ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 185-190
Volume 7 Nomor 1 Tahun 2023

Keamanan Aset Informasi pada Pt.Pln Tuntungan

Nurkosrina Aisah[1], Naila Umniati[2], Muhammad Dedi Irawan[3]

[1,2,3] Fakultas Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara

email: nurkosrina4@gmail.com[1], nailaumniati9@gmail.com[2], muhammaddediirawan@gmail.com[3]

Abstrak

PT PLN (Persero) merupakan salah satu perusahaan besar di Indonesia yang juga diaungi oleh pemerintah atau yang biasa disebut BUMN. Perusahaan ini adalah perusahaan yang mengatur segala aktivitas kelistrikan di Indonesia.Pada PT PLN tentu terdapat banyak sekali data pengguna dari konsumen listrik, tak jarang data tersebut banyak dicuri dan digunakan untuk keperluan pribadi. Keamanan sistem informasi ialah suatu langkah-langkah, serta pengukuran teknis yang dilakukan guna menghalangi saluran yang tidak legal, terjadinya susunan program yang berbeda, adanya pengambilan data, atau rusaknya bagian luar terhadap sistem informasi.Ancaman keamanan informasi dapat berupa seseorang, kelompok, mekanisme, atauperistiwa yang bisa memungkinkan timbulnya kejahatan pada sumber daya informasi. Maka dari itu keamanan pada sistem informasi yang digunakan harus benar terjamin terhadap batasan yang dapat diterima.Pentingnya nilai informasi berarti seringkali hanya orang-orang tertentu saja yang mendapatkan informasi yang diinginkan. Informasi yang sampai ke tangan pihak lain (misalnya mitra bisnis) dapat merugikan kepunyaan informasi tersebut. Ancaman keamanan adalah orang, organisasi, mekanisme, dll Peristiwa yang berpotensi merugikan aset informasi Perusahaan. Tujuan dilakukannya penelitian tersebut adalah untuk mengetahui sistem keamanan seperti apa yang diterapkan oleh PT PLN UPTD Tuntungan dalam melindungi data-data karyawan serta konsumen pemakai listik agar datanya tidak dicuri dan disalahgunakan. Dan disini kami menggunakan metode pengumpulan data dengan melakukan observasi dan wawanacara.

Kata Kunci: PT PLN, Sistem Informasi, Ancaman

Abstract

DictionaryPT PLN (Persero) is one of the large companies in Indonesia which is also covered by the government or commonly called BUMN. This company is a company that regulates all electrical activities in Indonesia.At PT PLN, of course there is a lot of user data from electricity consumers, not infrequently the data is stolen and used for personal interests. Information system security is a procedure, and technical measurements are carried out to prevent unauthorized access, the occurrence of different program structures, data theft, or physical damage to information systems.mAn information security threat can be a person, group, mechanism, or events that could allow crime to arise on information resources. Therefore, the security of the information system used must be properly guaranteed within acceptable limits.The importance of the value of information means that often only certain people get the information they want. Information that reaches other parties (e.g. business partners) may be detrimental to the owner of the information. Security threats are people, organizations, mechanisms, etc. Events that have the potential to harm the Company's information assets.nThe purpose of this research is to find out what kind of security system is implemented by PT PLN UPTD Tuntungan in protecting the data of employees and consumers who use electricity so that their data is not stolen and misused.

Keywords: PT PLN, Information Systems, Threats

PENDAHULUAN

Pengamanan adalah upaya untuk menghindari terjadinya atau ancaman kejahatan yang mengganggu. Keamanan harus mencakup elemen seperti perlindungan, integritas, keaslian data, danhak akses.Informasi adalah suatu pesan atau gabungan perintah yang terdiri dari sekumpulan lambang atau definisi yang terurut yang bisa diartikan dari pesan atau gabungan perintah tersebut. Data bisa disimpan maupun dikirim. Hal ini dapat direkam sebagai lambang atau simbol berbasis saluran. Menurut ISO/IEC 17799: 2005 tentang sistem manajemen keamanan informasi, bahwa keamanan informasi adalah usaha proteksi terhadap beragam bahaya untuk menjamin kelangsungan bisnis, meminimalkan risiko bisnis serta memajukan investasi dan harapan bisnis.

