Jurnal Riset Bisnis dan Ekonomi Digital
Publikasi oleh: Yayasan Literasi Emas Nusantara
E-ISSN: 3064-6367 | Doi : doi.org/jrbed.v2i3.2025

Dampak Audit Keamanan Siber Terhadap Perlindungan Data Organisasi

Dea Sirait [1] , Shafira Frarisya P [2], Juan Philip Samosir [3], Rio Partahi Pasaribu [4]

Jurusan Akuntansi, Universitas Prima Indonesia, deahasiholan@gmail.com

Abstract

Tujuan dari penelitian ini adalah untuk mengetahui serangan siber yang semakin marak terhadap organisasi pemerintah atau publik diikuti oleh peningkatan kecepatan teknologi informasi saat ini. Serangan siber mengakibatkan kerusakan materi dan infrastruktur serta informasi organisasi. Untuk mencegah ancaman siber, perlu dilakukan penjaminan kualitas untuk melindungi informasi dengan memastikan bahwa data tidak dapat diakses oleh pihak yang tidak berkepentingan dan bahwa informasi yang disimpan tetap akurat dan rahasia. Arsitektur TISA (Trust Information Security Architecture) digunakan untuk melakukan penjagaan serangan siber dan terdiri dari tahapan perlindungan data, aturan keamanan informasi, dan prosedur keamanan. Arsitektur ini diterapkan sesuai dengan kriteria kualitas pada sistem untuk menjamin keamanan yang baik dan berdasarkan framework penjaminan keamanan yang disesuaikan dengan masalah keamanan yang terjadi.

Keywords: Audit Keamanan Siber, Perlindungan Data Organisasi

Corresponding Author: Dea Sirait
Email: deahasiholan@gmail.com
Publication Date: Desember, 2025

Pendahuluan

Audit investigasi sendiri audit yang dilakukan sebagai upaya untuk mengungkap adanya indikasi kuat adanya kecurangan yang bisa mengakibatkan kerugian kepada sejumlah pihak terkait, baik itu terhadap perorangan maupun institusi, audit yang bertujuan untuk mengungkap dan membuktikan adanya dugaan penyimpangan atau kecurangan, serta mengidentifikasi pelaku dan bukti-bukti yang relevan untuk tindakan hukum selanjutnya Sementara teknik audit investigasi merupakan cara-cara atau metode yang digunakan auditor untuk mengumpulkan dan mengevaluasi bukti, mengaudit kewajaran dan memastikan keakuratan penyajian suatu catatan laporan keuangan dan hasil dari penerapan audit sendiri yang tidak lain adalah bukti audit serta mencapai tujuan audit. Audit investigasi suatu bentuk audit atau pemeriksaan yang bertujuan untuk mengidentifikasi dan mengungkap kecurangan atau kejahatan dengan menggunakan pendekatan, prosedur atau teknik-teknik yang umumnya digunakan dalam suatu penyelidikan atau penyidikan terhadap suatu kejahatan. ((Fiar & Jaeni, 2022)

Berdasarkan laporan Interpol Cyber Assessment Report 2021, terdapat sekitar 2,7 juta serangan ransomware yang terdeteksi di Asia Tenggara pada periode Januari-September 2020, dengan Indonesia berada di peringkat teratas dengan 1,3 juta kasus. Kemudian berdasarkan data dari Bareskrim Polri, terjadi peningkatan drastis dalam jumlah kasus kejahatan siber yang ditangani. Pada tahun 2022, terdapat 8.831 kasus kejahatan siber yang ditindak, meningkat hingga 14 kali lipat dibandingkan dengan tahun 2021, di mana jumlah kasus yang ditindak hanya 612. Selain itu, riset dari Fortinet mengungkapkan bahwa serangan siber ransomware di Indonesia meningkat dua kali lipat selama tahun 2023, dengan target utama adalah perusahaan swasta. Kasus spesifik termasuk peretasan terhadap aplikasi Jakarta Kini (Jaki) yang terjadi setelah disinggung dalam debat capres. Data-data di atas menunjukkan kejahatan siber yang terjadi di Indonesia. Kejahatannya yang terus meningkat dan besarnya kerugian yang dihadapi membuat kejahatan siber ini menjadi semakin mengkhawatirkan. Di samping itu, meskipun upaya pencegahan kejahatan siber ini telah dilakukan namun belum menunjukkan hasil sebagaimana yang diharapkan. Untuk menghadapi tantangan keamanan siber, Pemerintah Indonesia telah mengambil langkah proaktif dengan memperkuat infrastruktur keamanan digital nasional. Upaya ini meliputi pengembangan kebijakan, peningkatan

teknologi keamanan, dan program kesadaran masyarakat tentang risiko keamanan siber. Salah satu langkah utama yang telah diambil adalah pengesahan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). (Rahman Najwa, 2024)

