Civilia :
Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan (2024), 3 (1): 234–248
http://jurnal.anfa.co.id

ANALISIS PENERAPAN MANAGEMENT SEKURITI BERDASARKAN NILAI NILAI UUD 1945 DI ERA DIGITALISASI

Zulham Ilyas[1] , Edy Soesanto[2] , Rifki Kurniawan[3]
[1,2]Teknik Industri, Fakultas Teknik Universitas Bhayangkara Jakarta Raya, Jl. Raya Perjuangan Bekasi Utara, Kota Bekasi, Jawa Barat 17121. Telp : (+6221) 88955882
email : [1]202210215204@mhs.ubharajaya.ac.id , [2]202210215135@mhs.ubharajaya.ac.id

ABSTRAK

Penelitian ini bertujuan untuk menganalisis penerapan manajemen keamanan berdasarkan prinsip-prinsip yang tercantum dalam Undang-Undang Dasar 1945 dalam konteks era digitalisasi. Metode analisis dilakukan melalui studi literatur dan tinjauan terhadap praktik-praktik manajemen keamanan yang relevan dengan perkembangan teknologi informasi dan komunikasi. Hasil penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam tentang bagaimana nilai-nilai yang terkandung dalam UUD 1945 dapat diimplementasikan secara efektif dalam pengelolaan keamanan di era digitalisasi. Metode yang digunakan dalam penelitian kali ini yaitu studi literatur, yang dimana hal ini menyoroti urgensi manajemen keamanan dalam konteks era digitalisasi, hasilnya menunjukkan bahwa manajemen sekuriti merupakah suatu kebutuhan yang sangat penting bagi perusahaan atau organisasi terutama yang berbasis digital. Terapan yang terintregasi, manajemen risiko yang cermat dan pelaksanaan kebijakan yang keamanan yang jelas dapat menjaga informasi keamanan dan teknologi dari serangan dunia siber, sekaligus menyusutkan risiko keamanan yang akan timbul.

ABSTRACT

This research aims to analyze the implementation of security management based on the principles stated in the 1945 Constitution in the context of the digitalization era. The analysis method is carried out through literature studies and reviews of security management practices that are relevant to the development of information and communication technology. Hoped this results of this research will be provide a deeper understanding of how the values contained in the 1945 Constitution can be implemented effectively in security management in the era of digitalization. The research method used in this research is a literature study, which highlights the urgency of security management in the context of the digitalization era. The results show that security management is a very important need for companies or organizations, especially digital-based ones. Integrated implementation, careful risk management and implementation of clear security policies can protect security information and technology from cyber attacks, while reducing security risks that will arise.

2961-8754

Civilia :
Jurnal Kajian Hukum dan Pendidikan Kewarganegaraan (2024), 3 (1): 234–248
http://jurnal.anfa.co.id

PENDAHULUAN

Di zaman modern saat ini, integrasi teknologi ke dalam kehidupan sehari-hari sudah melekat kedalam masyarakat luas, hal ini juga menyebabkan diikuti dengan munculnya berbagai ancaman keamanan siber yang semakin hari bertambah canggih dan menimbulkan risiko yang sangat besar bagi organisasi nasional maupun global. Ancaman siber ini dapat menimbulkan banyak sekali kerugian finansial maupun non finansial yang besar dan bahkan dapat juga mengancam keberlangsungan kehidupan berorganisasi dari banyak pihak. Terutama bagi organisasi-organisasi kecil dan menengah yang hanya memiliki sumber daya yang terbatas untuk pulih setelah mereka terkena serangan. Karena itu peran manajemen sekuriti sangat amat penting dalam hal ini, Manajemen sekuriti mencakup banyaknya serangkaian kebijakan, praktik, dan prosedur yang sudah dirancang guna melindungi para organisasi dari ancaman /serangan keamanan, termasuk juga serangan dunia maya. Tujuannya adalah demi menjaga/melindungi informasi sensitif dan informasi penting dari orang yang ingin mengakses yang tidak sah dan melanggar hukum, modifikasi, atau penghapusan, serta menjaga keamanan sumber daya teknologi informasi dan komunikasi (TIK) yang digunakan dalam organisasi.

Manajemen sekuriti berisikan banyaknya pengenalan risiko keamanan informasi, pengembangan strategi keamanan yang sangat efektif guna mencegah serangan/kejahatan siber, dan penerapan praktik serta prosedur keamanan demi menjaga keamanan. Penggunaan teknologi keamanan layaknya perangkat lunak antivirus, firewall, kata sandi yang kuat, enkripsi, serta kontrol akses pengguna dan pelaporan keamanan rutin juga harus menjadi bagian integral dari manajemen keamanan. Namun hal-hal tersebut harus selalu kita perbarui atau update guna menjaga informasi dari ancaman keamanan siber yang terus berkembang, Terlebih lagi masih kurangnya kesadaran masyarakat akan besarnya resiko kejahatan siber yang mengahantui serta bisa sangat merugikan dan terbatasnya sumberdaya untuk menerapkan strategi keamanan yang efektif di negara Indonesia.