PT. PLN (Persero) adalah salah satu Badan Usaha Milik Negara yang membenahi semua kepentingan bidang listrik bagi rakyat Indonesia[1]. Diantaranya masalah yang timbul adalah aliran listrik ke konsumen dari PT PLN. Aliran arus ini bisa terdeteksi saat mitra usaha, atau sering disebut meteran listrik, terus mendeteksi arus meski peralatan elektronik sedang tidak digunakan. Hal ini disebabkan kebocoran aliran listrik yang pada dasarnya dilakukan tanpa keinginan dan sepengetahuan kami.

Tujuan dilakukannya penelitian tersebut adalah untuk mengetahui sistem keamanan seperti apa yang diterapkan oleh PT PLN UPTD Tuntungan dalam melindungi data-data karyawan serta konsumen pemakai listik agar datanya tidak dicuri dan disalahgunakan. Apabila terjadi kebocoran data tidak hanya pihak yang memakai listrik saja yang dirugikan tetapi juga pihak PLN dan tertunya akan berdampak terhadap nama baik PT PLN sendiri dan serta pihak konsumen dapat saja mengadukan pada pihak yang berwajib dan juga menuntut PT PLN untuk melakukan ganti rugi.

PT PLN (Persero) merupakan BUMN yang menyuplai bidang kelistrikkan di Indonesia[2]. Teknologi informasi merupakan sumber daya yang begitu penting baik bagi perusahaan atau instansi pemerintah yang menjalankan teknologi informasi pada setiap kegiatan bisnisnya[3]. Teknologi informasi pula memainkan kiprah krusial pada organisasi[4]. Sistem informasi berkomputerisasi adalah suatu bagian terpenting bagi perusahaan untuk mengelola seluruh kegiatan perusahaan[5]. Setiap perusahaan memiliki sistem dasar yaitu rangkaian tindakan yang dihubungkan kedalam suatu struktur yang terintegrasi dalam mencapai tujuan perusahaan[6].

Listrik sudah menjadi kebutuhan pokok manusia yang cukup untuk menunjang berbagai kegiatan baik itu dalam bekerja, belajar dan beragam kegiatan yang lain, di mana hampir semua kegiatan manusia didukung oleh listrik[7]. Bocornya listrik bisa disebabkan oleh arus listrik yang merambat dari saluran fasa (tegangan) ke bumi yang disebabkan bocornya isolasi pada pemasangan kabel yang buruk atau masalah pada alat yang dipakai sehingga menyebabkan percikan api yang bisa merusak instalasi listrik[8].

Selain kebocoran listrik ada juga yang disebut dengan kebocoran data, Kebocoran data adalah istilah yang dipakai dalam menyebut pengunggahan data-data pribadi yang bersifat sensitif oleh pengguna ke internet secara berlebihan. Biasanya pengguna yang melakukan hal ini sering mengabaikan dampak yang akan terjadi.Untuk mengatasi aliran data, tim analisis kinerja karyawan dibentuk. Kinerja pegawai merupakan pencapaian kerja yang dilakukan oleh seorang karyawan dalam melaksanakan tugas berdasarkan pada tanggung jawab yang dibebankan kepadanya[9].

PT PLN (Persero) merupakan perusahaan monopoli listrik negara yang dikenal memiliki aset besar, juga perlu memantau kinerja keuagannya. Jadi baik buruknya kinerja PLN sangat berdampak besar terhadap penerimaan Negara, yang berdampak besar pula terhadap pertumbuhan ekonomi Negara[10]. PT PLN (Persero) Udiklat Tuntungan pada mulanya dibangun sekitar tahun 1973 yang diberi nama Institut Pendidikan dan Pelatihan. Selanjutnya pada tanggal 17 maret 1980 Direksi PT PLN (Persero) memutuskan menjadi hari jadi PT PLN (Persero) Udiklat Tuntungan yang berlokasi di Jl. Lapangan Golf No. 35 Tuntungan Kecamatan Pancur Batu Kabupaten Deli Serdang Sumatera Utara.

METODE

Tempat Penelitian

Penelitian yang dilakukan bertempat di PT PLN (Persero) Udiklat Tuntungan yang beralamatkan di Jl. Lapangan Golf No. 35 Tuntungan Kecamatan Pancur Batu Kabupaten Deli Serdang Sumatera Utara.

