e-ISSN:2829-4580, p-ISSN: 2829-4599
DOI: https://doi.org/10.38035/jim.v2i1
Received: 10 Mei 2023, Revised: 30 Mei 2023, Publish: 31 Mei 2023

JIM
JURNAL ILMU MULTIDISIPLIN
E-ISSN:2829-4580, P-ISSN=2829-4599
https://greenpub.org/JIM
editor@greenpub.org
0811 7401 455

Keamanan Cyber dan Peretasan Etis: Pentingnya Melindungi Data Pengguna

Achmad Fauzi[1], Rido Akbar[2], Adela Rizkha[3], Safira Tamiya Putri[4], Intan Fadhilah[5], Nadia Putri Iskandar[6], I Gusti Ngurah Agung[7]
[1.] Universitas.Bhayangkara Jakarta Raya, Indonesia, achmad_fauzi@dsn.ubharajaya.ac.id
[2.] Universitas.Bhayangkara Jakarta Raya, Indonesia, 202010325390@mhs.ubharajaya.ac.id
[3.] Universitas.Bhayangkara Jakarta Raya, Indonesia, 202010325394@mhs.ubharajaya.ac.id
[4.] Universitas.Bhayangkara Jakarta Raya, Indonesia, 202010325400@mhs.ubharajaya.ac.id
[5.] Universitas.Bhayangkara Jakarta Raya, Indonesia, 202010325399@mhs.ubharajaya.ac.id
[6.] Universitas.Bhayangkara Jakarta Raya, Indonesia, 202010325440@mhs.ubharajaya.ac.id
[7.] Universitas.Bhayangkara Jakarta Raya, Indonesia, 202010325395@mhs.ubharajaya.ac.id

Corresponding Author: Rido Akbar

Abstract: *Cyber risk is a hazard or threat associated with the use of interconnected technology systems. This risk occurs when one or more of the three attributes of information namely confidentiality, integrity, and availability are affected. Basically, cyber risk is an operational risk that occurs in cyberspace. Somehow, cybersecurity mechanisms are expensive to implement. This study is to examine the importance of cybersecurity and the use of ethical hacking techniques for the protection of user data through globally defined characterizations. The method used is a literature review based on books, journals, and the internet.*

Keyword: *Cyber Security, Ethical Hacking, Cyber Risk, Data Protection.*

Abstrak: Risiko dunia maya adalah bahaya atau ancaman yang terkait dengan penggunaan sistem teknologi yang saling berhubungan. Risiko ini terjadi ketika satu atau lebih dari tiga atribut informasi yaitu kerahasiaan, integritas, dan ketersediaan terpengaruh. Pada dasarnya, risiko siber merupakan risiko operasional yang terjadi di dunia maya. Entah bagaimana, mekanisme keamanan siber mahal untuk diterapkan. Studi ini untuk menguji pentingnya cybersecurity dan penggunaan teknik hacking etis untuk perlindungan data pengguna melalui karakterisasi yang didefinisikan secara global. Metode yang digunakan adalah literature review berdasarkan buku, jurnal, dan internet.

Kata Kunci: Keamanan Siber, Peretasan Etis, Risiko Siber, Perlindungan Data.

PENDAHULUAN

Saat ini, berbagai layanan ditawarkan melalui Internet, dan di dunia maya, perusahaan dapat terhubung dengan perusahaan di berbagai lokasi secara global. Pada tahun 2019, dengan tegas menyoroti bahwa konektivitas Internet mempercepat pertumbuhan ekonomi sekaligus menghasilkan peluang untuk bisnis dan perdagangan. Meskipun demikian, ada risiko yang terkait dengan penggunaan teknologi informasi dalam model bisnis perusahaan. Di antara risiko tersebut adalah risiko cybernetic yang dapat menyebabkan kerusakan pada operasi organisasi – menyebabkan kerusakan secara khusus pada satu atau lebih dari tiga atribut informasi – yang mengarah pada kerusakan pada sistem teknologi organisasi. Seperti yang dilaporkan dalam di antara banyak organisasi, ada kecenderungan untuk menggunakan langkahlangkah termasuk nama pengguna dan kata sandi yang lemah, enkripsi data, firewall dengan pengaturan default, dan perlindungan virus, tetapi umumnya ada langkah-langkah canggih untuk menangani ancaman dunia maya dan untuk mengurangi risiko dunia maya. Pada tahun 2018, menunjukkan bahwa kegagalan dalam menggunakan langkahlangkah keamanan dasar dalam mengamankan data perusahaan dapat membuat organisasi rentan terhadap serangan cyber Cybersecurity mengacu pada bermacam-macam alat, praktik terbaik, pedoman, kebijakan, konsep keamanan, perlindungan keamanan, pendekatan manajemen risiko, tindakan pelatihan, jaminan dan teknologi yang dapat digunakan dalam melindungi lingkungan dunia maya, organisasi, dan aset pengguna ,Aset organisasi dan pengguna yang terhubung termasuk perangkat komputasi, infrastruktur, aplikasi, layanan, personel, sistem telekomunikasi, selain semua informasi yang dikomunikasikan dan / atau disimpan dalam lingkungan dunia maya.

