P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime

[1]Firdi Gunawan, [2]Ahmad Fadhilah, [3]Essy Malays Sari
[1,2,3]Informatika, Universitas Persada Indonesia YAI, kota Jakarta Pusat

E-mail: [1]firdi.gunawan.2144190005@upi-yai.ac.id ,
[2]ahmadfadhilah1108@gmail.com , [3]essy.malays@upi-yai.ac.id

ABSTRAK

Penelitian ini membahas pentingnya keamanan siber dalam melawan ancaman kejahatan siber dan bagaimana membangun benteng digital untuk memperkuat etika keamanan siber. Cybersecurity adalah kegiatan perlindungan digital terhadap sistem komputer dari serangan ilegal yang dapat mengancam keamanan data. Strategi untuk membangun kebudayaan cybersecurity berkelanjutan, prinsip-prinsip etika cybersecurity, serta tantangan dan solusi dalam penerapan etika cybersecurity juga dibahas. Pentingnya membangun sistem keamanan yang kuat untuk melindungi informasi pribadi pengguna di sektor seperti perbankan, pemerintahan, dan kesehatan disoroti. Solusi untuk memperkuat etika keamanan siber termasuk meningkatkan kesadaran etika, memperbaiki regulasi, dan melibatkan berbagai pemangku kepentingan. Etika memainkan peran penting dalam memperkuat pertahanan cybersecurity dengan prinsip-prinsip seperti kerahasiaan, integritas, dan keadilan. Upaya untuk mengurangi ketidakpastian dalam ekonomi digital termasuk peningkatan pelatihan keamanan siber, pengembangan chatbot untuk kesadaran keamanan siber, dan promosi perilaku etis dalam media sosial. Metode Penelitian Dalam penelitian ini, menggunakan metodologi kualitatif dengan pendekatan analisis konten. Sampel Sumber data yang digunakan dalam penelitian ini adalah jurnal-jurnal, buku, artikel dan situs website dari berbagai sumber terpercaya, seperti database ilmiah, repositori perpustakaan, dan situs web terkait.

Kata kunci : ***Cyber security, Etika Cyber security, Cyber Crime, Membangun benteng digital***

ABSTRACT

This research discusses the importance of cybersecurity in combating cybercrime threats and how to build a digital fortress to strengthen cybersecurity ethics. Cybersecurity is the activity of digital protection against computer systems from illegal attacks that can threaten data security. Strategies for building a sustainable cybersecurity culture, the principles of cybersecurity ethics, as well as challenges and solutions in the implementation of cybersecurity ethics are also discussed. The importance of building a robust security system to protect users' personal information in sectors such as banking, government, and healthcare is highlighted. Solutions to strengthen cybersecurity ethics include increasing ethical awareness, improving regulations, and involving various stakeholders. Ethics play a crucial role in strengthening cybersecurity defenses with principles such as confidentiality, integrity, and fairness. Efforts to reduce uncertainty in the digital economy include enhancing cybersecurity training, developing chatbots for cybersecurity awareness, and promoting ethical behavior on social media.

Keywords: ***Cyber security, Cyber security ethics, Cyber Crime, Building a digital fortress***

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

1. LATAR BELAKANG

1.1 Latar Belakang

Di Era modern digital dan Internet saat ini , Semua jenis teknologi informasi dan komputer dapat digunakan untuk membuat, menyimpan, mengubah, dan menggunakan informasi dalam bentuk apa pun (Essy Malays Sari, 2018). Pengunaan teknologi telah di gunakan pada semua bidang kehidupan, Hampir semua aspek kehidupan manusia kini bergantung pada teknologi digital, mulai dari aktivitas pribadi, bisnis, hingga pemerintahan. Namun, seiring dengan kemajuan teknologi, ancaman terhadap keamanan data dan informasi juga semakin meningkat. Cyber crime menjadi ancaman serius yang dapat merusak kepentingan individu, perusahaan, bahkan negara. Untuk melindungi diri dari serangan ini, perlindungan cyber security menjadi sangat penting. Salah satu cara efektif untuk memperkuat etika cyber security adalah dengan membangun benteng digital yang kuat. Dengan menjadikan etika cyber security sebagai prioritas utama, individu maupun organisasi dapat membangun pertahanan yang tangguh melawan ancaman cyber crime, menjaga kerahasiaan data, serta melindungi integritas sistem informasi secara menyeluruh.

1.2 Rumusan Masalah

1) Apa dampak negatif yang di timbulkan oleh cybercrime ?
2) Bagaimana peran etika dalam memperkuat pertahanan cyber security terhadap ancaman cyber crime?
3) Apa strategi untuk membangun kebudayaan cybersecurity berkelanjutan untuk terhindar dari ancaman cybercrime ?
4) Apa saja prinsip-prinsip utama etika cybersecurity?
5) Tantangan dan Solusi dalam penerapan etika cybersecurity ?

1.3 Batasan Masalah

Agar pembahasan fokus, maka penelitian ini ber fokus pada strategi untuk membangun kebudayaan cybersecurity berkelanjutan, prinsip-prinsip utama etika cybersecurity, serta tantangan dan solusi dalam penerapan etika cybersecurity.