Metode Pengumpulan Data

Tahapan pengumpulan data yang kami lakukan adalah sebagai berikut :

1. Observasi *(Observation)*; pada tahap ini kami langsung menngunjungi dan melakukan penelitian pada PT.PLN (Persero) Tuntungan agar memahami secara langsung apa kesulitan dan masalahannya selanjutnya dianalisa secara menyeluruh terpenting bagi sistem yang ada/saat ini.
2. Wawancara (*Interview*); pada metode ini melakukan beberapa tanya jawab yang dilakukan dengan orang terdekat.

Metode Analisa data

Metode analisis data merupakan tahapan proses penelitian di mana data yang terkumpul diolah sebagai jawaban atas rumusan masalah termasuk pengelolaan dan pengolahan data. Metode ini akan digunakan untuk mengetahui permasalahan yang dihadapi di PT.PLN (Persero) Tuntungan dan untuk mendapatkan informasi yang dibutuhkan untuk penyusunan penelitian.

Pembuatan Laporan

Laporan merupakan suatu cara penyajian fakta mengenai yang berkaitan dengan suatu keadaan atau kegiatan. Pada metode ini segala hasil observasi, wawancara , dan juga analisis data dikumpulkan menjadi satu membentuk sebuah laporan.

Metode Pengujian *(Testing)*

Teknik Pengujian adalah metode yang diterapkan untuk mengevaluasi suatu sistem atau komponen dengan tujuan untuk mengetahui apakah masih adanya kekurangan maupun ketidaklengkapan pada laporan yang dijelaskan.

HASIL DAN PEMBAHASAN

Pengetahuan dan informasi berkaitan erat dengan konsep sistem pemberitahuan sebagai salah satu komponen penting dalam pembentukan sistem informasi. Data merupakan nilai, status, atau kepunyaan yang berkarakter individual dan tidak tergantung konteks. Sistem informasi, pada sisi lain merupakan data yang sudah dijalankan dalam karakter yang berguna untuk penerimanya dan berguna untuk hasil sekarang atau masa depan.

Pertumbuhan teknologi informasi menyuruh pekerjaan pengembangan dalam dan luar perusahaan, yang telah menjadikan teknologi informasi sebagai bagian penting dari semua proses dan aktivitas bisnis yang mendukung pertumbuhan perusahaan dan pemerintah. Teknologi informasi ikut mengambil peran penting pada organisasi. Sepanjang waktu, TI tidak hanya menjadi pendukung tetapi juga kebutuhan dalam organisasi.

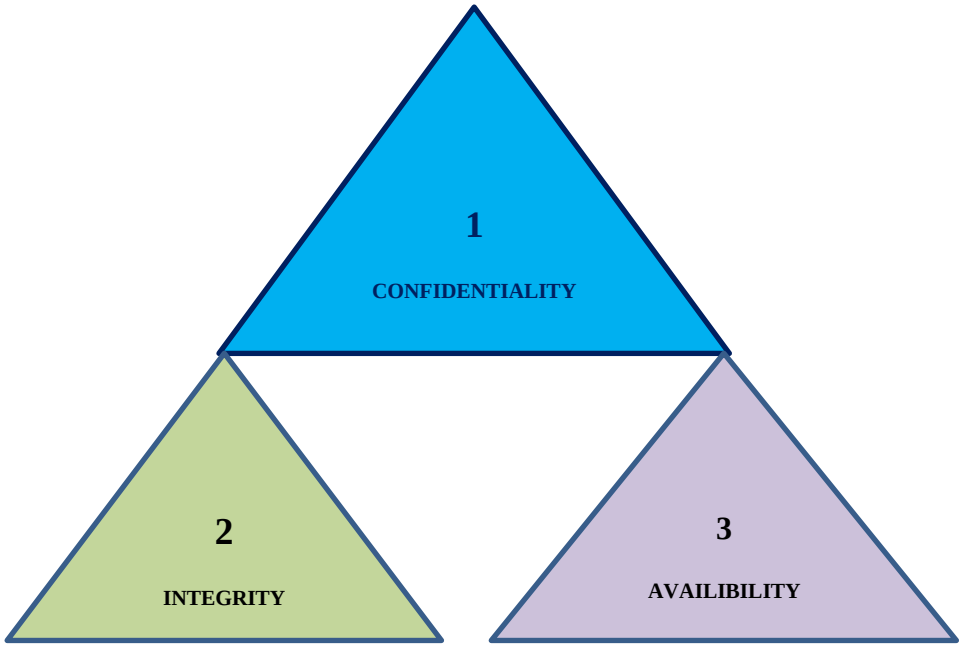
Seiring perkembangan dan kemajuan teknologi, hal ini menghadirkan masalah atau risiko keamanan yang meningkat pada modal informasi yang tersedia. Efek keamanan teknologi informasi merupakan masalah yang sering diabaikan oleh publik dan perusahaan yang menggunakan dan menggunakan teknologi informasi. Dengan adanya permasalahan diatas maka keamanan aset informasi harus dikembangkan secara baik untuk menurunkan resiko atau kegagalan keamanan informasi yang mengakibatkan terhalangnya kegiatan bisnis yang ada. Suatu cara dalam melindungi keamanan aset informasi yang ada adalah dengan mengadakan penyelidikan keamanan aset informasi yang ada serta membuat rekomendasi perlindungan efek yang diperlukan.

