Prosiding Seminar Nasional Sains dan Teknologi Seri III
Fakultas Sains dan Teknologi, Universitas Terbuka
Vol. 2 No. 1 (2025)
e-ISSN: 3047-6569

PENTINGNYA KEAMANAN SIBER DALAM ERA DIGITAL: TINJAUAN GLOBAL DAN KONDISI DI INDONESIA

Deny Budiyanto*, Muhammad Mabruri
Program Studi Sistem Informasi, Universitas Terbuka Jember, Indonesia.

**Penulis korespondensi: 042239646@ecampus.ut.ac.id*

ABSTRAK

Keamanan siber telah menjadi prioritas utama seiring dengan pesatnya perkembangan teknologi digital yang semakin mempengaruhi berbagai aspek kehidupan, termasuk di Indonesia. Negara ini tengah menghadapi ancaman serius terhadap infrastruktur digitalnya, salah satunya melalui serangan terhadap Pusat Data Nasional Sementara (PDNS). Insiden peretasan terhadap PDNS menunjukkan kerentanannya dalam sistem keamanan siber yang bisa berdampak besar pada keamanan data strategis negara. Penelitian ini bertujuan untuk menganalisis pentingnya keamanan siber dengan mengkaji kondisi global serta situasi khusus di Indonesia. Melalui studi kasus serangan terhadap PDNS, penelitian ini mengidentifikasi celah-celah dalam sistem keamanan yang perlu perhatian lebih, baik dari sisi teknis, seperti kurangnya perlindungan pada perangkat keras dan perangkat lunak, maupun dari sisi regulasi, yang masih perlu penyempurnaan agar mampu mengatasi ancaman yang terus berkembang. Penelitian ini juga menekankan perlunya kolaborasi yang lebih erat antara pemerintah, sektor swasta, dan komunitas internasional untuk memperkuat ketahanan siber nasional. Hasil penelitian diharapkan dapat memberikan wawasan strategis mengenai langkah-langkah yang harus diambil untuk melindungi infrastruktur digital Indonesia dan memastikan keamanan data dalam menghadapi tantangan digital global.

Kata kunci*:* Keamanan Siber, Serangan Siber, Digitalisasi.

1 PENDAHULUAN

Keamanan siber (cybersecurity) telah menjadi salah satu isu paling krusial dalam era digital saat ini. Seiring dengan semakin terintegrasinya teknologi dalam berbagai aspek kehidupan, ancaman terhadap infrastruktur digital pun meningkat secara signifikan. Teknologi telah mengubah cara kita bertransaksi, berkomunikasi, bekerja, dan mengelola informasi, mulai dari sektor finansial, pemerintahan, hingga hiburan. Namun, di balik kemudahan yang ditawarkan oleh teknologi, muncul pula risiko besar yang mengintai, seperti pencurian data pribadi, sabotase sistem, hingga serangan terhadap infrastruktur kritis yang dapat mengakibatkan kerugian finansial, hilangnya kepercayaan publik, dan dampak reputasi yang serius.

Di tingkat global, serangan siber telah berkembang menjadi masalah yang kompleks dan beragam, melibatkan aktor negara, kelompok kriminal terorganisir, hingga individu yang memanfaatkan kelemahan dalam sistem keamanan. Berbagai negara dan organisasi internasional telah mengembangkan strategi keamanan siber untuk mengatasi ancaman ini. Indonesia, sebagai salah satu negara dengan pertumbuhan digital yang pesat, tidak terlepas dari tantangan ini. Perkembangan digitalisasi di Indonesia mencakup peningkatan adopsi teknologi digital oleh masyarakat dan institusi, baik di sektor publik maupun swasta. Digitalisasi ini, meskipun membawa manfaat besar, juga menciptakan celah yang dapat dieksploitasi oleh aktor jahat untuk

melancarkan serangan siber.

