Security Management Control Pada Jaringan Komputer

Diah Komariah
Fakultas Ilmu Komputer, Jurusan Ilmu Komputer
Universitas Sriwijaya , Indralaya, Palembang
Jl. Raya Palembang - Prabumulih Km. 32 *Indralaya*
Kabupaten Ogan Ilir, Provinsi Sumatera Selatan
(0711) 580169
unsri.ac.id

ABSTRACT

Internet merupakan kumpulan dari berbagai jaringan komputer, yang saling terkoneksi satu sama lain dan dapat saling berkomunikasi. Penggunaan internet yang mencakup di segala bidang, membuat internet menjadi kebutuhan pokok dalam berkomunikasi. Pemakaian internet secara global harus memperhatikan dari segi manajemen jaringan. NMS (Network Management System) merupakan sebuah sistem yang memanajemen/mengelola, memonitoring jaringan antara client dan server. Konsep dari NMS ini terdiri dari 5 area yaitu Fault management, Configuration management, Accounting management, Performance management, dan Security management atau dikenal dengan istilah FCAPS. Manajemen Kinerja adalah kegiatan yang dilakukan untuk menilai indikator kinerja operasi jaringan secara berkelanjutan. Dengan Manajemen Kinerja diharapkan tingkat layanan dapat dipertahankan (mengoptimalkan QoS (Kualitas Layanan)), kondisi jaringan dapat diidentifikasi, kemungkinan interferensi dapat diprediksi dan dapat membuat laporan lengkap tentang kegiatan pengambilan keputusan dan perencanaan. Pada makalah ini kita focus pada Security management dari FCAPS . Securiy management mengatur akses ke sumber daya jaringan sehingga informasi tidak dapat diperoleh tanpa izin . Hal tersebut dilakukan dengan cara (1). Membatasi akses ke sumber daya jaringan , (2). Memberi pemberitahuan akan adanya usaha pelanggaran dan pelanggaean keamanan .

Keywords
Security Management; Network Security; Network management System (NMS); Security Management Controls; Computer Network

1. PENDAHULUAN

Latar Belakang

Perkembangan teknologi informasi saat ini begitu cepat dan memberikan kemudahan bagi manusia dalam mengatasi permasalahan yang dihadapi. Begitu juga dengan penggunaan Internet yang sangat pesat, hal ini membutuhkan pelayanan Quality of service (QoS) yang mumpuni. Keterhubungan setiap user didalam jaringan perlu dijaga performa kenektivitasnya sehingga dapat meningkatkan produktivitas maupun keberlangsungan transaksi yang dilakukan. Untuk meningkatkan kualitas jaringan yang ada, perlu dilakukan pengawasan terhadap kinerja jaringan dan tindakan untuk mengendalikan aliran trafik agar kapasitas pengoperasian pada sebuah jaringan dapat dilakukan secara maksimal.

Network Monitoring System (NMS) adalah sebuah layanan yang menggunakan alat, aplikasi dan perangkat yang digunakan untuk membantu manusia dalam mengatur dan mengamati jaringan. Dengan menggunakan alat Network Monitoring System (NMS) yang tepat akan sangat memudahkan pekerjaan seorang administrator atau pengguna dalam memantau dan merawat jaringan dilingkungannya

Network Monitoring System (NMS) merupakan sebuah sub sistem dalam manajemen jaringan (Network Management System) yang melibatkan penggunaan perangkat lunak dan perangkat keras. Berdasarkan International Standards Organtations(ISO), aplikasi Network Monitoring System memiliki

lima kriteria yaitu performance, managament, accounting managament, configuration managament, fault managament dan security management.

II. DASAR TEORI

A . Security Management

Security Management yaitu suatu sistem untuk memberikan pemahaman yang utuh/ terpadu serta kemampuan dan keterampilan dalam merencanakan dan mendesain Sistem Pengamanan yang tepat, efektif, dan efisien, sesuai dengan situasi dan kondisi yang dihadapi, khususnya Ancaman / Gangguan yang mungkin terjadi serta kemampuan Perusahaan sendiri dan berguna untuk mencegah sedini mungkin kerugian-kerugian bagi Perusahaan (*Loss Prevention*).

