Jurnal ilmiah Sistem Informasi dan Ilmu Komputer
Vol. 3 No. 2 Juli 2023
p-ISSN: 2827-8135 e-ISSN : 2827-7953, Hal 143-152
DOI: https://doi.org/10.55606/juisik.v3i2.496

Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review

Achmad Mukhlis
Universitas Pembangunan "Veteran" Jawa Timur, Indonesia

Baiq Laila Alfila
Universitas Pembangunan "Veteran" Jawa Timur, Indonesia
Korespondensi penulis: baiqlailaalfilaa@gmail.com

Aliya Zhafira Wastuyana
Universitas Pembangunan "Veteran" Jawa Timur, Indonesia

Abstract*. This research aims to analyze security threats that occur in information systems and ways to overcome them. The method used in this research is Systematic Literature Review, where articles related to security threats in information systems are collected and analyzed qualitatively. The results show that there are various kinds of security threats in information systems, such as hacking, sabotage, espionage, and others. These threats can damage data, steal information, or disrupt system integrity. To overcome these threats, prevention and treatment efforts are needed. Prevention is done to prevent damage, loss, or theft of data, while treatment is done if data has already been attacked. Some ways to improve information system security include improving HR knowledge related to cyber threats, implementing readiness certification, and adopting security domains from other countries. Mapping the types of cyberattacks and selecting appropriate security technologies are also important. Some other efforts include regular operating system updates, applying encryption to data, controlling access, using firewall technology, and implementing standard operating procedures (SOPs) and privacy policies. This research can serve as a guide in developing effective policies and measures in maintaining information system security.*

Keywords: *Information Systems, Security Threats, Information System Security, Prevention.*

Abstrak. Penelitian ini bertujuan untuk menganalisis ancaman keamanan yang terjadi dalam sistem informasi dan cara untuk mengatasinya. Pendekatan yang diterapkan dalam penelitian ini adalah Systematic Literature Review, di mana artikel-artikel terkait ancaman keamanan dalam sistem informasi dikumpulkan dan dianalisis secara kualitatif. Hasil penelitian menunjukkan bahwa terdapat berbagai macam ancaman keamanan dalam sistem informasi, seperti hacking, sabotase, spionase, dan lain-lain. Ancaman tersebut dapat merusak data, mencuri informasi, atau mengganggu integritas sistem. Untuk mengatasi ancaman ini, diperlukan upaya pencegahan dan pengobatan. Pencegahan dilakukan untuk mencegah kerusakan, kehilangan, atau pencurian data, sedangkan pengobatan dilakukan jika data sudah terkena serangan. Beberapa cara untuk meningkatkan keamanan sistem informasi termasuk meningkatkan pengetahuan SDM terkait ancaman siber, menerapkan sertifikasi kesiapan, dan mengadopsi domain

Received April 03, 2023; Revised Mei 01, 2023; Accepted Juni 20, 2023
* Baiq Laila Alfila, baiqlailaalfilaa@gmail.com

keamanan dari negara lain. Selain itu, pemetaan jenis serangan siber dan pemilihan teknologi keamanan yang sesuai juga penting. Beberapa upaya lain termasuk pembaruan sistem operasi secara berkala, menerapkan enkripsi pada data, mengontrol akses, menggunakan teknologi firewall, serta mengimplementasikan prosedur operasional standar (SOP) dan kebijakan privasi. Penelitian ini dapat menjadi panduan dalam mengembangkan kebijakan dan langkah-langkah yang efektif dalam mempertahankan keamanan sistem informasi.

Kata Kunci: Sistem Informasi, Ancaman Keamanan, Keamanan Sistem Informasi, Pencegahan.

LATAR BELAKANG

Sejalan dengan kemajuan teknologi dibidang komputer dan internet, muncul berbagai kemudahan dalam sistem informasi yang berdampak positif sehingga membuat masyarakat ketergantungan akan teknologi tersebut. Dengan alasan kemudahan, masyarakat akan dengan gampang memberikan data dirinya kedalam sistem. Oleh karena itu, terdapat banyak informasi yang sifatnya sangat rahasia dan perlu untuk dilindungi.

