Faktor Exacta 8(3): 261-265, 2015
ISSN: 1979-276X

CYBER CRIME: PENGGUNAAN SKIMMER TERHADAP PEMBOBOLAN ATM

DEWI MUSTARI
mustaridewi@yahoo.com
Program Studi Teknik Informatika
Fakultas Teknik, Matematika dan Ilmu Pengetahuan Alam
Universitas Indraprasta PGRI

Abstrak. Akhir-akhir ini Indonesia sedang diramaikan dengan berita pembobolan ATM yang dterjadi di Bali. Para nasabah tiba-tiba kehilangan saldo rekeningnya akibat dibobol oleh orang-orang yang tidak bertanggung jawab. Untuk masalah tipu menipu dan curi mencuri adalah hal yang sepertinya sudah sangat biasa di Indonesia. Secara makro hal ini mungkin diakibatkan oleh kurangnya kesempatan kerja dan tidak meratanya pendapatan. Teknik pembobolan ATM ini dikenal dengan teknik ATM *Skimmer Scan*. Namun adakah undang-undang di Indonesia yang mengatur mengenai kejahatan yang bermodus elektronik atau dikenal dengan istilah kejahatan dunia *Cyber Crime*. Akhir-akhir ini pula mulai berdengung desas-desus mengenai perumusan undang-undang dunia *Cyb*er atau dikenal dengan *Cyber Law*. Untuk mengatasi masalah pembobolan ATM tentunya ada beberapa cara yang dapat dilakukan diantaranya menjaga kerahasiaan PIN, memperhatikan kondisi fisik dari ATM, saat bertransaksi menggunakan kartu ATM pada *merchant* nasabah diharapkan memperhatikan kondisi alat EDC, blokir kartu ATM jika menemukan kejanggalan, cari lokasi yang aman, dan jangan mudah percaya dengan bantuan orang yang tidak dikenal.

Keyword: Cyber Crime, Skimmer, ATM

PENDAHULUAN

Perkembangan Teknologi Informasi dan Komputer (TIK) telah mengalamai kemajuan yang sangat pesat, terutama setelah diketemukannya teknologi yang menghubungkan antar komputer (*Networking*) dan Internet. Namun demikian, berbagai kemajuan tersebut ternyata diikuti pula dengan berkembangnya sisi lain dari teknologi yang mengarah pada penggunaan komputer sebagai alat untuk melakukan berbagai modus kejahatan. Istilah ini kemudian dikenal dengan *cybercrime*.

Baru-baru ini 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.

Selain itu ada cara lain untuk memancing nasabah yaitu dengan *Fishing* yaitu dengan membuat situs palsu untuk memancing nasabah pengguna layanan internet banking. Dengan mengirim pesan elektronik (*e-mail*) yang seakan-akan dari operator bank. Isinya meminta nasabah mengisi data kembali dengan alasan ada perbaikan sistem keamanan.

Kejahatan teknologi informasi atau kejahatan dunia maya (*Cyber Crime*) merupakan permasalahan yang harus ditangani secara serius, karena akibatnya sangat luas. Dan jika tidak ditanggulangi dan tidak terkendali akan sangat fatal bagi kehidupan masyarakat, khususnya bagi pengguna teknologi.

Cybercrime adalah tidak criminal yang dilakkukan dengan menggunakan teknologi computer sebagai alat kejahatan utama. *Cybercrime* merupakan kejahatan yang memanfaatkan perkembangan teknologi computer khusunya internet. *Cybercrime* didefinisikan sebagai perbuatan melanggar hukum yang memanfaatkan teknologi computer yang berbasasis pada kecanggihan perkembangan teknologi internet.
Karakteristik *Cybercrime* Dalam perkembangannya kejahatan konvensional *cyber crime* dikenal dengan:
1. Kejahatan kerah biru
2. Kejahatan kerah putih

Cybercrime memiliki karakteristik unik yaitu:
1. Ruang lingkup kejahatan
2. Sifat kejahatan
3. Pelaku kejahatan
4. Modus kejahatan
5. Jenis kerugian yang ditimbulkan

Dari beberapa karakteristik diatas, untuk mempermudah penanganannya maka *cybercrime* diklasifikasikan:

a) *Cyberpiracy* **:** Penggunaan teknologi computer untuk mencetak ulang software atau informasi, lalu mendistribusikan informasi atau *software* tersebut lewat teknologi komputer.
b) *Cybertrespass***:** Penggunaan teknologi computer untuk meningkatkan akses pada system computer suatu organisasi atau indifidu.
c) *Cybervandalism* **:** Penggunaan teknologi computer untuk membuat program yang menganggu proses transmisi elektronik, dan menghancurkan data dikomputer

