White Paper

Skimming: How To Work And Prevention at Atm (Automatic Teller Machine)

Disusun Oleh :

Nama : Aria Nasbi

Nim : 09011181621011

Dosen Pengampuh: Deris Stiawan. Ph.D

Jurusan Sistem Komputer
Fakultas Ilmu Komputer
Universitas Sriwijaya
2019

Latar Belakang.

Pada tahun 2015 telah terjadi pembobolan mesin ATM (Anjungan Tunai Mandiri) di Bali dengan menggunakan Skimmer, yaitu sebuah alat pencuri data nasabah. Modus operasi para pembobol bank yaitu memasang skrimmer di mulut ATM. Setelah data nasabah didapat, pelaku tinggal memasukkan kedalam kartu ATM nya. Yang nantinya pembobol akan dengan leluasa menguras uang nasabah. Satu skrimmer bisa menyimpan data sampai 2000 kartu dan ironinya skrimmer ternyata dijual bebas disejumlah pertokoan dengan harga Rp 1,5 juta.

Skimming: Bagaimana cara kerjanya ?

Kita harus bisa menghindari kejahatan skimming ini, bagaimana kita bisa tehindar, yaitu dengan mengetahui bagaimana cara kerja dari skimming itu sendiri dan apa saja yang di manfaatkan oleh pelaku dalam menjalankan aksinya.

Skimming adalah mengkloning data dari magnetic stripe yang terdapat pada kartu ATM milik nasabah dengan menggunakan alat yang bernama skimmer. Tetapi seiring perkembangan teknologi informasi yang semakin canggih, metode skimming pun semakin canggih pula, yaitu dengan memanfaatkan teknologi GSM atau WIFI sehingga pelaku dapat beroperasi dan atau mengambil data nasabah dari wilayah yang jauh dari ATM tersebut bahkan dapat dilakukan dari negara lain.

Apa saja alat ataupun komponen yang di manfaatkan oleh pelaku?

1. Skimmer : Dengan terpasangnya Skimmer pada mulut atm maka setiap yang nasabah datang melakukan transaksi dengan memasukan kartunya ke atm, sebelum data tersebut dibaca oleh mesin ATM, alat skimmer pun telah membaca dan merekam data kartu anda untuk selanjutnya akan di-copy-kan ke kartu magnetik lainnya (kartu buatan pelaku). Selanjutnya sang pencuri hanya mengambil alat skimmernya, dan menduplikasi kartu-kartu ATM milik nasabah-nasabah yang sempat mengakses ATM tersebut.

2. Kamera: para pelaku tersebut memasang hidden camera untuk merekam moment saat kita menekan nomor PIN di ATM tersebut. Camera tersebut bentuknya sangat kecil, dan memiliki internal memory yang cukup besar. Saat ini sangat mudah sekali mendapatkan camera seperti ini di Internet. pemasangan Camera untuk merekam aktifitas pemasukan PIN ATM.

3. Skimmer Pad: Dengan menggunakan Skimmer Pad (Pin Pad) palsu ini, setiap tombol yang ditekan akan direkam lengkap dengan waktu penekanan. Dengan demikian, usaha menutupi tangan saat menekan PIN untuk menghindari pencurian pin akan sia-sia belaka. kedua unit ini akan mengirimkan data data yang telah di rekamnya via bluetooth ke main-unitnya yang

teletak 25m (lebih kurang) yang telah di kontrol langsung oleh pelaku.

4. Pembuatan Kartu Magnetik Palsu: Pada saat pelaku telah mengambil kembali skimmer & camera miliknya, dia sudah mendapatkan data-data kartu kita lengkap dengan nomor PIN. Selanjutnya, sang pelaku tinggal membuat kartu magnetik baru dengan data-data kartu kita didalamnya.

Bagaimana cara menghindari ancaman ini ?

1. Selalu jaga kerahasiaan PIN

2. Perhatikan kondisi fisik dari ATM beserta keliling dan sekitarnya, jika terdapat yang mencurigakan segera lapor ke yang berwajib.

3. Segera lapor ke pihak bank atau segera blokir kartu atm jika terdapat transaksi yang mencurigakan.

4. Cari lokasi yang relatif aman, hindari lokasi-lokasi yang berada di tempat sepi., karena kondisi-kondisi yang sepi ini para pelaku lebih leluasa untuk melakukan pemasangan alat alt skimming.

5. jangan mudah percaya dan menerima dengan bantuan orang lain di sekitar ATM.

Untuk landasan hukum pada masalah skimming ini adalah sebagaimana diatur dalam pasal 30 ayat 2Daftar Pustaka Undang-undang Nomor 19 tahun 2016 tentang perubahan atas Undang-undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik atau dikenal dengan Undang-undang ITE., Lebih lengkap pasal 30 ayat 2 Undangundang ITE. Masih banyak landasan hukum yang lain.

Setelah kita mengetahui bagaimana skimming ini bekerja serta alat-alat yang mungkin akan berada di dekat kita, marilah kita lebih berhati-hati dalam menjaga ATM kita, dan jangan biarkan Skimming terjadi pada kita. Dan selanjutnya walaupun kita telah mengetahui proses dari skimming ini beserta komponen komponennya, jangan pernah berpikir untuk melakukannya, karena banyak sekali pasal-pasal yang akan menjerat kasus skimming ini.