1.4 Tujuan Dan Kegunaan

1. Tujuan

Tujuan penulisan penelitian ini, penulis berharap pembaca lebih mengerti akan bagaimana membangun benteng digital untuk memperkuat etika keamanan siber dalam melawan ancaman kejahatan siber yang semakin kompleks dan merajalela di era digital ini, sehingga mampu menciptakan lingkungan yang aman, terpercaya, dan tangguh terhadap berbagai jenis ancaman kejahatan siber yang dapat mengancam keberlangsungan individu, perusahaan, maupun entitas negara di era digital yang penuh dengan tantangan ini . Adapun tujuan dari penulisan penelitian ini adalah untuk :

- Memperkenalkan pentingnya membangun benteng digital untuk memperkuat etika keamanan siber dalam melawan ancaman kejahatan siber.
- Mendorong kesadaran masyarakat akan perlunya melindungi data dan informasi dari ancaman kejahatan dunia maya melalui pembangunan benteng digital yang solid.

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

- Mengidentifikasi prinsip-prinsip utama etika cybersecurity

2. Kegunaan

penulisan penelitian ini adalah Membangun benteng digital untuk memperkuat etika cyber security melawan ancaman cyber crime membantu dalam meningkatkan kesadaran akan pentingnya perlindungan data dan informasi pribadi, serta menciptakan lingkungan online yang lebih aman dan terpercaya bagi seluruh pengguna internet. Selain itu, upaya ini juga bertujuan untuk mengurangi kerentanan terhadap serangan cyber, memberikan 66endidikan tentang risiko cyber crime.

1.5 Manfaat Penelitian

Manfaat penelitian penelitian ini Penelitian ini dapat berkontribusi pada strategi pengembangan dan kebijakan yang dapat memperkuat etika keamanan siber dan mencegah kejahatan siber serta membantu dalam meningkatkan kesadaran akan pentingnya perlindungan data dan informasi pribadi, menciptakan lingkungan online yang lebih aman dan terpercaya bagi pengguna internet, mengurangi kerentanan terhadap serangan siber, dan memberikan edukasi tentang risiko kejahatan dunia maya

2. KAJIAN PUSTAKA

2.1 Pengertian Cybercrime

Setiap kali kita membahas suatu topik, penting untuk memperoleh pemahaman yang kuat tentang konteksnya. Ini membantu menambah wawasan dan memahami apa yang di bahas dengan lebih baik, untuk menghindari kesan kurang informasi. Berbicara tentang cybercrime. Cybercrime menurut journal (“Cyber Crime and Its Classification, 2021”), Cyber Crime adalah sekelompok kegiatan yang dilakukan oleh orang-orang dengan menciptakan gangguan dalam jaringan, mencuri data penting dan pribadi orang lain, dokumen, meretas rincian bank dan rekening dan mentransfer uang ke rekening mereka sendiri.(Goni, 2021), menurut sumber website (Cyber Crime Meningkat Tajam Di Masa Pandemi – Fakultas Ilmu Sosial Dan Ilmu Politik – Universitas Indonesia, n.d.), Cyber, Cybercrime merupakan tindakan ilegal yang dilakukan dengan penjahat yang menggunakan teknologi sistem informasi jaringan komputer untuk secara langsung menyerang teknologi sistem informasi korbannya. Namun dalam arti yang lebih luas, cybercrime juga dapat diartikan sebagai kegiatan ilegal yang difasilitasi oleh teknologi computer. Dan menurut Journal (“PENGARUH FENOMENA CYBERBULLYING SEBAGAI CYBER-CRIME DI INSTAGRAM DAN DAMPAK NEGATIFNYA, 2020”), Cybercrime merupakan suatu kegiatan kriminal yang menggunakan teknologi komputer berupa internet sebagai alat utama kejahatannya dan merupakan salah satu bentuk kegiatan kriminal yang melanggar hukum.(Jubaidi & Fadilla, 2020). Jadi, kesimpulan dari sumber-sumber tersebut adalah bahwa cybercrime melibatkan kegiatan kriminal yang menggunakan teknologi komputer, terutama internet, untuk melakukan berbagai jenis kejahatan, termasuk pencurian data, meretas, dan gangguan dalam jaringan salah satu bentu kegiatan ckriminal yang melanggar hukum. Tadi

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

Berebicara tentang pengertian cybercrime , cybercrime yang umum terjadi saat ini dapat di kategorikan sebagai berikut :

1. Penipuan Online:

- **Phishing:** Mengirim email atau pesan palsu untuk menipu korban agar memberikan informasi pribadi atau keuangan.
- **Social engineering**: Memanipulasi korban secara psikologis untuk menyerahkan informasi sensitif.
- **Penipuan berkedok investasi**: Menawarkan investasi palsu dengan keuntungan tinggi untuk menarik korban.

2. Kejahatan terhadap Data:

- **Pencurian data**: Mengambil data pribadi atau keuangan korban secara ilegal.
- **Ransomware**: Mengunci data korban dan meminta tebusan untuk membukanya.
- **Malware:** Menyebarkan virus atau program berbahaya untuk merusak perangkat atau mencuri data.

3. Cyberbullying:

- Melecehkan atau mengintimidasi seseorang secara online melalui pesan, gambar, atau video.
- Menyebarkan rumor atau informasi palsu tentang seseorang di internet.
- Mengganggu atau mengancam seseorang secara online.