Dibalik kemudahan yang ditawarkan teknologi informasi, terdapat berbagai kejahatan yang mengancam. Ancaman tersebut datang dari pelaku kejahatan yang memanfaatkan kemajuan teknologi untuk melakukan pencurian data, pemerasan informasi, pencemaran nama baik, provokasi, maupun propaganda dengan tujuan mencari keuntungan. Pelaku kejahatan tersebut tentunya akan melakukan berbagai cara seperti melakukan hacking, phising, malware, dan sebagainya untuk mencapai tujuannya. Tanpa adanya perlindungan atau pengawasan keamanan sistem yang baik maka tingkat kemungkinan terjadinya kehilangan aset informasi berharga akan semakin tinggi. Oleh sebab itu, perlu dilakukan tindakan pencegahan serta pengamanan sistem informasi agar meminimalisir terjadinya serangan siber yang dapat menimbulkan kerugian pada individu maupun kelompok tertentu.

Upaya pengamanan sistem informasi harus menerapkan berbagai kebijakan dan tindakan yang dapat mencegah, memantau, atau mengatasi segala akses yang tidak sah. Dengan dilakukannya pencegahan maka diharapkan agar berbagai data dan aset-aset penting tidak dapat diganggu, dirusak, ataupun dicuri oleh orang-orang yang tidak bertanggung jawab.

Dengan demikian, penelitian ini memiliki tujuan utama yaitu untuk mengidentifikasi apa saja ancaman-ancaman yang dapat terjadi pada keamanan sistem informasi dan juga terdapat langkah yang dapat dilakukan untuk mengatasi ancaman tersebut.

METODE PENELITIAN

Penelitian ini bertujuan untuk menganalisis ancaman keamanan yang ada dalam Sistem Informasi. Bahan yang diteliti adalah artikel-artikel yang dipublikasikan dalam periode lima tahun terakhir, yaitu antara tahun 2018 hingga 2023. Pendekatan yang diterapkan dalam penelitian ini adalah Systematic Literature Review. SLR merupakan metode yang melibatkan langkah-langkah sistematis dalam mengumpulkan, mengevaluasi, dan menyusun penelitian yang relevan dengan topik yang sedang diteliti (Lusiana & Suryani, 2014). Dalam penelitian ini, langkah-langkah SLR digunakan untuk mengidentifikasi dan menganalisis artikel-artikel yang relevan dengan ancaman keamanan sistem informasi.

HASIL DAN PEMBAHASAN

Artikel yang digunakan pada pembahasan ini diambil dari google scholar dengan rentang tahun 2018-2023, diperoleh hasil sebanyak 25.600 untuk kata kunci “ancaman keamanan”, 18.000 untuk kata kunci “penanganan keamanan”, dan 65.200 untuk kata kunci “keamanan”. Selanjutnya, dilakukan pemilihan artikel berdasarkan abstrak yang sesuai dengan penelitian ini. Dari hasil pemilihan tersebut, didapatkan sejumlah 16 artikel dari berbagai sumber.

Tabel 1. Klasifikasi Artikel Berdasarkan Tahun Terbit

Tahun	Jumlah
2018	1
2019	2
2020	5
2021	6
2022	2
Total	16

Tabel 2. Klasifikasi Artikel Berdasarkan Kata Kunci

Kata Kunci	Jumlah
Ancaman Keamanan	7
Penanganan Keamanan	5
Keamanan	4
Total	16

Tabel 3. Klasifikasi Artikel Berdasarkan Topik

Topik	Jumlah	Penulis
Ancaman dan Penanggulangan Keamanan Sistem Informasi	4	(Rahmawati, 2019; Bustami & Bahri, 2020; Yuliana et al., 2022; Munawar & Putri, 2020)
Peningkatan Keamanan sebagai Antisipasi	7	(Herdiana *et al.*, 2021; Dwinanto & Setiyani, 2021; Hariyadi & Nastiti, 2021; Yel & Nasution, 2022; Laksono & Prayudi, 2021; Putri *et al.*, 2021; Prakasa, 2020)
Upaya dan Kebijakan Indonesia Menghadapi Siber	5	(Arianto & Anggraini, 2019; Rumlus & Hartadi, 2020; Primawanti, 2020; Babys, 2021; Tumalun, 2018)