Kebijakan cyber security Indonesia mulai telihat saat pengesahan aturan hukum dalam Peraturan Menteri Komunikasi dan Informatik No. 26 / PER / M.Kominfo /5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Aturan lainya tentang cyber security Indonesia tertuang dalam pedoman pertahanan siber yang dikeluarkan oleh kementerian pertahanan Indonesia pada tahun 2014 yaitu peraturan menteri pertahanan republik Indonesia Nomor 82 Tahun 2014. Aturan lainya berkaitan dengan pendirian lembaga negara khusus yang mengatur dan mengurusi masalah siber di Indonesia yang diberi nama Badan Siber dan Sandi Negara (BSSN) lewat peraturan Presiden Nomor 53 Tahun 2017. Badan Siber dan Sandi Negara (BSSN) sendiri merupakan alat pemerintahan yang didirikan atas dasar tumpeng tindihnya kewenangan, tugas dan fungsi dari beberapa lembaga yang membidangi masalah siber sebelumnya seperti Kementerian Komunikasi dan Informasi (Kominfo), Badan Intelegen Negara (BIN), Aspek lainya pada bagian capacity building Indonesia terlihat mulai memberikan perhatian khusus terhadap penanganan masalah siber di Indonesia, seperti penggagasan aturan undang-undang ITE sebagai upaya pencegahan perbuatan yang dapat membahayakan persatuan dan keamanan dan pertahanan negara. (Rifqy et al., 2023)

Menurut Sondang dalam Othenk (2008) dimana efektivitas pemanfaatan sumber daya sarana dan prasarana dalam jumlah tertentu yang secara sadar ditetapkan sebelumnya untuk menghasilkan sejumlah barang atas jasa kegiatan yang dijalankan. Robbins (2003) mengatakan bahwa efektivitas berkaitan dengan kemampuan untuk memilih atau melakukan sesuatu yang paling sesuai atau tepat dan mampu memberikan manfaat secara langsung.(Permana & Zainol, 2025)

Resiko serangan, dalam konteks keamanan siber, kemungkinan terjadinya kerugian atau dampak negatif (seperti kehilangan data, gangguan operasional, atau kerugian keuangan) akibat serangan siber yang ditujukan kepada sistem, jaringan, atau data suatu organisasi atau individu. Dampak risiko siber kerusakan data, pencurian data, pencurian data intelektual, hilangnya produktivitas, kerusakan reputasi, kerugian keuangan, masalah hukum dan tanggung jawab, dan gangguan operasional.(Aji, 2023)

Insiden kebocoran data nasional tahun 2024 tidak hanya menjadi peristiwa teknis, tetapi juga fenomena sosial dan politik yang mengguncang kepercayaan masyarakat terhadap pemerintah. Dampaknya terasa luas, mulai dari gangguan layanan publik, potensi penyalahgunaan data pribadi, hingga meningkatnya kecemasan masyarakat akan keamanan digital di era keterbukaan informasi. Salah satu penyebab utama kebocoran data nasional adalah lemahnya implementasi kebijakan keamanan siber, baik dari aspek teknis maupun regulasi. Studi Tanjung & Febrianisa (2024) menyoroti bahwa penggunaan kata sandi yang lemah dan tidak adanya standar minimum keamanan yang ketat di banyak instansi pemerintah menjadi pintu masuk utama bagi peretas. Regulasi yang ada, seperti UU ITE dan beberapa peraturan turunan, dinilai belum cukup spesifik dan tegas dalam mengatur praktik keamanan teknis, seperti penggunaan autentikasi dua faktor, enkripsi, serta audit keamanan berkala. Selain itu, penegakan hukum yang lemah dan kurangnya sumber daya untuk pengawasan memperparah kerentanan sistem data nasional. Evaluasi terhadap kebijakan dan regulasi keamanan siber di Indonesia mengungkapkan adanya gap antara regulasi, implementasi, dan perkembangan ancaman siber. Penelitian Bahtiar (2022) dan Sarjito (2024) mengidentifikasi bahwa regulasi sistem perlindungan data pribadi di Indonesia masih lemah dan belum komprehensif, ditandai dengan lambatnya pengesahan UU Perlindungan Data Pribadi (PDP) dan belum adanya standar yang jelas untuk perlindungan data di sektor publik maupun swasta. Sementara itu, ancaman siber terus berkembang dengan teknik yang semakin canggih, menuntut respons kebijakan yang adaptif dan kolaboratif lintas sektor.(Bua & Idris, 2025)

