Jurnal Salome: Multidisipliner Keilmuan
Vol. 1 No. 4 September 2023, hal. 207-217
e-ISSN: 2986-4968

ANALISIS KEAMANAN SISTEM INFORMASI MANAJEMEN DALAM PEMANFAATAN TEKNOLOGI INFORMASI TERHADAP PT BANK CENTRAL ASIA Tbk. (BCA)

Edy Susanto
Manajemen, Fakultas Ekonomi Dan Bisnis, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

Hendrick Moses
Manajemen, Fakultas Ekonomi Dan Bisnis, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

Rendy Ramadan
Manajemen, Fakultas Ekonomi Dan Bisnis, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

Shabina Deanova*
Manajemen, Fakultas Ekonomi Dan Bisnis, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia
shabinadeanova90@gmail.com

ABSTRACT

The development of Internet banking in Indonesia will increase rapidly in line with developments in technology, market demand, geographical location and population. Structuring internet banking operations is needed to avoid problems in the future and facilitate supervision by Bank Indonesia.

Keywords: System, Management Information, Technology, PT Bank Central Asia Tbk. (Bca)

ABSTRAK

Perkembangan Internet banking di Indonesia akan meningkat pesat sejalan dengan perkembangan teknologi, permintaan pasar, letak geografis dan jumlah penduduk. Penataan operasi internet banking diperlukan untuk menghindari permasalahan dimasa mendatang serta memudahkan pengawasan yang dilakukan oleh bank Indonesia.

Kata Kunci: Sistem, Informasi Manajemen, Teknologi, PT Bank Central Asia Tbk. (Bca)

PENDAHULUAN

Kemajuan teknologi, khususnya di bidang transportasi dan telekomunikasi, dianggap sebagai lokomotif yang mempercepat proses globalisasi di berbagai bidang kehidupan. Internet multifungsi telah muncul sebagai akibat dari pesatnya kemajuan teknologi komputer dan teknologi telekomunikasi. Jika dilihat dari perspektif konstruksi pengetahuan manusia yang dicirikan dengan cara berpikir yang borderless, perkembangan ini menempatkan kita pada ambang revolusi keempat dalam sejarah pemikiran manusia. Jaring membuat dunia menjadi bulat, seolah-olah hanya "selebar daun kelor".

Dalam skala global, perkembangan ini mengakibatkan perubahan tatanan sosial dan budaya yang signifikan dan mendasar. Namun dibalik kenyamanan penyedia internet tersebut, terdapat bahaya dari segi keamanan. Peningkatan inovasi data menciptakan web multifungsi dan konsekuensi positif dan negatif pada keberadaan manusia. Internet adalah jaringan komputer global yang memungkinkan individu, bisnis, institusi pendidikan tinggi, museum, bank, individu, dan stasiun televisi dan radio untuk berkomunikasi satu sama lain.

Karena jaringan internet publik dan global sangat rentan terhadap berbagai kejahatan, maka penting untuk memperhatikan keamanan sistem informasi berbasis internet. Bahaya muncul ketika

seseorang benar-benar ingin mendapatkan izin masuk ilegal ke organisasi PC, merusak organisasi, mengambil informasi dengan menggunakan teknologi canggih ini untuk mencapai tujuan dengan melakukan kesalahan yang merugikan banyak pihak. Cybercrime atau kejahatan dunia maya adalah nama yang diberikan untuk kejahatan ini.

Pengaruh perkembangan teknologi informasi, serta menyangkut aspek ekonomi dan sosial-sosial, juga menyangkut aspek hukum, karena TIK pada akhirnya membuat sisi gelap dalam kehidupan manusia, khususnya kehadiran segelintir orang yang menggunakan inovasi untuk penambahan individu untuk merugikan kelompok lain (kejahatan digital) sehingga membutuhkan aktivitas yang sah. terpisah (cyberlaw). Model kasus: Kategori ini mencakup penipuan terhadap lembaga keuangan, serta penipuan yang dilakukan saat melakukan pembelian online dengan kartu kredit atau debit. Pemerasan sambil berpura-pura menawarkan transaksi, klasifikasi misrepresentasi ini dapat dilakukan oleh dua pihak; individu dan bisnis. biasanya dalam bentuk investasi atau penjualan dan pembelian barang dan jasa. Penipuan pajak, penipuan dalam proses e-procurement, dan penipuan dalam layanan e-government termasuk dalam kategori ini. Tidak masalah jika anggota masyarakat menipu pemerintah atau jika birokrat menipu rakyat.