Ancaman Sistem Informasi

Perkembangan sistem membuka celah bagi penjahat siber untuk memberi berbagai ancaman yang bisa merusak keamanan penggunanya. Berbagai macam cara dapat dilakukan oleh pelaku untuk merusak keamanan sistem informasi yang ada. Beberapa bentuk kejahatan siber yang dituliskan oleh Babys (2021) adalah hacking yang merupakan penerobosan kedalam program untuk merusak maupun mencuri data, sabotase yang merupakan proses membuat gangguan dan perusakan data, program, maupun sistem jaringan, spionase yang merupakan penggunaan internet untuk memata-matai pihak lain dengan penerobosan sistem jaringan korban, cyber attack yang merupakan proses untuk mengganggu kerahasiaan informasi dan integritas informasi dengan mencuri informasi khusus, garding yang merupakan penggunaan identitas orang lain untuk berbelanja, dan vandalism yang merupakan perusakan halaman web atau penggunaan denial of service yang merusak sumber daya komputer. Ancaman lain yang ditemukan oleh Laksono (2021) saat melakukan threat modelling pada Universitas XYZ adalah spoofing, tempering, dan repudiation.

Kondisi pandemi pada tahun 2019 lalu yang mengharuskan semua aktifitas dilakukan dari rumah dan banyak menggunakan internet, membuat banyak melakukan hal yang merugikan orang lain demi mendapatkan keuntungan pribadi dengan melakukan phising, ransoworm, dan malware (Hediana, 2021). Serangan phising hanya membutuhkan 30% tingkat keberhasilan untuk mendapatkan keuntungan pribadi yang merugikan orang lain. Untuk meningkatkan kewaspadaan kita dalam melihat ancaman siber, OSSEC dapat digunakan sebagai alat pemantau server dalam mode agent. Seperti hal yang dilakukan oleh Yuliana (2022) bersama dengan rekan-rekannya yang membangun server cloud dan melakukan percobaan serangan pada OSSEC agent. Hasil percobaan serangan menunjukkan bahwa OSSEC mampu mendeteksi serangan meskipun tidak selalu menampilkan alert karena koneksi tidak stabil dan lokasi pengujian telah memiliki sistem penjagaan dari DDoS.

Peningkatan Keamanan Sistem Informasi

Dalam meningkatkan keamanan sistem informasi, kesiapan Indonesia diperlukan. Pengetahuan mengenai bahaya serangan siber oleh masyarakat Indonesia serta sertifikasi kesiapan memasuki revolusi industry 4.0 diperlukan setiap perusahaan (Rahmawati, 2019). Selain itu, Rahmawati (2019), mengusulkan empat domain dari US yang dapat

diadopsi Indonesia. Domain tersebut meliputi operasional siber (pelindung ICT, penyedia dan pengoprasi jaringan militer, serta menjadi pelindung untuk ruang siber dengan cakupan net-centric, sistem serta jaringan), intelijen siber (pendukung operasi intelijen dengan siber), *cyber crime* (penegakkan hukum dan keamanan dalam dunia maya), dan operasional informasi (pengamanan informasi dengan penggunaan teknologi informasi dalam bidang ekonomi, ilmu dan pengetahuan, politik, militer, dan diplomatik). Selain kesiapan, pemetaan jenis serangan siber perlu ditentukan untuk penyesuaian teknologi keamanan. Teknologi keamanan yang sesuai dapat ditetapkan sebagai antisipasi dan perlindungan dari berbagai ancaman yang ada (Bustammi, 2020). Aspek keamanan CIA confidentiality, integrity, and availability) dapat menjadi acuan keamanan komputer yang dapat meminimalisir ancaman pada komputer dengan Linux Fedora sebagai OSnya (Dwianto, 2021). Ia juga menyebutkan bahwa pembaruan OS secara berkala, pengecekan data dengan tools hashing, pembuatan kata sandi pada file sebelum dikirim, dan membedakan user privilege dengan user biasa menjadi cara untuk meminimalisir ancaman yang bisa muncul. Enkripsi data, kontrol akses, dan teknologi firewall juga menjadi cara untuk mencegah datangnya ancaman yang dapat merusak keamanan (Munawar, 2020). Enkripsi data merupakan proses data khusus untuk menyembunyikan atau mengkhususkan data dalam bentuk pribadi maupun public, kontrol akses merupakan verifikasi data pengguna yang melakukan akses komputer, artinya informasi hanya terbuka untuk pengguna yang membutuhkan, sedangkan teknologi firewall adalah alat yang dapat mencegah orang lain menggunakan komputer pribadi, mencegah orang lain mendekati sistem pertahanan, dan memfilter situs yang dapat membahayakan komputer. SOP (Standar Operasional Prosedur) dan kebijakan privasi juga harus diterapkan oleh pengembang sistem karena administrator memiliki akses penuh pada data pengguna sehingga, mereka perlu membangun kepercayaan pengguna dan mencegah adanya keamanan informasi pengguna terjaga (Yel, 2020).