Dalam konteks ini, latar belakang masalah utama menyoroti pengimplementasian manajemen sekuriti yang berasaskan UUD 1945 dalam menjaga data-data sensitif dan informasi penting dari adanya serangan dunia maya yang dapat merugikan banyak pihak-pihak tertentu. Pada zaman modern saat ini terdapat peraturan peraturan seperti UU ITE yang menjadi poros hukum dalam mencegah kejahatan siber saat ini, UU ITE bertujuan untuk terus memberikan kepastian hukum dan mengakui serta menghormati hak dan kebebasan individu dalam ruang digital. UU ITE juga mencakup hukum elektronik, yang memuat banyak peraturan dalam rantai sistem elektronik, keamanan informasi data, tanda tangan elektronik dan tata cara dalam penyelesaian sengketa di dunia maya. Perubahan ini juga dapat memengaruhi bagaimana bisnis beroperasi online, cara individu berkomunikasi, dan melibatkan pihak ketiga di dalam transaksi daring.

Tujuan Penelitian :

1. Menganalisis penerapan manejemen sekuriti di Indonesia
2. Mengevaluasi strategi menghadapi ancaman yang muncul pada dunia maya
3. Mengidentifikasi langkah langkah untuk memperkuat keamanan di dunia maya guna menjaga informasi dari kejahatan siber

Dengan tujuan penelitian ini, akan dijelaskan bagaiamana penerapan manajemen sekurit di Indonesia dalam menghadapi kejahatan siber, strategi yang digunakan untuk mengurangi resiko ancaman siber, dan langkah langkah penguatan keamana siber.

2961-8754

METODOLOGI

Jenis penelitian yang kami gunakan dalam membuat jurnal ini adalah studi literatur. Metode studi literatur adalah metode penelitian yang mengambil serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka, membaca dan mencatat, serta mengelola bahan penelitian (Zed, 2008.3)

Studi kepustakaan dilakukan oleh peneliti berguna untuk mencari pokok-pokok dasar pijakan/fondasi demi memperoleh dan membangun landasan teori, kerangka berpikir dan menentukan dugaan sementara atau di sebut juga dengan hipotesis penelitian. Sehingga peneliti bisa mengelompokan, mengalokasikan dan meng-rganisasikan, variasi pustaka dalam bidang nya, dengan begitu peneliti mendapat pendalaman yang lebih luas dan mendalam terhadap masalah yang hendak di teliti sesuai dengan tujuan penelitian.

No	Judul	Penulis	Kesamaan	Perbedaan
1	**Pentingnya Manajemen Security di Era Digitalisasi**	**Rifqi Galuh Putra1, Achmad Fauzi2**	**Kedua artikel membahas penting nya peran manajemen sekuriti di era digitalisasi**	**Artikel terdahulu menjelaskan secara umum, sedangkan artikel ini berfokus pada pengimplementasian UUD 1945 pada manajemen sekuriti.**
2	**Manajemen Keamanan Cyber di Era Digital**	**Edy Soesanto, Lady Antira, Kevin Kevin.**	**Kedua artikel membahas bahaya nya serangan siber**	**Artikel yang terdahulu sangat menjelaskan secara spesifik serangan-serangan siber, sedangkan artikel ini hanya menjelaskan secara singkat(umum).**
3	**Analisis Manajemen Digital dalam Mengoptimalkan Kinerja Bisnis**	**Intan Astari Kusuma W1, Fajar Dwi Nur Afifah2**	**Kedua artikel ini membahas peran manajemen sekuriti dalam aspek bisnis**	**Artikel terdahulu hanya menyelidiki dan menganalisis bagaimana manajemen digital yang efektif dapat menjadi kunci sukses dalam mengoptimalkan kinerja bisnis, sedangkan artikel ini membahas peranan UU ITE dalam menjaga keamanan di dunia bisnis**