Penyuluhan dan pemahaman tentang dampak perkembangan teknologi informasi, diikuti dengan regulasi yang berkaitan dengan perkembangan teknologi informasi, seperti UU ITE No. 1, harus diberikan kepada masyarakat khususnya remaja yang saat ini sedang gandrung dengan website di internet dan memahami betul penggunaan internet, sehingga dapat mempelajari dampak negatif perkembangan teknologi informasi seperti internet dan pencegahan kejahatan cybercrime dari segi hukum. 11 Tahun 2008, yang melarang pencurian, penipuan, perjudian, pencemaran nama baik, dan pelanggaran lainnya.

Keunikan kejahatan digital sendiri di Indonesia semakin meluas dengan berbagai kasus, misalnya kasus penggunaan nama ruang Mustika Ratu. com, YKCI versus Indosat ('ring back tone' untuk kesetiaan). Kasus lain adalah pemusnahan kantor web banking BCA dengan membuat situs palsu www.klikbca.com oleh programmer, misalnya kilkbca.com, www.klickbca.com, klickbca.com, clickbca.com, satu model lagi telah terjadi di beberapa kota besar, misalnya di Yogyakarta, Bandung, Semarang, khususnya dengan tertangkapnya beberapa anak muda yang melakukan zalim digital dengan mode cek (pelanggaran web dengan membobol Visa untuk menukar dengan orang lain) yang menempatkan Indonesia salah satu negara di peta dalam kejahatan digital dan mode peretasan (penghancuran jaringan PC pihak lain). Kejadian mengejutkan lainnya melibatkan seorang hacker bernama Dani Hermansyah, yang pada 17 April 2004 meretas website www.kpu.go.id dan mengubah nama partai yang sudah ada menjadi pihak buah-buahan. Hal ini menurunkan kepercayaan masyarakat terhadap pemilu yang sedang berlangsung saat itu. Di Kota Surakarta sendiri, kasus kejahatan digital belum pernah mengemuka, namun yang terbaru adalah kasus pembobolan informasi melalui email oleh warga Pasar Kliwon. Kemajuan teknis yang cepat dapat mengakibatkan sejumlah masalah dengan keamanan data saat mengelola E-Banking di organisasi perbankan. Perlindungan fasilitas dan proses komputer terhadap gangguan yang disengaja atau tidak disengaja yang dapat menyebabkan perubahan, kerusakan, atau pencurian sumber daya sistem disebut sebagai kontrol dan keamanan sistem informasi memperoleh data secara tidak sah.

Berdasarkan paragraf diatas dijelaskan beberapa kasus yang sudah menimpa Bank BCA terhadap keamanan sistem informasi yang menganggu para nasabah dan juga tentunya menganggu operasioanal perusahaan. Kasus-kasus lain juga banyak menimpa bank di Indonesia bahkan sistem pemerintahan. Hal ini juga menjadi salah satu dampak dari kemajuan teknologi yang sangat siknifikan dan semakin

transparan, untuk itu penulis memilih untuk melakukan penelitian dengan materi pembahasan tentang analasis pemanfaatan keamaan sistem informasi terhadap Bank BCA yang tentunya berkaitan dengan permasalahan diatas.

METODE PENELITIAN

Desain Penelitian

Sebagian besar ahli dalam hal ini akan setuju, konfigurasi penelitian dapat diartikan sebagai rencana kerja yang disusun sejauh keterkaitan antar faktor secara lengkap sehingga hasil pemeriksaan dapat memberikan jawaban untuk mengeksplorasi pertanyaan. Menurut Umar (2007), rencana menguraikan kegiatan yang akan dilakukan peneliti, dimulai dengan perumusan hipotesis dan implikasi operasional dan diakhiri dengan analisis akhir.

Peneliti menggunakan strategi kuantitatif dalam melakukan hal ini. Pendekatan kuantitatif adalah metodologi penelitian yang didasarkan pada data positivistik (konkret); data penelitian berupa angka-angka yang akan diukur dengan menggunakan statistika sebagai alat penghitung tes; terkait dengan mata pelajaran yang dipelajari; dan terkait dengan kesimpulan yang akan ditarik. Pada beberapa populasi atau sampel diterapkan konsep positivistik (Sugiyono, 2018:13).

Sumber data dalam penelitian ini menggunakan data primer dan data sekunder yang mendukung penelitian mengenai Keamanan Sistem Informasi Manajemen Dalam Pemanfaatan Teknologi Informasi Terhadap PT Bank Central Asia Tbk (BCA).