Komputasi awan yang merupakan penggabungan beberapa teknologi yang memanfaatkan internet sebagai jaringan pengiriman bisa menjadi salah satu alat untuk membantu meningkatkan keamanan sistem (Putri, 2021). Ia menyebutkan, teknologi yang disediakan pihak ketiga ini dapat membantu melakukan pelacakan sumber serangan melalui Cloud TraceBack. Selain itu, teknologi ini dapat melakukan pemeriksaan, filter, dan identifikasi banyak pesan serangan beserta sumbernya dalam waktu singkat. Tetapi,

teknologi ini memiliki beberapa faktor yang dapat melumpuhkan penggunaan. Salah satunya adalah transparansi yang melarang adanya izin bagi para pelanggan untuk memantau, sehingga pelanggan tidak tahu apa yang terjadi dan bagaimana data tersimpan. Pelanggan juga tidak bisa mengetahui saat ada penyerangan yang datang. Selain komputasi awan, Sudomy dan OWASP ZAP dapat menjadi alat yang membantu penggunanya untuk mengetahui seberapa besar ancaman keamanan yang bisa masuk. Hariyadi (2021) bersama beberapa rekannya melakukan analisis dengan menggunakan OWASP ZAN dan Sudomy yang merupakan *software* berlisensi free open source software, pemindaian berkala dengan metode information gathering dan network mapping dilakukan di domain udb.ac.id pada Universitas Duta Bangsa Surakarta. Mereka melakukan pemindaian dari aplikasi Sudomy menghasilkan daftar alamat IP yang memiliki beberapa sub-domain dengan status aktif berdasarkan pendeteksian dengan teknik ping sweep. Hasil sudomy kemudian dipetakan dengan phyton pyvis yang menunjukkan persebaran jaringan penggunaan dan alokasi alamat IP dan gambar sub-domain udb.ac.id. Selanjutnya vulnerability identification dilakukan menggunakan OWASP ZAP yang menunjukkan grafik potensi celah keamanan yang memiliki 4 tingkatan, yaitu high, medium, low, dan informational. Grafik menunjukkan bahwa sebagian besar domain dan subdomain memiliki celah keamanan dengan tingkat low.

Upaya dan Kebijakan Indonesia dalam Menghadapi Ancaman Siber

Indonesia merupakan negara yang menduduki posisi pertama pada besarnya potensi untuk menjadi target hacker. Berdasarkan studi Geometri Politika, fungsional siber memiliki dua domain yaitu geometrik militer dan geometrik sipil (Arianto, 2019). Geometrik militer merupakan fungsionalitas siber dalam politik tingkat tinggi yang berupa pembentukan dan pengaktifan kekuatan siber untuk menghadapi *global cyber war, geometric international war,* dan kompleksitas pembangunan negara siber. Sedangkan geometric sipil merupakan fungsionalitas dalam politik tingkat normal dalam bentuk perlindungan terhadap seluruh aktivitas siber sipil. Indonesia sebagai salah satu anggota aktif ASEAN dapat dimanfaatkan dalam membangun keamanan siber yang merupakan kepentingan nasional. Dalam forum regional ASEAN pada tahun 2015, Indonesia mengusulkan pembentukan kurikulum khusus untuk meningkatkan capacity building dalam menghadapi ancaman siber tingkat regional, upgrade Internet Protocol ver.4 ke Internet Protocol ver.6, pembentukan lembaga cybersecurity untuk menangani

kejahatan siber, dan membuat kontak poin (point of contacy) dari masing-masing anggota ASEAN untuk memudahkan Indonesia dalam proses diplomasi dengan pencapaian bersama (Primawati, 2020).