Tiga elemen dasar *confidentiality, integrity,* dan *availability* (CIA) merupakan dasar diantara program program keamanan yang dikembangkan. Ketiga elemen tersebut merupakan mata rantai yang saling berhubungan dalam konsep *information protection.*
Keamanan bisa dicapai dengan beberapa cara atau strategi yang biasa dilakukan secara simultan atau dilakukan dalam kombinasi satu dengan yang lainnya. Strategi-strategi dari keamanan informasi masing-masing memiliki fokus dan dibangun tujuan tertentu sesuai kebutuhan. Contoh dari keamanan informasi antara lain :

1. **Physical security**

   Keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. **Personal security**
   Keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup physical security.
3. **Operasional security**
   Keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
4. **Communication security**
   Keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada didalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. **Network security**
   Keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Masing masing komponen tersebut berkontribusi dalam program keamanan informasi secara keseluruhan. Jadi keamanan informasi melindungi informasi baik sistem maupun perangkat yang digunakan untuk menyimpan dan mengirimkannya.

C. Network Security

Keamanan jaringan (*network security*) terdiri dari kebijakan dan praktik untuk mencegah dan memantau akses yang tidak sah, penyalahgunaan, maupun penolakan yang terjadi di jaringan komputer. *Network security* melibatkan otorisasi akses ke data di dalam jaringan, yang dikendalikan oleh administrator jaringan. Pengguna (*users*) memilih atau diberi ID dan *password* atau informasi otentikasi lain yang memungkinkan mereka untuk mengakses informasi dan program dalam wewenang mereka sendiri. *Network security* mencakup berbagai jaringan komputer, baik publik maupun pribadi, yang digunakan dalam pekerjaan sehari-hari; melakukan transaksi dan komunikasi di antara bisnis, instansi

pemerintah dan individu. Jaringan tersebut dapat bersifat pribadi, seperti di dalam perusahaan, dan lainnya yang mungkin terbuka bagi akses publik.

Network security terlibat dalam organisasi, perusahaan, dan jenis lembaga lainnya. Seperti bagaimana mengamankan jaringan, serta melindungi dan mengawasi operasi yang dilakukan. Dimana cara paling umum dan sederhana untuk melindungi sumber daya jaringan (*network resource*) adalah dengan menetapkan nama yang unik dan *password* yang sesuai.

Gambar 1. *Network Security*

Konsep Network Security

Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA yang merupakan *Confidentiality* (kerahasiaan), *Integrity* (integritas)dan *Availability* (ketersediaan).

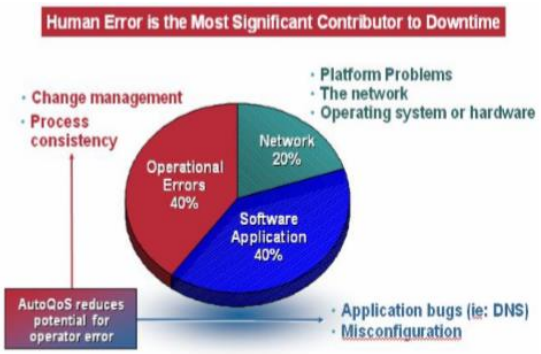
1. *Confidentiality* (kerahasiaan)Kerahasiaan setara dengan privasi. Kerahasiaan dirancang untuk mencegah informasi sensitif dan memastikan bahwa orang yang mempunyai akses adalah orang yang tepat. Terkadang menjaga kerahasiaan data dapat melibatkan pelatihan khusus bagi mereka yang mengetahui dokumen tersebut.

2. *Integrity* (integritas)Integritas melibatkan menjaga konsistensi, akurasi, dan kepercayaan data. Data tidak boleh diubah, dan langkah-langkah harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang-orang yang tidak berkepentingan.

3. *Availability* (ketersediaan)Ketersediaan (*availability*) adalah konsep terbaik yang dapat dipastikan dalam memelihara semua *hardware*, melakukan perbaikan terhadap *hardware* sesegera mungkin saat diperlukan. Selain itu juga dapat memelihara lingkungan sistem operasi.