Penelitian mengenai audit keamanan siber terhadap perlindungan data organisasi perusahaan sangat penting dilakukan mengingat tingginya angka kecurangan yang terjadi di berbagai sektor. Kecurangan tidak hanya merugikan perusahaan secara finansial, tetapi juga dapat menghancurkan reputasi dan kepercayaan publik terhadap institusi. Dengan semakin kompleks teknologi informasi, metode kecurangan juga semakin canggih, sehingga diperlukan pendekatan yang efektif untuk mendeteksinya. Penelitian ini dapat

memberikan wawasan tentang bagaimana audit keamanan siber dapat berfungsi sebagai alat pencegah yang efektif.(Mauliza et al., 2022). Berdasarkan latar belakang di atas peneliti mengajukan sebuah penelitian dengan judul "**Dampak Audit Keamanan Siber terhadap Perlindungan Data Organisasi**".

TELAAH LITERATUR DAN HIPOTESIS PENELITIAN

Dampak Audit

Secara umum, dampak audit didefinisikan sebagai segala pengaruh atau konsekuensi yang ditimbulkan oleh proses audit terhadap kualitas laporan keuangan, tingkat kepercayaan pemangku kepentingan, pencegahan kecurangan, efisiensi pelaporan, dan pengelolaan risiko dalam organisasi. Menurut Ciciliawanti (2023), Budiantoro et al. (2022), dan Astuti & Suprantiningrum (2022) Dampak audit, khususnya audit internal, adalah pengaruh signifikan terhadap kualitas laporan keuangan. Audit internal meningkatkan keandalan, transparansi, dan kredibilitas laporan keuangan, sehingga laporan tersebut dapat dipercaya oleh para pemangku kepentingan. Semakin baik pelaksanaan audit internal, semakin tinggi kualitas pelaporan keuangan yang dihasilkan. (Fianda Prathitaningtyas et al., 2024) Menurut penelitian internasional tahun 2020, audit TI (IT audit) berperan penting dalam memastikan kerahasiaan, integritas, dan ketersediaan data. Audit ini juga membantu organisasi menyesuaikan praktik pengelolaan data sesuai standar global seperti GDPR, serta melakukan penilaian risiko secara proaktif guna mencegah pelanggaran data dan memastikan kepatuhan

Pengaruh Dampak Audit terhadap Perlindungan Data Organisasi

Audit keamanan informasi berperan penting dalam mengevaluasi kepatuhan organisasi terhadap kebijakan dan standar keamanan data. Dengan melakukan audit secara rutin, organisasi dapat mengidentifikasi kerentanan sistem, aktivitas mencurigakan, serta potensi ancaman keamanan yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Kombinasi audit dan pemantauan aktif membantu mencegah insiden keamanan dan memastikan perbaikan dilakukan tepat waktu. (Ripa Sabila Usni Sitompul & Muhammad Irwan Padli Nasution, 2023)

Keamanan Siber

Kaspersky (2020) mendefinisikan keamanan siber sebagai praktik perlindungan sistem, jaringan, dan program dari serangan digital yang bertujuan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu operasi bisnis. Definisi ini menekankan perlindungan terhadap berbagai bentuk serangan digital yang semakin kompleks. CISCO (2021) menyatakan cybersecurity sebagai praktik melindungi sistem, jaringan, dan program dari serangan digital yang bertujuan mengakses, mengubah, menghancurkan informasi sensitif, memeras pengguna, atau mengganggu operasional keamanan siber praktik atau upaya melindungi sistem komputer, jaringan, aplikasi perangkat lunak, sistem elektronik, dan data dari ancaman atau serangan digital yang berpotensi merusak, mencuri, atau mengakses informasi secara ilegal.(Budiyanto et al., 2025)