4. Kejahatan terhadap Konten:

- **Penyebaran pornografi anak:** Membagikan atau memiliki konten pornografi yang melibatkan anak-anak.
- **Hate speech:** Menyebarkan ujaran kebencian atau SARA di internet.
- **Cyberespionage**: Mencuri rahasia dagang atau informasi sensitif dari perusahaan atau organisasi.

5. Kejahatan terhadap Keamanan Siber:

- **Hacking:** Membobol sistem komputer atau jaringan secara ilegal.
- **Denial-of-service attack (DoS):** Melumpuhkan situs web atau server dengan serangan traffic yang besar.
- **Defacement:**Mengubah tampilan situs web tanpa izin.

Cybercrime telah menjadi ancaman serius bagi individu, perusahaan, dan pemerintah di seluruh dunia. Dengan meningkatnya kompleksitas dan kerentanan dalam ekosistem digital, perlindungan dan kesadaran terhadap risiko cybercrime menjadi semakin penting bagi semua pemangku kepentingan.

2.2 Pengertian Cyber Security

Cyber crime menjadi ancaman serius yang dapat merusak kepentingan individu, perusahaan, bahkan negara membutuhkan sistem keamanan yang lebih dan karena itu pula Cyber Security hadir. Apasih cybersecurity itu, Menurut journal (“Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital”., 2022) Cybersecurity adalah suatu kegiatan perlindungan digital terhadap suatu sistem komputer dari beberapa serangan atau akses ilegal yang dapat mengganggu keamanan data dan informasi dalam suatu jaringan.(Wahib et al., 2022), Menurut journal (“Taxonomy of cyber security metrics to measure strength of cyber security”., 2023) Cybersecurity adalah

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

menjaga sistem komputer, data, jaringan, dan sumber daya lainnya dari akses tidak sah dan pengguna jahat.(Gupta Bhol et al., 2023) dan menurut sumber website(*Kenalan Dengan Tugas Pekerjaan Cyber Security, Yuk! - Universitas Bakrie*, n.d.) Namun, menurut definisi, Cybersecurity adalah praktik melindungi komputer, server, perangkat seluler, sistem elektronik, jaringan, dan data dari serangan jahat.

Jadi, kesimpulan dari sumber-sumber tersebut adalah. Cybersecurity merupakan serangkaian kegiatan perlindungan digital yang bertujuan untuk melindungi sistem komputer, data, jaringan, dan sumber daya elektronik lainnya dari berbagai serangan atau akses ilegal yang dapat mengancam keamanan informasi. Hal ini termasuk menjaga sistem dari akses tidak sah, mencegah serangan jahat, serta memastikan keamanan dan integritas data. Dengan kata lain, Cybersecurity merupakan praktik yang penting dalam menjaga keamanan digital, baik bagi individu, perusahaan, maupun negara, mengingat ancaman cybercrime yang semakin meningkat.

2.3 Pengertian Etika

Menurut buku ("BUKU AJAR ETIKA HUKUM", 2021). Kata "etika" berasal dari kata Yunani "ethos", yang berarti "dapat dijabarkan kembali" dan berarti "kebiasaan." Beberapa makna etika berhubungan satu sama lain. Ini termasuk:

1) Makna pertama berarti nilai-nilai yang dimiliki oleh kelompok tertentu, seperti kode etik, etika kerja, dan kelompok profesi.
2) Makna yang kedua berarti nilai-nilai yang dimiliki oleh masyarakat atau kelompok masyarakat untuk menentukan mana yang baik dan benar.
3) Makna yang ketiga berarti pengetahuan yang dimiliki orang tentang apa yang baik dan benar. Etika dapat didefinisikan sebagai pemikiran tentang hal-hal yang kritis dan dapat diterima secara logis tentang norma-norma. Etika Cyber Law dapat dilihat dalam tindakan seseorang.(Tanhela Zein Vitadiar, 2021).

Dengan demikian, dapat disimpulkan bahwa etika adalah bidang yang mempelajari dan menjelaskan tentang hak dan kewajiban yang menunjukkan tindakan yang baik atau buruk. Itu juga dapat menjelaskan tanggung jawab seseorang dan mempengaruhi moral manusia dan komitmen mereka terhadap masyarakat.(Tanhela Zein Vitadiar, 2021).

3. METEDOLOGI

3.1 Metodologi Penelitian

Metode Penelitian Dalam penelitian ini, menggunakan metodologi kualitatif dengan pendekatan analisis konten. Metodologi kualitatif digunakan karena topik penelitian ini membutuhkan pemahaman yang lebih dalam mengenai konteks, makna, dan interpretasi dari fenomena yang sedang dibahas. Pendekatan analisis konten digunakan untuk menganalisis data yang berasal dari sumber-sumber yang terpercaya, seperti jurnal-jurnal, buku, artikel dan situs website.

