**3 Kasus data bocor**

*Pada tanggal 20 Juni 2024, Indonesia digemparkan dengan insiden kebocoran data yang melibatkan Pusat Data Nasional Sementara (PDNS).*

**Kerahasiaan (Confidentiality):** Kelemahan dalam pengelolaan keamanan siber, seperti yang disebutkan oleh Pratama Persadha, menunjukkan bahwa data pemerintah Indonesia yang bersifat "open source" mempermudah akses tanpa izin. Hal ini menunjukkan kurangnya kontrol akses yang memadai, seperti enkripsi yang kuat atau autentikasi multi-faktor.

**Integritas (Integrity):** Serangan ransomware ini tidak hanya mencuri data, tetapi juga menghapus beberapa filesystem penting dan menanamkan file malicious. Hal ini menunjukkan pelanggaran integritas karena data penting diubah atau dihancurkan.

**Ketersediaan (Availability):** Serangan ini menyebabkan lebih dari 210 instansi pemerintah mengalami down pada layanan publik, terutama di sektor imigrasi. Hal ini menunjukkan pelanggaran ketersediaan karena sistem informasi tidak dapat diakses untuk waktu yang signifikan.

**Masalah Utama:** Availability. Dampak langsung dari gangguan layanan publik memiliki konsekuensi luas bagi masyarakat dan pemerintahan, dengan pemulihan yang memakan waktu lama (tahap recovery stage 1 dan 2).

*Kebocoran Data Pribadi Warga Jabar, Pemprov Jabar Disarankan Melakukan Audit Investigatif*

**Kerahasiaan (Confidentiality):** Pemprov Jabar membantah bahwa data berasal dari sistem mereka, dengan menyatakan bahwa tidak ada pelanggaran keamanan setelah penelusuran oleh Diskominfo dan tim Cybercrime Polda Jabar, keraguan publik tetap ada karena reputasi DigitalGhostt sebagai pelaku aktif di forum dark web untuk jual beli data hasil peretasan.

**Integritas (Integrity):** Sekretaris Daerah Jabar, Herman Suryatman, menyatakan bahwa data yang diklaim bocor tidak sesuai dengan data asli di sistem Pemprov Jabar (misalnya, NIK, usia, dan alamat tidak cocok). Hal ini menunjukkan bahwa jika kebocoran benar terjadi, data tersebut mungkin telah dimanipulasi atau berasal dari sumber lain, sehingga integritasnya dipertanyakan.

**Ketersediaan (Availability):** Pemprov Jabar menyatakan bahwa sistem mereka tetap beroperasi normal, dengan tim keamanan siber yang memantau 24 jam dan tidak mendeteksi pelanggaran. Namun, pernyataan ini dipertanyakan oleh praktisi seperti Budi Rahardjo dari ITB, yang menyebut kemungkinan besar klaim kebocoran benar adanya, meskipun perlu verifikasi lebih lanjut.

**Masalah Utama:** Confidentiality. Fokus utama adalah potensi paparan data pribadi warga, yang dapat menyebabkan penyalahgunaan seperti pencurian identitas, terutama karena data sensitif seperti NIK sangat berisiko jika bocor.

*Kebocoran data yang melibatkan sekitar 419.000 pelanggan Louis Vuitton di Hong Kong, sebagaimana dilaporkan pada Juli 2025, menyoroti kerentanan keamanan siber di perusahaan mewah global.*

**Kerahasiaan (Confidentiality):** Kebocoran data ini melibatkan informasi sensitif seperti nama, nomor paspor, alamat, alamat email, nomor telepon, riwayat pembelian, dan preferensi produk dari sekitar 419.000 pelanggan Louis Vuitton di Hong Kong. Hal ini menunjukkan pelanggaran serius terhadap kerahasiaan karena data pribadi pelanggan diakses oleh pihak yang tidak berwenang.

**Integritas (Integrity):** Penundaan dalam mendeteksi dampak kebocoran (dari 13 Juni hingga 2 Juli) dan melaporkannya ke regulator (17 Juli) menunjukkan potensi kelemahan dalam mekanisme pemantauan dan respons, yang dapat memengaruhi kemampuan perusahaan untuk menjaga integritas sistem secara keseluruhan.

**Ketersediaan (Availability):**

Dokumen tidak menyebutkan gangguan langsung pada layanan pelanggan atau sistem operasional Louis Vuitton akibat kebocoran ini, sehingga dampak terhadap ketersediaan tampaknya minimal. Namun, insiden ini dapat memengaruhi kepercayaan pelanggan, yang berpotensi mengurangi interaksi mereka dengan platform digital Louis Vuitton di masa depan.

**Masalah Utama:** Confidentiality. Paparan data pribadi pelanggan adalah isu utama, dengan potensi konsekuensi seperti penyalahgunaan identitas dan kerusakan reputasi merek.