Analisis Data

Menyusun, mengurutkan, mengklasifikasikan, memberi kode/tanda, dan mengkategorikan data agar sampai pada suatu masalah berdasarkan fokus atau pokok bahasan yang dibahas. Ketika peneliti mulai mengumpulkan data, pertama-tama mereka memilah informasi mana yang penting dan mana yang tidak. Kontribusi data dalam upaya mencapai tujuan kajian inilah yang dimaksud dengan ungkapan “langkah penting” atau “tidak” (Gunawan, 2013: 209).

Teknik yang digunakan untuk mengkaji informasi dalam penelitian ini adalah information handling system atau information programming, khususnya SPSS. Uji t dan uji hipotesis digunakan dalam penelitian ini untuk mengetahui ada atau tidaknya variabel dependen dipengaruhi oleh variabel independen.

Tahapan Penelitian

Menurut Husein Umar (1999), ada beberapa prosedur yang terlibat dalam melakukan analisis data kuantitatif. Berikut ini adalah proses yang terlibat dalam melakukan penelitian ilmiah dengan menggunakan pendekatan kuantitatif.:

1. Mencirikan dan mencari tahu masalah, khususnya masalah yang dihadapi harus direncanakan dan jelas.
2. Studi Perpustakaan, dalam mencari referensi teori yang relevan untuk masalah ini.
3. Memformulasikan Hipotesis yang diajukan.
4. Untuk dapat membayangkan kemungkinan setelah asumsi dibuat, tentukan Modelnya.
5. Mengumpulkan informasi, memanfaatkan informasi yang tepat tentang berbagai teknik dan berhubungan dengan strategi pemeriksaan yang digunakan.

6. Menggunakan teknik analisis data yang sesuai dengan maksud dan tujuan penelitian, mengolah dan menyajikan data.
7. Menganalisis dan menginterpretasikan hasil pengolahan data (pengujian hipotesis yang diajukan).
8. Generalisasi, menarik kesimpulan, dan membuat rekomendasi.
9. Siapkan laporan konklusif tentang temuan penelitian.

Populasi dan Sampel Penelitian

Populasi dalam penelitian ini adalah pengguna Aplikasi BCA *Mobile*. Pengambilan sampel dilakukan dengan menggunakan Teknik *purposive sampling* dengan kriteria pengguna aktif Aplikasi BCA *Mobile*, sehingga responden yang mengisi kuesioner dalam penelitian ini benar-benar pengguna dari Aplikasi BCA *Mobile*.

Dengan mempertimbangkan jumlah populasi yang banyak, keterbatasan waktu dan biaya, sejumlah 100 orang pengguna sistem menjadi sampel pada penelitian ini. Ukuran sampel yang sesuai adalah 100-200 responden agar dapat digunakan estimasi interprestasi menggunakan SPSS, hal ini dikarenakan apabila jumlah sampel terlalu besar akan menyulitkan dalam mendapat model yang tepat (Zarvedi et al., 2016)

Instrumen Penelitian

Instrumen penelitian yang digunakan peneliti adalah kuesioner yang terdiri dari 2 bagian, yaitu bagian pertama terdiri dari penjelasan penelitian dan bagian kedua merupakan bagian pengisian kuesioner yang terdiri dari pertanyaan terkait dengan profil responden dan pertanyaan terkait dengan analisis kepuasan pengguna Aplikasi BCA Mobile. Pertanyaan yang ada dalam kuesioner terdiri dari 2 bagian, diantaranya adalah :

1. Pertanyaan profil responden yang terdiri dari Nama, Jenis Kelamin, Umur.
2. Pertanyaan terkait dengan penelitian yang telah disusun berdasarkan indikator dari variabel.

Pilihan jawaban pada setiap pertanyaan dalam kuesioner disusun menggunakan 5 Skala Likert dengan penjelasan:

a. Angka 1 menunjukkan “Sangat Tidak Setuju”
b. Angka 2 menunjukkan “Tidak Setuju”
c. Angka 3 menunjukkan “Netral”
d. Angka 4 menunjukkan “Setuju”
e. Angka 5 menunjukkan “Sangat Setuju”

Teknik Analisis Data

Uji Validitas

Uji validitas dilakukan dengan bantuan software SPSS, kolom Corrected Item Total Correlation menampilkan nilai validitas. Item, pertanyaan, atau indikator dikatakan valid jika nilai r hitungnya positif dan lebih besar dari r tabel (Ghozali, 2011).