Cybersecurity memastikan bahwa organisasi mencapai dan mempertahankan properti keamanan dan aset pengguna terhadap risiko keamanan dalam lingkungan cyber. Dalam hal ini, cybersecurity dan teknik hacking keamanan etis dapat diterapkan oleh organisasi dalam mengurangi risiko cyber dan potensi efek pada reputasi organisasi dan datanya. Peretasan etis dapat menjaga privasi digital pengguna. Pada saat yang sama, organisasi dapat memperkirakan potensi serangan dunia maya dan mencegah terjadinya. Oleh karena itu, penerapan teknik keamanan siber dan peretasan etis dapat memfasilitasi organisasi dalam menjaga aset digitalnya.

Ketidaksiapan sebagian besar pengguna Internet dan perusahaan dalam melindungi informasi dari penjahat dunia maya. Kemudian lagi, mekanisme keamanan komputer mahal untuk diterapkan sementara sumber daya untuk tujuan tersebut langk . Dengan demikian, banyak perusahaan memutuskan untuk tidak menerapkan kebijakan dan prosedur keamanan siber dalam pencegahan ancaman siber. Keputusan semacam itu dapat mengarah pada peningkatan tingkat risiko dunia maya, dan ini menempatkan perusahaan pada risiko kerugian finansial ketika informasi bisnis yang sensitif terpengaruh.

Studi ini mengkaji pentingnya keamanan dunia maya dan penggunaan teknik peretasan etis dalam melindungi data pengguna, dan berbagai standar dan teknik yang ditetapkan secara global, untuk tujuan mencegah potensi ancaman dunia maya dan untuk memastikan perlindungan data pengguna.

METODE

Metodologi kualitatif dengan cakupan deskriptif telah dipilih dalam penelitian ini. Oleh karena itu, karakteristik yang terkait dengan cybersecurity dapat dijelaskan dari konsep dasar keamanan siber dari beragam analisis, standar, dan metodologi yang digunakan dalam organisasi. Yang terpilih metodologi digunakan dalam menganalisis pentingnya keamanan dunia maya dan penggunaan peretasan etis teknik dalam melindungi data pengguna. Fase-fase berikut termasuk dalam pengembangan studi: Mengumpulkan informasi yang relevan,

konseptualisasi informasi yang dikumpulkan, dan analisis tentang pentingnya keamanan siber.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Konsep Dasar

Ancaman: Setiap tindakan yang mengeksploitasi kerentanan untuk merusak keamanan sistem informasi atau infrastruktur teknologi, memberikan dampak buruk pada elemen tertentu dari sistem tertentu.

Kerentanan: Cacat atau kegagalan dalam sistem informasi yang membahayakan keamanan informasi, memberikan kesempatan kepada penyerang dalam mengorbankan integritas, ketersediaan atau kerahasiaan sistem, dan karena itu harus diberantas.

Risiko Cyber: Risiko operasional yang terjadi di dunia maya, dan secara khusus mencakup bahaya atau ancaman dari penggunaan sistem teknologi yang saling berhubungan, dan menjadi terlihat ketika di setidaknya salah satu dari tiga atribut informasi terpengaruh

Cyber-Attack: Suatu tindakan yang dilakukan oleh kelompok yang terdiri dari para ahli komputer untuk merusak yang diberikan jaringan atau sistem, tetapi umumnya untuk mengekstraksi informasi pribadi, mencuri, memata-matai atau memeras.

Hacker: Seorang ahli dalam penanganan komputer, khususnya dalam keamanan sistem dan dalam membentuk teknik perbaikan . Tiga kelas hacker dengan niat yang berbeda dalam melanggar sebuah organisasi, dan mereka adalah Black Hat Hacker, Grey Hat Hacker dan White HatHacker.Dengan rincian masing-masing adalah sebagai berikut:

1. Peretas Black Hat mencari kesalahan dalam infrastruktur teknologi perusahaan dan mengeksploitasi kerusakan ini untuk melakukan tindakan yang salah seperti mencuri data untuk keuntungan ekonomi
2. Peretas Grey Hat menggunakan teknik yang mirip dengan rekan Black Hat tetapi dengan tujuan menginformasikan perusahaan tentang masalah keamanan mereka daripada untuk pribadi sendiri keuntungan.
3. Peretas Topi Putih adalah peretas etis dan mereka menggunakan teknik tertentu dalam menjelajahi, menguji dan memperbaiki kelemahan dalam sistem organisasi. Teknik yang digunakan oleh hacker ini dikenal perusahaan.