2961-8754

4	**Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo**	**Farhan Saputra, Edy Soesanto , Kumalasari Indah Cahyaningtyas , Zaidan Lukmanul Hakim4**	**Kedua artikel tersebut membahas tentang management security dalam aspek siber**	**Artikel terdahulu memfokuskan bagaimana penerapan management sekuriti di kominfo, sedangkan artikel ini memfokuskan terhadap hanya memfokuskan di era digitalisasi**
5	**Metode Pembelajaran Inovatif di Era Digitalisasi**	**Hasriadi Hasriadi**	**Kedua artikel tersebut membahas tentang era digitalisasi**	**Artikel terdahulu memfokuskan tentang metode pembelajaran inovatif di era digitalisasi, sedangkan artikel ini membahas tentang penerapan manejemen sekuriti di era digitalisasi**
6	**DIGITALISASI PENDIDIKAN DITINJAU DARI PERSPEKTIF HUKUM**	**Edelweisia Cristiana**	**Kedua artikel tersbut membahas tentang digitalisasi dari prespektif hukum**	**Artikel terdahulu memfokuskan tentang digitalisasi pendidikan dari prespektif hukum, sedangkan artikel ini membahas tentang management sekuriti.**
7	**DIGITALISASI BAHASA DAERAH SEBAGAI UPAYA MENINGKATKAN KETAHANAN BUDAYA DAERAH**	**Yaya Mulya Mantri**	**Kedua artikel tersebut membahas tentang digitalisasi**	**Artikel terdahulu membahas tentang upaya meningkatkan ketahanan budaya daerah dengan menggunakan digitalisasi, sedangkan artikel ini membahas tentang upaya penerapan managemen securiti dalam era digitalisasi**

2961-8754

8	**ANALISIS STRATEGI BISNIS PERCETAKAN DI ERA DIGITALISASI PADA SEGMEN PRODUK LABEL DAN KEMASAN STUDI PADA PERUSAHAAN PT. XYZ**	**Fauzi Dwi Krisdianto,Sri gunawan**	**Kedua artikel tersebut membahas tentang digitalisasi**	**Artikel terdahulu membahas tentang strategi bisnis di era digitalisasi, sedangkan artikel ini membahas tentang managemen security di era digitalisasi**
9	**Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher**	**Edy Soesanto1, Farhan Saputra2,Dita Puspitasari3,Bayu Putra Danaya4**	**Kedua artikel tersebut membahas tentang manajemen sekuriti dan pengamanan cyber.**	**Artikel terdahulu memfokuskan terhadap analisis objek vital dan pengamanan file pada yayasan siber publisher, sedangkan artikel ini membahas tentang era digitalisasi.**
10	**Analisis Sistem Manajemen Sekuriti: K3 dan Beban Kerja di PT. XYZ**	**Edy Soesanto, Farhan Saputra, Dita Puspitasari, Bayu Putra Danaya**	**Kedua artikel tersebut mebahas tentang sistem manajemen sekuriti.**	**Artikel terdahulu membahas tentang k3 dan beban kerja di PT. XYZ, Sedangkan artikel ini membahas tentang era digitalisasi.**
11	**Analisis Pola Komunikasi Petugas pada Manajemen Sekuriti di Lembaga Pemasyarakatan**	**Fernanda Agung Pradhana, Padmono Wibowo**	**Kedua artikel tersebut membahas tentang management security**	**Artikel terdahulu membahas tentang managemen security di lembaga pemasyarakatan, sedangkan artikel ini membahas tentang manajemen sekuriti di era digitalisasi**

12	**PENGARUH SISTEM PENGAMANAN OBJEK VITAL, FILE DAN CYBER TERHADAP MANAJEMEN SEKURITI PADA PT FREEPORT INDONESIA**	**Edy Soesanto, Fadila Kurniasih, Putri Mutiara, Salsabila Taqwaning Afifi**	**Kedua artikel membahas tentang manajemen sekuriti dan siber.**	**Artikel terdahulu membahas tentang pengaruh sistem pengamanan objek fital dan file pada PT FREEPORT INDONESIA, sedangkan artikel ini membahas tentang manajemen sekuriti pada era digitalisasi.**
13	**Peran Manajemen Sekuriti Bank BRIuntuk Menjaga Kepercayaan Nasabah**	**Edy Soesanto1, Firyaal Salsabilah2, Intan Cahyani Abadi3,Muhammad Rizky4**	**Kedua artikel membahas tentang managemen sekuriti**	**Artikel terdahulu membahas tentang peran Manajemen Sekuriti Bank BRI untuk Menjaga Kepercayaan Nasabah, sedangkan artikel ini membahas tentang era digitalisasi**
14	**AssessmentManajemenSekuritiPT AQUA**	**Edy Soesanto, Vina Hariyanti, Munisari Munisari, Navia Naveli**	**Kedua artikel membahas tentang manajemen sekuriti.**	**Artikel terdahulu membahas tentang assesment di PT AQUA, sedangkan artikel ini membahas tentang di era digitalisasi**
15	**Mengoptimalkan Sistem Keamanan pada Industri Penerbangan dengan Konsep Dasar Manajemen Sekuriti**	**Alfadilla Khunaini1,Achmad Fauzi2JumawanJumawan3Alfina Sri Rahayu DNS4, Cayla Salsa Raya5, Vira Anggita Sukma6, Widya Meliawati7**	**Kedua artikel membahas tentang manajemen sekuriti.**	**Artikel terdahulu membahas tentang sistem keamanan pada industri penerbangan, sedangkan artikel ini membahas tentang era digitalisasi.**

2961-8754

HASIL/PEMBAHASAN

Penerapan manajemen sekuriti di Indonesia.

