Cross-border
Vol. 6 No. 1 Januari-Juni 2023, page 653-663

p-ISSN: 2615-3165
e-ISSN: 2776-2815

SISTEM KEBIJAKAN OBJEK VITAL, PENGAMANAN FILE, DAN PENGAMANAN *CYBER* PT. BANK NEGARA INDONESIA (Persero) Tbk.

Edy Soesanto
Program Studi Teknik Perminyakan, Universitas Bhayangkara Jakarta Raya, Indonesia

Arya Bayu Sayeti
Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia

Nikken Syakira Haq*
Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia
nikkensyakira2401@gmail.com

Rewang Budi Prasetyo
Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia

ABSTRACT

To prevent unsettling influences and errors that can derail repair cycles, a viable and effective security framework is needed. Through the Presidential Decree of the Republic of Indonesia No. Pamobvitnas (National Vital Objects Security) of 2004 regulates how the National Police, the Government, and related stakeholders work together to strive to create national security stability and specifically organize security for vital object countries. This study used qualitative research. The research design used in this study is qualitative descriptive. Data obtained from research conducted at Bank Negara Indonesia branch offices. In addition to direct research into the field, data acquisition is also from various sources on the internet. The research location in this study is the Bank Negara Indonesia Branch Office which is located at Jl. Pramuka, Pengasinan, Kec. Rawalumbu, Kota Bekasi, West Java 17114. A circular instructing all branches to increase vigilance was issued in response to efforts to find out the situation and conditions before the robbery occurred. The general nature of the instructions in the Circular and the fact that they do not provide technical instructions on how to raise awareness and what actions should be taken to improve security pose obstacles in their implementation. Security management is designed to prevent unwanted things from happening in the company that cause a sense of insecurity and comfort in the company. Bank Negara Indonesia, which is engaged in Indonesian banking institutions, in addition to creating a safe and comfortable corporate environment for employees, must also maintain customer data properly so that it is not leaked and misused by irresponsible parties.

Keywords*: Vital objects, File Security, Cyber Security, Security Management.*

ABSTRAK

Untuk mencegah pengaruh dan kesalahan yang meresahkan yang dapat menggagalkan siklus perbaikan, diperlukan kerangka kerja keamanan yang layak dan efektif. Melalui Keputusan Presiden Republik Indonesia No. Pamobvitnas (Pengamanan Objek Vital Nasional) tahun 2004 mengatur bagaimana Polri,

Pemerintah, dan pemangku kepentingan terkait bekerja sama untuk mengupayakan terciptanya stabilitas keamanan nasional dan khususnya menyelenggarakan pengamanan bagi negara-negara objek vital. Penelitian ini menggunakan penelitian kualitatif. Desain penelitian yang digunakan dalam penelitian ini adalah deskriptif kualitatif. Data diperoleh dari penelitian yang dilakukan di kantor cabang Bank Negara Indonesia. Selain penelitian langsung ke lapangan, akuisisi data juga dari berbagai sumber di internet. Lokasi penelitian dalam penelitian ini adalah Kantor Cabang Bank Negara Indonesia yang beralamat di Jl. Pramuka, Pengasinan, Kec. Rawalumbu, Kota Bekasi, Jawa Barat 17114. Surat edaran yang menginstruksikan seluruh cabang untuk meningkatkan kewaspadaan dikeluarkan sebagai tanggapan atas upaya mengetahui situasi dan kondisi sebelum perampokan terjadi. Sifat umum dari instruksi dalam Surat Edaran dan fakta bahwa mereka tidak memberikan instruksi teknis tentang cara meningkatkan kesadaran dan tindakan apa yang harus diambil untuk meningkatkan keamanan menimbulkan hambatan dalam implementasinya. Manajemen keamanan dirancang untuk mencegah hal-hal yang tidak diinginkan terjadi di perusahaan yang menimbulkan rasa tidak aman dan nyaman di perusahaan. Bank Negara Indonesia yang bergerak di bidang institusi perbankan Indonesia, selain menciptakan lingkungan perusahaan yang aman dan nyaman bagi karyawan, juga harus menjaga data nasabah dengan baik agar tidak bocor dan disalahgunakan oleh pihak yang tidak bertanggung jawab.
Kata Kunci: Objek vital, Keamanan File, Keamanan Siber, Manajemen Sekuriti.

