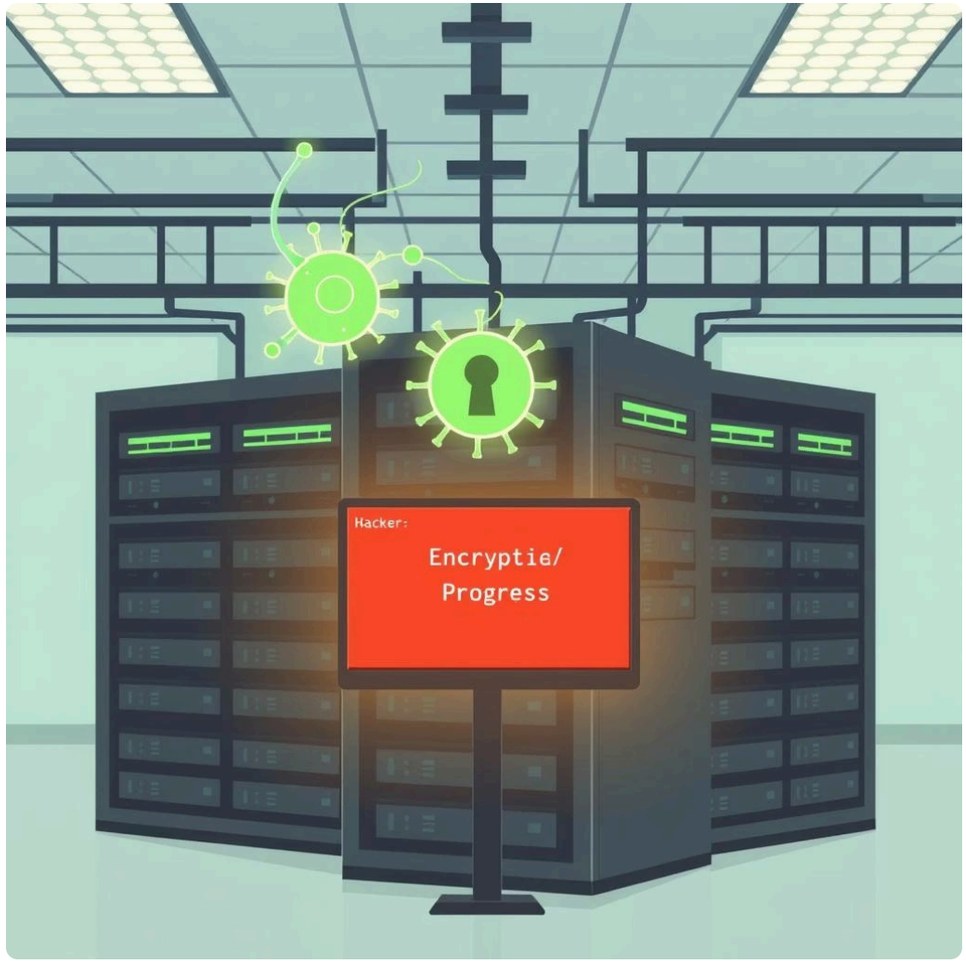
Ancaman Cybercrime di Indonesia

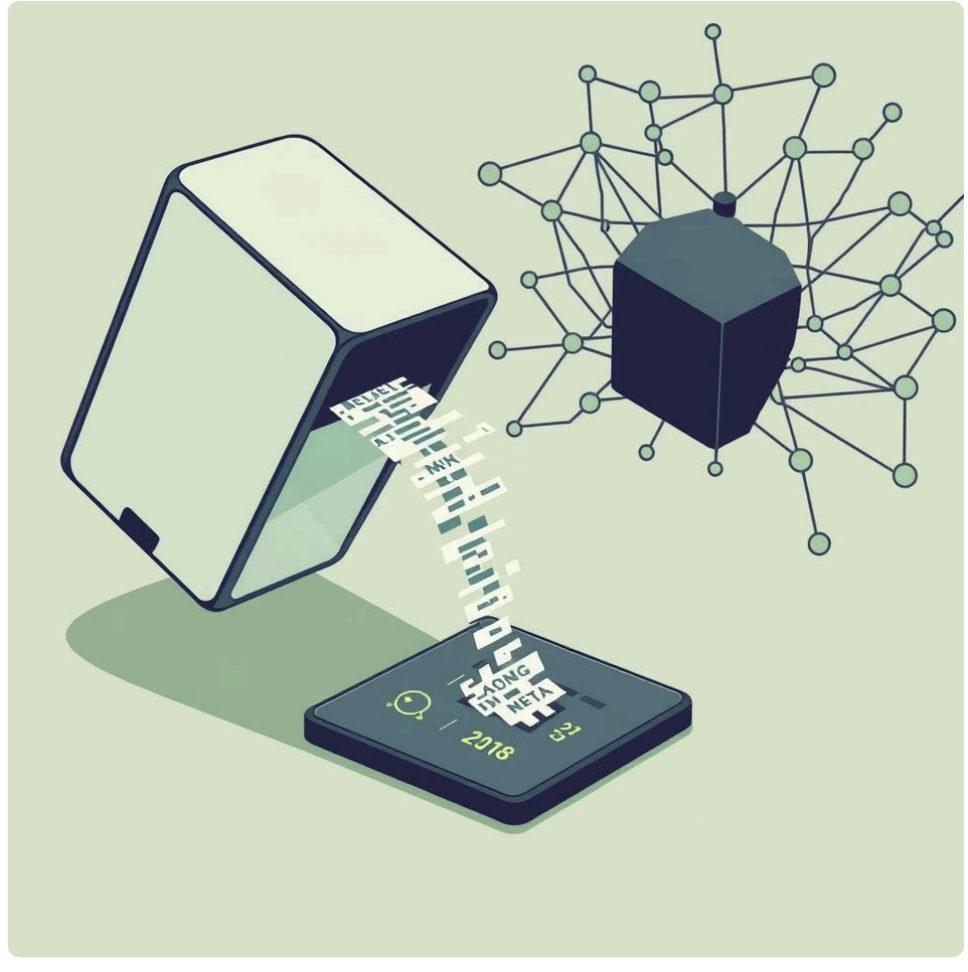
Perkembangan teknologi digital membawa manfaat besar, namun juga menghadirkan ancaman cybercrime. Indonesia, dengan tingkat penggunaan internet yang tinggi, sangat rentan terhadap kejahatan siber yang dapat merugikan finansial, reputasi, bahkan stabilitas negara.