Uji Reliabel

Untuk mengukur suatu polling yang merupakan tanda suatu variabel termasuk padat atau tidak. Cronbach's Alpha (α) digunakan dalam uji statistik untuk menentukan apakah suatu variabel dapat dipercaya atau tidak. Ukuran yang digunakan adalah suatu variabel dianggap solid dengan asumsi memberikan nilai α > 0,70 (Ghozali, 2011).

Uji Normalitas

Dilakukan menggunakan uji statistik nonparametik Kolmogorov-Smirnov (K-S) dengan melihat Asymp. Sig. (2-tailed) apakah lebih besar dari 0,05, jika lebih besar maka data terdistribusi normal (Ghozali,2011). penelitian ini terbukti normal. Dan juga dapat didukung dengan melihat grafik histogram dan grafik normal P-P PlRA dibawah ini. Berdasarkan gambar dibawah dapat disimpulkan bahwa model regresi ini memenuhi asumsi normalitas yaitu dimana dapat dilihat dari titik – titik yang mengikuti arah garis diagonal. Jika data menyebar di sekitar garis diagonal dan mengikuti arah garis diagonal, maka model regresi memenuhi asumsi normalitas (Ghozali, 2011).

Uji Multikolonieritas

Bertujuan untuk menguji apakah model regresi ditemukan adanya korelasi antar variabel bebas (independen). Multikolonieritas dapat terlihat dari hasil Tolerance dan Variance Inflation Factor (VIF) yang terdapat dalam tabel Collinearity Statistic. Standar tidak terjadi multikolonieritas dalam penelitian ini adalah nilai Tolerance diatas 0,1 dan VIF kurang dari 10.

Uji Heteroskedastisitas

Bertujuan menguji apakah dalam model regresi terjadi ketidaksamaan variance dari residual satu pengamatan ke pengamatan lainnya. Dalam penelitian ini untuk mendeteksi ada atau tidaknya heteroskedastisitas digunakan uji Glejser yang dapat dilihat dari nilai probabilitas signifikasinya atas tingkat kepercayaan 5% atau heteroskedastisitas ditunjukkan dengan hasil uji signifikan Glejser dibawah 0,05. (Ghozali, 2011).

Uji statistik t

Merupakan pengujian untuk menunjukkan seberapa jauh pengaruh satu variabel independen secara individual dalam menjelaskan variabel dependen. Hasil dapat dilihat dari tabel Coefficients dengan standar pengaruh signifikan jika nilai Signifikansi t lebih kecil dari alpha kasus penelitian.

Uji statistik F

Merupakan model pengujian selain model pengujian stsistik t, uji ini untuk menunjukkan apakah setiap faktor otonom atau faktor bebas dalam model pengujian mempengaruhi variabel terikat. Hasil harus terlihat dari tabel ANOVA dengan norma dampak yang besar jika nilai kepentingan F lebih rendah daripada alfa kasus tinjauan.

Koefisien Determinasi

Sejauh mana model dapat memperhitungkan variasi dalam variabel dependen ditunjukkan oleh koefisien determinasi. Hasil temuan R-Square dengan nilai kontrol Adjusted R-Square dapat digunakan untuk menentukan nilai koefisien determinasi dari data. Nilai Adjusted R-Square harus positif untuk memperhitungkan data yang baik.

HASIL DAN PEMBAHASAN

Pembahasan ini difokuskan pada penelitian yang dimana menggunakan metode kuantitatif yang didasarkan pada data positivistik (konkret); data penelitian berupa angka-angka yang akan diukur dengan menggunakan statistika sebagai alat penghitung tes; terkait dengan mata pelajaran yang dipelajari; dan terkait dengan kesimpulan yang akan ditarik. Penelitian ini juga diihat dari pengguna Aplikasi BCA *Mobile*. Pengambilan sampel dilakukan dengan menggunakan Teknik *purposive sampling* dengan kriteria pengguna aktif Aplikasi BCA *Mobile*. Perkembangan pelayanan yang dilakukan prbankan berbasis teknologi *(electronic transaction)* dalam bentuk internet banking, mobile banking yang berbasis handphone *(phone banking)*, penggunaan ATM *(Authomatic Teller Machine), Credit Card* dan lain sebagainya merupakan keharusan bagi bank-bank di Indonesia untuk merebut pangsa pasar. *Online Banking* diperkenalkan sebagai *channel* dimana nasabah bank dapat melakukan aktivitas finansial perbankan secara elektronik melalui *website* bank. Nasabah dapat melakukan transaksi *non cash* setiap saat dengan mudah dan nyaman dengan mengakses melalui komputer (jaringan internet).

