Pelindungan Data Pribadi terhadap Packet Sniffing Attack Melalui Pesan Mengatasnamakan Kurir di Indonesia = Personal Data Protection Against Packet Sniffing Attack through Message on Behalf of Courier in Indonesia.

Nurulazmi, author

Abstrak

Permintaan yang besar akan pelayanan jasa ekspedisi menghadirkan tingginya jumlah titik layanan jasa ekspedisi yang tersedia di Indonesia. Perkembangan permintaan akan pelayanan jasa ekspedisi tersebut kemudian dimanfaatkan oleh pihak yang tidak bertanggung jawab dengan munculnya kasus yang memanfaatkan pemanfaatan teknologi, salah satunya yaitu Packet Sniffing Attack. Penelitian ini akan menganalisis mengenai rumusan masalah atas bagaimana cara Packet Sniffing Attack dapat bekerja hingga pengaruhnya terhadap keamanan sistem informasi. Selain itu, akan menganalisis pula mengenai apakah penyedia layanan jasa ekspedisi dapat dimintakan pertanggungjawaban atas dugaan adanya kebocoran data pribadi. Penelitian ini dilakukan dengan pendekatan yuridis normatif yang melibatkan analisis data sekunder yang mengacu pada norma hukum yang berlaku, seperti peraturan-peraturan dan bahan hukum tertulis, serta bahan pustaka. Hasil analisis dari Penelitian ini menunjukkan bahwa rangkaian langkah dari Packet Sniffing Attack dari pengiriman APK yang akan melakukan penginstalan sniffer hingga pengendusan data informasi akan membahayakan keamanan sistem informasi berupa kerahasiaan, integritas, dan ketersediaan terhadap perangkat fasilitas komunikasi, jaringan perangkat, sampai pada data dan informasi korban. Atas hal tersebut, perbuatan pelaku Packet Sniffing Attack dapat diberlakukan Pasal 30 ayat (2) j.o. Pasal 36 UU ITE sebagaimana telah dicabut oleh Pasal 332 ayat (2) KUHP mengenai pengaksesan komputer dan/ atau sistem elektronik dengan cara apa pun secara tidak sah serta Pasal 31 ayat (1) j.o. ayat (2) j.o. Pasal 36 UU ITE sebagaimana telah dicabut oleh Pasal 258 ayat (1) KUHP mengenai intersepsi/penyadapan. Apabila dapat dibuktikan kebocoran data pada penyedia layanan jasa ekspedisi sehingga pelaku dapat menyebarkan Packet Sniffing Attack, penyedia layanan jasa ekspedisi mempunyai tanggung jawab secara hukum pada Pasal 15 ayat (2) UU ITE dan Pasal 3 ayat (2) PP PSTE mengenai pengoperasian Sistem Elektroniknya yang tidak terselenggara secara andal dan aman.

.....The large demand for expedition services presents a high number of expedition services available in Indonesia. The development of demand for expedition services is then exploited by irresponsible parties with the emergence of cases that utilize the use of technology, one of which is Packet Sniffing. This research will analyze how Packet Sniffing Attack’s mechanism and its effect on information system security. In addition, it will also analyze whether the expedition service provider can be held liable for the alleged leakage of personal data. This research is conducted with a normative juridical approach involving secondary data analysis that refers to applicable legal norms, such as regulations and written legal materials, as well as literary research. This research shows that the series of mechanisms of Packet Sniffing Attack from sending the APK that will install the sniffer to sniffing information data will jeopardize information system security in the form of confidentiality, integrity, and availability of communication facility devices, network devices, to the victim's data and information. For this reason, the actions of the Attackers of Packet Sniffing Attack can be applied Article 30 paragraph (2) j.o. Article 36 of the ITE Law as revoked by Article

332 paragraph (2) of the Criminal Code regarding unauthorized access to computers and/or electronic systems by any means and Article 31 paragraph (1) j.o. paragraph (2) j.o. Article 36 of the ITE Law as revoked by Article 258 paragraph (1) of the Criminal Code regarding interception/tapping. If it can be proven that the data leakage at the expedition service provider so that the perpetrator can spread the Packet Sniffing Attack, the expedition service provider has legal responsibility in Article 15 paragraph (2) of the ITE Law and Article 3 paragraph (2) of the PSTE PP regarding the operation of its Electronic System which is not carried out reliably and safely.