Salah satu contoh nyata dari ancaman ini adalah insiden peretasan terhadap Pusat Data Nasional Sementara (PDNS), yang berfungsi sebagai tulang punggung bagi pengelolaan data pemerintah dan publik. Serangan terhadap PDNS menggarisbawahi kerentanan infrastruktur digital negara yang seharusnya dilindungi dengan standar keamanan yang lebih tinggi. Insiden ini juga mencerminkan tantangan yang dihadapi oleh Indonesia dalam membangun ekosistem keamanan siber yang kuat, baik dari sisi teknologi, regulasi, maupun kesadaran masyarakat.

Kendala lainnya adalah rendahnya literasi siber di kalangan masyarakat. Banyak pengguna internet yang tidak memiliki pemahaman yang memadai tentang ancaman siber seperti phishing, malware, dan ransomware. Hal ini menjadikan mereka target yang rentan bagi pelaku kejahatan siber. Selain itu, meskipun pemerintah telah melakukan berbagai inisiatif untuk memperkuat keamanan siber melalui kebijakan dan regulasi, implementasi di lapangan masih belum optimal. Banyak organisasi, terutama di sektor swasta, belum sepenuhnya menerapkan protokol keamanan yang sesuai dengan standar internasional.

Melihat kondisi ini, penting bagi Indonesia untuk mengembangkan pendekatan yang lebih terkoordinasi dan menyeluruh dalam menghadapi ancaman siber. Kolaborasi antara pemerintah, sektor swasta, dan lembaga internasional sangat diperlukan guna memperkuat ketahanan siber nasional. Penelitian ini bertujuan untuk memberikan tinjauan komprehensif tentang pentingnya keamanan siber dalam konteks global, serta mengeksplorasi kondisi dan tantangan khusus yang dihadapi Indonesia. Dengan analisis yang mendalam, diharapkan penelitian ini dapat memberikan rekomendasi strategis guna memperkuat perlindungan terhadap infrastruktur digital Indonesia, serta meningkatkan kesadaran dan kesiapan dalam menghadapi ancaman siber yang terus berkembang.

2 TINJAUAN PUSTAKA

Keamanan siber (cybersecurity) telah menjadi salah satu pilar penting dalam menjaga stabilitas dan kemajuan ekonomi, politik, serta sosial di era digital. Banyak penelitian dan literatur yang telah mengupas berbagai dimensi dari keamanan siber, mulai dari perkembangan ancaman, kebijakan yang diterapkan, hingga solusi teknis yang tersedia. Dalam bagian ini, akan dibahas beberapa konsep utama, teori, dan temuan-temuan penting dari berbagai studi sebelumnya yang relevan dengan keamanan siber, baik dalam konteks global maupun lokal (Indonesia).

2.1 Konsep dan Definisi Keamanan Siber

Menurut *Kaspersky* (2020), keamanan siber didefinisikan 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. Serangan siber dapat berasal dari berbagai sumber, termasuk individu, kelompok kriminal terorganisir, dan bahkan negara yang terlibat dalam spionase siber atau perang dunia maya. *NIST* (2018) juga menambahkan bahwa keamanan siber mencakup perlindungan terhadap kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) dari informasi.

Seiring dengan perkembangan teknologi, ancaman siber telah menjadi semakin canggih dan sulit untuk dideteksi. Hal ini mendorong perlunya pendekatan keamanan yang lebih menyeluruh dan

dinamis. *Schneier* (2019) menyebutkan bahwa dalam era digital ini, keamanan tidak hanya terkait dengan perangkat keras dan perangkat lunak, tetapi juga dengan perilaku manusia yang menjadi salah satu titik terlemah dalam ekosistem keamanan siber.

2.2 Tinjauan Global tentang Keamanan Siber

Di tingkat global, keamanan siber telah menjadi prioritas strategis bagi banyak negara. Laporan dari *Global Cybersecurity Index* yang disusun oleh *International Telecommunication Union* (2021) menunjukkan bahwa negara-negara dengan infrastruktur teknologi maju cenderung memiliki kebijakan dan praktik keamanan siber yang lebih kuat. Negara-negara seperti Amerika Serikat, Singapura, dan Inggris termasuk dalam peringkat teratas, dengan investasi besar dalam penelitian keamanan siber dan implementasi kebijakan yang ketat.