Indonesia memiliki beberapa kebijakan mengenai perlindungan data pribadi dalam beberapa undang-undang. Salah satunya tercantum dalam UU ITE (Informasi dan Transaksi Elektronik) yang membahas mengenai perlindungan dari penggunaan dan akses illegal (Rumlus, 2020). Kemudian ada peraturan pemerintah No.17 tahun 2019 membahas mengenai penyelenggaraan sistem dan transaksi elektronik, UU No.10 tahun 1998 membahas mengenai perbankan, dan UU No.11 tahun 2008 yang membahas mengenai informasi dan transaksi elektronik. Pada pasal 30 UU ITE, pelarangan mengenai akses ilegal dijabarkan, dan pada pasal 46 UU ITE, ketentuan pidana mengenai pasal 30 UU ITE dijelaskan. Meskipun Indonesia sudah membuat undang-undang mengenai hukum pidana kejahatan siber yang ada, tetapi penggunaannya belum maksimal. Hal ini ditunjukkan dengan munculnya berbagai laporan mengenai kejahatan siber yang meningkat pada berbagai pengamat dan laporan statistik kejahatan siber di Indonesia.

KESIMPULAN

Berdasarkan penelitian systematic review terkait artikel ancaman, penanganan, dan keamanan sistem informasi, diambil kesimpulan bahwa saat ini terdapat banyak cara yang dilakukan penjahat siber untuk merusak dan mengganggu keamanan sistem seperti hacking, spoofing, tempering, repudiation, phising, ransoworm, dan malware. Dengan mengetahui berbagai serangan, maka dapat dilakukan pengamanan serta antisipasi untuk menjaga keamanan dalam berbagai aspek. Untuk langkah awal pengamanan, kesiapan Indonesia beserta pengetahuan dari sumber daya manusianya tentang bahaya serangan siber sangat diperlukan. Selanjutnya, beberapa cara yang dapat dilakukan adalah dengan memperbaharui sistem secara berkala, mengecek data menggunakan tools hashing, mengenkripsi data, menerapkan SOP (Standar Operasional Prosedur), dan menggunakan komputasi awan, Sudomy, atau OWASP ZAP untuk mengetahui seberapa besar ancaman yang bisa masuk.

DAFTAR REFERENSI

Arianto, A. R., & Anggraini, G. (2019). MEMBANGUN PERTAHANAN DAN KEAMANAN SIBER NASIONAL INDONESIA GUNA MENGHADAPI ANCAMAN SIBER GLOBAL MELALUI INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, *9*(1), 13-29. http://download.garuda.kemdikbud.go.id/article.php?article=2421466&val=23123&title=MEMBANGUN%20PERTAHANAN%20DAN%20KEAMANAN%20SIBER%20NASIONAL%20INDONESIA%20GUNA%20MENGHADAPI%20ANCAMAN%20SIBER%20GLOBAL%20MELALUI%20INDONESIA%20SECURITY%20INCIDENT%20RESPONSE%

Babys, S.A.M. (n.d.). ANCAMAN PERANG SIBER DI ERA DIGITAL DAN SOLUSI KEAMANAN NASIONAL INDONESIA. *JURNAL ORATIO DIRECTA*, *3*(1), 425-442. https://www.ejurnal.ubk.ac.id/index.php/oratio/article/view/163/116

Bustami, A., & Bahri, S. (2020). ncaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review. *Jurnal Pendidikan dan Aplikasi Industri (UNISTEK)*, *7*(2), 60-70. https://core.ac.uk/reader/337313970

Dwinanto, I., & Setyiani, H. (2021). IMPLEMENTASI KEAMANAN KOMPUTER PADA ASPEK CONFIDENTIALITY, INTEGRITY, AVAILABILITY (CIA) MENGGUNAKAN TOOLS LYNIS AUDIT SYSTE. *Jurnal Maklumatika*, *8*(1), 35-46. https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/117