PENDAHULUAN

Pada umumnya ketertiban dalam negeri merupakan tanggung jawab Polri sebagai aparatur negara. Dapat disadari bahwa tanggung jawab utama Polri telah dituangkan dalam Pasal 13 Undang-Undang Nomor 2 Tahun 2002 yang mengatur tentang kewajiban Polri dalam memelihara keamanan masyarakat, melindungi masyarakat, melayani masyarakat, dan menjunjung tinggi hak asasi manusia dengan bantuan kemanusiaan (Yuhantini, 2020). Negara sedang dalam proses melaksanakan berbagai program pembangunan; Oleh karena itu, untuk mempercepat pembangunan tersebut, situasi negara yang aman dan kondusif harus menyertainya agar semua program prioritas nasional dapat berjalan lancar. Segala bentuk gangguan dan kejahatan yang akan menghambat atau menggagalkan program Pembangunan Nasional harus dicegah atau dihentikan.

Jadi untuk mencegah pengaruh dan kesalahan yang meresahkan yang dapat menggagalkan siklus perbaikan, diperlukan kerangka kerja keamanan yang layak dan efektif. Melalui Kepres RI No. Pamobvitnas (Keamanan Obyek Vital Nasional) Tahun 2004 ini mengatur bagaimana Polri, Pemerintah, dan pemangku kepentingan terkait bekerja sama untuk berusaha menciptakan stabilitas keamanan nasional dan secara khusus menyelenggarakan keamanan bagi negara objek vital tertentu berdasarkan Perpol No. 3 Tahun 2019 tentang Pemberian bantuan pengamanan dan Sistem Manajemen Pengamanan (SMP) (Romadhon, 2020). Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (disebut juga UUD 1945) menjamin usaha di bidang

lembaga keuangan pada alinea keempat Pembukaan yang menyatakan bahwa "melindungi segenap bangsa dan seluruh tumpah darah Indonesia" Teori teori Perlindungan hukum bagi seluruh warga negara Indonesia di bidang ekonomi, termasuk perlindungan hak-hak konsumen dan nasabah perbankan, telah ditetapkan dalam alinea keempat Pembukaan UUD 1945.

Manusia secara alami menginginkan keharmonisan dalam semua aspek kehidupan untuk menciptakan lingkungan yang aman dan menyenangkan. Sebagai makhluk sosial, manusia tetap melakukan kejahatan, khususnya pencurian, yang sulit dicegah karena kurangnya kontrol lingkungan, terutama di perkotaan (Al Azis Nisfani, 2021). Pemerintah Indonesia telah memberikan jabaran yang luas untuk menciptakan keamanan di dalam negeri, hal ini tercantum dalam Pembukaan Undang-Undang Dasar 1945 alinea keempat, dan dalam Ketetapan Majelis Permusyawaratan Rakyat Republik Indonesia No. IV/MPR/1999 tentang Garis garis Besar Haluan Negara 1999-2004 dalam huruf I angka 2 tentang Pertahanan dan Keamanan, serta dalam Amandemen Ke-IV Undang-Undang Dasar 1945 Bab XII tentang Pertahanan dan Keamanan Negara, Pasal 30 ayat (1). Untuk antisipasi dan perencanaan, keamanan juga menjadi hal yang krusial dalam dunia bisnis, baik itu di Perusahaan Negara maupun Perusahaan Swasta. Perusahaan telah mengambil tindakan dengan menggunakan jasa satpam dan petugas untuk menjaga keamanan di PT. Bank Negara Indonesia (Persero) Tbk.