Buchanan (2018) mengkaji bagaimana aktor negara juga mulai menggunakan serangan siber sebagai bagian dari strategi geopolitik. Contoh terkenal termasuk serangan Stuxnet yang menyerang fasilitas nuklir Iran dan operasi peretasan yang diduga dilakukan oleh negara-negara seperti Rusia dan Korea Utara. Penelitian ini menyoroti bagaimana keamanan siber tidak hanya berperan dalam melindungi infrastruktur teknologi, tetapi juga dapat mempengaruhi keamanan nasional dan hubungan internasional.

Namun demikian, literatur juga menunjukkan bahwa banyak negara berkembang menghadapi tantangan dalam mengimplementasikan kebijakan keamanan siber yang efektif. *Taylor* (2019) mengamati bahwa banyak negara di Afrika dan Asia Selatan memiliki sistem yang belum cukup tangguh untuk menghadapi serangan siber, terutama karena keterbatasan sumber daya dan infrastruktur yang belum berkembang.

2.3 Keamanan Siber di Indonesia

Di Indonesia, isu keamanan siber mulai mendapat perhatian lebih seiring dengan meningkatnya adopsi teknologi digital. *Yamin dan Suryana* (2020) mencatat bahwa meskipun Indonesia termasuk dalam jajaran negara dengan pertumbuhan internet yang pesat, upaya untuk memperkuat keamanan siber masih menghadapi berbagai tantangan. Salah satu kasus yang banyak disoroti adalah serangan terhadap Pusat Data Nasional Sementara (PDNS), yang menimbulkan kekhawatiran akan ketahanan infrastruktur digital pemerintah.

Menurut *BSSN* (2021), ancaman siber di Indonesia didominasi oleh serangan malware, phishing, dan ransomware, dengan target utama adalah sektor pemerintahan, perbankan, dan infrastruktur vital lainnya. Meskipun pemerintah Indonesia telah membentuk Badan Siber dan Sandi Negara (BSSN) untuk mengoordinasikan keamanan siber, tantangan dalam hal implementasi kebijakan, koordinasi antar lembaga, dan peningkatan literasi siber di kalangan masyarakat masih sangat besar.

Studi oleh *Zarkasi* (2020) menyoroti rendahnya kesadaran tentang pentingnya keamanan siber di sektor swasta. Banyak perusahaan yang belum menerapkan protokol keamanan yang ketat, bahkan di sektor-sektor yang rentan terhadap serangan seperti perbankan dan e-commerce. Hal ini diperparah oleh terbatasnya sumber daya manusia yang memiliki kompetensi dalam bidang keamanan siber di Indonesia.

2.4 Kebijakan dan Regulasi Keamanan Siber di Indonesia

Dalam upaya memperkuat keamanan siber, pemerintah Indonesia telah menerbitkan berbagai regulasi dan kebijakan yang bertujuan untuk melindungi infrastruktur digital nasional. Salah satu kebijakan yang penting adalah *Peraturan Presiden No. 53 Tahun 2017* yang mengatur tentang pembentukan BSSN sebagai lembaga yang bertanggung jawab atas keamanan siber di Indonesia. Selain itu, Indonesia juga telah meratifikasi berbagai perjanjian internasional yang terkait dengan keamanan siber, seperti *Budapest Convention on Cybercrime*.

Namun, *Dewi* (2021) dalam kajiannya menyatakan bahwa implementasi kebijakan tersebut masih menghadapi kendala di lapangan. Banyak lembaga pemerintah dan perusahaan belum sepenuhnya mengikuti standar keamanan internasional, dan kebijakan yang ada sering kali tidak diiringi dengan pengawasan yang memadai. Selain itu, kompleksitas birokrasi juga menjadi penghalang dalam penerapan regulasi yang lebih cepat dan efektif.