3.2 Sumber Data

Sampel Sumber data yang digunakan dalam penelitian ini adalah jurnal-jurnal, buku, artikel dan situs website dari berbagai sumber terpercaya, seperti database ilmiah, repositori perpustakaan, dan situs web terkait. Sumber-sumber ini dipilih karena mengandung informasi yang relevan dan

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

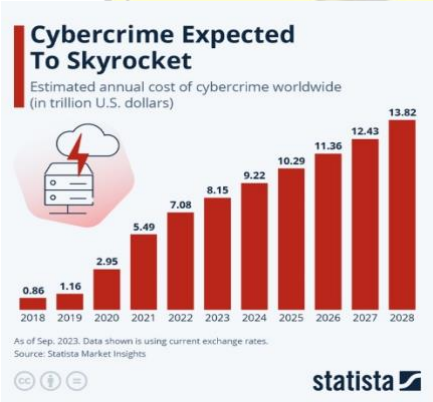
berkaitan dengan topik penelitian. Selain itu, sumber-sumber ini telah terverifikasi dan dicatat sebagai referensi ilmiah yang diterima. Alur penelitian ini :

Gambar1.Alur penelitian
sumber:pribadi

4. PEMBAHASAN

4.1 Dampak Negatif Cybercrime

Cyber crime seperti yang kita bahas . Kerugian yang disebabkan oleh kejahatan Cyber crime sangat besar dampak nya, Kejahatan Cybercrime Diperkirakan Akan Meroket di Tahun-Tahun Mendatang menurut sumber data Statista's Market Insights (*Cybersecurity - Worldwide | Statista Market Forecast*, n.d.)



Gambar1. Cybercrime Expected To Skyrocket
Sumber:
(*Cybersecurity - Worldwide | Statista Market Forecast*, n.d.)

Kerugian akibat cybercrime global akan meningkat selama empat tahun ke depan, meningkat dari $9,22 triliun pada tahun 2024 menjadi $13,82 triliun pada tahun 2028.
Sumber Majalah Cybercrime (Top 10 Cybersecurity Predictions and Statistics For 2024,n.d.)
mendefinisikan kejahatan dunia maya sebagai "bahaya dan kerusakan", penghancuran data,
pencurian uang, hilangnya produktivitas, pencurian kekayaan intelektual, pencurian informasi pribadi dan keuangan, penggelapan, penipuan, pasca-serangan terhadap jalannya
bisnis normal ,penyelidikan forensik, pemulihan dan penghapusan data dan sistem yang
diretas, dan kerusakan reputasi.
Data Dampak kerugian cyber crime yang berbeda menurut sumber data Surfshark(Cybercrime Statistics, n.d.)

Gambar2.Impactof different Cybercrime
Sumber: (Cybercrime Statistics, n.d.)

Data Data ini menyoroti dampak finansial yang signifikan dari kejahatan dunia maya, dengan penipuan investasi yang menyebabkan kerugian rata-rata tertinggi per korban sebesar $108,479 dan mengakibatkan

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

total kerugian sebesar $3,3 miliar. Penipuan dukungan teknis dan penipuan kepercayaan atau percintaan juga berkontribusi terhadap kerugian finansial yang besar.

Di sisi lain, phishing memiliki jumlah korban terbanyak, dengan 300,5 ribu orang terkena dampaknya, sehingga mengakibatkan kerugian total sebesar $52,1 juta. Pelecehan online dan serangan malware memiliki total biaya yang lebih rendah dibandingkan jenis kejahatan dunia maya lainnya, namun tetap menimbulkan ancaman bagi pengguna internet.
Penting bagi individu dan organisasi untuk mewaspadai kejahatan dunia maya ini dan mengambil tindakan pencegahan yang diperlukan untuk melindungi diri mereka dari potensi kerugian finansial dan reputasi.

Kerugian yang disebabkan oleh kejahatan Cyber crime dapat beragam. Pertama-tama, korban dapat berupa individu , masyrakat , dan negara . korban dapat dipengaruhi dengan cara yang sangat berbeda, mulai dari kerugian kecil hingga kerugian besar, dan bahkan efek yang halus dan tidak berwujud pada korban dapat terjadi.(Hidayatullah, 2023). Cybercrime dapat berdampak negatif pada individu, masyarakat, dan negara seperti berikut:

- Dampak negatif cybercrime terhadap individu :
    - Menurut sumber website (*Cybercrime: Pengertian, Tipe, Dan Langkah Mencegahnya* , n.d.) Cybercrime dapat menyebabkan kerugian finansial yang signifikan Menurut laporan McAfee, "The Economic Impact of Cybercrime No Slowing Down", cybercrime telah menyebabkan kerugian sebesar $600 miliar di seluruh dunia.
    - Menurut sumber website (*Apa Itu Cybercrime? Motif, Dampak Negatif Dan Tindak Pencegahannya - Cloud Service Provider*, n.d.), Cyber crime dapat merusak reputasi seorang individu , terutama jika data pribadi atau informasi sensitif bocor.
    - Hilangnya Data Penting terhadap individu sepeti data pribadi, data keuangan , data rekam medis yang di punyai seorang individu (Utari Dwi Nelvenia, n.d.).
- Dampak negatif Cybercrime terhadap masyrakat :
    - Cyber crime dapat merusak kepercayaan masyarakat terhadap teknologi dan internet. Ini dapat menghambat adopsi dan penggunaan teknologi baru.
    - Menurut sumber website (*Hadirnya Cybercrime Menuai Dampak Negatif Bagi Masyarakat Indonesia Halaman 1 - Kompasiana.Com*, n.d.) Pertumbuhan dan Perkembangan Cybercrime: Dengan semakin banyaknya pengguna internet, cybercrime juga semakin berkembang dan menimbulkan dampak negatif yang lebih luas.
- Dampak negatif Cybercrime terhadap negara :
    - Dampak negatif Cybercrime terhadap negara adalah Kerugian Ekonomi
      Cybercrime dapat menyebabkan kerugian ekonomi yang signifikan bagi negara. Hal ini dapat terjadi karena:

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

- Pencurian data keuangan dan informasi sensitif
- Gangguan pada infrastruktur dan layanan penting Penurunan kepercayaan investor

- Dampak negatif Cybercrime terhadap negara Kerusakan Reputasi
  Serangan siber dapat merusak reputasi negara di mata internasional. Hal ini dapat:

- Mengurangi kepercayaan investor
- Menghambat perdagangan dan investasi
- Mempengaruhi hubungan diplomatic.