Penerapan manajemen keamanan (security management) di negara Indonesia melibatkan banyak nya serangkaian praktik dan kebijakan yang mempunyai tujuan untuk melindungi organisasi, infrastruktur, dan sumber daya informasi dari berbagai ancaman/serangan keamanan. Seperti serangan siber, kejahatan korporasi, terorisme, dan lain sebagainya. Berikut adalah beberapa aspek penting dalam penerapan manajemen keamanan di negara Indonesia:

1. Regulasi dan Kebijakan: Pemerintah Indonesia telah menerapkan banyak regulasi terkait dengan keamanan informasi, seperti adanya Undang-Undang ITE (Informasi dan Transaksi Elektronik), serta adanya regulasi sektor-sektor khusus seperti perbankan, keuangan, dan sektor kritikal lainnya. Penerapan regulasi seperti ini mengharuskan untuk organisasi wajib dan harus mematuhi standar tertentu dalam mengelola keamanan mereka sendiri sesuai peraturan setiap negara.

2. Kesadaran dan Pelatihan: Peningkatan kesadaran masyarakat tentang keamanan informasi dan pelatihan bagi semua karyawan yang menjadi bagian penting dari penerapan manajemen keamanan.

3. Teknologi Keamanan: Penggunaan perangkat teknologi keamanan seperti firewall, antivirus, enkripsi data, dan lainnya menjadi bagian integral dari strategi keaman yang semua orang harus paham.

4. Manajemen Akses: Pengelolaan akses-akses pada sistem dan data merupakan aspek yang sangat penting dari manajemen keamanan. Ini juga melibatkan adanya penerapan dalam kebijakan mengakses yang tepat, termasuk otentikasi multi-faktor dan manajemen hak akses pengguna.

5. Pemantauan dan Respons: Organisasi juga harus memiliki sistem pemantauan yang efektif guna mendeteksi aktivitas yang mencurigakan atau serangan keamanan demi menjaga kemanan dari serangan siber.

6. Audit dan Penilaian: Audit dalam keamanan secara teratur harus dilakukan guna mengevaluasi keefektifan sistem keamanan dan memastikan kepatuhan organisasi terhadap regulasi yang berlaku.

7. Kerjasama dan Konsultasi: Organisasi juga memakai jasa diluar instansi guna membantu dalam menjaga dari serangan siber seperti penyedia layanan keamanan, badan pemerintah terkait, dan lembaga keamanan lainnya untuk mendapatkan wawasan dan bantuan dalam meningkatkan manajemen keamanan mereka.

Strategi dalam mencegah kejahatan siber

Ditengah-tengah percepatan penggunaan otomasi digital zaman ini, risiko serangan yang terjadi di dunia maya maka semakin berkembang dari tahun ke tahun. Di jaman sekarang bhanyak sekali perusahaan yang telah memanfaatkan teknologi transformatif seperti

2961-8754

kecerdasan buatan, *Internet of things* dan jaringan 5G. Selama pandemi virus Covid19, transformasi informasi digital juga semakin dirasa meningkat serta semakin singkat dan mudah, setiap bisnis pasti memanfaatkan teknologi digital agar terus dapat beroperasi di era digitalisasi ini. Disamping itu kebijakan work from home (WFH) di hampir semua perusahaan yang harus beroperasi memaksa karyawannya untuk bekerja memanfaatkan teknologi dan perangkat modern, tetapi masih banyaknya celah kejahatan untuk kejahatan siber yang dapat merugikan banyak pihak yang terlibat .

Jenis serangan siber yang paling banyak menyerang adalah trojan activity sebesar 56% kemudian disusul dengan serangan aktifitas terhadap pengumpulan informasi sebesar 43%, sedangkan1% sisanya merupakan *web application attack*. Sementara itu, penetrasi penggunaan jaringan internet di negara Indonesia saat ini cukup signifikan yaitu sebesar 64%. Hal ini menunjukkan bahwa negara Indonesia mempunyai pasar tersendiri, baik yang berdampak positif untuk kegiatan di dunia siber, maupun menjadi ancaman tersendiri untuk keamanan siber.

Untuk itu upaya-upaya yang dapat dilakukan untuk mencegah dari kejahatan siber, antara lain :

- Memberikan informasi terhadap strategi dalam perkembangan siber sekuriti.
- Meningkatkan kewaspadaan akan kejahatan siber di masyarakat umum.
- Memberikan saran dan informasi terkini ke masyarakat yang berkecimpung di dunia digital

Langkah-langkah dalam memperkuat keamamanan siber di dunia maya.