D. Network management System (NMS)

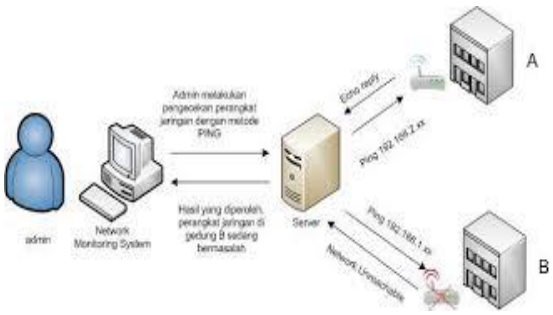
Network management system (NMS) adalah upaya untuk mengkoordinasikan dan mendistribusikan sumber daya atau resource untuk merencanakan, menganalisa, mengevaluasi, mendesain, mengadministrasikan dan mengembangkan jaringan, sehingga memperoleh kualitas pelayanan yang baik pada seluruh waktu dengan biaya yang sesuai dan kapasitas yang optimal. Manajemen jaringan adalah kemampuan menerapkan suatu metode untuk memonitor suatu jaringan, mengontrol suatu jaringan dan merencanakan sumber serta komponen sistem dalam sebuah jaringan komputer. Model NMS mencakup 5 area konseptual yaitu Fault Management, Configuration Management, Accounting Management, Performance Management dan Security Management (FCAPS). Model NMS adalah upaya untuk meminimalisir gangguan pada elemen jaringan atau keseluruhan jaringan. Gambar berikut beberapa faktor yang menyebabkan terjadinya downtime sebuah jaringan.



Gambar 2. *Faktor-faktor penyebab network down*

Dari gambar terlihat beberapa faktor yang menyebabkan permasalahan didalam jaringan dimana sebanyak 40% permasalahan pada bidang operasional, 40% permasalahan pada software aplikasi dan 20% terkait jaringan. Dari gambaran diatas perlunya dilakukan NMS dan salah satunya adalah dalam Performance management. Performance management (PM) adalah kegiatan yang dilakukan untuk menilai indikator unjuk kerja dari operasi jaringan secara berkesinambungan. Dengan PM diharapkan gangguan didalam jaringan dapat diprediksi dan QoS dapat terus dipertahankan.

Network management system (NMS) sangat berguna dalam *network device discovery*, *network device monitoring*, *network performance analysis*, *network device management*, pemberitahuan cerdas atau peringatan yang dapat disesuaikan.



Gambar 3. *Implementasi NMS*

NMS dapat di*instal* secara *on-premise* di server khusus. Perangkat lunak NMS dapat mengelola beragam komponen jaringan besar yang diproduksi oleh beberapa *vendor*. Instalasi NMS *on-premise* dapat memungkinkan kontrol dan kustomisasi perangkat lunak untuk bertemu tujuan yang spesifik. Selain itu, NMS dapat digunakan juga untuk memonitor unsur jaringan kabel dan nirkabel (*wired* dan *wireless*). Perangkat lunak NMS juga dapat mengijinkan perusahaan untuk melacak performa di seluruh jaringan mereka sendiri, maupun melalui jaringan external, seperti dioperasikan oleh cloud dan penyedia

E. Computer Network

Sebuah jaringan komputer(Computer Network) adalah jaringan telekomunikasi yang memungkinkan komputer untuk bertukar data. Koneksi fisik antara perangkat komputasi jaringan didirikan dengan menggunakan media baik kabel atau media nirkabel. Yang paling terkenal jaringan komputer adalah Internet. Perangkat jaringan yang berasal, rute dan mengakhiri data disebut node jaringan. Nodes dapat mencakup host seperti server dan komputer pribadi, serta perangkat keras jaringan. Dua perangkat dikatakan jaringan ketika proses dalam satu perangkat dapat bertukar informasi dengan proses pada perangkat lain.Dukungan aplikasi jaringan komputer seperti akses ke World Wide Web, berbagi penggunaan aplikasi server dan penyimpanan, printer, dan mesin faks, dan penggunaan email dan aplikasi instant messaging. Sisa dari artikel ini membahas teknologi jaringan area lokal dan mengklasifikasikan mereka sesuai dengan karakteristik sebagai berikut: media fisik yang digunakan

untuk mengirimkan sinyal, protokol komunikasi yang digunakan untuk mengatur lalu lintas jaringan, bersama dengan ukuran jaringan, topologi dan niat organisasinya.

F. Manajemen Kontrol Keamanan (Security Management Controls)

Aset Sistem Informasi yang harus di lindungi melalui sistem keamanan dapat diklasifikasikan menjadi 2 yaitu Aset Fisik yang meliputi Personnel, Hardware (termasuk media penyimpanan, dan periperalnya), Fasilitas, Dokumentasi, dan Supplies. Dan Aset Logika meliputi Data (informasi), dan Sofware (sistem dan aplikasi).