Layanan perbankan untuk transaksi keuangan banyak diberikan oleh bank dengan tujuan utama memberikan kemudahan nasabah dalam bertransaksi. Selain pelayananan di kantor bank, terdapat layanan menggunakan internet banking dan juga ATM. Saat ini nasabah lebih memilih bertransaksi melalui delivery channel alternatif seperti ATM, Internet Banking, SMS Banking, bukan lagi melalui antri di bank. Dengan semakin banyaknya transaksi berbasis online maka memicu meningkatnya penggunaan delivery channel alternative, contohnya seperti Internet Banking yang semakin sering digunakan oleh masyarakat. Penulis akan meneliti keamanan sistem informasi dari internet banking yang digunakan dalam dunia perbankan.

Aspek Keamanan

Menurut Dony Ariyus, keamanan komputer meliputi beberapa aspek diantaranya :

1. **Authentication**, Agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi.

2. **Integrity**, Keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh yang berhak dalam perjalanan informasi tersebut.
3. **Non-repudiation**, Non- repudiation merupakan hal yang bersangkutan dengan si pengirim. Si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. **Authority**, Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
5. **Confidentiality**, Confidentiality merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
6. **Privacy**, Privacy merupakan lebih mengarah pada data yang sifatnya pribadi.
7. **Availability**, Aspek ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan.
8. **Access control**, Aspek ini berhubungan dengan cara pengaturan akses kepada informasi.

Menurut Budi Rahardjo mengungkapkan bahwa aspek keamanan yang harus dijaga dari internet Banking adalah :

1. **Confidentiality**, Aspek confidentiality memberi jaminan bahwa data-data tidak dapat disadap oleh pihak-pihak yang tidak berwenang. Serangan terhadap aspek ini adalah penyadapan nama account dan PIN dari pengguna Internet Banking.
2. **Integrity**, Aspek integrity menjamin integritas data, dimana data tidak boleh berubah atau diubah oleh pihakpihak yang tidak berwenang. Salah satu cara untuk memproteksi hal ini adalah dengan menggunakan checksum, signature, atau certificate
3. **Authentication**, Authentication digunakan untuk meyakinkan orang yang mengakses servis dan juga server (web) yang memberikan servis. Mekanisme yang umum digunakan untuk melakukan authentication di sisi pengguna biasanya terkait dengan: - Sesuatu yang dimiliki (misalnya kartu ATM, chipcard) - Sesuatu yang diketahui (misalnya userid, password, PIN, TIN) - Sesuatu yang menjadi bagian dari kita (misalnya sidik jari, iris mata)
4. **Non-repudiation**, Aspek non-repudiation menjamin bahwa jika nasabah melakukan transaksi maka dia tidak dapat menolak telah melakukan transaksi. Hal ini dilakukan dengan menggunakan digital signature yang diberikan oleh kripto kunci publik (public key cryptosystem). Mekanisme konfirmasi (misal melalui telepon) juga merupakan salah satu cara untuk mengurangi kasus.
5. **Availability**, Aspek availability difokuskan kepada ketersediaan layanan. Jika sebuah bank menggelar layanan Internet Banking dan kemudian tidak dapat menyediakan layanan tersebut ketika dibutuhkan oleh nasabah, maka nasabah akan mempertanyakan keandalannya dan meninggalkan layanan tersebut.

Keamanan Pada Enthernet Banking

Dalam usaha pengamanan data nasabah, diperlukan kerjasama antar pihak Bank dan pihak nasabah untuk menjaga sistem keamanan dalam bertransaksi menggunakan jasa layanan yang diberikan oleh pihak manajemen bank. Berikut adalah usaha yang dapat dilakukan pihak bank untuk meningkatkan keamanan sistem pada bank :

