Nama: Miftakhur Rizky
Npm:23753064

# ANALISIS KASUS SERANGAN RANSOMWARE PUSAT DATA NASIONAL DAN KEBOCORAN DATA TOKOPEDIA

## 1. Analisis Kasus Serangan Ransomware PDNS 2024

### a. **Karakteristik Cybercrime**

Pada tanggal 20 Juni 2024, Pusat Data Nasional Sementara (PDNS) Surabaya diserang oleh perangkat lunak ransomware yang diidentifikasi sebagai Brain Cipher, sebuah varian baru dari LockBit 3.0. Insiden ini menyebabkan beberapa layanan publik, termasuk layanan imigrasi, terganggu.

Berdasarkan laporan resmi dari BSSN dan Kominfo, penonaktifan fitur Windows Defender terjadi mulai 17 Juni 2024, sekitar pukul 23.15 WIB, yang kemudian membuka kesempatan bagi pelaku untuk melakukan instalasi file jahat, menghapus sistem file, dan mengganggu service penting pada server PDNS. Ruang lingkup kejahatan ini sangat luas karena PDNS melayani tenant instansi pemerintah pusat dan daerah, termasuk layanan keimigrasian yang berdampak langsung kepada masyarakat pengguna jasa keimigrasian. Sifat kejahatan ini bukan hanya akses ilegal, tetapi juga enkripsi data yang mengunci sistem (lock-out), tindakan destructive terhadap sistem file, dan permintaan tebusan.

Pelaku menyerang dengan modus yang sistematis: menonaktifkan proteksi (antivirus / Windows Defender), mengambil alih akses, menyisipkan malware, lalu mengenkripsi data dan layanan penting. Kerugian yang muncul mencakup kerugian operasional yang besar (lumpuhnya layanan publik), biaya pemulihan dan restorasi sistem, gangguan sosial (misalnya antrean panjang di bandara, penundaan layanan), potensi kebocoran data, dan kerugian reputasi pemerintah sebagai penyelenggara data nasional.

b. **Jenis Cybercrime**

Jenis aktivitas yang terjadi dalam kasus PDNS adalah serangan ransomware, yaitu jenis malware yang mengenkripsi data dan sistem, sehingga korban kehilangan akses kecuali membayar tebusan. Motif utama adalah finansial — pelaku menuntut tebusan; pemerintah menyatakan tidak akan memenuhi tuntutan tersebut. Sasaran kejahatannya adalah infrastruktur digital pemerintahan, khususnya server pusat data nasional (PDNS), tenant-tenant instansi pemerintah, dan layanan masyarakat melalui sistem imigrasi serta layanan pemerintahan lainnya yang bergantung pada PDNS.

c. **Hukuman**

Secara hukum, tindakan seperti ini dapat dijerat dengan Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, jo. UU No. 19 Tahun 2016, khususnya pasal yang mengatur akses ilegal, perusakan sistem elektronik, dan gangguan sistem. Contohnya Pasal 30 UU ITE mengenai akses tanpa hak ke sistem elektronik, Pasal 32 mengenai perubahan atau perusakan informasi elektronik, serta kemungkinan pasal pemerasan jika tebusan diminta. UU-nya tidak secara spesifik menyebut "ransomware", tetapi hukum sudah mencakup jenis aktivitas tersebut. (Peraturan UU ITE; Kominfo / BSSN siaran pers)

d. **Solusi**

Solusi pencegahan dan penanganan insiden ransomware PDNS harus mencakup aspek teknis, regulatif, dan edukatif. Dari aspek teknis, perlu diterapkan sistem keamanan berlapis (multi-layered security), enkripsi data yang kuat, patching dan update sistem rutin, pemantauan (monitoring) terus-menerus, backup data yang andal dan disaster recovery plan yang diuji secara berkala. Dari aspek regulatif, pemerintah perlu menetapkan standar keamanan minimum bagi instansi yang mengelola data publik kritis, memperjelas regulasi terkait tanggung jawab penyelenggaraan data dan keamanan siber, memperkuat kolaborasi antara BSSN, Kominfo, Polri (Cyber Crime), dan lembaga terkait. Dari aspek edukatif, pelatihan dan peningkatan literasi

keamanan siber bagi aparatur pemerintah sangat penting, begitu juga kesadaran masyarakat mengenai risiko kejahatan siber dan bagaimana melindungi data pribadi serta bersikap saat layanan publik terganggu.

e. **Ruang Lingkup**

Kasus ini termasuk dalam ruang lingkup pemerintahan/organisasi negara karena targetnya adalah sistem dan data milik pemerintah. Namun dampaknya tidak hanya internal pemerintahan: masyarakat pengguna layanan publik sangat terdampak, dan beberapa aspek seperti layanan keimigrasian melibatkan interaksi internasional. Dengan demikian, meskipun kasus dilokalkan di Surabaya / Indonesia, implikasinya berskala nasional dan sedikit menyentuh aspek internasional.