Skimmer

Skimmer atau ATM *Skimmer*, merupakan alat pencuri data nasabah yang dipasang di mulut ATM, alat ini akan menyalin data si korban jika ia memasukan kartu ATM melalui *skimmer* ini, setelah itu maka si penjahat yang menempatakn *Skimmer* pada lobang ATM akan memiliki data nasabah pemilik ATM.
Skimmer berarti alat yang bisa digunakan untuk aktivitas pencurian informasi yang dilakukan dari kartu nasabah, baik dari kartu ATM maupun kartu kredit. Dengan memasang alat ini di mulut ATM, pelaku bisa mendapatkan data di kartu nasabah. Kemudian tinggal memasukannya ke dalam kartu ATM bodong. Sementara untuk pin, pelaku menggunakan kamera pengintai mungil.

METODE

Metode yang digunakan oleh pembobol untuk membobol ATM nasabah yaitu:
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. Proses pemasangan *Skimmer*.

Gambar 1. Proses Pemasangan *Skimmer*

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 *skimmer*nya, dan menduplikasi kartu-kartu ATM milik nasabah-nasabah yang sempat mengakses ATM tersebut.

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.

Gambar 2. Kamera
Merekam Aktifitas

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 seperti gambar dibawah ini:

Gambar 3. Kartu Magnetik

Selanjutnya sang pencuri memiliki akses penuh selayaknya pemilik rekening yang dicuri. Untuk meminimasi resiko biasanya sang pencuri memilih ATM yang tidak ada camera

CCTVnya, oleh sebab itu tidak heran mengapa beberapa transaksi yg dilakukan pencuri memilih di ATM bank lain yang tidak memiliki CCTV (*switching*).

4. Mengenali bentuk-bentuk *Skrimmer*

Gambar 4. Bentuk-bentuk *Skimmer*

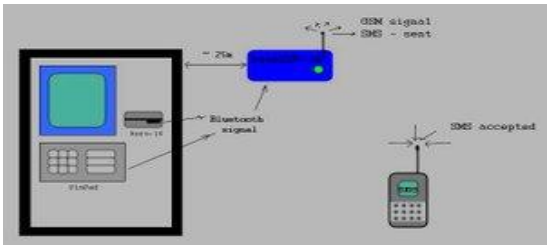
PEMBAHASAN

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 seperti gambar dibawah ini:

Gambar 5. 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. Lebih canggih lagi skimmer dewasa ini memanfaatkan teknologi *bluetooth* seperti diagram kerja dibawah ini:



Gambar 6. Teknologi Skimmer Bluetooth

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

PENUTUP

Mengingat semakin banyak kasus-kasus yang terindikasi sebagai *cyber crime,* maka selain aspek hukum maka secara teknis juga perlu disiapkan berbagai upaya preventif terhadap penangulangan kasus *cyber crime*. Oleh sebab itu, nasabah harus lebih berhati-hati dalam melakukan transaksi melalui ATM ataupun melalui internet. Untuk menghinadari pembobolan ada beberapa cara untuk menghindarinya:

1. Menjaga kerahasiaan PIN
2. 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.
3. 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.
4. Segera blokir kartu ATM bila menemukan kejanggalan transaksi.
5. Cari lokasi ATM yang relatif aman.
6. Jangan mudah percaya dengan bantuan orang lain di sekitar ATM.

DAFTAR PUSTAKA

Rendi Hari Kusuma, 2010, Cyber *Crime Pembobolan ATM di Bali Gunakan Skimmer*, detiknews.
Diakses tanggal 15 Juli 2011.
http://www.detiknews.com/read/2010/01/22/082729/1283721/10/bi-pembobolan-atm-teratasi
Diakses tanggal 28 Juli 2011.
http://kaufik.multiply.com/journal/item/1/MODUS_OPERANDI_PARA_PEMBOBOL_ATM.
Diakses tanggal 28 Juli 2011. *http://roniamardi.wordpress.com/definisi-cybercrime/*.
Diakses tanggal 14 Juli 2011.
h*ttp://berita.liputan6.com/hukrim/201001/260076/Pembobol.ATM.di.Bali.Gunakan.Skimmer*