Tantangan terbesar pemerintah Indonesia di era saat ini dalam memperkuat keamanan siber antara lain: Kurangnya ahli pakar teknologi dan pakar keamanan teknis untuk merancang dan menerapkan strategi keamanan siber. Risiko yang mungkin terjadi karena sifat keamanan siber yang bersifat lintas batas negara, artinya negara-negara dengan strategi ketahanan keamanan siber yang lemah dapat membahayakan keamanan siber negara lain. Pemakaian alat anonimisasi, seperti yang digunakan untuk memblokir rantai uang atau enkripsi, dalam kejahatan yang menggunakan Internet membuat pembuat kebijakan akan menjadi lebih sulit. Munculnya teknologi dan peraturan baru selalu berujung pada perlunya pemutakhiran standar audit secara terus menerus. Bagian dari kejahatan dunia maya baru seperti ransomware, peniruan identitas, rayuan seksual (grooming) dan pelecehan seksual melalui dunia maya. Kebutuhan menjelang menanggung aksi siber dan konstruksi perbedaan antarnegara lain bayaran tidak adanya etik dan sistem yang menyala. Sedangkan kritik hisab tempat swasta dan niaga adalah kesusahan menjelang berlangsung lulus yurisdiksi, yang bermakna dihadapkan ambang hukum, deraan maupun tadbir statuta yang absurd beda. Berpotensi tertular polusi sebutan tunduk serius turut cema mahkamah jika terkebat atau bertanggung sambut asal suatu insiden kesejahteraan siber. Tekanan menjelang sehat kekuatan tertinggi bagian dalam menjalin siber proteksi turut menentang onar bidang maya dan terorisme, yang bisa mencengap penyusunan jasa dan pengabaran konten, menamatkan jaringan, pemblokiran layanan, bahkan mengkompromikan kesejahteraan perlengkapan bergerak awak menjelang sehat pemeriksaan oleh kekuatan tertinggi. Keharusan konstruktif kualifikasi internal menjelang mengemong kesejahteraan data dan jaringan. Karena itu dibutuhkan langkah langkah untuk memperkuat keamanan siber di dunia maya saat ini demi melindungi informasi yang bersifat pribadi agar tidak jatuh ke tangan orang yang salah, strategi itu antara lain adalah:

2961-8754

- Capacity Building Program pedoman dan kenaikan keahlian siber sekuriti dilakukan dalam koordinasi Tim Kerja Pusat Operasi Dunia Maya. Selain itu diperlukan pemulihan sumberdaya jiwa terhadap pentingnya siber penjagaan faedah mempersangat persepsi ulah-ulah pencegahan bagian dalam mencegah segala cyber crime. Menyusun ppulih tata tembok yang beralas muka cyber defence dan cyber security, yang tentunya membutuhkan awalan yang masak dan tertata tambah naungan berpokok berbagai pihak. Sinergitas bagian dalam merasai bala siber mewujudkan sewujud kewajiban dan komitmen perbanyak Indonesia. Dengan sinergitas dan kepangan komunikasi, koordinasi, jaringan, dan peranan arah-arah teknis harus bangsa keragaman siber (cyber security community) yang bisa mencegah, mendeteksi, menangkis, dan menghalangi secara pagi-pagi berbagai ketangkasan serbuan bala siber sehingga bisa mendindingi keragaman dan toleransi Nasional. Pembuatan undang-undang khusus yang bertujuan menangani kejahatan siber. Kurang adanya landasan hukum keamanan siber berimplementasi pada struktur organisasi yang seharusnya mengatur keamanan siber. Hal ini juga dapat menimbulkan kebingungan terhadap pengoordinasian tanggung jawab keamanan siber itu sendiri. Rencana Undang-Undang Keamanan Siber saat ini tidak tersedia untuk umum,hanya RUU versi sebelumnya yang tersedia Hanya versi RUU sebelumnya yang tersedia, namun teks ilmiah RUU tersebut tersedia Peraturan perundang-undangan yang berlaku di sektor teknologi Indonesia masih belum memperhitungkan seluruh kejahatan siber. Oleh karena itu, terdapat informasi bahwa saat ini beberapa kejahatan siber yang terkait dengan keamanan (sebagai unsur pemeliharaan keamanan dan pengawasan pemerintah) belum diatur dalam peraturan nasional. Indonesia memerlukan peraturan khusus melawan kejahatan dunia maya Ketentuan khusus ini berlaku terhadap semua tindak pidana yang berkaitan dengan teknologi informasi dan komunikasi,kemudian tindak pidana yang berangkaian dengan kerahasiaan, integritas dan ketersediaan data atau sistem komputer/elektronik, pedoman pemidanaan, dan peraturan perundang-undangan yang mengatur penyidikan dan penyidikan di bidang teknologi informasi dan komunikasi menetapkan aturan umum yang akan diikuti. termasuk pencarian serta penyitaan bukti-bukti digital dan kerja sama di kancah internasional dalam memerangi berbagai kejahatan dunia maya. Hal ini dikarenakan Indonesia rentan terhadap serangan siber tetapi masih memiliki kelemahan hukum dalam menangani serangan siber.
- Peningkatan Sumber Daya Manusia merupakan elemen utama dalam membenarkan keamanan siber yang akan diterapkan sesuai dengan pedoman yang sudah ditetapkan menurut Pengetahuan dan keterampilan khusus yang diperoleh dan dipelihara untuk memenuhi persyaratan keselamatan yang akan terus berkembang. Tidak peduli sudah seberapa hati-hatinya kita, manusia pasti akan melakukan kesalahan atau kekeliruan suatu saat. Oleh karena itu, kesadaran sangat penting dalam melindungi terhadapa kejahatan keamanan siber.
- Kerja sama dalam isu keamanan siber sangatlah kompleks dan memerlukan pendekatan multifaset Oleh karena itu, pengaplikasian prinsip-prinsip kepentingan sangatlah penting yang digunakan untuk meningkatkan tata kelola keamanan siber. Terdapat kebutuhan untuk mekanisme terpadu yang memungkinkan keputusan bisa diverifikasi, dengan banyak nya pertimbangan kepentingan nasional dan pihak-pihak yang terkena dampak Kerja sama internasional .