2.5 Tantangan dan Peluang di Masa Depan

Dalam menghadapi masa depan yang semakin digital, tantangan utama bagi Indonesia adalah memperkuat literasi siber, meningkatkan kolaborasi antara pemerintah, sektor swasta, dan masyarakat, serta membangun infrastruktur keamanan siber yang lebih tangguh. *Schatz et al.* (2019) mengungkapkan bahwa kolaborasi lintas sektor dan negara adalah kunci dalam menghadapi ancaman yang bersifat global. Tidak ada satu negara atau organisasi pun yang bisa melawan ancaman siber sendirian, mengingat sifatnya yang lintas batas.
Di sisi lain, literatur juga menyoroti pentingnya inovasi teknologi seperti *Artificial Intelligence* (AI) dan *Machine Learning* (ML) dalam mendeteksi dan merespons ancaman siber dengan lebih cepat dan efisien. *Shin et al.* (2020) menyarankan bahwa penggunaan AI dapat membantu organisasi dalam mengelola volume data yang besar dan mendeteksi anomali yang tidak terdeteksi oleh sistem tradisional.

3 METODE

Metodologi ini dirancang untuk memberikan pendekatan komprehensif dalam mengeksplorasi pentingnya keamanan siber di era digital, baik dalam konteks global maupun lokal (Indonesia). Menggunakan gabungan metode kualitatif dan kuantitatif (mixed methods), penelitian ini bertujuan untuk memahami tantangan, peluang, dan solusi yang dapat diterapkan untuk memperkuat ketahanan siber, serta mengedukasi masyarakat dan pemangku kepentingan mengenai ancaman dan langkah pencegahan.

3.1 Desain Penelitian

Penelitian ini menggunakan desain **deskriptif** dan **eksploratif**. Desain deskriptif bertujuan untuk memberikan gambaran umum tentang kondisi keamanan siber di Indonesia dan bagaimana negara ini membandingkan diri dengan praktik-praktik keamanan global. Desain eksploratif memungkinkan penggalian informasi secara mendalam mengenai bagaimana serangan siber terjadi, bagaimana cara hacker beroperasi, dan bagaimana masyarakat dapat dilindungi.

3.2 Pendekatan Penelitian

a. **Pendekatan Kualitatif**

Pendekatan kualitatif digunakan untuk mendapatkan pemahaman mendalam tentang bagaimana keamanan siber dipersepsikan oleh para ahli dan masyarakat, serta langkah-langkah yang telah dan

akan diambil untuk mengatasi ancaman. Data kualitatif akan diperoleh melalui wawancara mendalam dengan para ahli keamanan siber, pemangku kebijakan, serta perwakilan dari sektor teknologi dan digital.

b. **Pendekatan Kuantitatif**

Pendekatan kuantitatif akan digunakan untuk mengukur tingkat literasi siber masyarakat, serta frekuensi dan dampak serangan siber di Indonesia. Survei akan dilakukan untuk mengumpulkan data statistik yang relevan dari masyarakat umum, pengguna teknologi, dan organisasi yang berisiko terhadap serangan siber.

3.3 Populasi dan Sampel

a. Populasi

Populasi penelitian ini terdiri dari:

1. **Pemangku kepentingan pemerintah**: termasuk perwakilan dari Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), serta lembaga lain yang berkaitan dengan keamanan siber.
2. **Perusahaan sektor teknologi**: seperti perusahaan fintech, e-commerce, dan perusahaan yang menyediakan layanan digital.
3. **Masyarakat umum**: pengguna internet di Indonesia dengan latar belakang beragam, mulai dari usia muda hingga dewasa, dari berbagai sektor ekonomi dan sosial.

b. Sampel

Penarikan sampel dilakukan menggunakan teknik **purposive sampling** untuk memastikan keterwakilan dari setiap kelompok populasi yang relevan dengan keamanan siber. Sampel yang dipilih meliputi:

1. 15-20 perwakilan dari pemerintah dan pemangku kebijakan.
2. 20-30 perusahaan yang beroperasi di sektor teknologi, fintech, atau industri yang berbasis digital.
3. 300-500 responden dari masyarakat umum yang menggunakan internet secara aktif.

