SKIMMING, CARA KERJA DAN PENCEGAHAN PADA ATM

Mugiatno Sumbodo[1],
Mugatnos@gmail.com[1]
Jafar Octo Fernas[2]
octojafar@gmail.com[2]
Program Studi Sistem Informasi
Universitas Persada Indonesia Y.A.I

ABSTRAK

Kejahatan *cyber crime* dilakukan dengan beberapa teknik, diantaranya adalah *Skimming*. *Skimming* adalah mengkloning data dari *magnetic stripe* yang terdapat pada kartu ATM milik nasabahakan 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. Untuk pencegahan *skimmimg* , nasabah diharapkan dapat menjaga PIN secara rahasia, melihat kondisi ATM sebelum melakukan transaksi dan jangan percaya kepada orang yang menawarkan kemudahan.

Keyword : *cyber crime*, *skimming*, *magnetic stripe*, ATM, PIN, *WIFI*

ABSTRAK

Cyber crime is done with several techniques, including Skimming. Skimming is to clone data from the magnetic stripe contained on the customer's ATM card but as information technology develops more and more sophisticated, the skimming method is also increasingly sophisticated, namely by utilizing GSM or WIFI technology so that actors can operate and or retrieve customer data from distant areas from the ATM can even be done from other countries. To prevent skimmimg, customers are expected to keep their PIN confidentially, see the condition of the ATM before making a transaction and do not trust anyone who offers convenience.

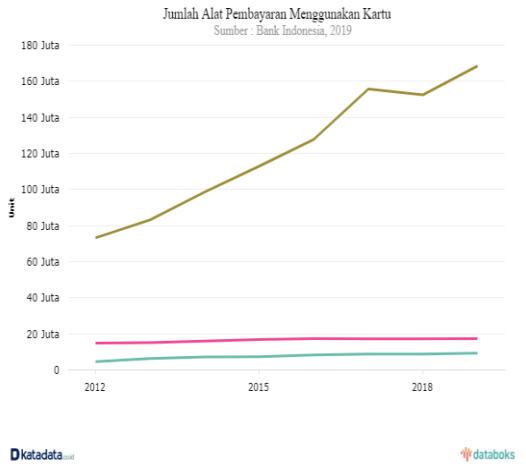
Keyword : *cyber crime*, *skimming*, *magnetic stripe*, ATM, PIN, *WIFI*

1. PENDAHULUAN

Dengan kemajuan Teknologi Informasi yang sangat berkembang, sehingga semua kebutuhan sehari sudah terganti dengan uang digital. Dengan semakin banyak mesin ATM (Anjungan Tunai Mandiri) yang berada disetiap sudut ruang publik seperti di Indomaret, Alfamart dan pojok ruang terbuka dibuatkan ATM center.

Menurut data dari Bank Indonesia (2019) menyatakan kartu debit yang

mengalami pertumbuhan dibandingkan Alat Pembayaran Menggunakan Kartu (APMK) lainnya. Tercatat, jumlah kartu ATM dan kartu kredit malah mengalami penurunan. Hingga Agustus 2019 jumlah kartu debit naik 10,39% dari 152,6 juta unit pada Agustus 2018 menjadi 168,5 juta unit. Sementara jumlah kartu Kredit mengalami penurunan 0,13% dari 17,3 juta menjadi 17,28 juta dan kartu ATM turun 4,91% dari 9,4 juta menjadi 8,9 juta. Sebenarnya, pada tahun lalu jumlah kartu debit sempat mengalami penurunan sebesar 2% menjadi 152,5 juta dari 2017 yang sebesar 155,7 juta unit. Adapun kartu Kredit meningkat 0,18% menjadi 17,3 juta dan kartu ATM meningkat 0,36% menjadi 8,8 juta unit.



Sumber : Bank Indonesia, 2019

Berdasarkan berita CNN Indonesia (2019), Pada bulan September 2019 ada laporan dari Bank Rakyat Indonesia mengenai banyak nasabah kehilangan uang. Nasabah kehilangan uangnya berasala dari ATM. ATM yang digunakan kemungkinan masih magnetik artinya kalau sudah ada chip pun masih gabungan belum 100 persen chip. Logikanya itu kemungkinan besar magnetik. Sehingga bisa dijadikan sumber skimming.