2961-8754

HIPOTESIS

NO	Hasil Perbedaan	Implementasi	Analisa
1	Perlindungan data pribadi di era digitalisasi	UUD 1945	Perlindungan data pribadi pada era digitalisasi berdasarkan UUD 1945, yaitu Undang-Undang Dasar NKRI Tahun 1945, perlu melihat pada bagaimana prinsip-prinsip dalam UUD 1945 tersebut diinterpretasikan dan diterapkan dalam konteks perlindungan data pribadi di era digital. Meskipun UUD 1945 tidak secara khusus membahas tentang perlindungan data pribadi karena lahir pada zaman di mana teknologi informasi belum sekompleks saat ini, beberapa prinsip dasar dalam UUD 1945 masih relevan untuk konteks ini. Berikut adalah beberapa analisisnya: 1. **Hak Asasi Manusia**: UUD 1945 mengamanatkan perlindungan terhadap hak asasi manusia. Perlindungan data pribadi dapat dilihat sebagai bagian dari hak asasi manusia, terutama hak atas privasi. Prinsip-prinsip seperti hak untuk tidak disalahgunakan oleh pihak lain dan hak atas privasi bisa diinterpretasikan sebagai perlindungan terhadap data pribadi. 2. **Kedaulatan Rakyat dan Keadilan Sosial**: UUD 1945 menekankan kedaulatan rakyat dan keadilan sosial. Dalam konteks perlindungan data pribadi, hal ini dapat diartikan sebagai perlunya kebijakan dan regulasi yang memastikan bahwa pemilik data memiliki kontrol atas data pribadinya sendiri, serta mencegah penyalahgunaan data oleh pihak yang lebih kuat, termasuk perusahaan atau pemerintah. 3. **Perlindungan Hukum**: UUD 1945 menjamin perlindungan hukum bagi setiap warga negara. Dalam konteks perlindungan data pribadi, ini mengimplikasikan perlunya adanya kerangka hukum yang jelas dan efektif untuk melindungi data pribadi, termasuk sanksi bagi pelanggaran serta

