CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 1, No. 2, November 2018, hlm 57-61

KEJAHATAN SIBER DALAM BIDANG PERBANKAN

Muhammad Khairul Faridi[1]

[1]Magister Informatika Universitas Islam Indonesia Yogyakarta
Email: [1]faridimuhammad5@gmail.com

Abstrak

Teknologi internet sudah banyak diterapkan pada berbagai perusahaan salah satunya pada perbankan. Penerapan teknologi internet perbankan mampu meningkatkan efisiensi dan menurunkan biaya operasional perusahaan. Selain itu, nasabah juga dimudahkan untuk melakukan transaksi online dimanapun dan kapanpun. Namun keamanan informasi menjadi issue utama dalam penerapan teknologi internet dalam perbankan, dan pada awal tahun 2018 dunia dikejutkan dengan terjadinya pencurian data melalui mesin ATM di 64 negara dan 13 diantaranya bank swasta dan milik pemerintah indonesia. Akibat dari kejadian tersebut bank swasta dan bank milik negara mengalami kerugian senilai 18 miliar rupiah. Tujuan dari makalah ini yaitu bagaimana mengidentifikasi jenis-jenis kejahatan perbankan berdasarkan peneliti sebelumnya serta bagaimana cara pencegahan dan penanggulangan tindak kejahatan pada perbankan. Dan hasil dari analisis terhadap beberapa penelitian tersebut terdapat 3 teknik kejahatan siber yang sering digunakan yaitu *skimming, hacking* dan *malware*. Dari ketiga jenis teknik kejahatan tersebut terdapat beberapa metode yang dapat digunakan untuk menanggulangi kejahatan pada perbankan yaitu dengan penerapan *triple otentikasi, biometric* dan *smart card.*

Kata kunci: *kejahatan siber, bank elektronik, skimming, hacking, malware*

CYBERCRIME IN BANKING

Abstract

Internet technology has been widely applied to various companies, one of them is banking. Implementing internet banking technology can improve efficiency and reduce the company's operational costs. In addition, customers are also facilitated to make online transactions wherever and whenever. But information security is a major issue in the application of internet technology in banking, and in early 2018 the world was shocked by the occurrence of data theft through ATM machines in 64 countries and 13 of them were private and Indonesian government banks. As a result of this incident private banks and state-owned banks suffered losses of 18 billion rupiah. The purpose of this paper is how to identify types of banking crimes based on previous researchers and how to prevent and overcome crime in banks. And the results of the analysis of some of these studies are 3 cybercrime techniques that are often used, namely skimming, hacking and malware. Of the three types of crime techniques, there are several methods that can be used to overcome crime in banks, namely the application of triple authentication, biometrics and smart cards.

Keywords: *cybercrime, e-banking, skimming, skimming, hacking, malware*

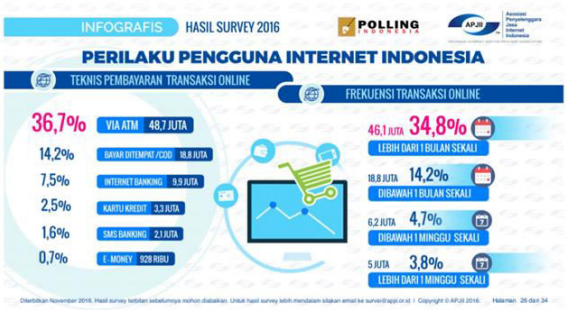
1. PENDAHULUAN

Perbankkan merupakan salah satu perusahaan penyedia layanan jasa keuangan yang telah memberikan pelayanan kepada masyarakat dan bisnis seperti layanan penitipan dan pinjaman uang (Kara, 2013). Pada awal berdirinya perbankkan yaitu pada tahun 1955, perbankkan hanyalah sebuah jasa pertukaran uang yang kemudian bertransformasi menjadi jasa penitipan uang atau pada saat ini kita menyebutnya tabungan (Fathurrahman, 2013). Dalam upaya meningkatkan pelayanan, perbankkan telah menerapkan teknologi di berbagai bidang salah satunya pada Anjungan Tunai Mandiri (ATM). ATM digunakan sebagai pengganti fungsi kasir dalam bertransaksi seperti penarikan tunai serta proses transaksi lainnya (Hutagaol and Sudarsono, 2015). Secara umum proses perbankkan yang telah menerapkan teknologi disebut dengan istilah *E-Banking* (Electronic Banking).