Dua Kasus Cybercrime Besar



Serangan Ransomware PDN 2024

Pusat Data Nasional diserang ransomware, melumpuhkan layanan publik seperti imigrasi dan menimbulkan keresahan luas.



Kebocoran Data Tokopedia 2020

91 juta data pengguna Tokopedia bocor dan dijual di forum gelap, menunjukkan lemahnya perlindungan data pribadi.

Rumusan Masalah

1 **Apa itu Cybercrime?**

Definisi dan bentuk cybercrime di Indonesia.

2 **Analisis Kasus**

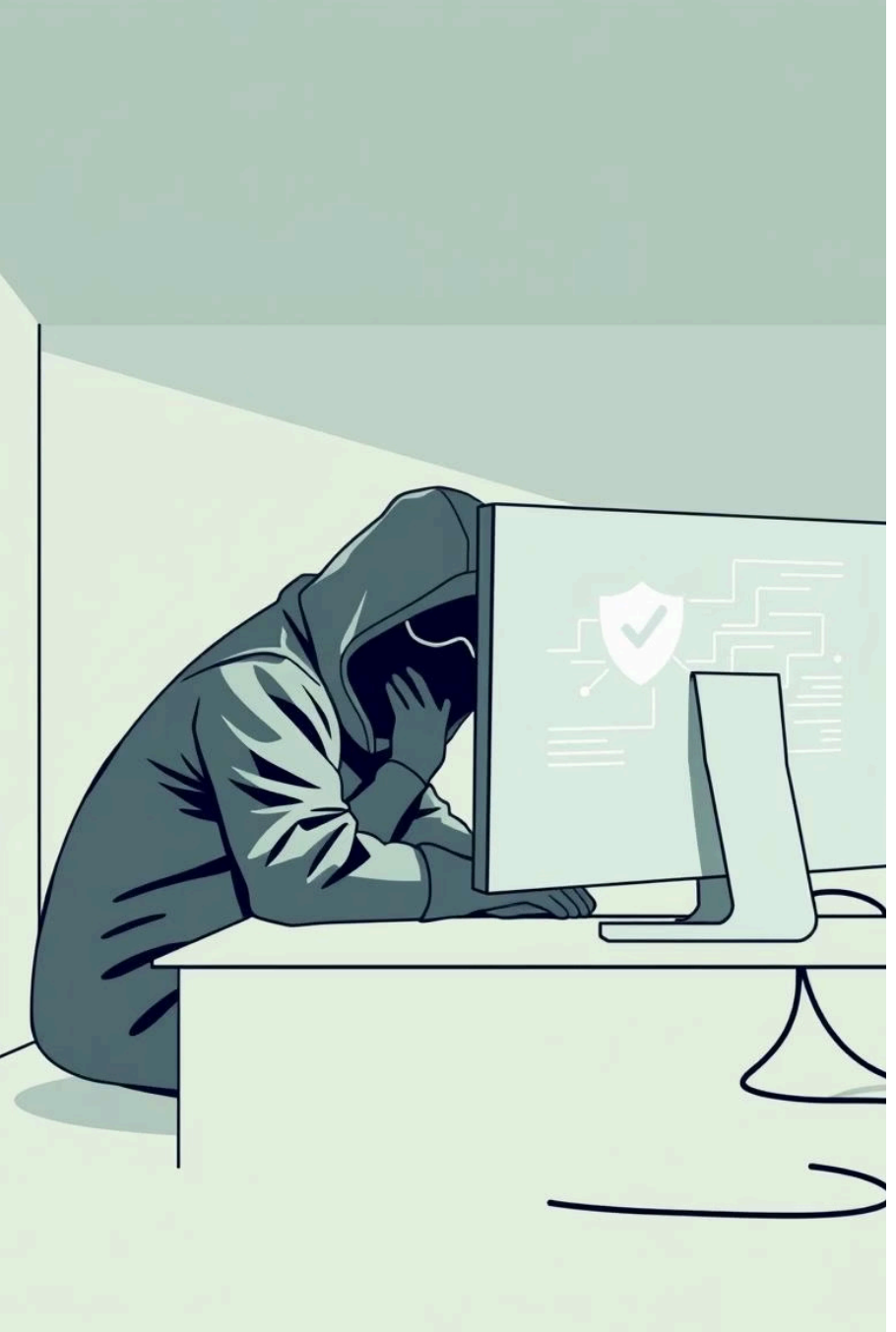
Karakteristik, jenis, dan dampak serangan ransomware PDN 2024 dan kebocoran data Tokopedia 2020.