PT PLN adalah perusahaan kepunyaan negara yang menguasai seluruh bidang ketenagalistrikan di Negara ini. Beragam masalah juga bisa timbul pada kehidupan sehari-hari jika menyangkut listrik. Diantaranya masalah yang timbul adalah aliran listrik ke konsumen dari PT PLN. Aliran arus ini bisa terdeteksi saat mitra usaha, atau sering disebut meteran listrik, terus mendeteksi arus meski peralatan elektronik sedang tidak digunakan.

Hal ini disebabkan kebocoran aliran listrik yang pada dasarnya dilakukan tanpa keinginan dan sepengetahuan kami.

Dari beragam asumsi di atas bisa dibuat kesimpulan bahwa bocornya listrik disebabkan oleh adanya gangguan maupun cacat pada aliran listrik sehingga menyebabkan arus mengalir melalui celah gangguan ke tempat yang tidak sesuai. Munculnya kebocoran listrik bisa membuat serangkaian kerugian, antara lain tagihan listrik bulanan yang meledak atau menggunakan listrik pulsa yang dianggap tidak perlu walaupun tidak memakai banyak alat elektronik pada waktu yang sangat lama, saat adanya listrik bocor dapat menyebabkan korsleting sirkuit mengakibatkan pedagang atau meteran menangkap kelebihan listrik dari sekitar lalu memotong aliran listrik atau sering juga kita menyebutnya dengan pemborosan listrik, menimbulkan kerugian yang sangat serius yaitu kebocoran listrik dapat mengakibatkan percikan api dari penyebab korsleting listrik rangkaian listrik yang dapat menimbulkan kebakaran.

Dengan adanya permasalahan diatas maka keamanan aset informasi harus dimanagemen secara baik untuk mengurangi resiko atau kegagalan keamanan informasi yang berujung pada gangguan kegiatan bisnis yang ada. Diantaranya dalam melindungi keamanan aset informasi yang ada adalah dengan mengadakan penyelidikan keamanan pada aset informasi yang ada untuk membuat pilihan perlindungan efek yang diperlukan. Keamanan informasi mengarah pada kegiatan dan metode yang didesain dan diterapkan untuk menjaga berita elektronik atau informasi rahasia, pribadi, dan sensitif lainnya dari saluran yang tidak resmi, salah dalam penggunaan, pengungkapan, pengerusakan dan pengubahan, dan penggunaan yang tidak sah. Prinsip keamanan data yang paling penting adalah kerahasiaan, integritas dan ketersediaan atau sering disingkat CIA[11].



Gambar 1. Prinsip Keamanan data

Berikut ini tahapan untuk prinsip keamanan data pada PT.PLN

1. Confidentiality (Kerahasiaan)

Yakni, untuk mengatasi pihak yang tidak berwenang menelusuri informasi rahasia yang harus dilindungi dari penyalinan. Sederhananya, kerahasiaan ini bisa berarti sama dengan privasi. Inti dari konsep kerahasiaan adalah menolak akses informasi kepada orang-orang yang misalnya tidak memiliki kewenangan atas informasi tersebut (disclosure of information).

Kerahasiaan adalah nomor satu, kerahasiaan dapat menghindari resiko kejahatan dan resiko kebocoran informasi. Contoh lain adalah adanya username dan password yang termasuk dalam prosedur default metode rahasia.