Analisis Keamanan

Analisis keamanan bervariasi dalam hal jenis, cakupan, dan kedalaman. Dalam kasus ini, Visibilitas dan positioning perlu dipertimbangkan, dimana yang pertama berhubungan dengan informasi itu akan disajikan sebelum keamanan sistem informasi dianalisis, sementara yang terakhir terkait ke lokasi analisis keamanan, baik di dalam maupun di luar organisasi. Di seluruh dunia, di sana ada tiga jenis analisis keamanan sebagai berikut

1. Penilaian kerentanan: Penilaian dengan kedalaman terendah tetapi membutuhkan yang terkecil jumlah waktu dan sumber daya. Identifikasi pelabuhan terbuka, layanan yang dapat diakses, dan diidentifikasi kerentanan dalam sistem informasi target, semuanya adalah bagian dari peniaian kerentanan.
2. Tes intrusi : Tes intrusi yang mencakup tugas-tugas yang terkait dengan eksploitasi dan pasca eksploitasi kerentanan. Sama halnya, tes ini mencakup sekelompok tes objektif yang dilakukan di mendeteksi kerentanan dalam suatu sistem, berdasarkan asumsi bahwa tidak ada sistem yang sepenuhnya aman.
3. Peretasan Etis: Suatu bentuk peretasan yang menganggap setiap elemen sebagai tujuan dan merupakan jenis analisis keamanan yang paling reflektif, dengan tujuan menganalisis keamanan secara sistematis sistem informasi untuk menentukan apa adanya, dan kelemahan yang dapat berdampak pada organisasi.

Selain yang disebutkan di atas, ada juga jenis analisis keamanan lainnya dilakukan pada sistem informasi. Diantaranya termasuk analisis risiko dan audit kode. Penggunaan setiap jenis analisis ditentukan oleh persyaratan dan tujuan organisasi.

Standar Keamanan

Dalam implementasi solusi Cybersecurity dan Ethical Hacking dalam suatu organisasi, pekerjaan standar dan kombinasi yang tepat perlu ditentukan terlebih dahulu untuk menghasilkan asolusi komprehensif. Oleh karena itu, standar keamanan siber utama adalah sebagai berikut:

1. ITU-T X.1205 (04/2008): Ini menyajikan definisi cybersecurity dan klasifikasi ancaman keamanan dari pandangan organisasi.
2. Kerangka Keamanan Siber NIST: Kerangka kerja sukarela yang terdiri dari standar, pedoman, dan praktik terbaik dalam pengelolaan risiko terkait keamanan siber. Kerangka Keamanan Siber menggunakan pendekatan yang fleksibel dan hemat biaya dan ini memfasilitasi promosi perlindungan dan ketahanan infrastruktur kritis.
3. Konvensi Budapest: Konvensi Budapest adalah alat internasional dengan tujuan standarisasi pendekatan yang digunakan oleh negara-negara anggota dalam menggambarkan dan menangani kejahatan dunia maya
4. Directive (EU) 2016/1148 Parlemen Eropa dan Dewan Eropa : Arahan ini untuk memperkuat pendekatan internasional di Persatuan yang berbadan hukum berbagi persyaratan minimum dalam hal pengembangan kapasitas dan perencanaan, informasi pertukaran, kerja sama, dan saling membutuhkan keamanan untuk operator layanan kritis dan digital penyedia layanan.
5. Executive Order (EO 13636) USA: Executive Order ini membahas tentang peningkatan cybersecurity dalam infrastruktur utama, kebutuhan untuk memberikan perlindungan yang sah bagi perusahaan yang berbagi dengan Pemerintah informasi mengenai ancaman dunia maya, dan kebutuhan untuk melindungi infrastruktur teknologi dari organisasi.
6. ISO/IEC 27032: Standar ini mempercepat kemitraan yang aman dan dapat diandalkan dalam melindungi privasi orang secara global, mengarah pada kemudahan dalam persiapan, deteksi, pemantauan dan tanggapan terhadap serangan
7. ISO/IEC TR 27103: Teknologi informasi - Teknik keamanan - Cybersecurity dan ISO dan standar IEC menunjukkan bagaimana standar keamanan informasi saat ini dapat dimanfaatkan oleh kerangka keamanan siber dalam pencapaian pendekatan keamanan siber yang terkontrol dengan baik manajemen.