**2. Analisis Kasus Kebocoran Data Tokopedia 2020**

a. **Karakteristik Cybercrime**

Pada kisaran Mei tahun 2020, platform e-commerce Tokopedia menghadapi kasus kebocoran data yang melibatkan hingga **91 juta akun pengguna**. Menurut laporan CNN Indonesia, jumlah data yang bocor mencakup nama pengguna, alamat email, nomor ponsel, serta hash dari password pengguna. Dalam prosesnya, data tersebut kemudian dijual di forum gelap daring (dark web) oleh pelaku — yang dalam laporan disebut sebagai pengguna bernama *Whysodank*. Ruang lingkup kejahatan ini adalah perusahaan swasta dengan basis pengguna nasional yang sangat besar. Sifat kejahatan adalah pencurian data pribadi (*data breach*), akses ilegal ke basis data, dan penyebaran data pribadi. Pelaku tidak diketahui secara publik seluruh identitasnya, tetapi jelas ada unsur eksploitasi sistem keamanan dan peretasan. Kerugian yang timbul termasuk hilangnya privasi, potensi penyalahgunaan identitas, risiko penipuan digital, selain kerugian reputasi bagi perusahaan dan kepercayaan publik.b. **Jenis** Cybercrime

Jenis aktivitas yang terjadi dalam kasus PDNS adalah serangan ransomware, yaitu jenis malware yang mengenkripsi data dan sistem, sehingga korban kehilangan akses kecuali membayar tebusan. Motif utama adalah finansial — pelaku menuntut tebusan; pemerintah menyatakan tidak akan memenuhi tuntutan tersebut. Sasaran kejahatannya adalah infrastruktur digital pemerintahan,

khususnya server pusat data nasional (PDNS), tenant-tenant instansi pemerintah, dan layanan masyarakat melalui sistem imigrasi serta layanan pemerintahan lainnya yang bergantung pada PDNS.

b. **Jenis Cybercrime**

Jenis aktivitas adalah data breach / data leak — pelaku memperoleh akses tanpa izin ke data pengguna, mengambil data tersebut, dan kemudian menjual atau menyebarkannya. Motif kegiatan yang paling tampak adalah finansial, karena data dijual di forum gelap. Sasaran kejahatannya adalah data pribadi (nama, email, nomor telepon, hash password, dan atribut pengguna lain yang ada dalam basis data) pengguna Tokopedia.

c. **Hukuman**

Secara legal, kebocoran data seperti ini dapat dihadapkan pada ketentuan dalam UU ITE No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016. Pasal 26 UU ITE mengatur persetujuan atas penggunaan data pribadi; jika data digunakan tanpa persetujuan, itu dapat menjadi pelanggaran. Pasal 30 (akses ilegal) dan Pasal 32 (pengubahan, penghapusan, transfer data), sangat relevan. Kemudian, sejak disahkannya Undang-Undang Perlindungan Data Pribadi (UU PDP) pada tahun 2022, ada kerangka hukum tambahan yang menegaskan kewajiban perusahaan dalam melindungi data pribadi, hak subjek data, dan sanksi administratif / pidana bila terjadi pelanggaran atau kelalaian. Jurnal hukum Indonesia juga menyebut bahwa Tokopedia dapat dipertanggungjawabkan secara pidana atas kelalaian sistem keamanan data pribadi pengguna.e. Ruang Lingkup

d. **Solusi**

Solusi terhadap kebocoran data Tokopedia harus dilakukan dengan pendekatan holistik. Dari sisi teknis, perlu diperkuat penggunaan enkripsi data, sistem hashing + salt yang kuat untuk password, autentikasi ganda (multi-factor authentication), audit keamanan secara rutin (vulnerability assessment, penetration testing), serta pemantauan keamanan jaringan dan akses data. Dari sisi regulatif / kebijakan, perusahaan harus patuh pada UU PDP, UU ITE, dan regulasi lainnya; harus ada prosedur respons insiden dan kewajiban pemberitahuan kepada pengguna jika terjadi kebocoran. Dari sisi edukasi, penting untuk memberikan literasi digital kepada pengguna

tentang pentingnya keamanan data, penggunaan kata sandi unik, waspada phishing, dan bagaimana melaporkan jika data pribadi mereka disalahgunakan**.**

e. **Ruang Lingkup**

Kasus ini terjadi pada ruang lingkup organisasi / perusahaan swasta (Tokopedia). Namun dampaknya meluas ke individu (pengguna), dan memiliki implikasi nasional karena jumlah pengguna sangat besar, serta internasional dalam aspek publikasi data di forum internasional (dark web), yang bisa diakses dari negara lain.