Pengaruh Keamanan Siber terhadap Perlindungan Data Organisasi

Pengaruh keamanan siber terhadap perlindungan data organisasi sangat krusial dan berdampak langsung pada kemampuan organisasi dalam menjaga kerahasiaan, integritas, dan ketersediaan data. (*Keamanan Siber Dalam UU Perlindungan Data Pribadi - Elitery*, n.d.). Keamanan siber membantu mencegah akses tidak sah dan kebocoran data yang dapat merugikan organisasi secara finansial dan reputasi. Dengan menerapkan teknologi seperti enkripsi data, manajemen akses dan identitas (IAM), serta sistem deteksi intrusi (IDS/IPS), organisasi dapat memastikan bahwa hanya pihak yang berwenang yang dapat mengakses data sensitif. Hal ini sangat penting untuk mencegah pencurian, manipulasi, atau penghapusan data yang dapat merusak kepercayaan pelanggan dan mitra bisnis.(Wicaksana et al., 2020)

a. Mencegah akses tidak sah dan kebocoran data

Keamanan siber berperan penting dalam mencegah akses tidak sah yang dapat menyebabkan kebocoran data pribadi maupun data organisasi. Dengan menerapkan teknologi seperti enkripsi, firewall, dan sistem deteksi intrusi, organisasi dapat mengurangi risiko pencurian atau manipulasi data oleh pihak yang tidak berwenang.

b. Mengurangi risiko kehilangan data akibat serangan siber
Strategi keamanan siber membantu organisasi mengurangi risiko kehilangan data jika terjadi serangan seperti malware, ransomware, atau kerusakan sistem. Hal ini penting untuk menjaga kelangsungan operasional dan reputasi organisasi.

c. **Memastikan kepatuhan terhadap regulasi perlindungan data**
Keamanan siber mendukung organisasi dalam memenuhi persyaratan hukum dan regulasi terkait perlindungan data, seperti pelaporan insiden kebocoran data dan penerapan standar keamanan yang sesuai. Kepatuhan ini penting untuk menghindari sanksi hukum dan menjaga kepercayaan pelanggan

Perlindungan Data Organisasi

Menurut Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (dikutip di sumber 2), data pribadi adalah setiap data yang dapat mengidentifikasi seseorang secara langsung atau tidak langsung. Perlindungan data pribadi meliputi hak individu atas keamanan dan kerahasiaan data serta kewajiban pengelola data untuk menjaga keamanan dan mencegah penyalahgunaan data tersebut. Menurut Sugeng (2020) dan Amboro & Puspita (2021), perlindungan data pribadi adalah upaya menjaga kerahasiaan data yang melekat pada individu, sehingga tidak boleh digunakan atau dikelola tanpa izin dari pemilik data. Secara filosofis, perlindungan data pribadi merupakan manifestasi pengakuan atas hak dasar manusia dan kebutuhan melindungi hak-hak individu dalam pengelolaan data.(Sari, 2020)

METODE PENELITIAN

SLR (Systematic Literature Review)

Systematic literature review (SLR) merupakan suatu metode untuk memahami kumpulan kumpulan informasi, dan sarana untuk berkontribusi pada jawaban atas pertanyaan tentang apa yang berhasil dan apa yang tidak-dan banyak jenis pertanyaan lainnya juga. Menurut Amin et al. (2022) SLR adalah proses sistematis untuk mengidentifikasi, menilai, dan mensintesis bukti penelitian yang relevan guna menjawab pertanyaan penelitian yang jelas. Berbeda dengan tinjauan literatur tradisional yang mungkin lebih naratif dan subjektif, SLR menggunakan strategi eksplisit untuk meminimalkan bias dan memaksimalkan objektivitas proses tinjauan.

Tahapan dari *systematic literature review* (SLR) :

1. Perencanaan (*Planning*) : Tentukan pertanyaan penelitian yang spesifik dan jelas. Gunakan format seperti PICO (*Population*, *Intervention*, *Comparison*, *Outcome*) atau PICOC (menambahkan Context) untuk studi kuantitatif.
2. Pelaksanaan (*Conducting*) : Melakukan pencarian literatur sistematis, seleksi studi kasus, evaluasi studi, ekstraksi data
3. Pelaporan (*Reporting*) : Gabungkan temuan dari studi yang relevan untuk menjawab pertanyaan penelitian. Tulis laporan yang mencakup latar belakang, metodologi, hasil, dan kesimpulan.

Fungsi dari systematic literature review (SLR) pada penelitian adalah sebagai berikut :

1. Memberikan gambaran komprehensif dan objektif : SLR menyajikan ringkasan yang menyeluruh dan objektif dari penelitian sebelumnya, membantu peneliti memahami status terkini dari topik yang diteliti.
2. Mengidentifikasi kesenjangan penelitian : Dengan menganalisis literatur yang ada, SLR memungkinkan peneliti untuk mengidentifikasi area yang belum banyak diteliti atau isu-isu yang masih membutuhkan perhatian lebih lanjut.
3. Menyediakan dasar teoritis yang kuat : SLR membantu dalam membangun dasar teoritis yang kokoh untuk penelitian lanjutan dengan menyintesis temuan dari berbagai studi yang ada.
4. Mendukung kengambilan keputusan berbasis bukti : Hasil dari SLR dapat digunakan sebagai panduan dalam pengambilan keputusan di berbagai bidang, mulai dari kebijakan publik hingga pengembangan produk.