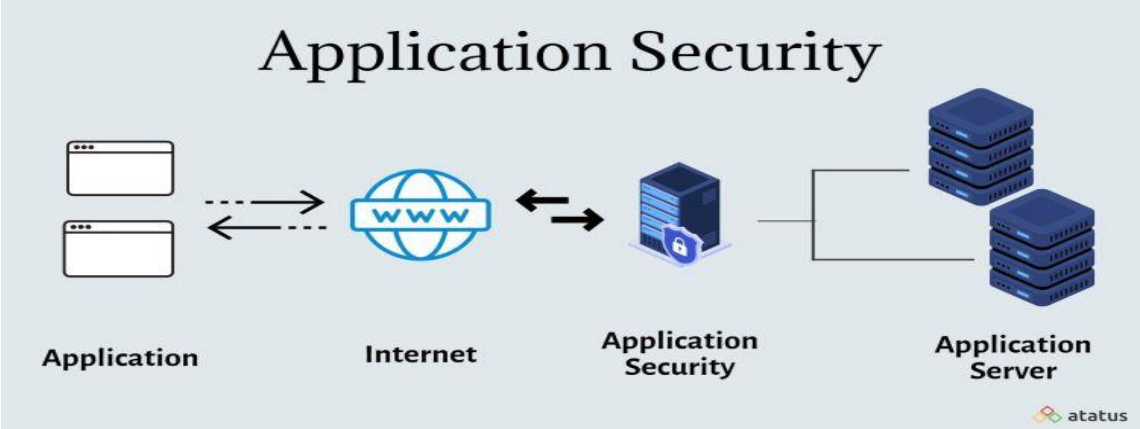
Standar dan analisis keamanan harus diterapkan bersama untuk memungkinkan evaluasi cyber risiko yang dihadapi perusahaan, dan perumusan keputusan yang tepat dalam mengelolanya.

Pembahasan

Sebelum penerapan kebijakan keamanan siber, perlu menyoroti kebutuhan organisasi dan mengenali kebutuhannya. Menggunakan kebutuhan ini, organisasi harus memilih standar yang paling tepat dan analisis keamanan dalam jangka waktu tertentu. Studi ini telah menentukan Peretasan Etis sebagai analisis keamanan yang direkomendasikan. Secara khusus, peretasan etis dilakukan secara mendalam dan rumit infrastruktur teknologi dan sistem informasi organisasi. Khususnya, perusahaan adalah segalanya rentan karena keamanan penuh tidak ada. Namun, perusahaan dapat melakukan upaya pengurangan risiko dunia maya. Sementara itu, kejahatan dunia maya akan terus berkembang, dan dengan munculnya Artificial Intelijen, organisasi harus bersiap untuk membela diri terhadap penjahat dunia maya, dan menanamkan kesadaran kepada karyawan mereka tentang risiko dunia maya yang mereka hadapi.

Conceptual Framewok

Berdasarkan hasil analisis dari berbagai literatur penelitian terdahulu yang relevan dan pembahasan memiliki pengaruh antar variabel, maka diperoleh hasil seperti ini :