**3. Tabel Perbandingan Antar Kasus**

Perbandingan antara kasus PDNS 2024 dan Tokopedia 2020 memperlihatkan bahwa meskipun keduanya sama-sama bermotif finansial, karakteristik, ruang lingkup, dan dampaknya sangat berbeda. Serangan ransomware terhadap PDNS menargetkan infrastruktur negara sehingga mengakibatkan kelumpuhan layanan publik vital dan kerugian besar pada tingkat nasional. Sementara itu, kebocoran data Tokopedia lebih terfokus pada data pribadi pengguna dengan konsekuensi berupa kerugian privasi, reputasi perusahaan, serta risiko penyalahgunaan identitas. Perbedaan ini menegaskan pentingnya penguatan keamanan siber baik di sektor publik maupun swasta, melalui penerapan teknologi, regulasi yang jelas, serta peningkatan literasi digital masyarakat.

| **Aspek** | **Kasus PDNS 2024 (Ransomware)** | **Kasus Tokopedia 2020 (Data Breach)** |
|---|---|---|
| Ruang Lingkup | Pemerintahan / organisasi negara; layanan publik nasional & beberapa aspek internasional | Perusahaan swasta; pengguna individu; nasional & dampak ke forum internasional |
| Sifat Kejahatan | Ransomware: enkripsi, pemerasan, layanan publik terlumpuhkan | Kebocoran data: pencurian, penyebaran data pribadi |
| Pelaku | Kelompok peretas internasional (Brain Cipher / LockBit 3.0) | Pelaku anonim / grup hacker (misalnya Whysodank) |

| Aspek | Kasus PDNS 2024 (Ransomware) | Kasus Tokopedia 2020 (Data Breach) |
|---|---|---|
| Modus Kejahatan | Penonaktifan proteksi, instalasi malware, penghapusan file sistem, penguncian data & layanan | Akses ilegal ke database, pengambilan data, penjualan atau penyebaran data |
| Motif | Finansial (tebusan) | Finansial (jual data) |
| Sasaran | Infrastruktur negara (server PDNS, layanan imigrasi dan publik) | Data pribadi pengguna Tokopedia |
| Kerugian | Gangguan besar layanan publik, kerugian reputasi, potensi kebocoran data, biaya pemulihan besar | Kerugian privasi, reputasi perusahaan, potensi penyalahgunaan identitas, risiko finansial bagi pengguna |
| Hukum yang Berlaku | UU ITE (Pasal 30, Pasal 32, kemungkinan KUHP untuk pemerasan) | UU ITE (Pasal 26, 30, 32), UU PDP |
| Solusi Utama | Backup & recovery, enkripsi, audit keamanan, regulasi & edukasi | Enkripsi & MFA, audit keamanan reguler, regulasi perlindungan data, literasi pengguna |
| Dampak | Melumpuhkan layanan publik, mengganggu administrasi keimigrasian | Ketidakpercayaan pengguna, potensi kerugian identitas dan penipuan |

Kedua kasus menunjukkan pola yang berbeda namun sama-sama mencerminkan kerentanan sistem digital Indonesia. Serangan PDNS lebih bersifat sabotase dengan tujuan financial gain, sementara kasus Tokopedia lebih pada eksploitasi data untuk diperdagangkan.

**4. Upaya Penanganan dan Pencegahan**

**Penguatan Infrastruktur:** Pemerintah telah mengeluarkan Peraturan Presiden No. 82 Tahun 2022 tentang Keamanan Siber Nasional untuk memperkuat koordinasi antar lembaga. BSSN

sebagai leading sector terus meningkatkan kapasitas monitoring dan respons terhadap ancaman siber.

**Regulasi dan Penegakan Hukum:** Revisi UU ITE dan penyusunan RUU Perlindungan Data Pribadi (yang kini telah menjadi UU PDP) menunjukkan komitmen pemerintah dalam memperkuat payung hukum cybersecurity. Pembentukan unit siber di Kepolisian juga memperkuat kemampuan investigasi.

**Kerja Sama Internasional:** Indonesia aktif dalam kerja sama internasional melalui ASEAN Cybersecurity Coordinating Committee dan berbagai forum multilateral lainnya. Pertukaran informasi threat intelligence dan joint operation menjadi kunci dalam menangani cybercrime lintas batas.

**Edukasi dan Kesadaran Masyarakat:** Program literasi digital dan kampanye kesadaran keamanan siber terus digalakkan. Pelibatan sektor swasta dan akademisi dalam program edukasi menjadi strategi penting untuk menciptakan cyber resilience di tingkat grassroots.