Kejahatan dengan metode *skimming* ini sebenarnya sudah sejak lama dilakukan oleh pelaku kejahatan dibidang perbankan, teknik pembobolan kartu ATM nasabah melalui teknik *skimming* pertama kali teridentifikasi pada 2009 lalu di ATM Citibank, Woodland Hills, California. Teknik skimming dilakukan dengan cara menggunakan alat yang ditempelkan pada slot mesin ATM (tempat memasukkan kartu ATM) dengan alat yang dikenal dengan nama *skimmer*. Modus operasinya adalah mengkloning data dari magnetic stripe yang terdapat pada kartu ATM milik nasabahakan tetapi seiring perkembangan teknologi informasi yang semakin canggih, metode skimmingpun 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.

2. METODOLOGI

Menurut Dewi Mustari (2015; 262-264) metodologi dalam pencurian uang nasabah yaitu:

2.1. Teknik Skimming

Pada ATM Pada saat kita memasukan kartu ATM ke mesin ATM, sang mesin ATM akan membaca informasi pada kartu ATM anda untuk digunakan sebagai KUNCI mengakses fasilitas perbankan anda. Salah satu jalan termudah untuk mencuri data informasi pada Kartu ATM anda di mesin ATM yaitu dengan memasang alat tambahan (*skimmer*) di depan mulut tempat anda memasukan kartu ATM

Dengan terpasangnya *skimmer* pada mulut atm, 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 (bodong). Selanjutnya sang pencuri tinggal mengambil alat skimmernya, dan menduplikasi kartu-kartu ATM milik nasabah-nasabah yang sempat mengakses ATM tersebut.

2.2 Cara mengetahui PIN nasabah

Para pencuri 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.

2.3 Pembuatan Kartu Magnetik Palsu

Saat sang pencuri mengambil kembali skimmer & camera miliknya, dia sudah mendapatkan data-data kartu kita lengkap dengan nomor PIN. Selanjutnya, sang pencuri tinggal membuat kartu magnetik baru dengan data-data kartu kita didalamnya dengan alat yang umum

3. LANDASAN TEORI

3.1. ATM (*Automatic Teller Machine*)

Menurut Dony Ariyus (2008), bahwa ATM (*Automatic Teller Machine*) adalah suatu perangkat komputer yang digunakan oleh nasabh untuk transaksi dalam perbankan. Kegunaa dari ATM sebagai berikut untuk menarik uang secara tunai (*cash withdrawal*). Kegunaan ATM sekarang ini sudah berkembang selain penarikan uang juga digunakan transfer uang, cek saldo, mebayar tagihan dan sebagainya.

Transaksi lewat ATM menggunakan kartu magnetic yang terbuat dari dari plastic dan kode PIN (*Personal Information*

Number) yang berasosiasi dengan kartu tersebut. PIN yang terdiri dari 6 angka yang harus dijaga kerahasiaanya.

PIN digunakan untuk mengverifikasi kartu ATM milik nasabah yang dimasukan kedalam mesin ATM. Proses verifikasi kartu ATM dilakukan oleh computer Pusat (Host) bank, maka harus ada komunikasi dua arah antara mesin ATM dengan computer Host.

3.2 Skimming

Skimming adalah Pengertian daripada *skimming* itu sendiri merupakan pelaku kejahatan mengambil data dari pita magnetik yang ada di belakang kartu debit/kredit/ATM. Bisa juga dikatakan *skimming* adalah tehnik foto kopi data yang ada di kartu korban.

4. HASIL DAN PEMBAHASAN

4.1. Cara Kerja *Skimming*

Dari hasil penelitian yang dilakukan dengan menganalisis bagaimana pembobol bisa mendapatkan informasi yang diinginkannya untuk bisa mendapatkan uang dengan mudah. Hasilnya menunjukan dengan memakai berbagai macam alat diantara *Skimmer* dan kamera kecil yang disimpan disamping dekat nasabah memasukkan pin. Dan ternyata cara yang dilakukan tidaklah begitu canggih seperti yang diperkirakan orang-orang, orang dengan pengetahuan praktis elektronika dan IT (Information Technology) bisa melakukan hal tersebut. Bahkan alat-alatnya pun bisa dibeli dari beberapa situs underground di Internet. Skimmer yang lebih canggih biasanya menggunakan alat-alat lebih canggih, dasarnya tetap sama namun teknologinya lebih canggih. Dalam hal pencurian PIN, Skimmers canggih menggunakan PIN PAD palsu.