Kebijakan yang masih berlaku serta masalah sosial yang baru muncul akan tunduk pada pemeriksaan kebijakan yang sedang berlangsung. Keamanan *cyber* adalah salah satu dari masalah ini. Ini berfungsi sebagai indikator utama keberhasilan kebijakan transformasi. Tidak ada cara untuk sepenuhnya mengesampingkan kemungkinan dampak negatif kebijakan, mengingat arah dan tujuan tujuan kebijakan yang tidak dapat disesuaikan dengan realitas social (Rudiatno & Cheryta, 2022).

Pada tanggal 5 Juli 1946, didirikan PT Bank Negara Indonesia (persero) Tbk atau BNI menjadi bank pertama milik negara yang lahir setelah kemerdekaan Indonesia. Lahir pada masa perjuangan kemerdekaan Republik Indonesia, BNI sempat berfungsi sebagai bank sentral dan bank umum sebagaimana tertuang dalam Peraturan Pemerintah Pengganti Undang-Undang No. 2/1946, sebelum akhirnya beroperasi sebagai bank komersial sejak tahun 1955. Pada tanggal 30 Oktober 1946, Oeang Republik Indonesia atau ORI resmi sebagai alat pembayaran pertama yang dicetak, diedarkan, dan dikeluarkan oleh Pemerintah Indonesia (Romdoni et al., 2018).

Berdasarkan uraian di atas, maka pembahasan dalam artikel ini ialah "Sistem Kebijakan Objek Vital Nasional, Pengamanan File, Dan Pengamanan *Cyber* PT. Bank Negara Indonesia (Persero) Tbk."

LANDASAN TEORI

Objek Vital

Istilah "objek", "tempat", "sasaran", atau "tujuan", dan "vital" berarti "sangat penting" dalam Kamus Besar Bahasa Indonesia (KBBI). Oleh karena itu, pengertian umum tentang objek vital nasional merupakan lokasi yang sangat penting bagi bangsa dan juga dapat disebut sebagai sumber daya nasional. Tempat Vital Nasional memegang peranan penting dalam kehidupan berbangsa dan bernegara. Harus dikaji secara menyeluruh dari segi ekonomi, politik, sosial, perbentengan, pertahanan, dan keamanan untuk memastikan tidak ada ancaman yang semakin besar terhadap byek Vital Nasional (Murdani, 2022).

Objek vital nasional memiliki peran yang sangat penting dan strategis dalam pembangunan suatu bangsa. Di sisi lain, keragaman risiko dan dampaknya memperluas dimensi keamanan ancaman dan gangguan. Ancaman dan gangguan Sistem ekonomi, stabilitas politik, dan keamanan negara semuanya terkena dampak, baik secara langsung maupun tidak langsung, oleh ancaman dan gangguan (Namudat et al., 2018).

Tujuan dilakukannya kegiatan pengamanan objek vital terhadap barang-barang penting adalah untuk memberikan rasa aman kepada nasabah dan pegawai bank, mengawasi orang-orang yang masuk ke dalam bank, mengingatkan nasabah yang keluar dari bank agar berhati-hati bila membawa uang dalam jumlah besar dan pihak kepolisian melakukan patroli di sekitar bank untuk mencegah hal-hal yang tidak diinginkan (Ulfiah, 2016). Obyek vital dalam PT. Bank Negara Indonesia yaitu memasang CCTV sebagai media teknologi dalam menjaga dan mengawasi kegiatan yang ada di lingkungan bank BNI. Dengan memasang CCTV, sudah dipastikan jangkauan pengawasan yang luas bisa dipantau oleh karyawan.

Pengamanan File

Masalah keamanan juga harus diperhitungkan saat mengelola bank data dan informasi. Sudut ini sangat penting untuk diingat bahwa mayoritas informasi bank adalah informasi sumber daya moneter yang dimiliki oleh pihak luar jumlah dan lalu lintas informasi sangat berfluktuasi cepat (Inggrawan, 2010). Dalam pengambilan informasi, dapat dimanfaatkan dengan cara yang sangat mudah karena informasi yang digunakan tipe yang sudah mahir dan tidak perlu menggunakan informasi tipe kronik. Informasi lanjutan paling sering digunakan oleh klien sekarang karena sangat efektif dan dapat disampaikan bersama dimanfaatkan dimana saja (Gunawan, 2021).