Keuntungan metode systematic literature review (SLR) pada suatu penelitian diabnding dengan metode penelitian lainnya :

1. SLR menggunakan metode yang sistematis dan transparan dalam mengidentifikasi, mengevaluasi, dan mensintesis hasil-hasil penelitian yang relevan. Dimana pendekatan ini akan meminimalkan subjektifitas dan meningkatkan suatu validitas dari sebuah temuan.
2. SLR membantu dalam mengidentifikasi area-area yang belum banyak diteliti atau memiliki hasil yang membingungkan. Maka dari itu SLR tidak hanya menyajikan apa yang telah diketahui, tetapi juga menyoroti aspek-aspek yang memerlukan penelitian lebih lanjut.
3. SLR menyediakan sintesis bukti yang komprehensif dan objektif, yang sangat berguna bagi pembuat kebijakan, praktisi, dan peneliti dalam membuat keputusan yang didasarkan pada bukti ilmiah yang solid.
4. Karena metodologi SLR yang ketat dan terstruktur, hasil dari SLR sering dianggap lebih kredibel dan dapat diandalkan dibandingkan dengan tinjauan literatur naratif, yang lebih subjektif dan kurang terstruktur.

Hasil Penelitian

Dampak Kejahatan Siber terhadap Bisnis dan Individu

Di era digital ini, internet telah menjadi bagian integral dari kehidupan kita sehari-hari, memberikan kemudahan dan kemungkinan tanpa batas. Namun, dengan kekuatan yang besar, terdapat pula tanggung jawab yang besar pula. Sayangnya, kemajuan teknologi juga telah melahirkan generasi penjahat baru – penjahat dunia maya (Manullang 2022). Dampak kejahatan dunia maya terhadap bisnis dan individu tidak dapat dianggap remeh, karena hal ini menimbulkan ancaman yang signifikan terhadap kesejahteraan finansial dan keamanan pribadi. Dalam dunia bisnis, kejahatan dunia maya dapat menimbulkan dampak buruk. Salah satu bentuk kejahatan dunia maya yang paling umum adalah peretasan, di mana penjahat menargetkan jaringan atau situs web perusahaan untuk mendapatkan akses tidak sah ke informasi sensitif. Ini dapat mencakup data pelanggan, rahasia dagang, dan bahkan catatan keuangan. Akibat dari serangan tersebut bisa menjadi bencana besar, menyebabkan kerugian finansial yang parah, rusaknya reputasi perusahaan, dan bahkan dampak hukum. Selain itu, operasional bisnis dapat terganggu ketika perusahaan mencoba memperbaiki kerusakan yang disebabkan oleh serangan siber, yang mengakibatkan biaya tambahan dan hilangnya produktivitas.(Halimah & Dewi, 2024)

Bentuk kejahatan dunia maya lain yang perlu diwaspadai oleh dunia usaha adalah phishing, yang melibatkan upaya menipu individu agar membocorkan informasi pribadi mereka, seperti kata sandi atau rincian kartu kredit. Dengan informasi ini, penjahat dunia maya kemudian dapat memperoleh akses ke sistem perusahaan, yang berpotensi mendatangkan malapetaka pada jaringan mereka atau mencuri data berharga. Konsekuensi dari menjadi korban serangan phishing bisa sangat luas, dengan potensi kerugian finansial, kepercayaan pelanggan yang terganggu, dan bahkan denda peraturan. Kejahatan dunia maya tidak hanya dialami oleh dunia usaha, namun individu juga terkena risikonya. Dengan banyaknya informasi pribadi yang disimpan secara online, individu dapat menjadi sasaran pencurian identitas. Penjahat dunia maya dapat menggunakan informasi pribadi yang dicuri untuk menggunakan identitas seseorang, melakukan pembelian palsu, atau bahkan mengajukan pinjaman atas nama korban. (Kairupan & Rahman, 2022)

