e-ISSN: 2964-7517, p-ISSN: 2964-7525
DOI: https://doi.org/10.38035/jpsn.v1i12
Received: 03 April 2023, Revised: 23 April 2023, Publish: 29 April 2023

Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan

Lanang Adi Saputra[1], Fadel Muhammad Akbar[2], Febrina Cahyaningtias[3], Mega Puspa Ningrum[4], Achmad Fauzi[5]
[1]Fakultas Ekonomi Universitas Bhayangkara Jakarta Raya, 202110315081@mhs.ubharajaya.ac.id
[2]Fakultas Ekonomi Universitas Bhayangkara Jakarta Raya, 202110315022@mhs.ubharajaya.ac.id
[3]Fakultas Ekonomi Universitas Bhayangkara Jakarta Raya, 202110315094@mhs.ubharajaya.ac.id
[4]Fakultas Ekonomi Universitas Bhayangkara Jakarta Raya, 202110315074@mhs.ubharajaya.ac.id
[5]Fakultas Ekonomi Universitas Bhayangkara Jakarta Raya, achmad.fauzi@dsn.ubharajaya.ac.id

Corresponding Author: Lanang Adi Saputra

Abstrak: Pengetahuan adalah asset terpenting perusahaan. Karena kemampuan memberikan informasi secara cepat dan akurat sangatlah penting. Sistem informasi (SI) dan teknologi informasi (TI) sering berperan dalam manajemen informasi. Namun, ketika berkembang, ITU sering terjadi yang dieksploitasi oleh pihak-pihak yang tidak bertanggung jawabmerupakan ancaman dan risiko yang dapat membahayakan organisasi. Sistem informasi manajemen adalah sarana terstruktur untuk menyediakan informasi tepat waktu bagi manajemen di luar organisasi dan untuk kegiatan operasional di dalam organisasi dengan tujuan memfasilitasi proses manajemen, meningkatkan proses perencanaan dan pengendalian serta mendukung proses pengambilan keputusan. Dengan kemajuan teknologi ancaman demi ancaman mulai bermunculan, beberapa ancaman terhadap system informasi ataralain: 1) Interruption, 3)Interception, 4)Modification. Pada dasarnya, sistem yang aman melindungi informasi yang dikandungnya, seperti Identifikasi pengguna, autentikasi pengguna, dan otorisasi pengguna. Beberapa kemungkinan serangan (peretasan) dapat dilakukan, seperti, Intrusi atau Denial of Service. Joyrider, vandalisme, pencurian, phishing, penipuan dan lain-lain. Sistem informasi terpapar berbagai ancaman, antara lain, Pencurian data, penggunaan sistem yang tidak sah, penghancuran data yang tidak sah, modifikasi data yang tidak sah, kerusakan sistem, kesalahan manusia (SDM sumber daya manusia), bencana alam.

Kata Kunci: Informasi, Keamanan Informasi, Sistem Informasi Manajemen

PENDAHULUAN

Teknologi informasi memegang peranan penting dalam mendukung kesuksesan bisnis era digital saat ini. Informasi merupakan salah satu aset suatu perusahaan/instansi/perguruan tinggi, baik swasta maupun pemerintah, yang dapat menjaga kelangsungan hidup organisasi dengan pertukaran informasi secara cepat dan mudah, mengorbankan keamanan informasi. Semakin berkembangnya jaringan computer dalam berbagi informasi menciptakan kerentanan pada keamanan informasi bahkan dengan risiko tinggi, karena para pihak dapat mengetahui atau Mengungkapkan informasi orang lain yang tidak memiliki hak akses, Selain adanya ancaman dari pihak luar (eksternal), ancaman juga bisa berasal dari dalam (internal) karyawan/personal yang melakukan penipuan berdasarkan lemahnya pengawasan terhadap prosedur keamanan informasi yang ada.

Jika informasi rahasia Perusahaan disebarluaskan dan disalahgunakan, dapat menimbulkan risiko kerugian bagi bisnis Perusahaan. Namun, isu terkait keamanan informasi masih kurang diperhatikan oleh manajemen perusahaan, padahal hal tersebut merupakan bagian penting dari sistem informasi yang diterapkan oleh perusahaan. Oleh karena itu, manajemen keamanan informasi sangat penting saat ini, karena dengan perkembangan teknnologi yang semakin maju ini dapat dengan begitu mudahnya mendapatkan informasi.