Dengan penggunaan data dalam bentuk file, sering kali terjadi penyerangan dan pembobolan data. Apabila data-data yang tersimpan itu terasa penting, pasti ada saja pihak-pihak yang tidak memiliki hak untuk melakukan pencurian data. Karena sangat mudah untuk menggunakan informasi dengan menggunakan penyimpanan media seperti *Cloud Drive*, pengguna tidak terlalu stres untuk menyimpan informasi lanjutan

mereka, karena informasi ini dapat diakses kapan saja dan di mana saja melalui ketersediaan web (Santiko & Rosidi, 2018).

Bank BNI mempunyai sistem pengamanan untuk menjaga data para nasabah dan melindungi dari kejahatan siber melalui Internet Banking yaitu sebagai berikut :

1. Menggunakan enkripsi SSL 128-bit Verisign bersama dengan sistem keamanan berstandar internasional. Lapisan pertama sistem keamanan BNI Internet Banking yang dikenal dengan SSL 128 bit (Secure Sockets Layer) banyak digunakan di industri perbankan. Dengan menggunakan SSL, semua data yang dikirim dari server BNI Internet Banking ke komputer klien dan kembali melalui proses enkripsi acak sistem dengan kode 128-bit yang hanya diketahui oleh komputer klien dan server BNI Internet Banking. Akibatnya, jika pihak lain menerima data transmisi, mereka tidak akan dapat menafsirkannya;
2. Keamanan entryways akses BNI Web Banking dengan firewall;
3. Dengan menggunakan PIN pada Kartu BNI Anda dapat melakukan pendaftaran Layanan BNI Internet Banking di ATM BNI;
4. Interaksi inisiasi melalui www.bni.co.id atau langsung ke https://ibank.bni.co.id menggunakan PIN pendaftaran dan nomor BNI Card yang digunakan untuk pendaftaran di ATM BNI;
5. Pada saat Pengguna mengaktifkan BNI Internet Banking, kombinasi alfanumerik alfabet dan angka digunakan untuk membuat User ID dan Password;
6. Pengguna BNI Internet Banking dapat mengubah kata sandinya setiap saat;
7. Sistem BNI Internet Banking memiliki *session timeout* yang menyebabkan pengguna logout sendiri;
8. Perangkat tambahan untuk penukaran uang menggunakan BNI e-Secure yang akan menghasilkan kombinasi angka yang terus berubah (PIN dinamis) setiap kali Nasabah melakukan penukaran.

Pengamanan *Cyber*

Menurut Ardiyanti, n.d., pengamanan siber adalah seperangkat instrumen, peraturan, prinsip keamanan, tindakan, pedoman risiko, strategi manajemen risiko, praktik terbaik, jaminan, dan teknologi yang dapat diterapkan untuk melindungi organisasi pengguna dan perangkat. Organisasi dan aset pengguna dalam cyber-security termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, dan sistem telekomunikasi. *Cyber-security* merupakan upaya untuk melindungi informasi dari adanya *cyber attack*, adapun elemen pokoknya adalah:

1. Dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi;
2. *Information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi hardware dan software. Contohnya adalah router, switch, server, sistem operasi, database, dan website;
3. *Perimeter Defense* merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan firewall.

4. *Network Monitoring System* merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan performance infrastruktur informasi;
5. *System Information and Event Management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan;
6. *Network Security Assessment* merupakan elemen cyber-security yang berperan sebagai mekanisme kontrol dan memberikan measurement level keamanan informasi;
7. *Human resource and security awareness* berkaitan dengan sumber daya manusia dan *awareness*-nya pada keamanan informasi.