Penelitian Terdahulu

1. Penelitian terdahulu yang dilaksanakan Adi Rio Arianto dkk dengan judul " Membangun Pertahanan dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Nasional Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII) Hasil studi menemukan bahwa ancaman siber di Indonesia sangat kompleks, melihat variasi dari aktor, motif, dan targetnya. Kompleksitas ini dapat dijelaskan melalui empat aspek berikut, yaitu: (1) berangkat dari studi Geometripolitika, fungsionalisme siber berada dalam dua domain, yaitu "fungsionalisme siber untuk tujuan politik tingkat tinggi (geometrik militer)" berupa formulasi dan aktivasi kekuasaan Siber guna menghadapi Perang Siber Global (PSG), Perang Geometri Antarbangsa (PGA), dan kompleksitas terbentuknya Negara Maya atau Pemerintahan Siber; dan "fungsionalisme siber untuk tujuan politik tingkat normal (geometrik sipil)" berupa perlindungan aktivitas sipil di dunia maya; (2) guna mencegah kejahatan siber, implementasi kebijakan ID-SIRTII terintegrasi dengan peran strategis institusi siber nasional; (3) guna menghadapi Ancaman Siber Global, implementasi kebijakan ID-SIRTII perlu terintegrasi dengan institusi siber regional dan global; dan (4) berangkat dari "fungsionalisme siber" dan untuk menciptakan suatu strukturalisme Pertahanan dan Keamanan Siber Nasional Indonesia, sudah saatnya Indonesia membentuk Angkatan Siber sebagai pelengkap dari Angkatan Darat, Agkatan Laut, dan Angkatan Udara.
2. Penelitian terdahulu yang dilaksanakan Fadjroel Rachman dengan judul "Modal Sosial Masyarakat Digital dalam Diskursus Keamanan Siber" hasil studi menemukan Masyarakat dan aktor sosial menghadapi berbagai ancaman sosiologis seperti pembajakan identitas, kejahatan dunia maya, dan kekerasan dan penelitian ini menekankan bahwa keamanan siber tidak hanya dilihat dari ancaman isu teknologi tetapi juga dari ancaman kesadaran radikal dari modal sosial masyarakat digital.
3. Penelitian terdahulu yang dilaksanakan Martanto Dkk dengan judul ' Analisis Dampak Pandemi Covid-19 Ditinjau dari Sudut Pandang Keamanan Siber" hasil studi menemukan bahwa Pendidikan tentang keamanan siber bagi masyarakat dan karyawan sudah menjadi kebutuhan utama saat ini. Organisasi perlu mulai berinvestasi terhadap pendidikan bagi karyawan tentang keamanan dunia maya, sehingga mereka mampu untuk melindungi diri mereka sendiri.

KESIMPULAN

Studi ini mengeksplorasi studi sebelumnya tentang keamanan siber dan peretasan etis. Mengingat itu, ada adalah kebutuhan bagi organisasi untuk merumuskan dan berinvestasi dalam kebijakan dan praktik keamanan siber yang etis peretasan sehingga mereka dapat melindungi infrastruktur teknologi mereka, terutama penggunanya informasi, karena dianggap sebagai aset mereka yang paling berharga. Kepercayaan pengguna dapat dirusak oleh suatu data pelanggaran, yang dapat sangat mempengaruhi keuangan perusahaan. Dalam hal ini, organisasi harus pertimbangkan untuk menerapkan mekanisme keamanan dasar untuk penyaringan paket, deteksi intrusi, sistem otentikasi, pemeliharaan dan pembaruan sistem operasi dan platform bisnis, dan enkripsi data. Semua ini untuk menjamin kerahasiaan, integritas dan ketersediaan informasi.

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). https://doi.org/10.33172/jpbh.v9i1.497

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis Of Cyber Security Knowledge Gaps Based On Cyber Security Body Of Knowledge. *Education and Information Technologies*, *28*(2). https://doi.org/10.1007/s10639-022-11261-8

Hadi, M. D. S., Widodo, P., & Putro, R. W. (2020). Analisis Dampak Pandemi Covid 19 Di Indonesia Ditinjau Dari Sudut Pandang Keamanan Siber. *Jurnal Kebangsaan*, *1*(1).

Jose, H. S. (2021). Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 di Forum Multilateral. *POPULIKA*, *9*(2). https://doi.org/10.37631/populika.v9i2.390

Munte, A. (2021). Analisis Keamanan Siber Dan Hukum Pidana Dari Perspektif Gender Dan Filsafat Politik Alison M. Jaggar. *Al' Adl: Jurnal Hukum*, *13*(2), 284–302.

Nugroho, I. I., Pratiwi, R., & Az Zahro, S. R. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2). https://doi.org/10.15294/ipmhi.v1i2.53698

Oktaviani, P. B., & Silvia, A. (2021). Strategi Keamanan Siber Malaysia. *Jurnal Kajian Ilmiah*, *21*(1). https://doi.org/10.31599/jki.v21i1.447

Primawanti, H., & Pangestu, S. (2020). Diplomasi Siber Indonesia Dalam Meningkatkan Keamanan Siber Melalui Association Of South East Asian Nation (Asean) Regional Forum. *Global Mind*, *2*(2). https://doi.org/10.53675/jgm.v2i2.89

Rachman, M. F., & Susan, N. (2021). Modal Sosial Masyarakat Digital dalam Diskursus Keamanan Siber. *Jurnal Indonesia Maju*, *1*(1).

Siagian, L., Budiarto, A., & Simatupang. (2018). Peran Keamanan Siber Dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional. *Jurnal Prodi Perang Asimetris*, *4*(3).

Weu, M. R. (2020). Kerjasama Pemerintah Indonesia Dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber. *Global Political Studies Journal*, *4*(2). https://doi.org/10.34010/gpsjournal.v4i2.5879

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1). https://doi.org/10.1080/08874417.2020.1712269