Praktik Terbaik dalam Menghadapi Serangan Kejahatan Siber

Kejahatan siber, atau yang sering disebut dengan cybercrime, semakin menjadi ancaman serius bagi banyak individu, organisasi, dan negara. Dalam era digital ini, serangan kejahatan siber dapat dengan mudah membobol sistem keamanan yang ada dan mengakibatkan kerugian yang besar. Oleh karena itu, sangat penting bagi kita untuk mengenal dan menerapkan praktik terbaik dalam menghadapi serangan kejahatan siber. Salah satu praktik terbaik yang dapat dilakukan adalah dengan meningkatkan pemahaman mengenai serangan kejahatan siber. Dalam dunia yang semakin kompleks ini, serangan kejahatan siber juga semakin beragam dan semakin canggih. Oleh karena itu, penting bagi kita untuk terus mempelajari dan memahami jenis-jenis serangan kejahatan siber yang mungkin terjadi, serta cara-cara yang biasa digunakan oleh para pelaku kejahatan. Dengan pemahaman yang baik, kita dapat meningkatkan upaya yang dilakukan untuk mencegah serangan tersebut.(Butarbutar, 2023)

Selain itu, penerapan kebijakan keamanan yang ketat juga merupakan praktik terbaik dalam menghadapi serangan kejahatan siber. Setiap organisasi harus memiliki kebijakan keamanan yang jelas dan tegas. Misalnya, semua karyawan harus memiliki password yang kuat dan rutin menggantinya, serta melaporkan segala aktivitas yang mencurigakan kepada pihak yang berwenang. Selain itu, organisasi juga harus melindungi data-data penting dengan menggunakan enkripsi dan firewall yang handal. Penting juga bagi kita untuk melakukan pemantauan terhadap sistem keamanan yang ada. Serangan kejahatan siber tidak akan dapat dihindari sepenuhnya, namun dengan melakukan pemantauan yang cermat kita dapat mengurangi dampak yang ditimbulkan. Dengan memantau sistem keamanan secara aktif, kita dapat lebih cepat mendeteksi serangan yang sedang berlangsung, sehingga dapat segera mengambil tindakan yang diperlukan untuk meminimalisir kerugian.(Aldriano & Priyambodo, 2022).

Selanjutnya, penting bagi kita untuk secara teratur melakukan pelatihan dan pemahaman tentang keamanan siber kepada seluruh anggota organisasi. Serangan kejahatan siber sering kali berhasil masuk ke dalam sistem karena adanya kecerobohan atau ketidaktahuan para pengguna. Oleh karena itu, setiap individu harus memiliki pemahaman yang baik tentang ancaman kejahatan siber, serta cara mengatasinya. Pelatihan dan pemahaman ini harus dilakukan secara berkala, mengingat serangan kejahatan siber juga terus berkembang. Terakhir, tetap terhubung dengan komunitas keamanan siber juga merupakan praktik terbaik yang penting. Dengan terhubung ke komunitas yang sama, kita dapat saling berbagi informasi dan pengalaman tentang serangan kejahatan siber yang mungkin telah terjadi. Hal ini dapat membantu kita dalam mengembangkan strategi dan langkah-langkah yang lebih efektif dalam menghadapi serangan kejahatan siber.(Rahman Najwa, 2024)

Dalam era digital ini, serangan kejahatan siber merupakan ancaman yang tidak dapat dihindari. Namun, dengan menerapkan praktik terbaik dalam menghadapi serangan tersebut, kita dapat meminimalisir dampak yang ditimbulkan. Pemahaman yang baik, kebijakan keamanan yang ketat, pemantauan yang cermat, pelatihan yang teratur, dan keterhubungan dengan komunitas keamanan siber adalah beberapa praktik terbaik yang dapat kita gunakan dalam menghadapi serangan kejahatan siber. Dengan demikian, kita dapat menciptakan dunia digital yang lebih aman dan terhindar dari serangan kejahatan siber.(Sari, 2020)

Tata Kelola Keamanan Siber Indonesia diBawah Kelembagaan BSSN

Pembentukan BSSN yang sebelumnya merupakan Lembaga Sandi Negara, membutuhkan proses transformasi sehingga menjadi sebuah lembaga yang kredibel dan sebagai pilar keamanan siber di Indonesia. Proses transformasi ini tertuang dalam Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019 yang terdiri dari 7 tahapan tema, yaitu:

a. Tahap tema yang pertama yaitu Integrasi
   Organisasi (Organization Integration) yang ditujukan untuk menghadapi tantangan terkait integrasi, internalisasi, dan harmonisasi organisasi dalam rangka membentuk fondasi organisasi yang kuat.
b. Tahapan tema yang kedua yaitu Sistem dan Pengembangan Standar (system and standard development) sebagai roadmap dalam mengembangkan keamanan siber pemerintahan (secured cyber government)dan keamanan siber negara (secured cyber nation).
c. Tahapan tema yang ketiga yaitu Akuisisi Kemampuan (Capabilities Acquisition) sehingga menciptakan SDM siber yang berkualifikasi dan tersertifikasi secarainternasional, di samping juga melakukan akuisisi dan pembaharuan infrastruktur, sarana, prasarana, fasilitas, dan teknologi di bidang keamanan siber.
d. Tahapan tema yang keempat yaitu Penerimaan dan Operasional (Acceptance and Operational) dalam rangka menciptakan kesadaran penerimaan di seluruh Kementerian/Lembaga Pemerintah Non Kementerian dan sektor swasta (private sector) tentang perlunya keamanan siber di Indonesia serta terbentuknya protokol keamanan siber yang tersinergi dan terkoordinasi sehingga operasi berjalan dengan lancar.
e. Tahapan tema yang kelima yaitu Pencapaian Skala Nasional (Nation-Wide Achievement) yaitu dengan menambah dan memperbaharui infrastruktur dan keamanan siber dan sandi daerah serta melakukan implementasi keamanan siber dan sandi di provinsi dan kabupaten/kota.
f. Tahapan tema yang keenam yaitu Keamanan Siber Nasional (Secured Cyber Nation) dalam artian memberikan pemahaman kepada masyarakat sehingga tercipta kesadaran yang tinggi tentang keamanan siber.
g. Tahapan tema yang ketujuh yaitu Tolak Ukur dan Praktek Terbaik (Best Practices and Benchmark) yaitu dengan menjalankan praktek-praktek terbaik di bidang keamanan siber di lingkup ASEAN, Asia, dan global. Hadirnya BSSN sebagai institusi siber nasional di sini berperan dalam menjalin koordinasi dan kerjasama antara institusi dan pemangku kepentingan di bidang siber di Indonesia, yang meliputi Kepolisian Republik Indonesia (cyber crime), TNI/Kementerian Pertahanan (cyber defense), Kementerian Luar Negeri (cyber diplomacy) dan Kementerian Komunikasi dan Informatika, serta lembaga- lembaga lainnya. (Makbull Rizki, 2022)

Pembahasan

Perkembangn teknologi informasi pada era digital menyebabkan munculnya tren, budaya, dan juga perilaku yang baru di masyarakat, baik hal yang positif dan membangun ataupun hal yang negatif. Hal yang dapat dilakukan dari sisi pengguna teknologi adalah bersifat cermat. Jika diperhatikan, banyak pengguna media sosial yang baik secara sengaja maupun tidak sengaja melakukan penyebaran atas informasi atau data pribadi miliknya ke media sosial, yang tentunya dapat meningkatkan risiko kerugian secara finansial ataupun non finansial. Pada umumnya, masyarakat belum mengetahui dampak penyalahgunaan informasi sehingga menyebabkan rendahnya kesadaran masyarakat tentang perlindungan

data pribadi. Meskipun begitu, pemerintah telah mengambil tindakan awal atas perlindungan data pribadi dengan melakukan pengesahan atas Undang-Undang Perlindungan Data Pribadi sehingga pada kedepannya diharapkan Undang-Undang tersebut dapat memberikan perlindungan hukum terhadap subyek data pribadi. Tindakan awal tersebut sangatlah penting mengingat pengungkapan data pribadi tanpa kendali dapat menimbulkan banyak risiko terhadap subyek data pribadi serta organisasi serta meningkatkan kemungkinan tindak kriminalitas, mulai dari ancaman, perundungan, penipuan hingga pembobolan akun yang dimiliki oleh subyek data pribadi.(Pokhrel, 2024)

Sehingga Audit keamanan siber, khususnya audit internal, memberikan pendekatan komprehensif untuk mengidentifikasi kerentanan organisasi dan membantu memastikan tata kelola yang efektif. Audit ini berperan dalam perlindungan data dengan menguji kepatuhan protokol keamanan dan memeriksa kontrak pihak ketiga, sehingga memberikan jaminan perlindungan yang lebih baik terhadap data organisasi.

Agar keseluruhan, audit keamanan siber memberikan kontribusi besar dalam memperkuat perlindungan data organisasi dengan mengidentifikasi dan mengatasi kerentanan, memastikan kepatuhan regulasi, serta meningkatkan kesiapsiagaan dan respons terhadap ancaman siber, sehingga membantu menjaga integritas dan kepercayaan terhadap data organisasi. (Vania et al., 2023).