Cyber-security merupakan salah satu upaya untuk menjamin pencapaian dan pemeliharaan properti keamanan organisasi dan aset pengguna terhadap potensi bahaya keamanan. Integritas di mana upaya untuk mengurangi timbulnya risiko dunia maya yang besar dimungkinkan adalah tujuan umum keamanan (Ardiyanti, 2014). Menurut (Ardiyanti, 2014), ada 5 area kerja digunakan untuk mengimplementasikan *cyber-security* secara global, antara lain:

1. Kepastian Hukum (*legalitas cyber-crime*);
2. Teknis dan tindakan prosedur;
3. Struktur Organisasi;
4. *Capacity building* dan pendidikan pengguna;
5. Kerjasama internasional.

Hal yang dilakukan oleh PT. Bank Negara Indonesia dalam menghindari ancaman siber agar nasabah aman dalam bertransaksi dan menyelamatkan data nasabah yaitu:

1. Mengedukasi Nasabah tentang Waspada *Phising Image*

   Phishing adalah jenis penipuan yang dilakukan oleh segelintir orang untuk mendapatkan informasi rahasia nasabah seperti user ID, PIN, dan informasi pribadi dengan berbagai cara, seperti :

   a. Membuat situs palsu yang memiliki alamat dan tampilan mirip dengan situs resmi milik Bank;
   b. Mengirim email atau SMS yang menginformasikan URL link atau login screen atau meminta nasabah login dengan cara memasukkan user ID dan PIN.

   Tips yang diberikan oleh Bank BNI untuk nasabah yaitu :

   a. Memastikan bahwa nasabah dalam mengakses BNI Internet Banking melalui *website* resmi situs BNI Internet Banking di www.bni.co.id dan klik tombol login, atau langsung ke halaman login BNI Internet Banking di https://ibank.bni.co.id;

b. Dipastikan untuk nasabah menghindari mengakses halaman web dengan meng-klik alamat URL/link yang mengarahkan untuk nasabah membuka halaman web palsu.

2. Mengedukasi Nasabah tentang Waspada *Malware Image*

Malware image yaitu perangkat lunak berbahaya, juga dikenal sebagai malware, adalah perangkat lunak yang dirancang untuk merusak, menghapus, menyembunyikan, dan bahkan mencuri data.

Virus adalah program yang menginfeksi komputer dan berpotensi merusak sistem, aplikasi, dan data di dalamnya. Umumnya digabungkan dengan dokumen yang memerlukan eksekusi dari pemilik PC.

Worm adalah sejenis virus yang mampu menggandakan diri. Jika worm telah memasuki PC atau organisasi PC, worm dapat berpindah ke PC lain dalam jaringan secara alami.

Spyware adalah program pengawasan yang dirancang untuk mencuri ID pengguna dan kata sandi serta informasi rahasia lainnya. ***Trojan*** sejenis virus yang menyamar sebagai berkas lain yang aman sehingga dapat mengelabui pengguna komputer.

Trojan terjadi saat PC yang tercemar dapat merusak atau mengambil data penting, termasuk ID klien dan kata sandi.

Tips yang diberikan oleh Bank BNI untuk nasabah yaitu :

a. Memastikan computer yang digunakan oleh ansabah bersih dari *malware, worm, trojan* atau *spyware* dan lakukan *scanning* dengan software anti virus secara rutin;
b. Hindari mengakses atau men-download file/program di halaman web yang tidak dikenal/tidak dapat dijamin keamanannya;
c. Pastikan *firewall* pada sistem operasi di komputer nasabah dalam keadaan aktif atau install personal firewall untuk mengamankan komputer nasabah.

METODE PENELITIAN

Desain Penelitian

Pembahasan yang dijadikan sebagai penelitian, maka penelitian ini menggunakan penelitian kualitatif. Desain penelitian yang digunakan dalam penelitian ini yaitu deskriptif kualitatif. Menggunakan desain penelitian ini karena penelitian ini memiliki tujuan untuk menemukan fakta dan meninjau tentang objek vital, pengamanan file, dan keamanan *cyber* yang ada di PT. Bank Negara Indonesia (Persero) Tbk.