Perbankan Elektronik adalah teknologi baru yang memiliki banyak keunggulan tapi juga memiliki potensial masalah yang besar yang dapat ditimbulkan sehingga mengakibatkan nasabah ragu untuk menggunakan sistem tersebut (Fatima, 2011).

Tindak kejahatan dalam perbankan berbeda dengan kejahatan konvensional namun memiliki tujuan yang sama yaitu untuk mendapatkan informasi rekening, kartu kredit, serta meretas sistem basis data bank serta merampok bank (AlMajed, dkk., 2015).

Dalam kejahatan cyber terdapat dua tipe kejahatan. Tipe yang pertama adalah kejahatan di mana komputer menjadi target aktivitas kriminal, sedangkan Tipe yang kedua adalah kejahatan yang menggunakan komputer sebagai alatnya (Librianty, 2015). Dari kedua jenis tindak kejahatan di atas, tindak kejahatan yang paling sering terjadi pada perbankan antaranya *skimming*, *hacking* dan *malware*. Target utama tindak kejahatan ini adalah nasabah yang menggunakan akses internet dalam melakukan transaksi. Berikut ini adalah survei yang dilakukan oleh IPJII (Asosiasi Penyelenggara Jasa Internet Indonesia) mengenai perilaku pengguna internet dalam bertransaksi secara online.



Gambar 1. Survei perilaku pengguna internet di Indonesia tahun 2016

Dalam gambar di atas dapat dilihat bahwa penggunaan internet dalam transaksi cukup besar yaitu lebih dari 40% atau tepatnya 60 juta lebih pengguna yang menggunakan internet dalam melakukan pembayaran transaksi online dan lebih dari 34% yang melakukan transaksi online dalam satu bulan sehingga dapat disimpulkan lebih dari 60 juta pengguna internet rentan terhadap kejahatan cyber.

Pada awal tahun 2018 terjadi tindak kejahatan pencurian informasi kartu debit dengan menggunakan metode skimming yang terjadi pada 64 bank yang tersebar di seluruh dunia dan 13 diantaranya bank swasta dan pemerintah Indonesia. Kejadian tersebut mengakibatkan bank yang terdampak harus mengembalikan dana nasabah mencapai 18 Miliar. Hal tersebut mengindikasikan pentingnya penanganan yang cepat untuk mengatasi permasalahan-permasalahan tersebut di masa yang akan datang.

Terdapat beberapa penelitian yang membahas terkait kejahatan cyber pada perbankan seperti penelitian yang menyatakan permasalah yang menyebabkan terjadinya tindak kejahatan pada perbankan yaitu kurangnya kewaspadaan pengguna dalam menjaga informasi pribadi. Untuk menanggulanginya peneliti menyarankan untuk menerapkan beberapa teknik dalam membantu memproteksi informasi pengguna diantaranya dengan menerapkan teknik *cryptography, biometric,* dan *phishing prevention,* yang diharapkan mampu melindungi pengguna dari tindak kejahatan pada bidang perbankan.

2. PENELITIAN TERKAIT

Dalam makalah ini akan dibahas beberapa penelitian yang telah dilakukan oleh peneliti sebelumnya terkait dengan kejahatan siber dalam bidang perbankan.

Fatima (2011) pola penyerangan menargetkan serangan ke pengguna atau nasabah yang menggunakan internet dalam bertransaksi, salah satu teknik serangan yang digunakan yaitu phishing Teknik phishing digunakan untuk menyusup ke dalam jaringan dengan memotong jalur data kemudian mengganti data dengan informasi palsu. Selain itu, teknik ini juga dapat digunakan untuk mengirim malware yaitu dengan mengirimkan informasi yang telah terinfeksi ke email korban.