Langkah-langkah utama Pelaksanaan Program Keamanan (Conducting a Security Program) yaitu:

- Persiapan Rencana Pekerjaan (Preparation of a Project Plan) untuk tinjaun kemanan mengikuti item tujuan review, ruang lingkup (scope) review, tugas yang harus dipenuhi, organisasi dari tim proyek, sumber anggaran (pendanaan), dan jadwal untuk menyelesaikan tugas.
- Identifikasi Kekayaan (Identification of asset) diantaranya yaitu meliputi, Personnel (end users, analyst, programmers, operators, clerks, guards), Hardware (Mainfarme, minicomputer, microcomputer, disk, printer, communication lines, concentrator, terminal), Fasilitas (Furniture, office space, computer rrom, tape storage rack), Dokumentasi (System and program doc.,database doc.,standards plans, insurance policies, contracts), Persediaan (Negotiable instrument, preprinted forms, paper, tapes, cassettes), Data/Informasi (Master files, transaction files, archival files), Software Aplikasi (Debtors, creditors, payroll, bill-of-materials, sales, inventory), Sistem Software (Compilers, utilities, DBMS, OS, Communication Software, Spreadsheets).
- Penilaian Kekayaan (Valuation of asset). Langkah ke tiga ini adalah penilaian kekayaan, yang merupakan langkah paling sulit. Parker (1981) menggambarkan ketergantungan penilaian pada siapa yang ditanya untuk memberikan penilaian, cara penilaian atas kekayaan yang hilang (lost), waktu periode untuk perhitungan atas hilangnya kekayaan, dan umur asset.
- Identifikasi Ancaman-ancaman (Threats Identification). Sumber ancaman terbagi atas sumber ancaman external (Nature / Acts of God, H/W Suppliers, S/W Suppliers, Contractors, Other Resource Suppliers, Competitors (sabotage, espionage, lawsuits, financial distress through fair, or unfair competition), Debt and Equity Holders, Unions (strikes, sabotage,harassment), Governmnets, Environmentalist (Harassment (gangguan), unfavorable publicity), Criminals/hackers (theft, sabotage, espionage, extortion)); sumber ancaman Internal (Management (contoh kesalahan dalam penyediaan sumber daya, perencanaan dan control yang tidak cukup)), Employee (contoh Errors, Theft (pencurian), Fraud (penipuan), sabotase, extortion (pemerasan), improper use of service (penggunaan layanan yg tidak sah)), Unreliable system (contoh Kesalahan H/W, kesalahan S/W, kesalahan fasilitas)).
- Penilaian Kemungkinan Ancaman (Threats LikeIihood Assessment), contohnya yaitu, perusahaan asuransi dapat menyediakan informasi tentang kemungkinan terjadinya kebakaran api dalam satu waktu periode tertentu.
- Analisis Ekspose (Exposures analysis); Tahap analisis ekspose terdiri dari 4 tugas yaitu, Identification of the controls in place, Assessment of the reliability of the controls in place, Evaluation of the likelihood that a threat incident will be successful, Assess the resulting loss if the threat is successful.

III. Bahan dan Analisa perancangan

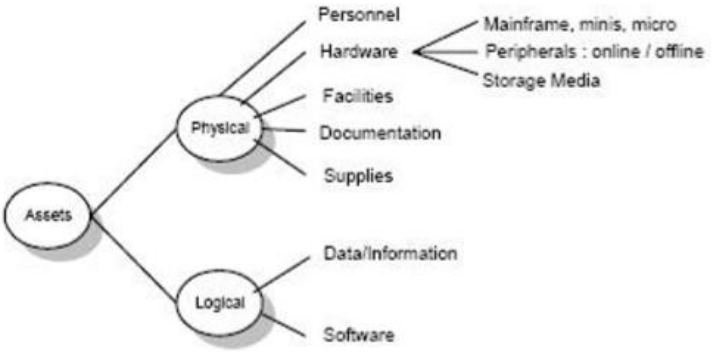
Aset Sistem Informasi yang harus di lindungi melalui sistem keamanan dapat diklasifikasikan menjadi 2yaitu:

1. Aset Fisik, meliputi:

a Personnel
b.Hardware (termasuk media penyimpanan,dan periperalnya)
c.Fasilitas
d.Dokumentasi
e.Supplies

2. Aset Logika

a. Data / Informasi
b.Sofware (Sistem dan Aplikasi



Gambar 4. *Kategori Aset Sistem Informasi*

Pelaksanaan Program Keamanan(Conducting a Security Program)

Langkah-langkah utama pelaksanaan Program keamanan yaitu :