Analisis Data

Model analisis data yang digunakan dalam penelitian ini adalah metode analisis deskriptif kualitatif. Data yang diperoleh dari penelitian yang telah dilakukan di kantor

cabang Bank Negara Indonesia. Selain penelitian langsung ke lapangan, perolehan data juga dari berbagai sumber di internet.

Lokasi Penelitian

Lokasi penelitian dalam penelitian ini adalah Kantor Cabang Bank Negara Indonesia yang beralamatkan di Jl. Pramuka No.8-9, RT.001/RW.017, Pengasinan, Kec. Rawalumbu, Kota Bks, Jawa Barat 17114.

HASIL DAN PEMBAHASAN

Gambaran tentang PT. Bank Negara Indonesia (Persero) Tbk

PT Bank Negara Indonesia (Persero) Tbk (atau biasa disebut sebagai "BNI") pada mulanya bertempat tinggal di Indonesia sebagai bank nasional dengan nama "Bank Negara Indonesia" mengingat Peraturan Pemerintah Pengganti Peraturan No. 1946 tanggal 5 Juli 1946. Disamping itu mengingat Peraturan No. 17 Tahun 1968, BNI diberi nama "Bank Negara Indonesia 1946", dan merupakan bank umum milik negara. UU No. 2 juga menegaskan bahwa BNI adalah bank yang memiliki mandat untuk membantu perekonomian rakyat dan berkontribusi dalam pembangunan nasional ditetapkan UU No. 17 Tahun 1968 tentang Bank Negara Indonesia 1946.

Saat ini BNI memiliki 978 cabang di seluruh Indonesia dan 5 di luar negeri (Singapura, Hong Kong, Tokyo, New York dan London), serta kantor agen di beberapa negara, seperti di Timur Tengah. dilengkapi dengan jaringan penyaluran kredit yang meliputi 63 cabang berdiri sendiri, 20 Sentra Kredit Menengah (SKM), 51 Sentra Kredit Kecil (SKC), 112 Unit Kredit Kecil (UKC), dan 54 Cabang Syariah. Untuk penyelenggaraan elektronik, BNI memiliki 2.350 ATM selain 6.900 ATM. untuk transaksi perbankan, dengan banyak fitur.

Gambaran tentang Objek Vital PT. Bank Negara Indonesia (Persero) Tbk

Bentuk pengamanan baik terbuka maupun tertutup digunakan dalam strategi pengamanan yang diterapkan Bank BNI. Petugas Pengamanan Bank BNI merupakan pelaksana utama pengamanan terbuka di Bank BNI, sedangkan Divisi Pengendalian Intern merupakan pelaksana utama pengamanan tertutup. Pelaksanaan patroli dalam rangka pengamanan terbuka hanya dilaksanakan dalam lingkup kantor cabang utama Bank BNI dengan berjalan kaki.

Pasca terjadinya perampokan, pengamanan yang menggunakan peralatan elektronik dan mekanik, termasuk penggunaan CCTV di seluruh cabang dan kantor pusat, menunjukkan bahwa pelaksanaannya impulsif dan tidak direncanakan dengan baik. Surat Edaran yang menginstruksikan seluruh cabang untuk meningkatkan kewaspadaan dikeluarkan sebagai respon atas upaya mengetahui situasi dan kondisi sebelum terjadi perampokan. Sifat umum dari instruksi dalam Surat Edaran dan fakta bahwa mereka tidak memberikan petunjuk teknis tentang bagaimana meningkatkan kesadaran dan tindakan apa yang harus diambil untuk meningkatkan keamanan menimbulkan hambatan dalam pelaksanaannya.

Jaminan keselamatan yang difokuskan di Bank BNI belum didasarkan pada kemungkinan kelemahan yang diketahui. Sasaran pengamanan yang dilakukan di Bank BNI mengingat sumber daya organisasi untuk jenis struktur, peralatan dan stok lainnya, informasi dan data nasabah yang diingat untuk misteri bank, latihan fungsional perbankan, otoritas organisasi (Direktur Utama), dan sumber daya Inovasi Data Bank BNI.