Berlandaskan latar belakang, Topik-topik yang dibahas dalam jurnal ini dapat dirumuskan sebagai berikut:

1. Apa saja ancaman terhadap sistem informasi manajemen?
2. Bagaimana cara mengamankan sistem informasi manajemen dari berbagai ancaman yang ada?

KAJIAN PUSTAKA

Sistem Informasi Manajemen

Entitas memiliki hubungan masukan yang memproses dan memaparkan data berguna untuk pengambilan keputusan dan pemantauan selanjutnya. Harus ada hubungan antara pekerjaan di masing-masing departemen perusahaan. Jika manajemen perusahaan masih dikelola secara manual dan tanpa adanya sistem informasi, maka dapat dikatakan kerja staf di departemen ini tidak efektif. Karena Perjalanan waktu, teknologi memungkinkan apa yang secara teknis menjadi mungkin dalam jangka panjang. Sistem informasi bisa dipahami sebagai alat yang memungkinkan pengguna untuk melakukan pekerjaannya secara akurat, efisien dan efektif (Aswiputri, 2022).

Sistem informasi manajemen adalah metode terstruktur untuk menyediakan informasi tepat waktu kepada manajemen di luar organisasi dan operasi di dalam organisasi untuk memfasilitasi proses manajemen, meningkatkan proses perencanaan dan pengendalian, dan mendukung proses pengambilan keputusan. Pada dasarnya sistem informasi dapat dibedakan menjadi sistem terstruktur (formal) dan sistem tidak terstruktur. (Endra, 2022).

Komponen sistem informasi manajemen menurut Susanto, 2016 dalam (Endra, 2022): Hardware atau perangkat keras adalah perangkat fisik yang dapat difungsikan dalam suatu tahap-tahapan mengumpulkan, memasukkan, menyimpan dan mencetak data hasil pengolahan berupa informasi;

Software, yaitu kumpulan dari beberapa program yang dapat digunakan menggunakan komputer atau aplikasi tertentu di komputer;

Brainware, yaitu. bagian terpenting atau terpenting dari suatu komponen sistem informasi manajemen;

Prosedur, yaitu rangkaian tindakan atau operasi yang dilakukan secara otomatis sama lagi dan lagi;

Database adalah organisasi dengan banyak data Koneksi atau hubungan untuk memudahkan menemukan sesuatu Informasi Jaringan Komputer dan Telekomunikasi

Manajemen Keamanan Informasi

Menurut ISO/IEC 27000: Sistem Manajemen Keamanan Informasi adalah pendekatan sistematis untuk membuat, menerapkan, memanfaatkan, memantau, mengaudit, memelihara, dan meningkatkan keamanan informasi organisasi untuk mencapai tujuan bisnis. Menurut ISO/IEC 27001 Keamanan sistem informasi tidak hanya terkait dengan penggunaan perangkat lunak anti-virus, firewall dan password komputer, tetapi merupakan pendekatan holistik.

Manajemen tidak hanya harus memastikan keamanan aset informasi, tetapi juga menjaga bisnis setelah bencana atau pelanggaran keamanan. Keamanan aset informasi disebut manajemen keamanan informasi (Ramadhani, 2018).

Manfaat manajemen keamanan informasi:

1. Membantu memenuhi persyaratan standar keamanan terverifikasi (praktik keamanan terbaik).
2. Tindakan pengendalian terkait dengan keamanan informasi lingkungan proses bisnis mereka, yang dapat menyebabkan risiko dan gangguan
3. Meningkatkan efektivitas dan keandalan keamanan informasi

Keamanan Informasi

Keamanan Informasi merupakan tindakan untuk menjaga nilai aset informasi dari kemungkinan bahaya. Proteksi informasi pada dasarnya memastikan kelangsungan usaha, mengurangi resiko yang timbul, dan memungkinkan Anda memaksimalkan pengembalian modal (Purwigati & Buana, 2020) dalam (Nurul et al., 2022a). Signifikansinya suatu data menghasilkan timbulnya istilah keamanan informasi. Saat ini sumber data dari dunia maya semakin banyak, sehingga pengamanan data harus melalui teknologi komputer dan jaringan serta informasi dan komunikasi. Tujuan keamanan data adalah untuk menjaga kelangsungan bisnis dan mengurangi hilangnya nilai bisnis dengan membatasi dampak insiden keamanan.

