Jurnal Ilmu Komputer, Ekonomi dan Manajemen (JIKEM)

E-ISSN: 2774-2075

Vol. 2 No. 2, Year [2022] Page 2739-2744

Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking

[1]**Angga Pradana Kusuma,** [2]**M. Irwan Padli Nasution**
Email: [1] pradanaangga555@gmail.com , [2] irwannst@gmail.com
[1]Mahasiswa Prodi Perbankan Syariah, [2]Dosen Prodi Perbankan Syariah
Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Sumatera Utara

ABSTRAK

Industri perbankan tampaknya tidak ketinggalan dalam perkembangan teknologi dan informasi. Hal ii dibuktikan dengan perbankan sekarang ini telah memajukanfasilitas dan layanan perbankan yang sesuai dengan perkembangan teknologi serta informasi. Perbankan telah merilis layanan yang disebut Perbankan Elektronik. Salah satu fasilitas e-banking merupakan Internet banking yang memudahkan nasabah melangsukan transaksi perbankan online baik finansial maupun non finansial. Agar tetap memiliki daya saing di era digital seperti sekarang ini, fasilitas perbankan yang aman harus tersedia bagi semua provider. Keamanan sistem informasi terkait transaksi-transaksi yang diberikan oleh perbankan, terutama fasilitas internet banking, sangat pokok guna menyokong layanan yang akuntabel.

Kata Kunci: *Perbankan, Internet Banking, sistem informasi*

PENDAHULUAN

Bank merupakan suatu perusahaan yang dalam kegiatan operasionalnya mengelola dana yang diterima dari para nasabah sebagai simpanan dan menyalurkan kembali dana tersebut kepada nasabah dalam wujud pinjaman atau simpanan. Ketika bank gagal, dampaknya dapat menyebar ke nasabah dan institusi yang menabung atau berinvestasi di bank tersebut, dan memiliki implikasi yang luas untuk pasar domestik dan internasional. Kehadiran teknologi informasi (TI) merupakan bagian utama dari proses bisnis bank karena hampir semuanya terkait dengan teknologi informasi. Penggunaan teknologi informasi telah menjadi hal yang mendasar dalam perbankan, dan dipakai untuk melakukan bsegama macam transaksi di perbankan multi channel. Itu juga merupakan tulang punggung toko. Teknologi informasi telah meningkatkan kinerja karyawan dan meningkatkan kepercayaan pelanggan dalam berbisnis.

Sesuai dengan kajian lain, sebagian penelitian yang dilakukan oleh Fristak dan Ward menunjukkan bahwa penerapan TI di perbankan yang dapat mengembangkan efisiensi operasional

dan membawa manfaat yang besar bagi bank yang mengimplementasikan sistem tersebut merupakan salah satu pemanfaatan TI di dunia perbankan. Dapat dikatakan bahwa bank semakin banyak menagih I -bank karena perkembangan Internet yang banyak dipakai oleh nasabah bank. Situasi ini memberikan peluang yang baik pada bank untuk memajukan fasilitas online. Situasi tersebut memperoleh daya tarik bidang perbankan yang bisa menarik nasabah baru.

Pesatnya kemajuan teknologi dapat memberikan ancaman masalah keamanan informasi yang ada di perbankaan dalam kegiatannya mengelola perbankan online. Pertahanan sistem informasi sering disebut sebagai kontrol dan melindungi sistem informasi, yang didefinisikan sebagai perlindungan perangkat keras dan langkah komputer dari intrusi yang disengaja atau tidak disengaja yang bisa mengubahkan perubahan, kerusakan, atau pencurian sumber daya sistem. Keamanan sistem informasi adalah subsistem organisasi internal yang bertugas mengelola risiko yang tergantung dengan sistem informasi terkomputerisasi.

Keamanan sistem informasi adalahpenerapan dari dasar-dasar pengendalian intern, yang digunakan terutama untuk memecahkan persoalan dalam sistem informasi. Bodnar dan William (2004) menyatakan bahwa kecurangan sistem informasi dapat dilakukan dengan enam cara, adalah:Manipulasi input, modifikasi rencana, modifikasi file langsung, pencurian data, manipulasi sumber data, dan penyalahgunaan.

METODE PENELITIAN

Metode yang digunakan peneliti dalam penelitian artikel ini memakai metode studi literatur. Metode kajian penelitian ini dilakukan dengan cara mencari berbagai sumber sastra, seperti buku, arsip, majalah, artikel dan majalah atau dokumen yang berkaitan dengan masalah yang sedang dipelajari. Oleh karena itu, informasi yang didapati dari kajian literatur ini digunakans sebagaireferensiuntuk mendukung bukti yang ada.