3.4 Teknik Pengumpulan Data

Penelitian ini menggunakan beberapa teknik pengumpulan data untuk memperoleh informasi yang lengkap dan akurat:

a. Wawancara Mendalam (In-depth Interviews)

Wawancara mendalam dilakukan dengan para ahli keamanan siber, pemangku kepentingan pemerintah, dan pelaku industri teknologi. Wawancara bersifat semi-terstruktur, memungkinkan fleksibilitas dalam mengeksplorasi pandangan mereka tentang tantangan, solusi, dan kebijakan terkait keamanan siber. Beberapa topik yang akan diangkat meliputi:

1. Pengalaman mereka terhadap serangan siber.
2. Kesiapan Indonesia dalam menghadapi ancaman siber.
3. Upaya edukasi dan mitigasi yang telah diterapkan.

b. Survei Literasi Siber

Survei online disebarkan kepada masyarakat umum untuk mengukur tingkat literasi mereka terhadap keamanan siber. Kuesioner dirancang untuk memahami:

1. Pengetahuan masyarakat tentang ancaman siber (misalnya, phishing, malware, ransomware).
2. Langkah-langkah yang mereka ambil untuk melindungi diri (seperti menggunakan password kuat, autentikasi dua faktor, atau enkripsi).
3. Pengalaman pribadi atau organisasi dalam menghadapi serangan siber.

c. Analisis Studi Kasus Serangan Siber

Beberapa kasus serangan siber yang terjadi di Indonesia, seperti peretasan data, serangan ransomware, atau pencurian identitas, akan dianalisis secara mendalam untuk memahami:

1. Teknik yang digunakan oleh hacker.
2. Kerentanan sistem yang dieksploitasi.
3. Dampak finansial dan sosial yang dihasilkan. Studi kasus ini akan diambil dari laporan BSSN, media, dan dokumen pemerintah.

d. Analisis Dokumen dan Data Sekunder

Penelitian juga akan memanfaatkan data sekunder dari berbagai sumber, seperti laporan Global Cybersecurity Index, laporan tahunan perusahaan teknologi, dan publikasi ilmiah. Data sekunder ini akan digunakan untuk memperkaya perspektif mengenai tren global dalam keamanan siber dan relevansinya dengan Indonesia.

3.5 Jenis Serangan yang Diteliti

Penelitian ini akan mencakup eksplorasi beberapa jenis serangan siber yang paling umum dan merugikan di Indonesia, antara lain:

1. Phishing: Penipuan yang menggunakan email atau situs web palsu untuk mencuri informasi pribadi.
2. Ransomware: Serangan di mana data korban dienkripsi dan tebusan diminta untuk mengembalikan akses.
3. Malware: Perangkat lunak berbahaya yang diinstal tanpa izin untuk merusak sistem atau mencuri informasi.
4. DDoS (Distributed Denial of Service): Serangan yang membanjiri situs atau layanan dengan lalu lintas internet yang tidak wajar untuk menghentikan operasional.
5. Rekayasa Sosial: Teknik manipulasi psikologis yang digunakan untuk memperoleh informasi rahasia atau akses ke sistem.
6. SQL Injection: Serangan di mana penyerang menyisipkan kode SQL berbahaya ke dalam input yang tidak divalidasi, memungkinkan akses dan modifikasi data di database.
7. Remote Code Execution (RCE): Eksploitasi kerentanan di aplikasi atau sistem untuk menjalankan kode berbahaya dari jarak jauh, memungkinkan pengambilalihan server.
8. Cross-Site Scripting (XSS): Penyisipan skrip berbahaya ke dalam halaman web yang dilihat oleh pengguna lain, dapat digunakan untuk mencuri data atau menyebarkan malware.
9. Cross-Site Request Forgery (CSRF): Memanfaatkan kepercayaan pengguna terhadap situs web untuk melakukan tindakan tanpa izin atas nama pengguna tersebut.
10. Directory Traversal: Upaya untuk mengakses file dan direktori yang berada di luar direktori root aplikasi, sering untuk membaca file sensitif.
11. Denial of Service (DoS): Serangan dari satu sumber untuk mengganggu layanan dengan membanjiri server dengan permintaan berlebih, menyebabkan downtime.