Menurut Sarno dan Iffano, dalam (Galih, 2019) Ada tiga elemen keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan.

A. Kerahasiaan merupakan faktor yang menjamin kerahasiaan data dan sumber informasi. Kepercayaan bahwa informasi hanya dapat dilihat oleh orang yang berwenang atau berwenang diperlukan untuk menjamin keamanan informasi yang disampaikan.

B. Integritas adalah elemen yang memastikan bahwa data tidak dapat diubah tanpa izin dari pihak yang berwenang, menjaga akurasi dan integritas data serta metode pemrosesan yang digunakan untuk memastikan integritas data.

C. Ketersediaan adalah faktor yang menjamin informasi dapat diakses pada saat dibutuhkan oleh pihak yang berwenang atau berwenang, serta memastikan bahwa pengguna yang memenuhi persyaratan dapat mengakses informasi tersebut.

Tabel 1. Penelitian Terdahulu

No	Author (Tahun)	Judul	Hasil Riset Terdahulu
1	(Endra, 2022)	LITERATURE REVIEW KOMPONEN SISTEM INFORMASI MANAJEMEN: SOFTWARE, DATABASE DAN BRAINWARE	Software, Database dan Brainware memiliki pengaruh terhadap Sistem Informasi Manajemen.
2	(Aswiputri, 2022)	LITERATURE REVIEW DETERMINASI SISTEM	Database, Brainware dan CCTV berpengaruh

`

		INFORMASI MANAJEMEN: DATABASE, CCTV DAN BRAINWARE	terhadap Sistem Informasi Manajemen.
3	(Nurul et al., 2022)	FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)	Keamanan Informasi, Teknologi Informasi dan Network berpengaruh terhadap Keamanan Sistem Informasi
4	(Chazar, 2015)	STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005	Pengelolaan keamanan sistem informasi harus dimulai ketika sebuah sistem informasi dibangun. Seri ISO/IEC 27000 dapat digunakan sebagai standar untuk pengelolaan keamanan sistem informasi.
5	(Ardhana, 2012)	KEAMANAN SISTEM INFORMASI	Mengerti dan memahami bagaimana aksi hacker dalam menerobos sistem, sehingga kegiatan hacking dapat dikontrol dan dicegah. Dapat mengetahui dan mengerti bagaimana melakukan teknik pengamanan data dan bagaimana menjaga kerahasiaannya.
6	(Ramadhani, 2018)	KEAMANAN INFORMASI	Keamanan informasi adalah upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Secara tidak langsung Keamanan informasi menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, mengoptimalkan pengembalian investasi
7	(Wahyudi, 2022)	LITERATUREREVIEW: DETERMINASI SISTEM INFORMASI MANAJEMEN DENGAN LINGKUNGANNYA	Studi pertama menunjukkan bahwa Fungsi Manajemen Komponen Sistem Informasi sebagai Model Integrasi menjadi fungsi manajemen (POAC) Studi kedua menunjukkan bahwa Tujuan perpustakaan dan konstruksi sistem didefinisikan sebagai memungkinkan perolehan pengetahuan ilmiah peserta didik. Studi ketiga menunjukkan bahwa Dukungan

	Manajemen puncak: diukur melalui tiga dimensi, yaitu mengevaluasi, mengarahkan dan memantau.