1. **Sistem Cryptography**, Sistem ini menggunakan angka-angka yang dikenal dengan kunci (key).Sistem ini disebut juga dengan sistem sandi. Ada dua tipe cryptography, yaitu simetris dan asimetris. Pada sistem simestris menggunakan kode kunci yang sama bagi penerima dan pengirim pesan. Kelemahan dari cryptography simestris adalah kunci ini harus dikirim pada pihak penerima dan halini memungkingkan seseorang untuk mengganggu di tengah jalan.Sistemcryptography asimetris juga mempunyai kelemahan yaitu jumlah kecepatan pengiriman data menjadi berkurang karena adanya tambahan kode.Sistem ini biasanya digunakan untuk mengenali nasabah da melindungi informasi finansial nasabah .
2. **Firewall**, Firewall merupakan sistem yang digunakan untuk mencegah pihak- pihak yang tidak diijinkan untuk memasuki daerah yang dilindungi dalam unit pusat kerja perusahaan. Firewall berusaha untuk mencegah pihak-pihak yang mencoba masuk tanpa ijin dengan cara melipatgandakan dan mempersulit hambatan-hambatan yang ada. Namun, yang perlu diingatkan adalah bahwa sitem firewall ini tidak dapat mencegah masuknya virus atau gangguan yang berasala dari dalam perusahaan itu sendiri

Dalam usaha pengamanan data nasabah pun peran nasabah dalam melakukan tindakan keamanan akun pribadi juga sangat diperlukan. Berikut adalah usaha yang dapat dilakukan pihak nasabah untuk meningkatkan keamanan sistem pada bank :

1. **Device Registering**, Metode ini membatasi akses ke sistem perbankan melalui perangkat yang belum dikenal atau terdaftar pada sistem. Perangkat ini menggunakan scan sidik jari untuk identifikasi penggunanya
2. **CAPTCHA**, Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) adalah metode baru yang diadopsi pada beberapa sistem perbankan yang bertujuan untuk menangkal serangan otomatis terhadap sesi atau halaman konfirmasi pada website. Metode ini mengharuskan pengguna yang sah untuk memasukkan informasi yang ditampilkan dalam gambar atau audio secara acak dan sulit bagi program otomatis (robot otomatis) untuk mengenali dan memproses gambar atau audio tersebut sebagai input konfirmasi
3. **Positive Identification**, Positive Identification adalah suatu model di mana nasabah bank diminta untuk memasukkan beberapa informasi rahasia yang hanya diketahui nasabah tersebut dalam rangka untuk mengidentifikasi dirinya. Hal ini diterapkan sebagai metode otentikasi kedua.
4. **Username dan Password**, Pengamanan paling umum yang dapat dilakukan oleh Nasabah adalah Username dan Password. Sebelum nasabah dapat mengakses akun miliknya, nasabah harus memasukan beberapa karakter pengaman akunnya. Username dan Password terdiri dari beberapa karakter, tergantung dari pihak bank penyedia layanan. Beberapa bank juga menyediakan persyaratan khusus dalam penentuan jumlah karakter maupun jenis karakter yang digunakan untuk Username dan Password. Berikut adalah contoh syarat username dan password yang telah ditetapkan oleh bank BCA dana Bank Syariah Mandiri.

Jenis Serangan Pada E-Banking

Terdapat serangan -serangan hacker yang biasanya dilakukan untuk merusak sistem keamanan bank. Serangan ini dilakukan baik dari sisi sistem bank yang tersedia maupun pola penggunaan nasabah dalam menggunakan layanan. Dalam usaha pengamanan yang dilakukan, diperlukan juga pemahaman

kemungkinan risiko tertinggi baik dilihat dari tingkat keseringan jaringan maupun tingkat pengaruh atas dampak yang dihasilkan dari risiko berikut. Berikut adalah daftar risiko serangan dari sisi sistem layanan bank :

1. **Brute force attack**, atau dalam bahasa Indonesia disebut juga dengan serangan brute force ini adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci password yang memungkinkan atau istilah gampangnya mungkin menggunakan Random password atau password acak. Pendekatan inipada awalnya merujuk pada sebuah program.
2. **Denial of service (DoS) attack**, merupakan sebuah usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya(denial of servis). Cara untuk melumpuhkan dapat bermacammacam dan akibatnyapun dapat beragam. Sistem yang diserang dapat menjadi hang atau crash, tidak berfungsi, atau menurunnya kinerja sistem karena beban CPU menjadi tingi. komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia.
3. **Virus, worm, Trojan**, Menyebarkan virus, worm, maupun Trojan dengan tujuan untuk melumpuhkan sistem komputer, memperoleh data-data dari sistem korban.