Gambar 4. *Langkahutama dalam pelaksanaan program keamanan*

Persiapan Rencana Pekerjaan (Preparation of a Project Plan)
Perencanaan proyek untuk tinjau kemanan mengikuti item sebagai berikut:

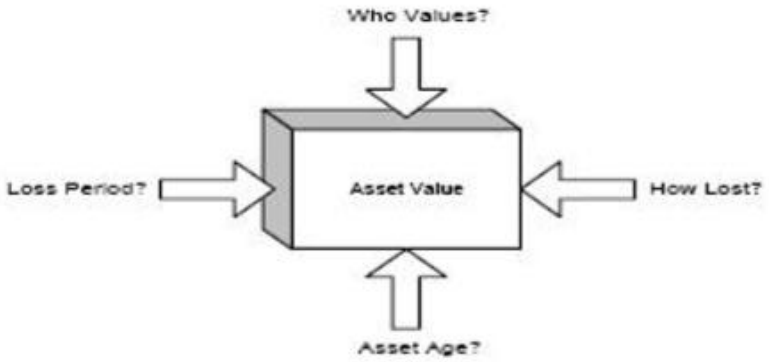
a. Tujuan Review
b. Ruang Lingkup (Scope) Review
c. Tugasyang harus dipenuhi
d. Organisasi dari Tim Proyek
e. Sumber Anggaran (Pendanaan)
f. Jadwal untuk Menyelesaikan Tugas

Identifikasi Kekayaan (Identification of asset)
Katagori asset:

a. Personnel(end users,analyst,programmers,operators,clerks,Guards)
b. Hardware (Mainfarme, minicomputer, microcomputer, disk, printer, communication lines, concentrator,terminal)
c. Fasilitas (Furniture, officespace,computerrrom,tape storagerack)
d. Dokumentasi (System and program doc.,database doc.,standards plans, insurance policies, contracts)
e. Persediaan (Negotiable instrument, preprinted forms, paper, tapes, cassettes)
f. Data/Informasi (Master files,transaction files, archival files)
g. Software Aplikasi (Debtors, creditors, payroll, bill-of-materials, sales, inventory)
h. Sistem Software (Compilers, utilities, DBMS,OS,Communication Software, Spreadsheets)

Penilaian Kekayaan(Valuation of asset)

Langkah ke tiga adalah penilaian kekayaan, yang merupakan langkah paling sulit. Parker (1981) menggambarkan ketergantungan penilaian pada siapa yang ditanya untuk memberikan penilaian, cara penilaian atas kekayaan yang hilang (lost), waktu periode untuk perhitungan atas hilangnya kekayaan,dan umur asset.



Gambar 5. *Faktor efek penilaian SI keamanan*

Identifikasi Ancaman-ancaman (Threats Identification)

		Nature of threat: Accidental (kebetulan/tdk sengaja)	Deliberate (sengaja)
Source of Threat	External	e.g. Acts of God	e.g. Hackers
	Internal	e.g. Pollution	e.g. Sabotage

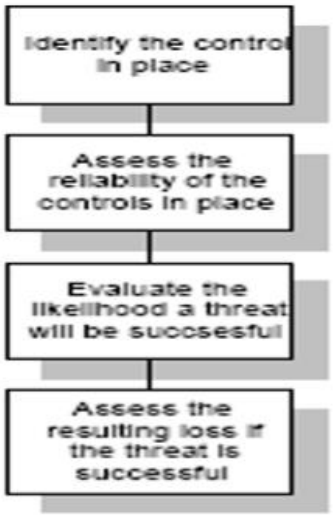
Gambar 6. *Lapisan jenis ancaman Aset SI*

Penilaian Kemungkinan Ancaman(Threats LikeIihood Assessment)

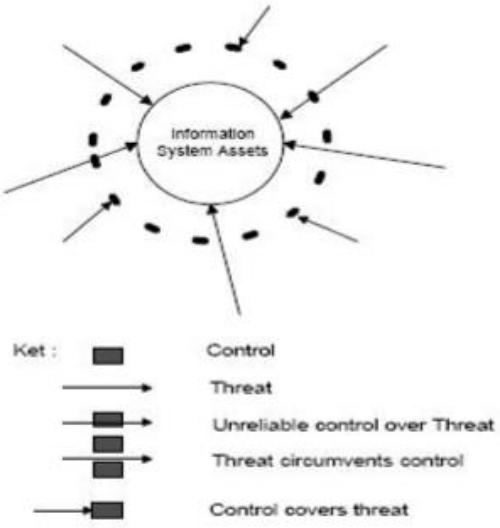
Contoh, perusahaan asuransi dapat menyediakan informasi tentang kemungkinan terjadinya kebakaran api dalam satu waktu periode tertentu.