Gambaran tentang Pengamanan File PT. Bank Negara Indonesia (Persero) Tbk

Hal yang dilakukan oleh PT. Bank Negara Indonesia dalam pengamanan file data nasabah yaitu sebagai berikut:

1. Dalam penggunaan internet banking, Bank BNI mengarahkan nasabah untuk memasukkan kata sandi numerik dan *biometric* (sidik jari). Penerapan biometric ini bertujuan untuk menghindari terjadinya kata sandi numerik yang mudah diketahui orang di sekitar nasabah saat melakukan transaksi;
2. Bank BNI menerapkan dua Langkah keamanan dalam nasabah melakukan transaksi yaitu memasukkan pin ATM dan password transaksi. Hal ini untuk menghindari kejadian kejahatan siber yang dapat meretas informasi pribadi nasabah yang merugikan.

Gambaran tentang Pengamanan *Cyber* PT. Bank Negara Indonesia (Persero) Tbk.

Hal yang dilakukan oleh PT. Bank Negara Indonesia dalam pengamanan *cyber* nasabah yaitu sebagai berikut:

1. Memastikan bahwa nasabah bertransaksi di website resmi Bank BNI;
2. Jangan memberikan kode otp kepada siapapun;
3. Memastikan bahwa nasabah paham soal virus yang ada di komputer maupun ponsel. Karena jika kedua perangkat tersebut terkena virus yang membahayakan, sangat disayangkan data nasabah dapat bocor dan akan disalah gunakan oleh orang lain.

KESIMPULAN

Berdasarkan uraian hasil dan pembahasan penelitian di atas, maka penulis dapat menyimpulkan bahwa manajemen sekuriti sangat penting di setiap perusahaan. Khususnya dalam industri perbankan, system kebijakan objek vital, pengamanan file, dan pengamanan *cyber* sangat penting guna kepentingan data nasabah. Pasca terjadinya perampokan, pengamanan yang menggunakan peralatan elektronik dan mekanik, termasuk penggunaan CCTV di seluruh cabang dan kantor pusat, menunjukkan bahwa pelaksanaannya impulsif dan tidak direncanakan dengan baik. Sifat umum dari instruksi dalam Surat Edaran dan fakta bahwa mereka tidak memberikan petunjuk teknis tentang bagaimana meningkatkan kesadaran dan tindakan apa yang harus diambil untuk meningkatkan keamanan menimbulkan hambatan dalam pelaksanaannya.

Dalam penggunaan internet banking, Bank BNI mengarahkan nasabah untuk memasukkan kata sandi numerik dan biometric (sidik jari). Jadi untuk mencegah pengaruh dan kesalahan yang meresahkan yang dapat menggagalkan siklus perbaikan, diperlukan kerangka kerja keamanan yang layak dan efektif. Tujuan dilakukannya kegiatan pengamanan objek vital terhadap barang-barang penting adalah untuk memberikan rasa aman kepada nasabah dan pegawai bank, mengawasi orang-orang yang masuk ke dalam bank, mengingatkan nasabah yang keluar dari bank agar berhati-hati bila membawa uang dalam jumlah besar dan pihak kepolisian melakukan patroli di sekitar bank untuk mencegah hal-hal yang tidak diinginkan (Ulfiah, 2016).

Manajemen sekuriti dirancang untuk mencegah terjadinya hal yang tidak diinginkan dalam perusahaan yang menyebabkan timbulnya rasa tidak aman dan nyaman dalam perusahaan. Bank Negara Indonesia yang bergerak di lembaga perbankan Indonesia selain menciptakan lingkungan perusahaan yang aman dan nyaman untuk karyawan, harus juga data nasabah dijaga dengan baik agar tidak bocor dan disalah gunakan oleh pihak yang tidak bertanggung jawab.