Dalam usaha pengamanan yang dilakukan, diperlukan juga pemahaman kemungkinan risiko tertinggi dari sisi pola penggunaan layanan oleh nasabah, baik dilihat dari tingkat keseringan jaringan maupun tingkat pengaruh atas dampak yang dihasilkan dari risiko. Berikut adalah daftar risiko serangan dari sisi penggunaan sistem oleh nasabah :

1. **DNS Hijacking**, Merupakan suatu serangan keamanan jaringan komputer di mana penyerang dapat meletakkan dirinya di antara klien dan server DNS. Kemudian penyerang dapat mengambil informasi dari klien dan mengirimkan kembali informasi yang palsu ke klien sebelum informasi asli sampai ke server DNS. Tipe serangan ini bergantung dari kondisi siapa yang lebih cepat. Jika penyerang ingin serangannya berhasil, maka pernyerang harus membalas informasi yang diterimanya kepada klien sebelum informasi asli sampai ke server yang sesungguhnya.
2. **Phishing**, Merupakan serangan jarak jauh yang paling sering terjadi terhadap layanan keuangan online. Seorang penyerang membuat website persis sama dengan website aslinya dan menggunakan alamat website mirip dengan aslinya sehingga tidak mudah dicurigai. Kemudian penyerang mengirimkan e-mail ke sejumlah akun e-mail dimana isinya memberikan link (alamat website palsu yang tersembunyi) untuk diklik. Kemudian korban di yakinkan oleh penyerang bahwa harus mengisi data karena ada perbaikan di server atau dengan alasan lain yang meyakinkan serta memberikan embelembel berupa hadiah atau uang. Sehingga akhirnya korban mengklik link palsu dan memasukan datadata pribadi yang digunakan untuk layanan keuangan online tertentu. Kemudian data-data pribadi tersebut disalahgunakan oleh penyerang untuk mencuri ataupun untuk keperluan negatif lainnya
3. **Typo Site**, Pelaku membuat nama situs palsu yang sama persis dengan situs asli dan membuat alamat yang mirip dengan situs asli. Pelaku menunggu kesempatan jika ada seseorang korban salah mengetikan alamat dan sirus palsu buatannya. Jika hal ini terjadi maka pelaku akan mudah memperoleh informasi user dan password korbannya dan dapat dimanfaatkan untuk merugikan korban.
4. **Interception**, Pihak yang tidak berhak berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan.

Kesalahan yang Dilakukan Nasabah

Meskipun berbagai cara pengamanan telah dilakukan, baik dari pihak bank maupun dari pihak nasabah sendiri, data nasabah tetap dapat dicuri jika nasabah sendiri sebagai pemilik akun melakukan kesalahan-kesalahan dalam mengakses akun miliknya. Berikut ini beberapa kesalahan yang sering dilakukan oleh nasabah :

1. **Password Yang Mudah Ditebak**, PIN, Password atau Kata Sandi merupakan langkah pengamanan pertama yang dihadapi oleh nasabah ketika hendak mengakses akun. Seringkali nasabah mengabaikan pentingnya menggunakan kata sandi yang aman. Beberapa nasabah lebih sering menggunakan kombinasi karakter yang mudah mereka ingat seperti, 123456, 000000, abcdef, atau bahkan tanggal lahir mereka. Hal dihindari karena penggunaan kata sandi tersebut mudah ditebak orang
2. **Jaringan Internet Yang Tidak Aman**, Tidak memperhatikan jaringan internet yang digunakan oleh nasabah juga menjadi salah satu kelalaian dari nasabah. Informasi yang kita miliki dapat dengan mudah dicuri oleh orang lain jika kita menggunakan jaringan internet yang tidak aman. Kita perlu waspada dalam menggunakan jaringan internet apalagi ketika kita berbagi jaringan internet dengan orang lain. Disamping itu, penggunaan VPN tidak disarankan terutama penggunaan VPN yang tidak dapat dipertanggungjawabkan keamanannya.
3. **Anti Virus Yang Kadaluarsa**, Perangkat yang kita miliki tentunya harus memiliki software anti virus yang dapat menjamin keamanan perangkat kita agar tidak terjangkit virus yang dapat mencuri data pribadi kita. Hampir semua anti virus dapat dijamin perlindungannya, tapi anti virus yang telah kadaluarsa tidak dapat menjamin lagi keamanan dari penggunanya. Hal ini disebabkan karena anti virus tersebut tidak mendapatkan update terbaru tentang virus atau bahkan anti virus tidak dapat bekerja lagi jika telah melewati tanggal kadaluarsa
4. **Jarang Memeriksa Akun**, Akun yang jarang diperiksa juga dapat diserang oleh hacker. Nasabah yang tidak memeriksa lagi akunnya tidak akan mendapatkan update atau perkembangan terbaru dari akunnya. Hal ini juga dapat menyebabkan nasabah tidak mengetahui hal-hal apa saja yang telah terjadi pada akunnya, entah itu dana masuk ke rekening, ataupun penarikan dana yang tidak diketahui oleh nasabah sendiri.