HASIL DAN PEMBAHASAN

Banyak fasilitas yang disediakan oleh pihak perbankan guna menunjang transaksi-transaksi keuangan fungsi utamanya adalah memberikan keringanan nasabah dalam bertransaksi. Selain layanan cabang bank, tersedia fasilitas internet banking serta ATM. Sekarang ini para nasabah lebih menerapkan untuk bertransaksi melalui alternatif delivery channel seperti ATM, internet banking, SMS banking tanpa harus mengantri lagi di bank. Dengan tumbuhnya transaksi online, telah meningkatkan pemakai saluran pengiriman alternatif, seperti perbankan online, yang umumnya menjadi lebih populer.

Bidang Keamanan

Seperti yang telah dikemukakan oleh Dony Ariyus, terdapat beberapa aspek yang ada dalam keamanan komputer diantaranya sebagai berikut:

a) Authentication, agar penerima informasi bisa memverifikasi keaslian pesan dari orang-orang yang telah menerima informasi tersebut.
b) Integrity, keaslian pesan yang dikirimkan melalui jaringan dan memastikan bahwa informasi yang dikirimkan tidak diubah oleh pihak yang berwenang.
c) Non-repudiation, non-repudiation mengacu pada pengirim. Pengirim tidak dapat menyangkal bahwa mereka.
d) Authority, pihak yang tidak memiliki hak atas informasi tidak dapat mengubah atau memodifikasi informasi yang terdapat dalam sistem jaringan perbankan.

e) Confidentiality, merupakan usaha dalam perlindungan informasi dari akses yang tidak sah.
f) Privacy, adalah lebih terfokus pada informasi pribadi.
g) Availability, aspek kesiapan mengacu pada kesiapan informasi pada saat diperlukan.
h) Access control, aspek ini merujuk pada pengaturan akses informasi.

Keamanan Pada Internet Banking

Untuk melindungi data nasabah dibutuhkan kerjasama antara bank dengan nasabah untuk memellihara sistem keamanan dalam hal-hal yang menyangkut penggunaan jasa manajemen bank. Bank dapat mengambil langkah-langkah berikut untuk mengembangkan keamanan sistem perbankan:

a) Sistem kriptografi, sistem ini memakai angka yang dikenal dengan kunci. Sistem ini juga dikenal sebagai sistem kata sandi. Ada dua jenis metode enkripsi, yaitu simetris dan asimetris. Sistem simetris memakai kode kunci yang mirip untuk penerima dan pengirim pesan. Kerugian dari enkripsi simetris yaitu bahwa kunci ini harus dikirim ke penerima, sehingga seseorang dapat mengutak-atiknya di sepanjang jalan. Sistem enkripsi asimetris juga memiliki kelemahan yaitu jumlah jangka waktu transfer data yang menurun akibat adanya kode tambahan. Sistem ini umumnya dipakaidala mengidentifikasi nasabah dan melindungi informasi keuangan nasabah.
b) Firewall adalah sistem yang mencegah akses tidak sah ke area yang dijaga di unit tempat kerja perusahaan. Firewall berupaya mengupayakan pihak-pihak masuk tanpa izin dengan cara menduplikasi dan memperumit penghalang yang ada. Tetapiharus dicatat bahwa firewall ini tidak bisa menghindari masuknya virus oleh perusahaan.

Untuk mengamankan data nasabah, tugas nasabah untuk menerapkan langkah-langkah keamanan untuk akun pribadi juga sangat penting. Pelanggan dapat mengambil langkah-langkah berikut untuk mengembangkan keamanan sistem di bank:

a) Device Registring, metode ini membatasi akses ke sistem perbankan dengan perangkat yang belum dikenali atau terdaftar di sistem. Perangkat ini memakai pemindaian sidik jari untuk mengidentifikasi penggunanya.
b) CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) adalah langkah baru yang digunakan di berbagai sistem perbankan untuk mencegah serangan otomatis pada sesi atau halaman verifikasi situs web. Langkah ini mengharuskan pemakai yang berwenang dalam secara acak memasukkan data yang diperlihatkan dalam gambar atau suara, dan susah bagi rencanaotomatis (Autobots) untuk menandai dan menangani.
c) Positive Identification,adalah model dimana nasabah bank diminta untuk menyerahkan data rahasia yang hanya diingat oleh nasabah untuk mengenali dirinya sendiri. Ini diimplementasikan sebagai langkah kedua.
d) Username danPassword,penjagaan paling dasar yang dapat dilakukan pelanggan adalah nama pengguna dan kata sandi. Sebelum pelanggan dapat membuka akunnya, nasabah wajib memasukkan beberapa token keamanan ke dalam akunnya. Bergantung pada bank penyedia layanan, nama pengguna dan kata sandi terdiri dari beberapa karakter. Beberapa

bank juga memiliki persyaratan khusus untuk menentukan jumlah dan jenis karakter yang digunakan dalam nama pengguna dan kata.