Dengan menggunakan 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. Dengan teknologi *skimmer* secanggih ini, setiap nasabah masuk ke mesin ATM, kartu otomatis dicopy ke mesin skimmer. PIN otomatis terkam pada pin-pad unit. Kedua alat ini akan mengirim data-data tersebut via bluetooth ke main-unit yang ditempatkan maksimal 25 meter dari mesin ATM. Selanjutnya main unit ini akan memberikan notifikasi ke sang pencuri via SMS. Bahkan bukan tidak mungkin, sang pencuri sudah mendapatkan apa yang ia hendaki tanpa mengambil kembali unit skimmer yang ada di ATM, karena seluruh data yang ia

inginkan sudah dikirimkan via GPRS ke notebook sang pencuri.

4.2 Pencegahan nasabah dari kejahatan skimming

Menurut dewi Mustari (2015, 264) ada beberapa cara pencegahan nasabah dari kejahatan *skimming* adalah :

a) Menjaga kerahasiaan PIN
b) kondisi fisik ATM dan sekelilingnya dan apabila ada hal-hal yang mencurigakan, nasabah diharapkan tidak menggunakan ATM tersebut dan segera melaporkan kepada pihak bank terdekat dan atau kepada pihak berwajib.
c) Pada saat bertransaksi menggunakan kartu ATM pada merchant (toko yang bekerja sama dengan pihak perbankan), diharapkan nasabah memperhatikan kondisi alat EDC, bila terdapat alat (device) mencurigakan yang menempel pada EDC atau hal lain yang mencurigakan, nasabah dihimbau tidak bertransaksi dan segera melaporkan kepada pihak bank terdekat atau kepada pihak berwajib.
d) Segera blokir kartu ATM bila menemukan kejanggalan transaksi.
e) Cari lokasi ATM yang relatif aman.
f) Jangan mudah percaya dengan bantuan orang lain di sekitar ATM

5. **KESIMPULAN**

Jika dilihat dari prosesnya skimming adalah aktivitas menggandakan informasi yang terdapat dalam pita magnetik (magnetic stripe) yang terdapat pada kartu kredit maupun ATM/debit secara ilegal. Ini artinya, dapat disimpulkan bahwa skimming adalah aktivitas yang berkaitan dengan upaya pelaku untuk mencuri data dari pita magnetik kartu ATM/debit secara ilegal untuk memiliki kendali atas rekening korban. Perbuatan skimming diatas termasuk perbuatan mengakses komputer dan atau sistem informasi milik orang lain dengan cara ilegal dengan maksud mengambil secara ilegal data-data pribadi yang terdapat dalam komputer dan atau sistem informasi tersebut. Menurut Dian ekawati (2018), Perbuatan tersebut termasuk dalam tindak pisana informasi dan transaksi elektornik yang melarang setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan atau sistem elektronik dengan cara apapun dengan tujuan untuk memperoleh informasi elektronik dan atau dokumen elektronik

sebagaimana diatur dalam pasal 30 ayat 2 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 berbunyi ” Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik”. Setiap perbuatan dapat dipidana jika memenuhi unsur pidana yang terdapat dalam pasal yang disangkakan, dalam pasal 30 ayat 2 Undang-undang ITE diatas dapat diketahui bahwa yang termasuk unsur-unsur pidananya yaitu :

1. Unsur Kesalahan yaitu Dengan Sengaja
2. Unsur Melawan Hukum yaitu Tanpa Hak atau Melawan Hukum
3. Unsur Perbuatan yaitu Mengakses dengan Cara Apapun
4. Unsur Obyek yaitu Komputer dan atau Sistem elektronik
5. Tujuan yaitu Dengan Tujuan Untuk Memperoleh Informasi Elektronik dan atau Dokumen Elektronik.

Daftar Pustaka

Dewi Mustari, (2015), Cyber crime: penggunaan skimmer terhadap pembobolan atm, *Faktor Exacta 8(3)*: 261-265, 2015, ISSN: 1979-276X

Dian Ekawati, (2018), Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan, *UnesLaw Review*, Volume 1, Issue 2, Desember 2018, ISSN Online : 2622-7045.

Donny Ariyus, (2008), *Pengantar Ilmu Kriptografi*, Penerbit Andi, Yogyakarta

Undang-undang Nomor 19 Tahun 2016 tentang Perubahan atas Undangundang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

https://www.cnnindonesia.com/teknologi/20190913095417-185-430132/mengenal-skimming-penyebab-atm-nasabah-bobol, diunduh pada tanggal 23 November 2019

https://databoks.katadata.co.id/datapublish/2019/10/09/berapa-jumlah-alat-pembayaran-menggunakan-kartu, diunduh pada tanggal 23 November 2019