Analisis Ekspose (Exposures analysis)

Tahapan analisis ekspose terdiri dari 4 tugas yaitu :
1.Identification of the controls in place
2.Assessment of the reliability of the controls in place
3.Evaluation of the likelihood that a threat incident will be successful
4.Assess the resulting loss if the threat is successful



Gambar 7. *Tugas utama tahap analisis ekspose*



Gambar 8. *Ancaman, keandalan kontrol, cakupan control,dan ekspose*

IV. Kesimpulan

Berdasarkan penjelasan mengenai security manajemen control pada jaringan computer, maka dapat disimpulkan hal-hal sebagai berikut :

1. Security Management menjadi pengamanan yang tepat, efektif, dan efisien, sesuai dengan situasi dan kondisi yang dihadapi, khususnya Ancaman / Gangguan yang mungkin terjadi serta kemampuan Perusahaan sendiri dan berguna untuk mencegah sedini mungkin kerugian-kerugian bagi Perusahaan (*Loss Prevention*).
2. Network Security yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.
3. Terdapat tiga elemen dasar *confidentiality, integrity,* dan *availability* (CIA) merupakan dasar diantara program program keamanan yang dikembangkan. Ketiga elemen tersebut merupakan mata rantai yang saling berhubungan dalam konsep *information protection.*
4. Terdapat beberapa faktor yang menyebabkan permasalahan didalam jaringan dimana sebanyak 40% permasalahan pada bidang operasional, 40% permasalahan pada software aplikasi dan 20% terkait jaringan.
5. Dalam menjaga kemanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut dengan CIA yang merupakan *Confidentiality (kerahasiaan) , Integrity (integritas), dan Availability (ketersediaan).*
6. Dengan tumbuhnya berbagai penipuan, spionase, virus, dan hackers sudah mengancam informasi bisnis manajemen oleh karena meningkatnya keterbukaan informasi dan lebih sedikit kendali/control yang dilakukan melalui teknologi informasi modern. Sebagai konsekuensinya , meningkatkan harapan dari para manajer bisnis, mitra usaha, auditor,dan stakeholders lainnya menuntut adanya manajemen informasi yang efektif untuk memastikan informasi yang menjamin kesinambungan bisnis dan meminimise kerusakan bisnis dengan pencegahan dan memimise dampak peristiwa keamanan.

DAFTAR PUSTAKA

[1] E. Harli, “Pemilihan Network Monitoring System Berdasarkan Kajian Efektifitas Sistem Informasi dengan Pendekatan AHP : Studi Kasus pada ‘PT.TUV,’” *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 1, pp. 64–70, 2016, doi: 10.26418/jp.v2i1.15555.

[2] A. A. Putra, O. D. Nurhayati, and I. P. Windasari, “Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 20071,” *J. Teknol. dan Sist. Komput.*, vol. 4, no. 1, p. 60, 2016, doi: 10.14710/jtsiskom.4.1.2016.60-66.

[3] A. Ključnikov, L. Mura, and D. Sklenár, “INFORMATION SECURITY MANAGEMENT IN SMES: FACTORS OF SUCCESS Aleksandr Ključnikov[1], Ladislav Mura [2] , David Sklenár[2] 2,3,” *Entrep. Sustain. Issues*, vol. 6, no. 4, pp. 2081–2094, 2019, doi: http://doi.org/10.9770/jesi.2019.6.4(37) Publisher.

[4] Y. Jung, M. Peradilla, and R. Agulto, “Software-defined security controller-based end-to-end packet key security management,” *Procedia Comput. Sci.*, vol. 155, no. 2018, pp. 89–96, 2019, doi: 10.1016/j.procs.2019.08.016.

[5] P. W. Purnawan and U. B. Luhur, “Managed Service Network Management System (Nms) Berdasarkan Fault , Configuration , Accounting , Performance , Security (Fcaps) Management Managed Service Network Management System (Nms) Berdasarkan Fault , Configuration , Accounting , Performance ,” no. January, 2018, doi: 10.13140/RG.2.2.18486.60481.

[6] T.-S. Chou and N. Hempenius, “An Assessment of Practical Hands-On Lab Activities in Network Security Management,” *J. Cybersecurity Educ. Res. Pract.*, vol. 2019, no. 2, p. 2, 2020.