Kesimpulan

Audit keamanan siber memiliki peran penting dalam meningkatkan perlindungan data organisasi. Melalui audit yang rutin dan menyeluruh, organisasi dapat mengidentifikasi celah keamanan, mengevaluasi kepatuhan terhadap regulasi seperti UU Perlindungan Data Pribadi (UU PDP) di Indonesia maupun GDPR di Eropa, serta mengoptimalkan sistem keamanan mereka untuk mencegah kebocoran dan penyalahgunaan data pribadi. Audit ini juga membantu organisasi dalam mengelola risiko keamanan siber secara proaktif, sehingga dapat meminimalisir dampak finansial dan reputasi akibat insiden siber. Selain itu, audit keamanan siber mendukung organisasi dalam memenuhi kewajiban hukum dan memperkuat kepercayaan pelanggan terhadap pengelolaan data yang aman dan professional.

References

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Aldriano, M. A., & Priyambodo, M. A. (2022). Cyber Crime Dalam Sudut Pandang Hukum Pidana. *Jurnal Kewarganegaraan*, *6*(1), 2169–2175.

Bua, I. T., & Idris, N. I. (2025). *Analisis Kebijakan Keamanan Siber di Indonesia : Studi Kasus Kebocoran Data Nasional pada Tahun 2024*. *2*, 100–114.

Budiyanto, D., Mabruri, M., Studi, P., Informasi, S., & Jember, U. T. (2025). *Pentingnya keamanan siber dalam era digital: tinjauan global dan kondisi di indonesia*. *2*(1), 981–994.

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Fianda Prathitaningtyas, Manda Azalia Nur Raissa, & Dien Noviany Rahmatika. (2024). Systematic Literature Review: Pengaruh Audit Laporan Keuangan dan Peran Internal Audit terhadap Kualitas Laporan Keuangan. *Jurnal Ilmiah Ekonomi, Akuntansi, Dan Pajak*, *1*(3), 52–66. https://doi.org/10.61132/jieap.v1i3.320

Fiar, A. A., & Jaeni. (2022). Pengaruh Audit Forensik, Audit Investigasi, Kompetensi Auditor, Profesionalisme dan Kecerdasan Spiritual Terhadap Pencegahan Fraud. *Kompak :Jurnal Ilmiah Komputerisasi Akuntansi*, *15*(1), 59–169. https://doi.org/10.51903/kompak.v15i1.628

Halimah, A. N., & Dewi, L. (2024). Systematic Literature Review (Slr): Implementasi Pembelajaran Menggunakan Pendekatan Understanding By Design (Ubd). *CaXra: Jurnal Pendidikan Sekolah Dasar*, *3*(1), 54–64. https://doi.org/10.31980/caxra.v3i1.874

Hendra Wicaksana, R., Imam Munandar, A., Samputra, P. L., Salemba, J., No, R., & Indonesia, J. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 143–158. http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158

Kairupan, V. A., & Rahman, A. A. (2022). Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Kalangan Mahasiswa Kota Bandung. *Jurnal Darma Agung*, *30*(1), 1164. https://doi.org/10.46930/ojsuda.v30i1.3167

Keamanan Siber dalam UU Perlindungan Data Pribadi - Elitery. (n.d.).

Makbull Rizki. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. *Politeia: Jurnal Ilmu Politik*, *14*(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, *1*(11), 2497–2516. https://doi.org/10.54443/sibatik.v1i11.395

Permana, R. A., & Zainol, Z. (2025). *Analisis Metode dan Teknologi untuk Perlindungan Data dan Informasi dari Ancaman Siber Analysis of Methods and Technologies for Data and Information Protection Against Cyber Threats*. *3*(2), 137–146.

Rahman Najwa, F. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, Dah Hukum*, *2*(1), 8–16. https://doi.org/10.32520/albahts.v2i1.3044

Rifqy, M., Arham, H., & Risal, M. C. (2023). Perlindungan Data Pribadi Bagi Pengguna Media Sosial. *Jurnal Al Tasyri'iyyah*, *3*(2), 109.

Ripa Sabila Usni Sitompul, & Muhammad Irwan Padli Nasution. (2023). Pentingnya Kepatuhan Keamanan Informasi Dalam Mengurangi Risiko Data Breach. *Maeswara : Jurnal Riset Ilmu Manajemen Dan Kewirausahaan*, *2*(1), 99–107. https://doi.org/10.61132/maeswara.v2i1.587

Sari, I. N. (2020). Perlindungan Data Pribadi di Era Digital. In *Jurnal Keamanan Siber Indonesia* (Vol. 1, pp. 34–36).

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber. *Jurnal Multidisiplin Indonesia*, *2*(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157