Universitas Indonesia Library >> UI - Skripsi Membership

Manajemen Insiden Siber Pada Industri Pembayaran Berbasis Kartu Di Indonesia = Cyber Incident Management In Payment Card Industry In Indonesia

Bonanza Haggai Rosairo, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=9999920567393&lokasi=lokal

---

Abstrak

Berkembangnya teknologi informasi dan komunikasi di berbagai sektor, termasuk pada Sistem Pembayaran, menjadikan pentingnya upaya terhadap pemenuhan keamanan siber. Pelaku industri pembayaran berbasis kartu, seperti merchants, pemroses, acquirers, penerbit, dan penyedia layanan pembayaran, perlu waspada dengan serangan siber yang selalu berkembang tiap saat dan dapat menjadi Insiden Siber. Terdapat peraturan perundang-undangan dan standar industri yang perlu diterapkan untuk mengantisipasi dan menanggulangi Insiden Siber. Indonesia telah memiliki aturan yang mengatur mekanisme operasional Penyelenggara Sistem Elektronik dalam menanggulangi Insiden Siber. Di lain sisi, asosiasi yang menaungi pelaku industri pembayaran berbasis kartu, yaitu PCI, juga telah memberikan panduan kepada anggotanya terkait penanggulangan insiden siber dengan mengeluarkan PCI DSS. Menarik untuk diteliti perbedaan mekanisme operasional dalam menanggulangi Insiden Siber yang diatur oleh pemerintah dengan yang dibuat oleh asosiasi swasta. Sebelum itu, perlu diteliti dulu apakah Sistem Elektronik yang digunakan dapat termasuk sebagai IIV di Indonesia. Lalu, bagaimana keberlakuan dari standar PCI DSS terhadap pelaku industri pembayaran berbasis kartu di Indonesia. Kemudian yang terakhir, bagaimana kesesuaian dari PCI DSS dengan hukum positif di Indonesia tentang penanggulangan insiden siber untuk mengetahui apakah ada tumpang tindih antara keduanya. Hasil penelitian ini menunjukkan bahwa Sistem Elektronik dalam industri pembayaran berbasis kartu, terutama yang berskala besar, memiliki potensi tinggi untuk dikategorikan sebagai IIV mengingat perannya yang krusial dalam transaksi dan ekonomi nasional. PCI DSS yang secara luas diadopsi sebagai praktik terbaik industri adalah relevan dan sejalan dengan regulasi keamanan siber di Indonesia, meskipun tidak bersifat wajib secara hukum, PCI DSS memberikan pedoman yang komprehensif bagi organisasi dalam melindungi data pemegang kartu. Namun, terdapat perbedaan dalam tingkat detail antara PCI DSS dan hukum positif di Indonesia. Oleh karena itu, untuk memastikan keamanan data yang optimal dan kepatuhan terhadap regulasi, entitas yang memproses data pemegang kartu perlu memenuhi baik persyaratan PCI DSS maupun hukum yang berlaku.

.....The development of information and communication technology in various sectors, including the Payment System, makes it important to fulfill cybersecurity efforts. Payment card industry, such as merchants, processors, acquirers, issuers, and service providers, need to be aware of cyber-attacks that are always developing at any time and can become Cyber Incidents. Indonesia already has rules governing the operational mechanisms of Operators in dealing with Cyber Incidents. The Payment Card Industry (PCI) has also provided guidance to its members regarding cyber incident response by issuing a standard, namely PCI DSS. It is interesting to investigate the differences in operational mechanisms in overcoming Cyber Incidents regulated by the government and those made by private associations. Before that, it is necessary to first investigate whether the Electronic System used can be included as IIV in Indonesia. Then, how is the

applicability of the PCI DSS to PCI in Indonesia. Finally, how is the compatibility of PCI DSS with law in Indonesia regarding cyber incident countermeasures to find out if there is an overlap between the two. The results of this study show that Electronic Systems in the card-based payment industry, especially large-scale ones, have a high potential to be categorized as IIV given their crucial role in transactions and the national economy. PCI DSS, which is widely adopted as an industry best practice, is relevant and in line with Indonesia's cybersecurity regulations. Although not legally mandatory, PCI DSS provides comprehensive guidelines for organizations in protecting cardholder data. However, there are differences in the level of detail between the PCI DSS and the positive law in Indonesia. Therefore, to ensure optimal data security and regulatory compliance, entities that process cardholder data need to meet both the requirements of PCI DSS and the applicable law.