DAFTAR PUSTAKA

Al Azis Nisfani, M. V. (2021). PERAN ORGANISASI MASYARAKAT FBR DALAM MENINGKATKAN KEAMANAN DAN KETERTIBAN LINGKUNGAN SEBAGAI UPAYA PENCEGAHAN PENCURIAN SEPEDA MOTOR DI WILAYAH KAVLING BNI 46 KECAMATAN JATI ASIH KOTA BEKASI. *Jurnal Kybernan*, *12*(1).

Ardiyanti, H. (n.d.). *CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA*. http://kominfo.go.id/index.php/content/detail/3980/

Ardiyanti, H. (2014). CYBER-SECURITY DAN TANTANGAN PENGEMBANGANNYA DI INDONESIA. *Jurnal POLITICA*, *5*(1). http://kominfo.go.id/index.php/content/detail/3980/

Gunawan, I. (2021). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *TECHSI - Jurnal Teknik Informatika*, *13*(1), 14. https://doi.org/10.29103/techsi.v13i1.2395

Inggrawan, A. Y. (2010). STUDI TENTANG CITRA PERUSAHAAN MELALUI KREDIBILITAS PERUSAHAAN PADA PT BNI (PERSERO) TBK DI SEMARANG. *JURNAL SAINS PEMASARAN INDONESIA*, *IX*(1), 32–44.

Murdani, R. (2022). *PENGATURAN PENGAMANAN OBJEK VITAL NEGARA YANG DILAKUKAN OLEH KEPOLISIAN (studi di Polda Nusa Tenggara Barat)*. 17.

Namudat, H., Karlina, N., & Rusli, B. (2018). ANALISIS KEBIJAKAN PENGAMANAN OBJEK VITAL DI PT FREEPORT INDONESIA. *Responsive*, *1*(2), 39–44.

Romadhon, M. I. (2020). Peran Sabhara dalam Mencegah Terjadinya Kericuhan dalam Pesta Demokrasi Pemilu 2019 di Wilayah Hukum Polres Salatiga. *Indonesian Journal of Police Studies*, *4*(1), 359–408.

Romdoni, M. R., Saepul, N., & Usmanti, R. L. (2018). PENGARUH KUALITAS LAYANAN M-BANKING DAN INTERNET BANKING TERHADAP KEPUASAN NASABAH PT. BANK NEGARA INDONESIA (PERSERO) TBK.CABANG TANJUNGPINANG. *Bangkit Indonesia*, *VII*(01).

Rudiatno, & Cheryta, A. M. (2022). EVALUASI KEBIJAKAN CYBER SECURITY SEKTOR PERBANKAN BANK BTN CABANG SURABAYA EVALUATION OF CYBER SECURITY POLICY IN THE BANKING SECTOR OF BANK BTN SURABAYA BRANCH. *Jurnal Apresiasi Ekonomi*, *10*(3), 321–331.

Santiko, I., & Rosidi, R. (2018). PEMANFAATAN PRIVATE CLOUD STORAGE SEBAGAI MEDIA PENYIMPANAN DATA E-LEARNING PADA LEMBAGA PENDIDIKAN. *JURNAL TEKNIK INFORMATIKA*, *10*(2), 137–146. https://doi.org/10.15408/jti.v10i2.6992

Ulfiah, S. F. (2016, February). *Cegah Krimanalitas Di Obyek Vital, Anggota Sat Sabhara Polres Pohuwato Melaksanakan Pengamanan Bank*. Https://Tribratanews.Gorontalo.Polri.Go.Id/Polres-Pohuwato/11016/Cegah-Krimanalitas-Di-Obyek-Vital-Anggota-Sat-Sabhara-Polres-Pohuwato-Melaksanakan-Pengamanan-Bank/.

Yuhantini, N. K. H. (2020). Tujuan Kewenangan Antara Satpol PP dan POLRI dalam Menciptakan Ketertiban dan Keamanan. *Jurnal Kertha Semaya*, *8*(6), 961–971.