Dari dampak – dampak negatif dari cybercrime mengelola risiko dan mencegah ancaman terhadap sistem informasi dan jaringan komputer sangat penting. Etika cybersecurity memastikan bahwa sistem informasi digunakan dengan benar dan etis serta menjamin keamanan data, privasi, dan integritas informasi.

4.2 Peran Etika Dalam Memperkuat Pertahanan CyberSecurity Terhadap Ancaman Cyber Crime

Etika memainkan peran penting dalam Cyber security, karena membantu memandu tindakan para profesional dan organisasi dalam dunia digital yang kompleks. Mengapa etika sangat penting dalam keamanan siber :

1. **Kepercayaan dan kredibilitas:** Etika penting untuk membangun kepercayaan dan kredibilitas di kalangan profesional keamanan siber, organisasi, dan masyarakat. Ketika profesional cyber security bertindak dengan integritas dan transparansi, mereka mendapatkan kepercayaan dari pelanggan dan pemangku kepentingan. Hal ini penting dalam memerangi kejahatan dunia maya.

2. **Perilaku Bertanggung Jawab:** Etika mendorong perilaku bertanggung jawab di kalangan profesional cyber security dan mendorong mereka untuk bertindak hati-hati dan bijaksana ketika bekerja dengan informasi dan sistem sensitif. Hal ini mencegah terjadinya hal yang tidak diinginkan seperti kebocoran data dan kegagalan sistem.

3. **Akuntabilitas:** Etika memastikan bahwa para profesional keamanan siber bertanggung jawab atas tindakan dan keputusan mereka. Tanggung jawab ini membantu mencegah perilaku tidak bertanggung jawab atau jahat yang dapat membahayakan keamanan siber dan merugikan individu dan organisasi.

4. **Perlindungan hak asasi manusia:** Etika dalam keamanan siber berkontribusi terhadap perlindungan hak asasi manusia seperti privasi dan kebebasan berekspresi. Para profesional keamanan siber harus memastikan bahwa tindakan mereka tidak melanggar hak-hak ini, bahkan ketika berupaya mencegah kejahatan siber.

4.3 Prinsip – prinsip Etika Cyber Security

Menganalisis konten dari sumber website (*Prinsip Etika Profesi Dalam Keamanan Cybersecurity - Linuxhackingid*, n.d.) Prinsip-prinsip etika mengarahkan tindakan dan keputusan para profesional Cyber Security agar mereka tetap pada jalurnya yang benar dan akuntabel. Di dalam konten website ini ada 4 perinsip etika cyber security yaitu :

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

- **Kerahasiaan:** Profesional Cyber Security harus mempertahankan kerahasiaan informasi dan sistem yang sensitif.

- **Integritas:** Profesional Cyber Security harus bertindak dengan integritas, menghindari perilaku yang dapat mengompromikan keamanan sistem atau data.

- **Ketersediaan:** Profesional Cyber Security harus memastikan bahwa sistem dan data tersedia bagi pengguna yang berwenang, sementara mencegah akses yang tidak sah.

- **Non-Maleficence:** Profesional Cyber Security harus menghindari menyebabkan kerugian pada individu, organisasi, atau masyarakat secara keseluruhan.

- **Keadilan:** Profesional Cyber security harus memastikan bahwa tindakan mereka adil dan tidak diskriminatif terhadap individu atau kelompok mana pun.

4.4 Strategi Untuk Membangub Kebudayaan CyberSecurity Berkelanjutan Untuk Terhindar Dari Ancaman CyberCrime

Strategi membangun benteng digital cyber security adalah penting karena ancaman cybercrime semakin menjadi isu yang serius dan kompleks. Berbagai macam gangguan siber, seperti gangguan sistem komputerisasi, pencurian identitas, hacking, dan pelanggaran keamanan jaringan, menjadi dampak yang sangat merugikan. Dengan membangun Membangun benteng digital cyber security, masyarakat dapat memahami dan membantu menangani isu-isu ini.

Berbagai macam sektor, seperti pendidikan, perbankan, pemerintahan, dan kesehatan, memiliki peran penting dalam membangun budaya keamanan siber. Misalnya, di bidang pendidikan, sekolah harus mengutamakan keamanan siber dan mengalokasikan sumber daya untuk melindungi data, privasi, dan sistem mereka agar proses pembelajaran dapat berjalan dengan aman dan efektif (Raharjo et al., 2024). Dalam perbankan, institusi perbankan harus membangun sistem keamanan yang kuat untuk melindungi transaksi dan informasi pribadi pengguna. Di pemerintahan, lembaga keamanan siber harus membangun sistem keamanan yang efektif dan efisien untuk melindungi sistem dan informasi negara(Haryanto & Sutra, 2023). Di bidang kesehatan, institusi kesehatan harus membangun sistem keamanan yang memungkinkan penggunaan teknologi informasi dan komunikasi (TIK) dalam pendiagnosis, pengobatan, dan pengelolaan kesehatan secara aman dan efektif.