2961-8754

			mekanisme penyelesaian sengketa yang efisien. 4. **Kemerdekaan Berpendapat dan Mengeluarkan Pendapat**: UUD 1945 melindungi kemerdekaan berpendapat dan mengeluarkan pendapat. Dalam era digitalisasi, perlindungan data pribadi juga berhubungan dengan kemerdekaan berpendapat dan mengeluarkan pendapat secara online tanpa takut akan penyalahgunaan data pribadi untuk menyensor atau melawan pendapat individu. 5. **Kesejahteraan Bersama**: UUD 1945 menegaskan pentingnya kesejahteraan bersama bagi seluruh rakyat Indonesia. Perlindungan data pribadi juga dapat dipahami sebagai bagian dari upaya untuk memastikan kesejahteraan bersama dengan mencegah penyalahgunaan data yang dapat merugikan individu atau masyarakat secara luas. Dalam kesimpulannya, meskipun UUD 1945 tidak secara langsung membahas perlindungan data pribadi, prinsip-prinsip dalam UUD tersebut masih relevan dan dapat diinterpretasikan dalam konteks perlindungan data pribadi di era digitalisasi. Penting bagi pemerintah dan pemangku kepentingan lainnya untuk mengembangkan regulasi dan praktik terkait yang sesuai dengan prinsip-prinsip tersebut guna memastikan perlindungan yang memadai terhadap data pribadi masyarakat.
2	Ancaman ancaman siber di era digitalisasi	UUD 1945	ancaman siber dari perspektif prinsip-prinsip dalam UUD 1945. Berikut adalah beberapa ancaman siber di era digitalisasi yang dapat dianalisis: 1. **Pelanggaran Privasi**: Ancaman siber terhadap privasi individu dapat dilihat sebagai pelanggaran terhadap hak asasi manusia, termasuk hak atas privasi, yang diamanatkan oleh UUD 1945. Serangan siber seperti peretasan data pribadi, pemantauan ilegal, atau

2961-8754

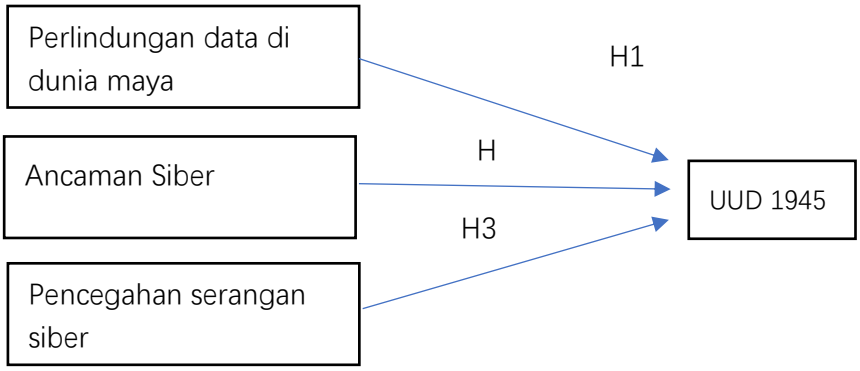
			penyebaran informasi pribadi tanpa izin adalah bentuk pelanggaran yang mencoreng prinsip-prinsip tersebut. 2. **Kejahatan Korporasi dan Ekonomi**: Ancaman siber yang ditujukan pada perusahaan dan institusi keuangan juga dapat dilihat sebagai melanggar prinsip kesejahteraan bersama dan perlindungan hukum, yang diatur dalam UUD 1945. Serangan seperti pencurian data perusahaan, penipuan online, atau manipulasi pasar dapat merugikan kesejahteraan ekonomi bersama serta membutuhkan perlindungan hukum yang kuat. 3. **Serangan Terorisme dan Keamanan Nasional**: Ancaman siber terhadap infrastruktur kritis, pemerintah, atau lembaga keamanan juga dapat diinterpretasikan sebagai ancaman terhadap kedaulatan negara dan keamanan nasional, yang dilindungi oleh UUD 1945. Serangan siber seperti serangan DDoS (Distributed Denial of Service), pencurian informasi rahasia negara, atau sabotase terhadap infrastruktur kritis dapat mengganggu stabilitas dan keamanan negara. 4. **Kekerasan Online dan Cyberbullying**: Ancaman siber dalam bentuk kekerasan online, pelecehan, atau cyberbullying juga bisa dipandang sebagai pelanggaran terhadap hak asasi manusia dan prinsip-prinsip keadilan sosial yang diamanatkan oleh UUD 1945. Perlindungan terhadap individu dari serangan dan pelecehan online menjadi penting untuk mewujudkan lingkungan online yang aman dan beradab. Dalam konteks ini, penting bagi pemerintah dan pemangku kepentingan lainnya untuk mengembangkan kebijakan, regulasi, dan kerangka hukum yang sesuai dengan prinsip-prinsip dalam UUD 1945 guna melindungi masyarakat dari ancaman siber yang semakin

