang masih aktif, memungkinkan mereka untuk mengakses dan mengenkripsi data penting di dalam sistem BSI.

Sumber:

1. <https://www.cnnindonesia.com/teknologi/20230513093401-185-949046/ransomware-lockbit-30-klaim-lumpuhkan-bsi-dan-curi-data-pengguna>
2. <https://www.cnbcindonesia.com/tech/20230510174928-37-436279/bsi-diserang-ransomware-nasib-uang-nasabah-gimana>
3. <https://www.asdf.id/serangan-ransomware-menghantam-bank-syariah-indonesia/>
4. <https://finansial.bisnis.com/read/20240627/90/1777564/begini-serangan-ransomware-bsi-tahun-lalu-mirip-dengan-penyebab-pdn-down>

Solusi untuk Mengatasi Ransomware:

1. Melakukan pencadangan data secara rutin dan menyimpannya di lokasi yang aman, seperti drive eksternal yang tidak terhubung dengan jaringan, dapat memastikan data tetap tersedia jika terjadi serangan.
2. Memastikan semua sistem dan perangkat lunak diperbarui secara rutin untuk menutup celah keamanan yang dapat dimanfaatkan oleh peretas.
3. Memasang program antivirus dan anti-malware yang andal untuk mendeteksi dan mencegah infeksi ransomware.
4. Memberikan pelatihan kepada karyawan tentang cara mengenali email phishing dan praktik keamanan siber lainnya untuk mencegah infeksi awal.
5. Data 204 Juta DPT Milik KPU Diduga Bocor dan Dijual Hacker Senilai Rp 1,2 Miliar

Pada November 2023, situs resmi Komisi Pemilihan Umum (KPU) dilaporkan diretas, mengakibatkan kebocoran data sensitif sekitar 204 juta pemilih yang kemudian dijual secara daring oleh seorang peretas dengan nama samaran "Jimbo." Data yang bocor mencakup NIK, nomor KK, nama lengkap, alamat, tempat dan tanggal lahir, serta informasi pribadi lainnya, yang ditawarkan seharga 74.000 dolar AS atau sekitar Rp 1,2 miliar. Kebocoran ini menimbulkan kekhawatiran serius terkait potensi penyalahgunaan data pribadi dan merusak kepercayaan publik terhadap proses pemilu. Dalam menanggapi insiden ini, KPU bekerja sama dengan BSSN, Kominfo, Polri, dan BIN untuk menyelidiki sumber kebocoran serta meningkatkan keamanan sistem. Ketua KPU, Hasyim Asy'ari, menegaskan bahwa data pemilih juga didistribusikan ke partai politik dan Bawaslu, membuka kemungkinan kebocoran dari pihak lain. Berbagai pihak mendesak KPU untuk bertanggung jawab, memperbaiki keamanan data, dan melakukan audit forensik untuk mencegah kejadian serupa di masa depan.

Sumber:

1. Tempo.co. (2023). Data 204 Juta Pemilih Diduga Bocor dan Dijual Online. Diakses dari [tempo.co](https://www.tempo.co).
2. Kompas.id. (2023). KPU dan Keamanan Data Pemilih: Sebuah Tinjauan. Diakses dari [kompas.id](https://www.kompas.id).
3. Liputan6.com. (2023). Kebocoran Data KPU: Kronologi dan Reaksi Pemerintah. Diakses dari [liputan6.com](https://www.liputan6.com).

Solusi:

1. Melakukan audit keamanan menyeluruh (penetration testing dan vulnerability assessment) untuk mengidentifikasi celah dalam sistem dan infrastruktur yang memungkinkan peretasan.
2. Terapkan enkripsi data baik saat data disimpan (at rest) maupun saat data dikirimkan (in transit). Gunakan enkripsi dengan standar industri seperti AES-256 bertujuan untuk elindungi data sensitif, seperti data pemilih, agar tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang meskipun data tersebut bocor.
3. Terapkan autentikasi multifaktor (MFA) untuk semua akses ke sistem yang menyimpan atau mengelola data sensitif agar menambahkan lapisan keamanan ekstra agar peretas tidak dapat mengakses sistem meski berhasil mendapatkan kredensial pengguna.
4. Implementasikan sistem pemantauan ancaman (SIEM – Security Information and Event Management) untuk memantau dan menganalisis lalu lintas jaringan dan aktivitas sistem secara real-time bertujuan mendeteksi dan merespons ancaman secara cepat sebelum menyebabkan kerusakan lebih lanjut.
5. Gunakan firewall canggih dan sistem deteksi/pencegahan intrusi (IDS/IPS) untuk melindungi jaringan dari serangan eksternal mencegah akses tidak sah dan memblokir aktivitas mencurigakan yang dapat mengarah pada peretasan.
6. Secara rutin lakukan pembaruan perangkat lunak dan pemasangan patch keamanan pada semua perangkat keras dan perangkat lunak yang digunakan di sistem KPU bertujuan menutup kerentanannya dengan memperbarui sistem dan aplikasi untuk mencegah eksploitasi celah keamanan yang sudah diketahui.
7. Pisahkan data sensitif (seperti data pemilih) dari data non-sensitif dan simpan di server terpisah dengan pengamanan lebih ketat bertujuan mengurangi risiko kebocoran data dalam jumlah besar dengan membatasi akses ke data sensitif.
8. Terapkan strategi backup data yang baik dan pastikan backup data disimpan di lokasi yang terpisah dan aman untuk memastikan data dapat dipulihkan dengan cepat jika terjadi peretasan atau kerusakan sistem.
9. Siapkan tim respons insiden (incident response team) dan prosedur yang jelas untuk menangani kebocoran atau peretasan data dengan cepat bertujuan memastikan bahwa setelah terjadi insiden, langkah-langkah mitigasi dilakukan segera untuk mencegah kerusakan lebih lanjut.
10. Pertimbangkan untuk menggunakan teknologi blockchain untuk mencatat data pemilih secara transparan dan aman, karena sifatnya yang tidak bisa diubah dan terenkripsi bertujuan menjamin integritas data pemilih dan mencegah perubahan atau manipulasi data.
11. Kembangkan dan terapkan kebijakan keamanan TI yang ketat, termasuk kontrol akses berbasis peran (role-based access control/RBAC), serta pelatihan dan kesadaran tentang keamanan data bagi semua pengguna bertujuan membatasi akses ke data hanya untuk pihak yang berwenang dan memastikan bahwa semua pihak yang terlibat dalam pengelolaan data memahami pentingnya perlindungan data