Jenis Serangan Pada *e- Banking*

Beberapa ancaman hacking yang biasanya terjadi untuk menghancurkan sistem keamanan bank. Serangan ini menargetkan sistem perbankan yang tersedia dan kebiasaan penggunaan nasabah. Dalam pekerjaan keamanan, kemungkinan risiko tertinggi juga harus dipahami menurut kepadatan jaringan dan besarnya dampak dari ancaman berikut. Berikut adalah ancaman terjadinya serangan terhadap sistem pelayanan bank:

a) Brute forceattack, disebut juga Brute Force Attack dalam bahasa Indonesia Ini adalah teknik penyerangan kepada sistem keamanan komputer yang memakai semua kemungkinan kunci password atau bisa dengan mudah memakai kata sandi acak atau random password. Pendekatan ini awalnya terkait dengan program.
b) Denial of service (DoS) attack, adalah upaya (dalam bentuk ancaman) untuk menghalangi sistem target samapai sistem tidak dapat lagi memberikan layanannya (denial of service). Jalan menuju kelumpuhan bisa berbeda dan konsekuensinya juga bisa berbeda. Sistem yang diserang dapat rusak karena beban CPU yang tinggi, crash atau mempengaruhi kinerja sistem
c) Virus, worm, Trojan, menyebarkan virus, worm, atau Trojan dengan target untuk menghalangi sistem komputer, mendapatiinformasi dari sistem korban.

Langkah-langkah keamanan yang diterapkan juga harus memahami kemungkinan risiko terbesar terkait dengan kebiasaan penggunaan nasabah, dan sesuai dengan kepadatan jaringan dan besarnya dampak yang ditimbulkan oleh risiko tersebut. Berikut ini adalah daftar ancaman yang terkait dengan penggunaan sistem oleh nasabah:

a) DNS Hijacking,adalah ancaman keamanan komputer yang memungkinkan penyerang memposisikan dirinya antara klien dan server DNS. Penyerang kemudian dapat mengekstrak informasi dari klien dan mengirim kembali informasi yang salah ke klien sebelum informasi asli mencapai server DNS. Jenis serangan ini berdasarkan pada statistik siapa yang lebih pesat. Jika penyerang ingin serangan berhasil, penyerang wajib menanggapi informasi yang diterima dari klien sebelum data asli mencapai akses yang benar.
b) Phishing, adalah ancaman jarak jauh yang paling umum kepadafasilitas keuangan online. Penyerang menciptakan situs web mirip seperti situs web asli dan menggunakan situs web yang mirip dengan situs web asli sampai tidak mudah dicurigai. Penyerang kemudian mengirimkan email ke beberapa akun email yang isinya berisi link (alamat email palsu tersembunyi) yang bisa diklik. Penyerang kemudian meyakinkan korban bahwa mereka harus mengisi informasi tersebut karena ada perubahan pada aksesatau karena alasan memaksa lainnya, dan menawarkan hadiah tambahan berupa hadiah atau uang. Terakhir, korban mengklik tautan palsu dan memasukkan informasi pribadi yang dipakai dalam beberapa fasilitaa keuangan online. Penyerang selanjutnya menyalahgunakan informasi pribadi ini untuk mencurinya atau untuk tujuan negatif lainnya.

c) Typo Site, pelakunya memberikan nama dan alamat situs palsu yang mirip dengan situs aslinya. Pelaku menunggu korban salah memasukkan alamat dan membuat situs palsu. Dalam hal ini pelaku dapat dengan mudah mendapatkan data user dan password korban dan merugikan korban.
d) Interception, pihak yang tidak berwenang telah berhasil mengakses aset atau informasi Contoh dari ancaman ini yaitu penyadapan.

Kesalahan Yang Dilakukan Nasabah

Meskipun berbagai macam tindakan penjagaan telah dijalankan baik oleh bank atau nasabah sendiri, namun informasi nasabah tetap bisa dicuri jika nasabah sendiri selaku pemilik rekening melakukan kelalaian dalam mengakses rekeningnya. Berikut beberapa kelalaian yang sering dibuat pelanggan:

a) Password yang mudah ditebak, PIN, Password adalah tindakan keamanan pertama yang dihadapi pelanggan saat mencoba mengakses akun. Nasabah sering mengabaikan penggunaan kata sandi yang kuat.
b) Jaringan Internet yang tidak aman, mengabaikan jaringan internet yang dipakai nasabah juga merupakan bagian dari kesalahannasabah. Orang lain dapat dengan mudah mencuri informasi kita ketika kita memakai jaringan internet yang tidak aman. Kita wajib berhati-hati saat memakai internet, terutama saat kita berbagi internet dengan orang lain. Selain itu, pemakai VPN juga tidak disarankan, apalagi jika menggunakan VPN yang keamanannya tidak bisa dianggap remeh.
c) Anti Virus yang Kadaluarsa, perangkat kitaharus mempunyai perangkat lunak antivirus yang dapat menjamin keamanan perangkat kita agar tidak terinfeksi virus yang dapat mencuri informasi pribadi kita. Hampir semua program antivirus dapat dijamin, tetapi program antivirus yang sudah usang tidak dapat lagi menjamin keamanan penggunanya. Ini karena program antivirus tidak menerima pembaruan virus terbaru atau program antivirus mungkin berhenti bekerja jika sudah kedaluwarsa.
d) Jarang periksa akun, Peretas juga dapat menargetkan akun yang jarang diverifikasi. Pelanggan yang tidak memverifikasi ulang akunnya tidak akan menerima pembaruan atau kemajuan terbaru di akunnya. Hal ini juga bisa mengakibatkan nasabah tidak memahami apa yang terjadi pada rekeningnya, apakah uang masuk ke rekening atau uang ditarik yang tidak diketahui nasabah.

Langkah Pengamanan Yang Dilakukan Nasabah

Dari pembahasan terkait kelalain yang sering dilakukan nasabah, maka ada beberapa cara pengamanan yang wajib diperhatikan nasabah untuk mengoptimalkamn keamanan pada akun sistem e-banking yang dipakai:

a) Pastikansitus, pastikan nasabah mengunjungi situs web yang benar. Pencuri sering mencoba mengirimkan pesan penipuan yang berisi alamat situs web yang mirip dengan alamat asli Bank yamg telah dipalsukan.
b) Ubah kata sandi secara teratur, gunakan kata sandi atau PIN yang sulit ditebak, dan jangan pernah menggunakan tanggal lahir sebagai PIN Anda. Ganti juga password anda secara berkala agar tidak bocor.

c) Gunakan jaringan yang Aman, selalu memakai jaringan internet pribadi saat mengakses E-Banking. Jangan menggunakan jaringan bersama saat membuka E-Banking. Selain itu, pastikan jaringan yang Anda gunakan tidak terganggu oleh orang lain.
d) Antivirus yang diperbarui, pastikan antivirus perangkat Anda diperbarui secara berkala. Perlindungan virus yang diperbarui berisi data terbaru tentang virus yang dapat mencuri informasi Anda.

KESIMPULAN

Kemajuan internet banking di Indonesia berkembang cepat sesuai dengan kemajuan teknologi, permintaan pasar, geografi dan populasi. Pengarahan perbankan online dibutuhkan untuk menjauhi permasalahan di kemudian hari dan memudahkan pengawasan Bank Indonesia. Hal ini dipastikan dengan data dari temuan dan pengkajian ini mengenai beberapa persoalan keamanan online banking di atas, seperti:pembajakan DNS, phishing, dll. Ada juga kesalahan yang dilakukan oleh pelanggan yang juga menimbulkan masalah keamanan bagi bank online, akun yang jarang diperbarui dan kata sandi yang mudah ditebak. Seiring dengan upaya sadar (baik dari manajemen hingga pelanggan), tetapkan praktik/prosedur terbaik dan evaluasi sistem secara teratur.Sebagian hal yang harus diperhatikan oleh nasabah untuk menjaga keamanan akun E-bankingyaitu hindari membuka internet banking dari tempat umum seperti warnet. Karena aspek perlindungannya sangat rendah. Gunakan perangkat dengan firewall dan antivirus untuk meminimalkan terjadinya proses phishing.

DAFTAR PUSTAKA

Subsom, P, dan Limwiriyakul, S, 2011. *A Comparative Analysis of Internet Banking Security in Thailan : A Customer Perspective*. pp260-272.

Pratiwi, 2016. JUTISI. Penerapan *Sistem Biometrik pada Nasabah Pengguna ATM (Studi kasus IKPIA Perbanas Jakarta),* 5 (2), pp.1042–1047[3]

O. Andriyani, H. Cangara, dan S. Rhiza S, 2014. J. Komun. KAREBA. *Penggunaan Teknologi Informasi Online Dalam Kecepatan Pelayanan Dan Pengamanan Pada Bank BCA Makassar (Sebuah Studi Komunikasi Organisasi),* 3(1), pp.58–67

Ronny 2017. *Enam Kekuatan Layanan Jasa Internet banking Tinjauan Dari Presepsi Nasabah*. Surabaya.

Annisya, Rialda dan Hastuti, Maynina Norshela. 2012. *Security System Layanan Internet Banking PT. Bank Mandiri (Persero)* Tbk. Jakarta.

Hendarsyah, Decky, 2019. *Keamanan Layaan Internet Banking Dalam Transaksi Perbankan.* Sekolah Tinggi Ilmu Ekonomi (STIE) Syariáh Bengkalis.