METODE PENELITIAN

Dalam penelitian ini digunakan metode kuantitatif dan literature review dengan menyelidiki dan memahami konsep serta hubungan antar variabel yang diteliti dari jurnal yang bersumber dari Google Scholar dan ResearchGate, kemudian direview Quote using Mendeley app. Dalam penelitian kualitatif, penelitian literatur harus dilakukan sesuai dengan asumsi metodologis. Ini berarti bahwa itu harus digunakan secara induktif agar tidak menjawab pertanyaan yang diajukan oleh peneliti. Salah satu alasan utama untuk melakukan penelitian kualitatif adalah sifatnya yang eksploratif. (Ali & Limakrisna, 2013) dalam (Aswiputri, 2022)

HASIL DAN PEMBAHASAN

Ancaman Sistem Informasi

Ancaman adalah tindakan atau kejadian yang dapat merugikan suatu organisasi atau perusahaan. Kerugian dapat berupa uang, pekerjaan, peluang usaha (business opportunity), Reputasi organisasi bahkan dapat menyebabkan kebangkrutan. Menurut W Stallings dalam (Chazar, 2015) Ada beberapa kemungkinan ancaman,

1. Interruption, perangkat sistem macet atau menjadi tidak tersedia Ancaman dari segi ketersediaan (availability).
2. Interception (Mencegat), akses data tidak sah.
3. Modifikasi oleh pihak yang tidak berwenang tidak hanya membawa informasi tetapi juga mengubah informasiBerikut beberapa kasus cyber attack yang pernah menyerang beberapa institusi ataupun perusahaan di Indonesia:

1. Pada tahun 2004 terjadi penyerangan terhadap website milik KPU. Hacker bernama Xnuxer ini menggunakan cara spoorfing yang melibatkan pengalihan IP status sehingga memyngkinkan situs bisa di ambil alih. Serangan Xnuxer ini berhasil dan bisa memodifikasi website serta mengubah informasi-informasi yang terdapat dalam website milik KPU.
2. Tahun 2016 website milik Tiket.com dan Citilink di retas oleh orang tidak dikenal. Karena kejadian peretasana tersebut perusahaan Tiket.com mengalami kerugian sebesar 4,1 miliar sedangan perusahaan penerbangan citilink mengalami kerugian sebanyak 2 miliar.
3. Di tahun 2020 terdapat berita yang tidak menyenangkann untuk perusahan yang bergerak di bidang e-commerce, Tokopedia. Hal ini karena 91 juta data para pengguna aplikasi Tokopedia ini bocor karena diretas oleh hacker bernama ShinyHunters.
4. Satu tahun berselang terjadi pula peretasan pada data nasabah BRI Life, tepatnya pada bulan juli 2021. Sekitar 2 juta data pelanggan diduga bocor dan dijual secara online oleh pihak yang tidak bertanggung jawab.

Aspek-aspek Keamanan Informasi

Informasi merupakan salah satu aset terpenting perusahaan. Perusahaan memproses data, kemudian hasilnya disimpan dan dibagikan. Menurut Syafrizak, 2015 dalam (Chazar, 2015) Keamanan sistem informasi mencakup perlindungan aspek-aspek berikut:

1. Confidentiality (Kerahasiaan)
   Aspek keamanan data memastikan bahwa hanya orang yang berwenang yang dapat mengakses data dan memastikan keamanan data yang dikirim, diterima, dan disimpan
2. Integrity (Integritas)

Pihak menjamin bahwa data tidak akan dimodifikasi tanpa izin dari otoritas (yang kompeten). Menjaga akurasi dan integritas data dan metode pemrosesan untuk memastikan integritas.

3. Availability (Ketersediaan)
   Aspek yang memastikan bahwa informasi tersedia saat dibutuhkan dan memastikan bahwa pengguna yang berwenang dapat mengakses informasi dan perangkat (aset) terkait.
   hubungi kami jika perlu)

Gambar 1 Aspek Keamanan Informasi

Ancaman Terhadap Sistem Informasi Manajemen (SIM)

Sistem informasi manajemen (SIM) perusahaan melibatkan pengelolaan informasi yang berkaitan dengan berbagai aspek operasional, keuangan, dan manajerial organisasi. Ancaman keamanan dapat berasal dari berbagai sumber, termasuk faktor internal dan eksternal. Berikut ini adalah beberapa ancaman umum yang sering dihadapi oleh sistem informasi bisnis:

1. Serangan Malware:
   Malware seperti virus, worm, Trojan, ransomware, atau spyware dapat merusak atau mencuri informasi perusahaan. Serangan malware dapat datang melalui email, unduhan berbahaya, atau situs web yang terinfeksi.
2. Serangan Peretasan:
   Hacker atau peretas dapat mencoba menyusup ke sistem informasi organisasi untuk mencuri data, mengganggu operasi, atau memanipulasi data. Mereka dapat mengeksploitasi kerentanan perangkat lunak atau melakukan serangan dunia maya.
3. Serangan Denial of Service (DoS):
   Serangan DoS bertujuan untuk menghancurkan ketersediaan sistem dengan membanjiri server dengan lalu lintas yang tidak terkendali. Ini menyebabkan sistem menjadi tidak responsif dan pengguna yang tidak berwenang tidak dapat mengaksesnya.