Membangun benteng digital cyber security juga membutuhkan peningkatan kesadaran dan etika siber. Misalnya, generasi Z harus memahami privasi, keadilan, dan tanggung jawab digital, serta membangun kesadaran etika siber yang dapat membantu menangani isu-isu seperti keamanan data pribadi, privasi, dan penyebaran konten negatif(Pambudi et al., 2023). Dalam konteks generasi Z, media sosial berperan penting dalam membentuk karakter, namun konten yang diposting dapat mempengaruhi sikap dan perilaku mereka (Pambudi et al., 2023)

Strategi untuk meningkatkan kesadaran etika keamanan siber dapat diterapkan, Berikut adalah beberapa strategi yang dapat digunakan:

1. **Pendidikan dan Awareness**: Menyediakan informasi dan pelatihan mengenai keamanan siber dan etika digital untuk masyarakat. Hal ini bertujuan untuk membantu masyarakat

https://doi.org/10.37817/tekinfo.v25i1
P-ISSN: 1411-3635
E-ISSN: 2962-5645

memahami pentingnya keamanan siber dan bagaimana cara mengatasi ancaman siber.

2. **Gamifikasi:** Menggunakan gamifikasi untuk membuat pengguna lebih berpikir pada kesadaran cybersecurity. Contohnya, pengembangan aplikasi gamifikasi untuk meningkatkan kesadaran keamanan siber(Hadiprakoso & Agus Satria, 2022)

3. **Pengembangan Chatbot:** Mengembangkan chatbot sebagai media informasi centralized tentang cybersecurity, teknologi, dan internet untuk internet users (Muhyidin & Venica, 2023)

4. **Pelatihan SDM:** Menyediakan pelatihan Cyber Securitys untuk sumber daya manusia (SDM) di bidang keamanan siber (Machlul, 2024)

5. **Pengabdian kepada Masyarakat:** Menggunakan metode Participatory Action Research (PAR) untuk memberikan pendampingan kepada masyarakat mengenai kesadaran keamanan siber (Sussolaikah et al., 2023)

6. **Pengembangan Kode Etik:** Menyusun dan mengembangkan kode etik untuk masyarakat, perusahaan, dan institusi terkait keamanan siber

Dengan menerapkan strategi-strategi inovatif seperti pendidikan dan pelatihan yang terfokus, penggunaan gamifikasi yang kreatif, pengembangan chatbot yang efisien, pelatihan SDM yang mendalam, pengabdian kepada masyarakat melalui metode PAR, dan pengembangan kode etik yang berkelanjutan, kita dapat menciptakan lingkungan online yang lebih aman. dan dilindungi. Hal ini akan meningkatkan kesadaran dan etika keamanan siber secara signifikan, mengurangi risiko kejahatan siber, dan membangun masyarakat yang lebih terampil dan tangguh dalam menghadapi tantangan digital yang semakin kompleks.

4.5 Tantangan Dalam Penerapan Etika Cyber Security

Dalam menerapkan etika keamanan siber, dunia pada umumnya dihadapkan pada berbagai tantangan. keamanan Menjaga tanpa privasi, menghadapi serangan tanpa hak individu, serta menjaga keseimbangan antara kebutuhan teknis dan nilai-nilai kemanusiaan. Tantangan ini membutuhkan kecermatan, integritas, dan kesadaran yang akan berdampak sosial. setiap langkah yang diambil.

Ada berbagai tantangan dalam menerapkan etika keamanan siber antara lain:

- Kurangnya Kesadaran Etika :
  - Banyak masyarakat yang kurang memiliki kesadaran mengenai etika keamanan siber, sehingga semakin sulit menerapkan prinsip-prinsip etika di bidangnya (Flechais & Chalhoub, 2023)
  - Kurangnya kesadaran etis terkait dengan pengelolaan data, penggunaan teknologi, dan dapat mengakibatkan kesalahan etika dalam berperilaku lingkungan digital

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i1

- Ketidak Jelasan Regulasi :
    - Kegagalan dalam regulasi dan kebijakan keamanan siber dapat mengakibatkan kesulitan dalam penerapan etika keamanan siber
    - Banyaknya peraturan yang tidak jelas atau berbeda-beda, sehingga menyulitkan penerapan etika keamanan siber
- Kemajuan Teknologi yang pesat :
    - Kemajuan teknologi dapat mengakibatkan kesulitan dalam penerapan prinsip-prinsip etika, seperti kesulitan dalam mengatur akses dan pengelolaan data yang sesuai dengan prinsip etika

4.6 Solusi Untuk Memperkuat Etika Cyber Security

Untuk mengatasi tantangan dalam penerapan etika keamanan siber, ada beberapa solusi yang dapat dilakukan seperti :

- Mempertinggi kesadaran etika dalam bidang keamanan siber, seperti melalui pendidikan dan pelatihan yang mencakup prinsip-prinsip etika (Bajwa et al., 2023)
- Memperbaiki regulasi dan kebijakan keamanan siber, seperti melalui pengembangan regulasi yang jelas dan konsisten. (Kurpayanidi Konstantin Ivanovich, 2023)
- Memperbaiki sistem pengelolaan data dan teknologi, seperti melalui sistem pengembangan yang memungkinkan pengelolaan data sesuai dengan prinsip-prinsip etika
- Memperbaiki kemajuan teknologi, seperti melalui pengembangan teknologi yang memungkinkan pengelolaan data yang efisien dan efektif(Alkamil et al., 2021)