Fachrezi, M. I., Cahyonno, A. D., & Tanaem, P. F. (2021). Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga. *Jurnal Teknik Informatika dan Sistem Informasi*, *8*(2), 764-773. https://jurnal.mdp.ac.id/index.php/jatisi/article/view/789

FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM). (2022). *JEMSI: Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(3), 564-573. https://doi.org/10.31933/jemsi.v3i5

Hariyadi, D., & Nastiti, F.E. (2021). Analisis Keamanan Sistem InformasiMenggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta. *urnal Komtika (Komputasi danInformatika)*, *5*(1), -42. http://journal.unimma.ac.id/index.php/komtika/article/view/5134

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology*, *20*(1), 42-52. http://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/58

Laksono, A. C., & Prayudi, Y. (2021). p-ISSN : 2502-5724; e-ISSN : 2541-5735 9Threat Modeling Menggunakan Pendekatan STRIDEdan DREADuntuk Mengetahui Risiko dan Mitigasi Keamananpada Sistem Informasi Akademik. *Jurnal Sistem dan Teknologi Informasi Indonesia*, *6*(1), 9-21. http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO/article/view/3944/3023

Lusiana, & Suryani, M. (2014). Metode SLR untuk Mengidentifikasi Isu-Isu dalam Software Engineering. *SATIN: Sains dan Teknologi Informasi*, *3*(1), 1-11. http://bpm.stmik-amik-riau.ac.id/index.php/satin/article/view/347#:~:text=Dengan%20metode%20SLR%20isu-isu%20yang%20berhubungan%20dalam%20software,to%20solve%20the%20problem%E2%80%9D%20%28bagaimana%20memecahkan%20masalah%20tersebut%29

Munawar, Z., & Putri, N.I. (2020). KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA. *Jurnal Sistem Informasi*, *2*(1), 14-20. https://unibba.ac.id/ejournal/index.php/j-sika/article/view/275

Primawanti, H., & Pangestu, S. (2020). DIPLOMASI SIBER INDONESIA DALAM MENINGKATKAN KEAMANAN SIBER MELALUI ASSOCIATION OF SOUTH EAST ASIAN NATION (ASEAN) REGIONAL FORUM. *Jurnal Ilmiah Hubungan Internasional*, *2*(2), 1-15. https://journal2.unfari.ac.id/index.php/globalmind/article/view/89

Putri, N.I., Musadad, D.Z., Munawar, Z., & Komalasari, R. (2021). STRATEGI DAN PENINGKATAN KEAMANAN PADA KOMPUTASI AWAN. *Jurnal Sistem Informasi*, *3*(1). https://ejournal.unibba.ac.id/index.php/j-sika/article/view/533

Rahmawati, C. (2019). Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. *Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU*, *1*(1), 299-306. https://aau.e-journal.id/senastindo/article/view/116

Rumlus, M.H., & Hartadi, H. (n.d.). KEBIJAKAN PENANGGULANGAN PENCURIAN DATA PRIBADI DALAM MEDIA ELEKTRONIK. *Jurnal HAM*, *11*(2), 285-299. https://ejournal.balitbangham.go.id/index.php/ham/article/view/1059

Tumalun, B. (2018). UPAYA PENANGGULANGAN KEJAHATAN KOMPUTER DALAM SISTEM ELEKTRONIK MENURUT PASAL 30 UNDANG-UNDANG NOMOR 11 TAHUN 2008. *Lex Et Societatis*, *VI*(2), 24-31. https://ejournal.unsrat.ac.id/index.php/lexetsocietatis/article/view/19950

Yel, M.B., & Nasution, M.K. (2022). KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92-101. https://jurnal-backup.kaputama.ac.id/index.php/JIK/article/view/768

Yuliana, Y., Mooduto, H. A., & Hadi, R. (n.d.). Deteksi Ancaman Keamanan Pada Server dan Jaringan Menggunakan OSSEC. *Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 8-15. https://jurnal-itsi.org/index.php/jitsi/article/view/58