Cara Pengamanan yang Perlu Dilakukan Nasabah

Dari ulasan terkait kesalahan yang sering dilakukan nasabah, maka berikut adalah cara pengamanan yang perlu dilakukan nasabah untuk meningkatkan keamanan pada akun sistem e-banking yang digunakan.

1. **Pastikan Situs**, Pastikan nasabah mengakses situs yang benar. Seringkali beberapa upaya yang dilakukan oleh pencuri adalah dengan mengirim pesan penipuan yang mencantumkan alamat website yang dibuat mirip dengan alamat asli milik bank yang ditiru
2. **Ganti Password Secara Berkala**, Gunakan kata sandi maupun PIN yang tidak mudah ditebak, dan usahakan jangan menggunakan tanggal lahir untuk PIN. Selain itu, pastikan juga untuk mengganti kata sandi secara berkala untuk menghindari jika kata sandi telah diketahui oleh pihak yang tidak berkepentingan

3. **Gunakan Jaringan yang Aman**, Gunakan selalu jaringan internet milik pribadi ketika mengakses Ibanking. Hindari penggunaan jaringan yang digunakan bersama ketika hendak mengakses Ibanking. Pastikan juga jaringan yang digunakan bebas dari intervensi dari pihak lain.
4. **Anti Virus Terupdate**, Pastikan anti virus yang dimiliki oleh perangkat sudah terupdate secara berkala. Anti virus yang telah diupdate memiliki informasi terbaru mengenai virus yang mungkin bisa menyerang atau mencuri informasi.

KESIMPULAN

Perkembangan Internet banking di Indonesia akan meningkat pesat sejalan dengan perkembangan teknologi, permintaan pasar, letak geografis dan jumlah penduduk. Penataan operasi internet banking diperlukan untuk menghindari permasalahan dimasa mendatang serta memudahkan pengawasan yang dilakukan oleh bank Indonesia.

Hal tersebut diperkuat dengan adanya informasi dari hasil dan pembahasan kami mengenai beberapa masalah keamanan internet banking diatas, seperti misalnya: DNS Hijacking, Phishing, dll. Selain itu, terdapat juga kesalahan yang dilakukan nasabah yang menyebabkan juga masalah keamanan internet banking seperti Jarang mengupdate akun dan memberi password yang mudah ditebak. Selain itu dengan usaha untuk meningkatkan Awareness (Baik dari manajemen hingga nasabah), membuat policy/prosedur yang baik dan mengevaluasi sistem secara berkala. Beberapa hal yang perlu dilakukan oleh nasabah untuk meningkatkan pengamanan akun e-banking pribadi antara lain; a) Hindari untuk mengakses Internet Banking dari tempattempat umum, seperti, warnet, dll. Karena aspek keamanannya sangat minimalis; b) Meminimalisir terjadinya proses phishing dengan menggunakan perangkat yang memiliki Firewall dan Antivirus.

DAFTAR PUSTAKA

Nurul Ichsan, R. (2020). Pengaruh Sistem Informasi Manajemen Terhadap Kinerja Pegawai Bpjs Ketenagakerjaan Cabang Medan. *Jurnal Ilmiah METADATA*, *2*(2), 128–136. https://doi.org/10.47652/metadata.v2i2.26

Rigawan, G., & Afriyeni, A. (2019). PENERAPAN SISTEM INFORMASI BANK PADA PT. BANK CENTRAL ASIA Tbk (BCA). *Jurnal Ekonomi Dan Keuangan*, 1–9.

Sabatini, N. S., Soesanto, H., & Sukresna, I. M. (2016). *Analisis Pengaruh Persepsi Manfaat, Kemudahan Dan Kepercayaan E-Banking Terhadap Reputasi Sistem Dalam Meningkatkan Minat Bertransaksi On Line Ulang (Studi Pada Nasabah Pt. Bank Central Asia Tbk Kcu Semarang)*. 1–14.

Safitri, E. M., & Larasati, A. S. (2020). Analisis Keamanan Sistem Informasi E-Banking Di Era Industri 4.0: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi Dan Robotika*, *2*(1), 12–16. https://doi.org/10.33005/jifti.v2i1.25