Tantangan dalam penerapan etika keamanan siber seringkali melibatkan kompleksitas yang memerlukan pendekatan yang cermat dan holistik. Dalam menghadapi kompleksitas tersebut, diperlukan pemahaman yang mendalam tentang prinsip-prinsip etika yang berkaitan dengan keamanan siber serta kemampuan untuk mengidentifikasi, menganalisis, dan menanggapi berbagai permasalahan etika yang muncul dalam konteks informasi teknologi. Di sisi lain, perlu juga mempertimbangkan aspek-aspek hukum, kebijakan, dan regulasi yang relevan dalam lingkup keamanan siber, yang bisa beragam antar negara dan wilayah. Selain itu, penting juga untuk membangun budaya organisasi yang mendorong kesadaran akan pentingnya etika dalam setiap aspek pengembangan dan penerapan teknologi keamanan siber. Dengan demikian, mengatasi tantangan dalam penerapan etika keamanan siber memerlukan pendekatan yang komprehensif dan terintegrasi, serta melibatkan berbagai pemangku kepentingan baik dari segi teknis maupun non-teknis.

P-ISSN: 1411-3635
E-ISSN: 2962-5645

5. KESIMPULAN

5.1 Kesimpulan

Pentingnya Strategi membangun benteng digital cyber security yang berkelanjutan dengan memperkuat etika cyber security untuk melawan ancaman cybercrime. Cyber Security Etika mencakup prinsip-prinsip seperti kerahasian , integritas , ketersediaan , Non-Maleficence, Keadilan. Tantangan dalam penerapan etika keamanan siber meliputi kurangnya kesadaran etika, ketidakjelasan regulasi, dan kemajuan teknologi yang pesat. Solusi untuk memperkuat etika keamanan siber antara lain adalah meningkatkan kesadaran etika, memperbaiki regulasi dan kebijakan, serta memperbaiki sistem pengelolaan data dan teknologi. Diperlukan pendekatan komprehensif dan terintegrasi serta melibatkan berbagai pemangku kepentingan untuk mengatasi tantangan tersebut.

5.2 Saran

meningkatkan kesadaran etika, memperbaiki regulasi dan kebijakan terkait keamanan siber, serta memperbaiki sistem pengelolaan data dan teknologi. Selain itu, pendekatan komprehensif dan terintegrasi serta melibatkan berbagai pemangku kepentingan juga diperlukan untuk mengatasi tantangan dalam menerapkan etika keamanan siber. Strategi seperti pendidikan, awareness, gamifikasi, pengembangan chatbot, dan pelatihan SDM juga dapat digunakan untuk membangun budaya keamanan siber yang lebih kuat

REFERENSI

Alkamil, E. H. K., Mutlag, A. A., Alsaffar, H. W., & Sabah, M. H. (2021). The role of hybrid IoT with cloud computing and fog computing to help the oil and gas industry recover from Covid-19 and face future challenges. *Proceedings - SPE Annual Technical Conference and Exhibition, 2021-September*. https://doi.org/10.2118/206067-MS

Apa itu Cybercrime? Motif, Dampak Negatif dan Tindak Pencegahannya - Cloud Service Provider. (n.d.). Retrieved April 2, 2024, from https://cloudku.id/apa-itu-cybercrime/

Bajwa, M. H. A., Richards, D., & Formosa, P. (2023). Evaluation of embodied conversational agents designed with ethical principles and personality for cybersecurity ethics training. *Proceedings of the 23rd ACM International Conference on Intelligent Virtual Agents, IVA 2023*. https://doi.org/10.1145/3570945.3607359

Cyber Crime Meningkat Tajam di Masa Pandemi – Fakultas Ilmu Sosial dan Ilmu Politik – Universitas Indonesia. (n.d.). Retrieved March 31, 2024, from https://fisip.ui.ac.id/bhakti-cybercrime-menjadi-jenis-kejahatan-yang-mengalami-peningkatan-cukup-tinggi/

Cybercrime: Pengertian, Tipe, dan Langkah Mencegahnya . (n.d.). Retrieved April 2, 2024, from https://www.goldenfast.net/blog/cybercrime-adalah/

Cybercrime statistics. (n.d.). Retrieved May 1, 2024, from https://surfshark.com/research/data-breach-impact/statistics

Cybersecurity - Worldwide | Statista Market Forecast. (n.d.). Retrieved April 30, 2024, from https://www.statista.com/outlook/tmo/cybersecurity/worldwide#cost

Essy Malays Sari. (2018). *PENGGUNAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK) PADA USAHA MIKRO, KECIL DAN MENENGAH (UMKM)*.