4. Pencurian/Peniruan identitas:
   Ancaman ini melibatkan pencurian informasi pribadi atau keuangan dari karyawan atau pelanggan, yang dapat digunakan untuk tujuan penipuan atau mendapatkan akses tidak sah ke sistem sistem informasi perusahaan.
5. Pencurian data:
   Pencurian data adalah ancaman di mana orang yang tidak berhak memperoleh akses dan mencuri informasi sensitif perusahaan, seperti informasi pelanggan, rahasia dagang, atau strategi bisnis, yang dapat digunakan untuk tujuan jahat.
6. Serangan fisik:
   Ancaman fisik meliputi pencurian atau kerusakan pada perangkat keras, server, atau infrastruktur fisik organisasi. Serangan ini dapat mengakibatkan hilangnya dan kerusakan data yang signifikan.

7. Menyerang melalui jaringan nirkabel:
   Bisnis yang menggunakan jaringan nirkabel rentan terhadap serangan seperti peretasan Wi-Fi, akses jaringan tanpa izin, atau penyalahgunaan data yang dikirimkan melalui jaringan nirkabel.
8. Kesalahan pengguna:
   Kesalahan atau kelalaian pengguna, seperti memakai kata sandi yang lemah, membuka lampiran email yang mencurigakan, atau mengungkapkan informasi rahasia, dapat menimbulkan risiko keamanan untuk sistem informasi organisasi.

Pengamanan Data Sistem Informasi Manajemen

Menurut (Ardhana, 2012) Ada banyak cara untuk mengamankan data atau informasi pada suatu sistem. Secara umum, keamanan data dapat diklasifikasikan menjadi dua kategori, yaitu:

pencegahan (perwakilan) dan pengobatan (pemulihan)

1. Kontrol akses.
   Kontrol akses dapat dicapai dalam tiga langkah, yaitu:

a. Identifikasi pengguna (user identifier).
   Pengguna pertama mengidentifikasi dirinya dengan menawarkan sesuatu dikenal dengan password atau kata sandi. Pengidentifikasi tersebut dapat mencakup lokasi pengguna, seperti titik akses jaringan dan hak akses telepon.
b. Bukti keaslian pengguna (user authentication).
   Setelah identifikasi pertama, pengguna dapat membuktikan hak aksesnya dengan memberikan informasi sesuatu yang dimilikinya, seperti kartu identitas (smart card, ID dan chip pengenal), tanda tangan, suara atau pola bahasa.
c. Otorisasi pengguna.
   Setelah individu tersebut lulus pemeriksaan identifikasi dan otentikasi, individu tersebut dapat dicocokkan Hak untuk mengakses dan melakukan perubahan pada file atau data.

2. Kontrol serangan pada sistem.
   Sistem pengawasan dirancang untuk mendeteksi penyusup ke dalam sistem (intruder) atau serangan hacker (serangan). Sistem ini sering disebut “Intruder”. "Sistem Pengakuan" (IDS). Sistem ini dapat memberitahu administrator melalui email atau oleh mekanisme lain. Ada beberapa cara untuk mendeteksi penyusup. Ada yang aktif dan pasif IDS secara pasif, misalnya dengan memonitor file log. Berbagai perangkat lunak IDS antara lain:

a. Auotbuse yaitu deteksi port scanning dengan memantau file protokol.
b. Pemblokiran port. Memblokir port tertentu terhadap serangan. Biasanya untuk membuat gerbang blok memerlukan perangkat lunak khusus seperti NinX atau sejenisnya.
c. Courtney and Portsentry, yaitu pendeteksian port scanning dengan monitoring pengiriman paket data.
d. Snort, yang mengenali pola dalam paket data yang dikirimkan dan mengirimkan instruksi siaga ketika sebuah pola dikenali. Template disimpan dalam file yang disebut library dapat dikonfigurasi sesuai kebutuhan.