Untuk menghindarinya perbankan dapat menerapkan otentikasi 2 faktor yaitu untuk memvalidasi data atau informasi yang akan diterima oleh nasabah. Dua otentikasi tersebut ialah menggunakan password dan token seperti smartcard. Namun, untuk keamanan yang lebih baik disarankan menambahkan proses validasi biometrik untuk menjamin keamanan nasabah.

Naam (2017) melakukan penelitian khususnya mengenai bagaimana pertahanan diri dari serangan malware dengan mengidentifikasi jalur kerja serta jenis dari malware itu sendiri. Tujuan dari penelitiannya adalah bagaimana memberikan solusi dari serangan malware dengan menganalisis cara kerja dan jenis malware untuk mengetahui langkah-langkah yang dapat lakukan untuk menanggulangi dampak dari infeksi malware pada sistem komputer.

Simon & Anderson (2013) telah melakukan penelitian terkait penggunaan teknik skimming untuk mendapatkan PIN pada smartphone dengan menggunakan kamera dan mikrofon. Teknik ini diujikan pada smartphone Nexus S dan Galaxy S3 yang sistem operasinya menggunakan sistem operasi android. Penelitian ini bertujuan untuk menganalisis sistem keamanan smartphone terhadap pencurian PIN dengan menggunakan teknik skimming.

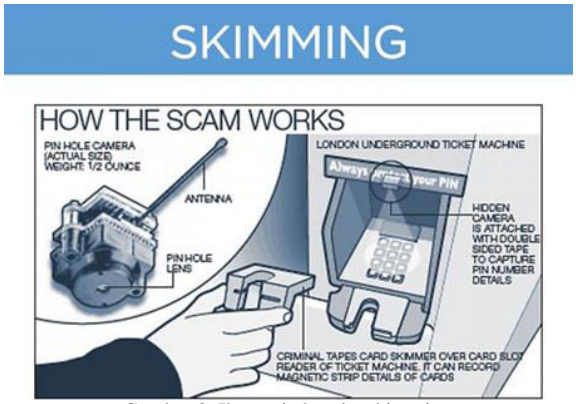
Azhar (2017) meneliti tentang bagaimana mendeteksi peretasan (hacking) pada mobile banking dengan mengembangkan sebuah prototipe aplikasi yang diharapkan mampu memberikan notifikasi berupa aktivitas transaksi yang dilakukan pengguna melalui mobile banking. Setelah notifikasi diterima kemudian pengguna dapat membuat keputusan apakah notifikasi tersebut berupa fraud atau bukan.

3. PEMBAHASAN

Dari hasil penelitian yang telah dilakukan oleh peneliti sebelumnya. Penelitian tersebut menjelaskan beberapa metode yang sering digunakan oleh pelaku tindak kejahatan, namun makalah ini akan membahas 3 metode yaitu metode *skimming*, *hacking* dan *malware*:

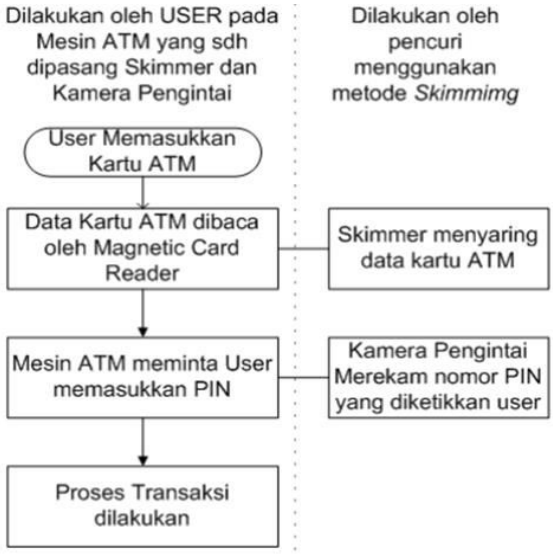
3.1. Skimming

Metode Skimming merupakan metode yang digunakan untuk mencuri informasi nasabah pada saat bertransaksi menggunakan ATM (Arifianto, 2018). Dalam tindak kejahatan ini terdapat 3 alat utama yang digunakan seperti tampak pada ilustrasi berikut:



Gambar 2. Ilustrasi alat-alat skimming
(Sumber: http://www.criminalelement.com)

Dari gambar diatas terdapat 3 komponen utama yang digunakan dalam menjalankan metode skimming yaitu *skimmer, hidden camera* dan *keypad.* Alat skimmer berfungsi untuk merekam aktivitas nasabah dalam menggunakan mesin ATM, alat ini mampu merekam strip elektromagnetik yang ada pada kartu korban pada saat kartu dimasukkan ke mesin ATM. Kamera tersembunyi dan keypad digunakan untuk merekam aktivitas korban pada saat melakukan penginputan PIN pada mesin ATM. Untuk mengetahui bagaimana proses skimming itu berlangsung, maka berikut ini adalah proses skimming pada mesin ATM:



Gambar 3. Alur proses yang digunakan
(Sumber: https://diakbar.wordpress.com)

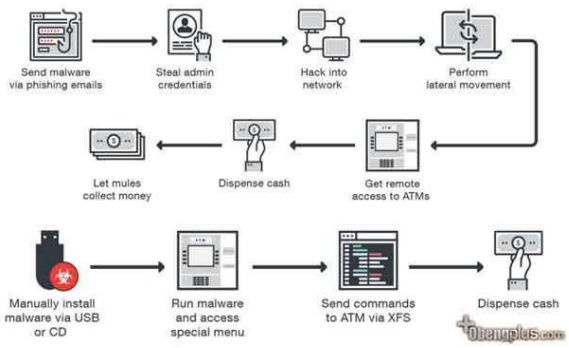
Dari gambar diatas dapat terlihat bagaimana proses skimming itu berjalan, mulai pada saat korban memasukkan kartu debit ke ATM sampai dengan proses transaksi selesai dilakukan. Sebelum kartu debit korban terbaca oleh mesin ATM, alat skimmer telah melakukan scanning terhadap *magnetic card* yang ada pada kartu debit korban yang kemudian kode-kode yang terdapat pada *magnetic card* disimpan. Setelah proses scanning yang dilakukan mesin ATM selesai kemudian mesin ATM akan menampilkan instruksi untuk memasukkan PIN, dan pada proses ini kamera tersembunyi atau keypad palsu yang sudah dipasang akan merekam PIN yang dimasukkan oleh korban. Setelah berhasil mendapatkan data-data korban kemudian proses terakhir yaitu pembuatan kartu magnetik palsu yang kemudian digunakan untuk menarik saldo tanpa diketahui oleh korban.

Terdapat beberapa langkah untuk menghindari dari tindak kejahatan skimming yaitu: 1. Jangan menggunakan ATM yang ada di daerah sepi, 2. Awasi sekitar sebelum melakukan transaksi seperti mengecek mulut ATM, mengecek keypad dan kamera tersembunyi, 3. Tutuplah tangan dengan apa pun pada saat memasukkan PIN dan 5. Gunakanlah layanan perbankan seperti SMS Banking untuk mengetahui aktivitas transaksi yang terjadi pada nomor rekening (Anjani, 2018).

3.2. Malware

Malware merupakan singkatan dari *malicious software* yang artinya software yang tidak diinginkan dalam sistem komputer, biasanya malware dibuat untuk mencuri data informasi yang bahkan dapat merusak sebuah sistem komputer (Kurniawan, 2014). Malware sangat sulit untuk dideteksi oleh sistem komputer. Pada tahun 2017 serangan malware pernah menjadi di 150 negara di dunia dan target utamanya adalah instansi

pemerintah dan perusahaan-perusahaan besar di seluruh dunia (Praditya, 2017). Sehingga sampai saat ini malware masih menjadi ancaman serius bagi dunia maya secara global dan terus perkembangan dan beberapa fakta terkait malware ini menjadikannya topik menarik untuk diangkat menjadi tema sebuah penelitian (Ibrahim, 2012). Berikut ini adalah ilustrasi alur bagaimana malware itu dapat berjalan di sistem komputer:



Gambar 4. Ilustrasi alur proses terinfeksi malware
(Sumber: http://www.obengplus.com)

Terdapat dua jalur yang menyebabkan sistem komputer terkena oleh malware yaitu dengan melalui USB Drive dan melalui jaringan internet. Sistem Komputer yang terinfeksi malware melalui USB Drive biasanya tidak memiliki pengaman seperti antivirus atau sejenisnya sehingga malware yang sudah terinstall di USB dapat dengan mudah masuk ke sistem komputer. Selanjutnya sistem komputer yang terinfeksi melalui jaringan internet yaitu ketika pengguna membuka email atau website. Pada email yang berbahaya biasanya akan langsung disaring ke spam oleh sistem namun tidak banyak dari email tersebut juga masuk ke inbox. Malware ini akan berjalan ketika objek yang terinfeksi di dalam email itu di klik dan selanjutnya ketika sistem komputer yang sudah terinfeksi malware maka informasi pribadi termasuk data-data perbankan yang tersimpan di komputer.

Ada beberapa tip untuk terhindar dan tip untuk mengatasi dampak dari infeksi malware pada sistem komputer yaitu dengan mengidentifikasi sumber malware kemudian klasifikasikan jenis malware, setelah mengetahui sumber dan jenis malware kemudian update atau install anti virus yang memiliki list data terkait jenis malware yang terdapat pada sistem komputer. Jika belum berhasil update sistem operasi yang terinstall pada sistem komputer dan jika malware masih ada maka langkah yang terakhir dengan memformat partisi yang ada pada sistem komputer (Naam, 2017).

3.3. Hacking

Hacking adalah kegiatan menyerang program komputer dan mengeksploitasi komputer milik orang pribadi atau perusahaan dan seiring berjalannya waktu, hacking seringkali dianggap sebagai tindak kejahatan, namun dalam sudut pandang tertentu hacking merupakan salah satu aktivitas mengisi waktu luang yang produktif (Retnaningrum, 2017).

Semua tidak kejahatan siber di kategorikan sebagai serangan hacking dan berikut ini beberapa serangan hacking yang mungkin terjadi pada transaksi pada perbankan seperti Distributed Denial of service (DDOS). DDOS merupakan salah satu serangan yang sering dilakukan pada sistem server baik pada perusahaan maupun perbankan. Untuk dapat melakukan peretasan, hacker akan melakukan scan port yang terbuka kemudian mulai malukan menyerang pada jaringan bank (Islam, 2014). Selain DDOS, malware juga termasuk pada software yang digunakan untuk melakukan peretasan dan banyak lagi teknik dalam melakukan hacking.

4. KESIMPULAN

Dari uraian diatas dapat ditarik kesimpulan bahwa penerapan teknologi internet pada perbankan sangat penting dilakukan. Namun sayangnya, penerapan teknologi tersebut masih rentan terhadap aktivitas tindak kejahatan seperti skimming, hacking dan malware. Oleh karena itu, inovasi terhadap sistem keamanan perbankan sangat dibutuhkan untuk melindungi dan menanggulangi tindak kejahatan dalam transaksi elektronik.

Dari penelitian terkait terdapat beberapa solusi yang ditawarkan untuk menanggulangi permasalahan tersebut diantaranya seperti dengan menerapkan triple otentikasi yaitu menggunakan password, token dan biometrik. Selain itu pengamanan dapat juga menggunakan big data untuk memproses transaksi keuangan yang tidak wajar.

5. DAFTAR PUSTAKA

ALMAJED, N., MAGLARAS, L., SIEWE, F., JANICKE, H. AND BAGHERI ZADEH, P., 2015. Prevention of crime in B2C E-Commerce: How E-Retailers/Banks protect themselves from Criminal Activities. *Security and Safety*.

