Profil Risiko Siber

Sistem Pembayaran

www.bssn.go.id

Latar Belakang

Data secara global yang rilis oleh Checkpoint dan Finansial Services Information Sharing And Analysis Centre (FSISAC) selama tahun 2022 sampai dengan 2023 serangan siber terhadap sektor keuangan meningkat sampai 9%. Dalam skala nasional data BSSN menunjukkan terjadi peningkatan serangan siber yang signifikan disektor keuangan dari tahun 2020 sampai dengan 2022 dari 1.551 serangan menjadi 1.130.681 pertahun.

BSSN bersama regulator, asosiasi, dan industri sistem pembayaran berupaya mengidentifikasi ancaman, kerentanan, dan prioritas peringkat risiko. Disamping itu, juga memberikan rekomendasi penerapan keamanan guna mencegah dan mengatasi insiden siber pada industri sistem pembayaran.
Hal tersebut dikemas dala buku profil risiko siber sistem pembayaran

Tujuan

Untuk memberikan gambaran prioritas
risiko siber Sistem Pembayaran pada platform Penyedia Jasa Pembayaran atau Penyelenggara Infrastruktur Sistem Pembayaran (PJP/PIP), dan memberikan langkah rekomendasi pencegahan (preventif) - peringanan (mitigation) atas dampak risiko siber yang dapat di timbulkan.

Manfaat

- Menjadi referensi bagi Industri Sistem Pembayaran dalam mengidentifikasi risiko siber di Indonesia yang perlu mendapatkan perhatian.
- Menjadi rekomendasi kepada Industri Sistem Pembayaran di Indonesia dalam meringankan dampak risiko siber yang telah diidentifikasi, khususnya terkait dengan platform PJP/PIP.
- Menjadi referensi bagi pihak terkait (regulator, akademisi, asosiasi, dan pelaku industri pembayaran) dalam mengembangkan platform PJP/PIP

Metodologi

Penyusunan dokumen ini menggunakan metode dengan pendekatan deskriptif kuantitatif. Data primer dikumpulkan menggunakan instrumen berupa katalog risiko, kemudian diolah dan dideskripsikan dengan memperhatikan realitas dan framework penilaian risiko. Tahap selanjutnya dilakukan kategorisasi, penyusunan prioritas terhadap 10 risiko siber, dan rekomendasi mitigasi yang dapat dilakukan organisasi pada industri sistem pembayaran untuk mengurangi risiko-risiko tersebut.

Pencegahan & Peringanan

Rekomendasi yang diberikan menggunakan pendekatan pencegahan (preventif) dan peringanan (mitigation) yang merupakan pendekatan yang saling melengkapi. Upaya pencegahan membantu menahan kemungkinan dapat terjadinya risiko, sedangkan upaya peringanan membantu mengurangi dampak jika risiko benar terjadi.

Top 10 Kategori Profil risiko

1 Kelangkaan Talenta Bidang Keamanan Siber

Kelangkaan kompetensi keamanan siber merujuk pada terbatasnya jumlah sumber daya yang kompetensi dalam
keamanan siber, dibandingkan dengan tingginya kebutuhan pasar.

2 Kerentanan Infrastruktur Informasi Vital

Kerentanan IIV dapat muncul dari lemahnya sistem keamanan siber pada sistem elektronik, kurangnya proteksi yang memadai, kurangnya Business Continuity Planning (BCP), serta adanya risiko serangan siber.

3 Penyalahgunaan Informasi Data Pribadi

Penyalahgunaan data pribadi disebabkan karena faktor lemahnya sistem dan kurangnya pengawasan dari organisasi.

4 Social Engineering

Social engineering dapat menargetkan Industri Sistem Pembayaran melalui lemahnya security awareness SDM.

5 Risiko Penyalahgunaan Telepon Seluler

Risiko pada telepon seluler menyasar pada penyalahgunaan nomor, aplikasi, informasi maupun kredensial yang ada dalamnya oleh orang tidak berhak.

6 Lemahnya Mekanisme Identity Proofing

Kelemahan identity proofing dapat disebabkan oleh rendahnya tingkat keamanan atau kurangnya program peningkatan awareness keamanan siber dalam organisasi atau pada nasabah.

7 Risiko Operasional Pihak Ketiga/Third Party Risk

Risiko pihak ketiga melibatkan pihak eksternal ke
dalam ekosistem, infrastruktur, atau rantai pasok organisasi. Risiko pihak ketiga dapat menyebabkan potensi penyusupan ke jaringan internal, akses illegal hingga kebocoran data organisasi.

8 Kerentanan Software

Kerentanan software dapat menjadi target serangan siber dimana threat actor mengeksploitasi kerentanan dan melakukan eskalasi serangan terhadap sistem.

9 Risiko Perangkat End of Support/End of Life

Resiko perangkat EoS/EoL merupakn tahap kritis dalam siklus hidup perangkat keras atau perangkat lunak di mana produsen atau penyedia tidak lagi memberikan dukungan pemeliharaan dan pembaruan.

10 Malware & Ransomware as a Service

Keberadaan malware dan RaaS dapat menjadi ancaman serius yang dapat menyebabkan gangguan besar dalam proses pembayaran.

Jika ingin mendapatkan e-book Profil Risiko Siber Sistem Pembayaran secara lengkap, Anda dapat mengirimkan email ke alamat tu.d41@bssn.go.id, dengan subjek "Permintaan e-book Profil Risiko Siber SP"