3 **Penerapan Hukum**

Bagaimana UU ITE diterapkan pada kasus cybercrime di Indonesia?

4 **Solusi Pencegahan**

Langkah-langkah untuk mencegah terulangnya kasus serupa di masa depan.



Tinjauan Teoritis Cybercrime

Cybercrime adalah perbuatan melawan hukum menggunakan teknologi komputer dan internet. Diatur dalam UU ITE, kejahatan ini meliputi hacking, malware, penipuan online, pencurian identitas, hingga konten ilegal.

Target Komputer

Hacking, Malware

Alat Komputer

Penipuan Online, Pencurian Identitas

Konten Ilegal

Pornografi, Ujaran Kebencian

Serangan Ransomware PDN 2024

Karakteristik & Dampak

PDNS diserang varian LockBit 3.0, Brain Cipher, pada 20 Juni 2024. Penonaktifan Windows Defender membuka celah. Dampaknya meliputi kelumpuhan layanan publik, kerugian operasional, dan gangguan sosial.

Jenis & Motif

Serangan ransomware dengan motif finansial, menargetkan infrastruktur digital pemerintahan. Pelaku menuntut tebusan.

Tindakan ini dapat dijerat UU ITE Pasal 30 (akses ilegal) dan Pasal 32 (perusakan sistem elektronik).

Solusi Pencegahan Ransomware PDN

Teknis

Sistem keamanan berlapis, enkripsi data, patching rutin, monitoring, backup data, dan disaster recovery plan.

Regulatif

Standar keamanan minimum, regulasi tanggung jawab data, kolaborasi antar lembaga (BSSN, Kominfo, Polri).

Edukasi

Pelatihan siber bagi aparatur pemerintah dan peningkatan kesadaran masyarakat.

Kebocoran Data Tokopedia 2020

Karakteristik & Dampak

91 juta akun pengguna Tokopedia bocor, termasuk nama, email, nomor ponsel, dan hash password. Data dijual di dark web. Kerugian meliputi hilangnya privasi, potensi penyalahgunaan identitas, dan reputasi perusahaan.

Jenis & Motif

Data breach/leak dengan motif finansial, menargetkan data pribadi pengguna Tokopedia.

Dapat dijerat UU ITE Pasal 26, 30, 32, serta UU Perlindungan Data Pribadi (UU PDP).

Solusi Pencegahan Kebocoran Data Tokopedia

Teknis

Enkripsi data, hashing + salt, MFA, audit keamanan rutin, pemantauan jaringan.

Regulatif

Kepatuhan UU PDP dan UU ITE, prosedur respons insiden, kewajiban pemberitahuan kebocoran.

Edukasi

Literasi digital bagi pengguna tentang keamanan data, kata sandi unik, dan waspada phishing.

Perbandingan Kasus

Ruang Lingkup	Pemerintahan, layanan publik nasional	Perusahaan swasta, pengguna individu
Sifat Kejahatan	Ransomware, enkripsi, pemerasan	Pencurian, penyebaran data pribadi
Motif	Finansial (tebusan)	Finansial (jual data)
Sasaran	Infrastruktur negara	Data pribadi pengguna

Kedua kasus menunjukkan kerentanan sistem digital Indonesia, dengan pola dan dampak yang berbeda namun sama-sama merugikan.

Kesimpulan & Saran

Penguatan Infrastruktur

Penerapan standar keamanan berlapis, pembaruan sistem rutin, dan mekanisme pemulihan data yang andal.

Penegakan Regulasi

Penerapan tegas UU ITE dan UU PDP, serta pengawasan kepatuhan hukum.

Peningkatan Literasi Digital

Edukasi masyarakat tentang perlindungan data pribadi dan modus kejahatan siber.