ANJANI, P. T., 2018. *5 Tips Agar Kartu ATM Terhindar dari Skimming, No 2 Sepele Tapi Sering Dilupakan.* [Online] Available at: http://jatim.tribunnews.com/2018/03/14/5-tips-agar-kartu-atm-terhindar-dari-skimming-no-2-sepele-tapi-sering-dilupakan [Accessed 8 Agustus 2018].

ARIFIANTO, T., 2018. Penerapan Fingerprint Recognition Dengan Metode Learning Vector Quantization (LVQ) dalam Automatic Teller Machine (ATM). *Jurnal SPIRIT*, 9(2).

DREHMANN, M. AND NIKOLAOU, K., 2013. Funding liquidity risk: definition and

measurement. *Journal of Banking & Finance*, 37(7), pp.2173-2182.

FATHURRAHMAN, A., 2013. Meninjau Ulang Landasan Normatif Perbankan Syariah di Indonesia (Telaah atas Teori Konstruksi Fiqh Klasik). *Al-Mawarid*, 11(1).

FATIMA, A., 2011. E-Banking Security Issues-Is There A Solution in Biometrics?. *Journal of Internet Banking and Commerce*, 16(2), p.1.

HERMAWAN, R., 2015. Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia. *Faktor Exacta*, 6(1), pp.43-50.

HUTAGAOL, V. AND SUDARSONO, B., 2015. Penentuan Potensi Lokasi Atm Bni Menggunakan Analytical Hierarchy Process (Ahp) Dan Sistem Informasi Geografis (Studi Kasus: Kecamatan Tembalang). *Jurnal Geodesi Undip*, 4(2), pp.25-32.

IBRAHIM, L.M. AND THANOON, K.H., 2012. Detection of Zeus Botnet in Computers Networks and Internet. vol, 6, pp.84-89.

ISLAM, S., 2014. Systematic literature review: Security challenges of mobile banking and payments system. *International Journal of u-and e-Service, Science and Technology*, 7(6), pp.107-116.

KALIGIS, Y., 2013. Analisis Tingkat Kesehatan Bank Dengan Menggunakan Metode Camel Pada Industri Perbankan Bumn Yang Terdaftar Di Bursa Efek Indonesia. *Jurnal EMBA: Jurnal Riset Ekonomi, Manajemen, Bisnis dan Akuntansi*, 1(3), pp. 263-272.

KARA, M., 2013. Kontribusi Pembiayaan Perbankan Syariah Terhadap Pengembangan Usaha Mikro Kecil dan Menengah (UMKM) Di Kota Makassar. ., 47(1).

KURNIAWAN, A. AND PRAYUDI, Y., 2014. Teknik Live Forensics Pada Aktivitas Zeus Malware Untuk Mendukung Investigasi Malware Forensics. *HADFEX (Hacking and Digital Forensics Exposed)*, pp.1-5.

LIBRIANTY, A., 2015. *Mengenal Modus Pembobolan ATM Melalui Teknik Skimming*. [Online] Available at: http://tekno.liputan6.com/read/2302264/mengenal-modus-pembobolan-atm-melalui-teknik-skimming [Accessed 8 Agustus 2018].

NAAM, J., 2017. METODA PERTAHAN DIRI PROGRAM VIRUS. *Jurnal MEDIA PROCESSOR*, 8(2).

PRADITYA, I. I., 2017. *BI Pastikan Sistem Perbankan Aman dari Ransomware WannaCry*. [Online] Available at: https://www.liputan6.com/bisnis/read/2952211/bi-pastikan-sistem-perbankan-aman-dari-ransomware-wannacry [Accessed 8 Agustus 2018].

RETNANINGRUM, M.A., 2017. Perilaku Penemuan dan Pemanfaatan Informasi di Kalangan Hacker(Doctoral dissertation, Universitas Airlangga).

SIMON, L. AND ANDERSON, R., 2013. Pin skimmer: Inferring pins through the camera and microphone. *In Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices* (pp. 67-78). ACM.