3. Penggunaan enkripsi.
   Salah satu mekanisme untuk meningkatkan keamanan sistem adalah penggunaan teknologi enkripsi data. Informasi yang dikirimkan diubah sedemikian rupa sehingga tidak mudah diketahui orang lain yang tidak berhak. Ada tiga kategori enkripsi, yaitu:

a. Enkripsi rahasia.
   Ada kunci yang dapat digunakan untuk mengenkripsi dan mendekripsi data.
b. Enkripsi publik.
   Dua kunci digunakan, satu kunci digunakan untuk melakukan enkripsi dan kunci lainnya digunakan untuk melakukan proses dekripsi.

c. Operasi searah.
Proses mengenkripsi data untuk membuat "signnature" untuk data asli dapat digunakan untuk tujuan otentikasi.
Enkripsi didasarkan pada algoritme yang dapat mengacak data ke dalam format yang tidak dapat dibaca atau rahasia, sedangkan dekripsi didasarkan pada algoritme pemulihan data yang sama dicampur dengan bentuk asli atau dapat dibaca.

4. Buat cadangan secara teratur.
Agar penyusup tidak dapat mencuri, menghapus, atau bahkan mengubah seluruh konten file penting, pencadangan data reguler sangat penting.

KESIMPULAN DAN SARAN

Kesimpulan

Keamanan informasi adalah cara untuk mencegah penipuan (scam) atau setidaknya mendeteksi penipuan dalam sistem data di mana data itu sendiri tidak memiliki arti fisik. Karena ruang lingkup keamanan informasi telah diperluas, demikian pula pandangan tentang tanggung jawab manajemen. Manajemen diharapkan tidak hanya memastikan keamanan aset informasi, tetapi juga menjaga agar bisnis tetap berjalan setelah bencana atau pelanggaran keamanan.

Saran

Keamanan sistem informasi manajemen harus dimulai ketika sistem Informasi tidak diciptakan hanya untuk melengkapi sistem informasi. Keamanan sistem informasi manajemen yang baik harus memungkinkan perusahaan untuk mengantisipasi risiko yang timbul dari penggunaan sistem informasi sehingga risiko yang dapat merugikan perusahaan dapat dihindari atau dikurangi.

DAFTAR PUSTAKA

Ardhana, Y. M. K. (2012). *KEAMANAN SISTEM INFORMASI* (Vol. 2, Issue 2). Www.Klikbca.Co.Id,

Aswiputri, M. (2022). LITERATURE REVIEW DETERMINASI SISTEM INFORMASI MANAJEMEN: DATABASE, CCTV DAN BRAINWARE. *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(3). Https://Doi.Org/10.31933/Jemsi.V3i3

Chazar, C. (2015). STANDAR MANAJEMEN KEAMANAN SISTEM INFORMASI BERBASIS ISO/IEC 27001:2005. *Jurnal Informasi*, *7*(2).

Galih, A. P. (2019). KEAMANAN INFORMASI (INFORMATION SECURITY) PADA APLIKASI PERPUSTAKAAN Ipusnas. *Journal Of Data And Information Quality*, *11*(2). Https://Doi.Org/10.1145/3297721

Endra, W. G. B. (2022). LITERATURE REVIEW KOMPONEN SISTEM INFORMASI MANAJEMEN: SOFTWARE, DATABASE DAN BRAINWARE. *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(3). Https://Doi.Org/10.31933/Jemsi.V3i3

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022a). FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM). *Jurnal Ekonomi Manajemen Sisitem Informasi*, *3*(5). Https://Doi.Org/10.31933/Jemsi.V3i5

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022b). *FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)*. *3*(5). Https://Doi.Org/10.31933/Jemsi.V3i5

Ramadhani, A. (2018). KEAMANAN INFORMASI. In *JILS Journal Of Information And Library Studies* (Vol. 1, Issue 1).

Wahyudi, I. (2022). LITERATURE REVIEW: DETERMINASI SISTEM INFORMASI MANAJEMEN DENGAN LINGKUNGANNYA. *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(3). Https://Doi.Org/10.31933/Jimt.V3i3