2. Integrity (Integritas)

Integritas ini berarti menjaga konsistensi, akurasi, dan kepercayaan data. Prinsip integritas memastikan bahwa data terkandung. dihapus dan dimodifikasi oleh pengguna atau pemilik data yang sama, sehingga orang lain atau penyerang tidak dapat masuk, menghapus, atau mengubah data. Dengan kata lain, integritas memastikan bahwa data yang diterima tidak diubah selama transmisi, apakah itu dimodifikasi, digandakan, disalin, atau dipulihkan.

Maka harus ada izin dan kontrol akses. Pemeriksaan ini berguna untuk memastikan bahwa pengguna yang sah tidak menghapus data secara tidak sengaja, sehingga memerlukan cadangan/redundansi.

3. Availibility (Ketersediaan)

Yakni, untuk memastikan ketersediaan sistem agar dapat digunakan kapanpun pengguna memintanya. Ketersediaan berarti bahwa informasi dapat diperoleh, yaitu jaminan akses yang dapat dipercaya untuk memproses informasi dari orang yang berwenang.Pada dasarnya, kerahasiaan dalam pembahasan ini merupakan sekumpulan perintah yang menyekat akses informasi. Integritas adalah garansi bahwa data bisa diandalkan dan akurat. Terakhir, ketersediaan adalah garansi akses yang bisa dipercaya untuk memproses data oleh individu yang berwenang.

Dalam keamanan informasi, terdapat sebutan ancaman yang artinya setiap kejadian yang bisa merusak sistem dan mengakibatkan kerahasiaan hilang, kesiapan atau kredibilitas. Ancaman dapat berbahaya seperti dengan sengaja mengubah informasi penting seperti nomor transaksi atau menghapus file. Ancaman datang dengan kerentanan, yaitu kelemahan operasi yang dapat didayagunakan oleh bahaya tersebut. Meminimal bidang kerentanan sistem bisa mengurangi kemungkinan bahaya kepada sistem.

Sistem informasi bisa diartikan sebagai gabungan jalur yang terorganisir secara berbeda
untuk mengumpulkan, menangkap, memproses, menyimpan, dan mengelola data dilaporkan untuk mendapatkan maksud dari organisasi. Keamanan sistem informasi bisa diartikan sebagai operasi jaringan dari semua jenis mekanisme. Tujuannya supaya sistem terlindungi dari berbagai ancaman yang memiliki resiko berbahaya
terhadap keamanan informasi data[12] .Keamanan data merupakan upaya untuk melindungi data dari potensi ancaman. Dengan tidak langsung, keamanan informasi memastikan kelangsungan bisnis, meminimal efek yang ada dan memaksimalkan pengembalian modal yang diinvestasikan[13].

Hasil pengkajian ini memaparkan bahwa jika kita hanya mengadalkan teknologi semata tidaklah komplit dalam menanggulangi kehilangan data. Aspek manusia adalah bagian terlemah daripada sistem informasi. Apabila model penyerangan semakin banyak diarahkan pada pemakai sistem informasi,dikarenakan lebih mudah serta cenderung berhasil daripada menerobos sistem informasi itu sendiri. Oleh karena itu, pelatihan keamanan informasi bagi pengguna sistem informasi diperlukan untuk meminimalkan bocornya informasi[14].

SIMPULAN

Keamanan data adalah cara untuk menanggulangi pemhongan (fraud) atau lebih baik memeriksa penipuan dalam sistem data dimana data itu sendiri tidaklah memiliki bentuk fisik. Keamanan data merupakan upaya untuk melindungi data dari potensi ancaman. Dengan kata lain keamanan informasi menjamin kelangsungan bisnis, meminimal efek yang muncul, dan memaksimalkan pengembalian modal yang diinvestasikan. Bidang penting dari keamanan data yaitu kerahasiaan, kredibilitas serta ketersediaan.

Pelatihan adalah cara paling efektif untuk mengurangi serangan terhadap sistem informasi. Pelatihan memungkinkan pengguna untuk memahami hal-hal yang dapat dikerjakan serta kejadian yang dapat membahayakan. Untuk menguatkan keamanan pada kerahasiaan data perlu menerapkan pedoman/aturan menggunakan sistem informasi.