Flechais, I., & Chalhoub, G. (2023). Practical Cybersecurity Ethics: Mapping CyBOK to

Ethical Concerns. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3633500.3633505

Goni, O. (2021). Cyber Crime and Its Classification. *International Journal of Electronics Engineering and Applications*, *10*(2). https://doi.org/10.30696/ijeea.x.i.2022.01-17

Gupta Bhol, S., Mohanty, J. R., & Kumar Pattnaik, P. (2023). Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings*, *80*. https://doi.org/10.1016/j.matpr.2021.06.228

Hadiprakoso, R. B., & Agus Satria, W. (2022). RANCANG BANGUN APLIKASI GAMIFIKASI UNTUK MENINGKATKAN KESADARAN KEAMANAN SIBER. *JURNAL ILMIAH ILMU KOMPUTER*, *8*(2). https://doi.org/10.35329/jiik.v8i2.232

Hadirnya Cybercrime Menuai Dampak Negatif bagi Masyarakat Indonesia Halaman 1 - Kompasiana.com. (n.d.). Retrieved April 2, 2024, from https://www.kompasiana.com/rafi77742/607430338ede482fda3bd633/hadirnya-cybercrime-menuai-dampak-negatif-bagi-masyarakat-indonesia

Haryanto, A., & Sutra, S. M. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) Tahun 2017-2020. *Global Political Studies Journal*, *7*(1). https://doi.org/10.34010/gpsjournal.v7i1.8141

Hidayatullah, C. (2023). Jenis dan Dampak Cyber Crime. *Prosiding SAINTEK: Sains Dan Teknologi*, *2*(1).

Jubaidi, M., & Fadilla, N. (2020). PENGARUH FENOMENA CYBERBULLYING SEBAGAI CYBER-CRIME DI INSTAGRAM DAN DAMPAK NEGATIFNYA. *Shaut Al-Maktabah : Jurnal Perpustakaan, Arsip Dan Dokumentasi*, *12*(2). https://doi.org/10.37108/shaut.v12i2.327

Kenalan dengan Tugas Pekerjaan Cyber Security, Yuk! - Universitas Bakrie. (n.d.). Retrieved April 2, 2024, from https://bakrie.ac.id/articles/384-kenalan-dengan-tugas-pekerjaan-cyber-security-yuk.html

Kurpayanidi Konstantin Ivanovich. (2023). INSTITUTIONAL ASPECTS AND RISKS IN THE DIGITAL ECONOMY: WAYS TO REDUCE UNCERTAINTY FOR ECONOMIC AGENTS. *QO‘QON UNIVERSITETI XABARNOMASI*, *9*. https://doi.org/10.54613/ku.v9i9.827

Machlul, M. (2024). Peningkatan Kualitas SDM Melalui Pelatihan Cyber Security Pada Anggota Polisi Daerah Jawa Timur. *Parta: Jurnal Pengabdian Kepada Masyarakat*, *4*(2). https://doi.org/10.38043/parta.v4i2.4655

Muhyidin, H. A. F., & Venica, L. (2023). Pengembangan Chatbot untuk Meningkatkan Pengetahuan dan Kesadaran Keamanan Siber Menggunakan Long Short-Term Memory. *Jurnal Informatika Dan Rekayasa Perangkat Lunak*, *5*(2). https://doi.org/10.36499/jinrpl.v5i2.8818

Pambudi, R., Budiman, A., Rahayu, A. W., Sukanto, A. N. R., & Hendrayani, Y. (2023). Dampak Etika Siber Jejaring Sosial Pada Pembentukan Karakter Pada Generasi Z. *JURNAL SYNTAX IMPERATIF : Jurnal Ilmu Sosial Dan Pendidikan*, *4*(3). https://doi.org/10.36418/syntax-imperatif.v4i3.262

Perbedaan Bentuk Kejahatan Yang Dikategorikan Sebagai Cyber Crime Dan Cyber Warfare. (2014). *JURNAL SISTEM INFORMASI UNIVERSITAS SURYADARMA*, *10*(1). https://doi.org/10.35968/jsi.v10i1.1002

Prinsip Etika Profesi Dalam Keamanan Cybersecurity - Linuxhackingid. (n.d.). Retrieved April 30, 2024, from https://linuxhacking.or.id/prinsip-etika-profesi-dalam-keamanan-cybersecurity/

Raharjo, S., Suradiradja, K. H., & Ramdani, D. (2024). Peningkatan Kesadaran Keamanan

P-ISSN: 1411-3635
E-ISSN: 2962-5645

Siber di Mahad IT Anamta Syameela. *Jurnal Pengabdian Masyarakat Madani (JPMM)*, *4*(1). https://doi.org/10.51805/jpmm.v4i1.157

Sussolaikah, K., Laksono, R. D., & Andria, A. (2023). Pelatihan Media Edukasi Kesadaran Keamanan Siber di SDN 01 Pandean Kota Madiun. *ABDIMAS IPTEK*, *3*(2). https://doi.org/10.53513/abdi.v3i2.8749

Tanhela Zein Vitadiar, dkk. (2021). *BUKU AJAR ETIKA HUKUM CYBER* . CV. AE MEDIA GRAFIKA.

Top 10 Cybersecurity Predictions and Statistics For 2024. (n.d.). Retrieved April 30, 2024, from https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/

Utari Dwi Nelvenia. (n.d.). *Bijak Bermedia Sosial*. Retrieved April 2, 2024, from https://djpb.kemenkeu.go.id/kppn/sijunjung/id/data-publikasi/artikel/3099-bijak-bermedia-sosial.html

Wahib, P., Tunggal Narotama, A., Muhamad Rijki, N., Sahrudin, Permana, F., Sagara, D., Ibrahim Azkhal, D., Anwar, M., & Rifqi Juniawan, M. (2022). Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Ajp-Abdi Jurnal Publikasi*, *1*(2).