2961-8754

			kompleks di era digitalisasi. Upaya perlindungan tersebut harus mencakup kolaborasi antar sektor publik dan swasta, serta keterlibatan aktif dari masyarakat dalam memperkuat keamanan siber secara keseluruhan.
3	Peran management sekuriti dalam Upaya pencegahan kejahatan siber	UUD 1945	Peran manajemen keamanan dalam upaya pencegahan kejahatan siber dapat dilihat dari perspektif prinsip-prinsip yang tercantum dalam UUD 1945. Meskipun UUD 1945 tidak secara khusus membahas kejahatan siber karena lahir pada zaman di mana teknologi informasi belum sekompleks saat ini, prinsip-prinsip dalam UUD tersebut masih relevan dalam konteks pencegahan kejahatan siber. Berikut adalah beberapa peran manajemen keamanan dalam upaya pencegahan kejahatan siber yang dapat dikaitkan dengan prinsip-prinsip dalam UUD 1945: 1. **Perlindungan Hak Asasi Manusia**: Peran manajemen keamanan adalah untuk melindungi hak asasi manusia, termasuk hak atas privasi, yang diamanatkan oleh UUD 1945. Dalam konteks kejahatan siber, manajemen keamanan bertanggung jawab untuk melindungi data pribadi individu dari peretasan dan penyalahgunaan oleh pihak yang tidak berwenang. 2. **Kesejahteraan Bersama**: Manajemen keamanan bertugas untuk memastikan kesejahteraan bersama masyarakat dengan mencegah kerugian akibat kejahatan siber. Ini mencakup melindungi infrastruktur kritis, perusahaan, dan lembaga keuangan dari serangan siber yang dapat mengganggu stabilitas dan kesejahteraan ekonomi bersama. 3. **Keadilan Sosial dan Perlindungan Hukum**: Manajemen keamanan memiliki peran dalam memastikan keadilan sosial dengan mencegah penyalahgunaan data dan penipuan online yang dapat merugikan individu

2961-8754

			atau kelompok yang lebih lemah. Ini mencakup pengembangan kebijakan dan regulasi yang memastikan perlindungan hukum bagi korban kejahatan siber serta memberlakukan sanksi bagi pelaku kejahatan. 4. **Kedaulatan Rakyat dan Keamanan Nasional**: Manajemen keamanan juga memiliki peran dalam menjaga kedaulatan rakyat dan keamanan nasional dari ancaman siber. Ini termasuk melindungi sistem informasi pemerintah, infrastruktur kritis, dan data sensitif negara dari serangan siber yang bertujuan untuk mengganggu stabilitas dan keamanan negara. Dalam konteks pencegahan kejahatan siber, manajemen keamanan bertanggung jawab untuk mengembangkan dan melaksanakan strategi keamanan yang holistik dan proaktif, yang mencakup identifikasi risiko, implementasi kontrol keamanan yang tepat, pelatihan karyawan, pemantauan keamanan, respons terhadap insiden, dan penilaian secara berkala terhadap keefektifan sistem keamanan. Penting bagi pemerintah dan pemangku kepentingan lainnya untuk bekerja sama dalam mengatasi ancaman siber dengan memperhatikan prinsip-prinsip dalam UUD 1945 serta memastikan bahwa upaya mencegah kejahatan siber dan juga untuk menghormati hak asasi manusia dan prinsip-prinsip keadilan sosial yang diamanatkan oleh konstitusi.



2961-8754

H1 = Perlindungan data pengguna sosial media
H2 = Macam-macam ancaman siber di dunia maya
H3 = Cara mencegah serangan siber

KESIMPULAN

Jadi kesimpulan yang bisa di dapat dari yang kita bahas yaitu bahwa implementasi manajemen sekuriti haruslah mengakomodasi prinsip-prinsip yang tercantum dalam UUD 1945, sambil menyesuaikan dengan tantangan dan dinamika yang muncul dalam konteks digitalisasi. Ini meliputi upaya untuk memastikan keamanan data dan informasi, melindungi hak-hak individu, serta memperkuat keberlangsungan dan kedaulatan negara dalam era digital yang semakin kompleks. Selain itu, penting untuk menjaga keseimbangan antara perlindungan keamanan dan kebebasan individu serta memastikan bahwa kebijakan yang diimplementasikan sesuai dengan nilai-nilai demokrasi dan keadilan yang tertuang dalam UUD 1945.

DAFTAR PUSTAKA

49.+Krisdianto+JMBI+Agustus+2023. (n.d.).

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of Multidisciplinary Science*, *2*(1). https://jurnal.intekom.id/index.php/njms

Pemasyarakatan, P. I. (n.d.). *IMPLEMENTASI MANAJEMEN SECURITY DALAM MENCEGAH TERJADINYA KONFLIK ANTAR NARAPIDANA DI LEMBAGA PEMASYARAKATAN Ronaldo Adi Wiratama*. http://publishing-widyagama.ac.id/ejournal-v2/index.php/yuridika/

Soesanto, E., Saputra Program Studi Manajemen, F., Bhayangkara Jakarta Raya Dita Puspitasari Program Studi Manajemen, U., & Bhayangkara Jakarta Raya Bayu Putra Danaya, U. (2023). Analisis Sistem Manajemen Sekuriti: K3 dan Beban Kerja di PT. XYZ. *Jurnal Riset Dan Inovasi Manajemen*, *1*(2), 139–150. https://doi.org/10.59581/jrim-widyakarya.v1i2.393

2961-8754