Didukung dengan prosedur yang standar, sangat efektif dalam membendung ancaman kepada sistem informasi, karena semuanya harus dilakukan sesuai petunjuk.

DAFTAR PUSTAKA

G. Maulani, D. Septiani, P. Noer Fauziyah Sahara, J. Jenderal Sudirman No, and M. Cikokol, "RANCANG BANGUN SISTEM INFORMASI INVENTORY FASILITAS MAINTENANCE PADA PT. PLN (PERSERO) TANGERANG Dosen Sistem Informasi STMIK Raharja 1 , Sarjana S1 (alumni) Sistem Informasi STMIK Raharja 2 , Mahasiswa jurusan Sistem Informasi STMIK Raharja 3," vol. 4, no. 2, pp. 156–167, 2018.

M. Rasyid, R. Galela, and U. I. Buru, "2020-Analisis Kualitas Pelayanan Listrik Terhadap Kepuasaan," vol. 1, no. April, 2020.

R. Kurnia and S. Suryayusra, "ANALISIS RISIKO KEAMANAN ASET INFORMASI PADA UNIVERSITAS BINA DARMAAnalisis Risiko Keamanan Aset Informasi," *Bina Darma Conf. …*, pp. 799–809, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2405%0Ahttps://conference.binadarma.ac.id/index.php/BDCCS/article/download/2405/1109

T. P. Purbani, "Plagiat Merupakan Tindakan Tidak Terpuji Plagiat Merupakan Tindakan Tidak Terpuji," *Repository.Usd.Ac.Id*, pp. 1–85, 2011, [Online]. Available: https://eprints.uny.ac.id/25714/2/BAB II.pdf

B. Prasetyo, T. J. Pattiasina, and A. N. Soetarmono, "Perancangan dan Pembuatan Sistem Informasi Gudang (Studi Kasus : PT. PLN (Persero) Area Surabaya Barat)," *Teknika*, vol. 4, no. 1, pp. 12–16, 2015, doi: 10.34148/teknika.v4i1.30.

F. Ceteri, Y. Arafat, and N. Nurmala, "Analisis Sistem Pengendalian Intern Atas Sistem Akuntansi Penerimaan dan Pengeluaran Kas pada PT. PLN (Persero) U1WS2JB Area Palembang ULP Ampera," *J. Media Akunt.*, vol. 2, no. 1, p. 1, 2019, doi: 10.31851/jmediasi.v2i1.4894.

A. Aladin, F. Febriani, and M. Mardiana, "PENGELOLAAN KAS KECIL PADA PT PLN (Persero) UNIT PENDIDIKAN DAN PELATIHAN PALEMBANG," *Eksistansi*, vol. 10, no. 1, 2021, [Online]. Available: http://jurnal.polsri.ac.id/index.php/eksistansi/article/view/4554%0Ahttp://jurnal.polsri.ac.id/index.php/eksistansi/article/view/4554/1807

A. E. Widodo and S. Suleman, "Detektor Kebocoran Listrik Rumah Berbasis Arduino," *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 2, pp. 40–49, 2020, doi: 10.31294/evolusi.v8i2.8948.

N. S. B2041142031, "Pengaruh Manajemen Perubahan Pada Kinerja Karyawan PT PLN (Persero) Unit Induk Wilayah Kalimantan Barat," *Equator J. Manag. Entrep.*, vol. 8, no. 1, pp. 18–33, 2020, doi: 10.26418/ejme.v8i1.38546.

Imansyah, "Analisis Kinerja Keuangan Pada Pt Pln (Persero)," pp. 46–78, 2018.

N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

I. Ava Dianta, E. Zusrony, and S. Tinggi Elektronika dan Komputer, "Analisis Pengaruh Sistem Keamanan Informasi Perbankan pada Nasabah Pengguna Internet Banking Analysis of Influence of Banking Information Security System to Internet Banking User Customer," *Intensif*, vol. 3, no. 1, pp. 2549–6824, 2019.

A. Ramadhani, "Keamanan Informasi," *Nusant. - J. Inf. Libr. Stud.*, vol. 1, no. 1, p. 39, 2018, doi: 10.30999/n-jils.v1i1.249.

J. E. W. Prakasa, "Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi," *J. Ilm. Teknol. Inf. Asia*, vol. 14, no. 2, p. 75, 2020, doi: 10.32815/jitika.v14i2.452.