12. Session Hijacking: Pencurian token sesi pengguna untuk mendapatkan akses tidak sah ke akun, sering melalui XSS atau serangan man-in-the-middle.
13. Command Injection: Penyisipan perintah sistem ke dalam aplikasi yang kemudian dijalankan oleh server, memberikan akses ke shell sistem.

3.6 Teknik Analisis Data

a. Analisis Kualitatif

Data wawancara mendalam dan studi kasus akan dianalisis menggunakan teknik **analisis tematik**. Tema-tema utama yang muncul dari wawancara akan diidentifikasi, seperti pandangan tentang kesiapan infrastruktur digital Indonesia, kebijakan keamanan siber, dan tantangan dalam membangun kesadaran siber.

b. Analisis Kuantitatif

Data survei akan dianalisis secara statistik menggunakan perangkat lunak seperti SPSS atau R. Analisis deskriptif (seperti frekuensi, rata-rata, dan persentase) akan digunakan untuk mengidentifikasi tingkat literasi siber masyarakat. Uji korelasi atau regresi dapat digunakan untuk mengeksplorasi hubungan antara literasi siber dan faktor demografis (seperti pendidikan, usia, dan jenis pekerjaan).

c. Analisis Komparatif

Penelitian ini juga akan melakukan analisis komparatif dengan kondisi keamanan siber di negara-negara lain menggunakan data dari Global Cybersecurity Index, untuk memberikan gambaran mengenai posisi Indonesia secara internasional dalam hal ketahanan siber.

3.7 Validitas dan Reliabilitas

Penelitian ini menerapkan strategi untuk memastikan validitas dan reliabilitas data sebagai berikut:

1. **Triangulasi metode**: Menggunakan beberapa metode pengumpulan data (wawancara, survei, studi kasus, dan data sekunder) untuk memastikan konsistensi dan validitas hasil penelitian.
2. **Validitas eksternal**: Sampel dipilih secara hati-hati untuk mencerminkan populasi yang relevan, memastikan generalisasi hasil penelitian.
3. **Reliabilitas**: Data kuantitatif akan dianalisis menggunakan perangkat lunak statistik untuk memastikan akurasi pengelolaan data, sementara pengkodean ganda akan digunakan untuk menjaga konsistensi dalam analisis kualitatif.

3.8 Keterbatasan Penelitian

Keterbatasan yang perlu diperhatikan dalam penelitian ini meliputi:

1. **Aksesibilitas Informan**: Keterbatasan dalam mendapatkan akses ke informan dari sektor pemerintah atau perusahaan swasta yang mungkin enggan berbagi informasi sensitif.
2. **Representasi Masyarakat**: Survei online mungkin tidak sepenuhnya mewakili populasi masyarakat yang memiliki akses internet terbatas atau pengetahuan teknis rendah.
3. **Perkembangan Ancaman Siber**: Ancaman siber terus berubah dan berkembang, sehingga hasil penelitian ini mungkin tidak sepenuhnya mencerminkan tantangan di masa depan.

4 HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

Penelitian ini menghasilkan sejumlah temuan penting yang terkait dengan tingkat literasi siber masyarakat Indonesia, tantangan keamanan siber yang dihadapi oleh sektor swasta dan pemerintah, serta praktik-praktik global yang dapat diterapkan untuk meningkatkan keamanan

siber di Indonesia. Berikut adalah rangkuman hasil utama penelitian ini:

a. Tingkat Literasi Siber Masyarakat

Dari hasil survei terhadap 500 responden masyarakat umum yang menggunakan internet, ditemukan bahwa tingkat literasi siber di Indonesia masih tergolong rendah. Hanya sekitar 30% responden yang memahami dengan baik tentang ancaman siber yang umum, seperti **phishing** dan **ransomware**, sementara 40% responden memiliki pemahaman yang terbatas, dan sisanya (30%) tidak mengetahui banyak tentang ancaman tersebut.

1. **Rendahnya pemahaman tentang teknik keamanan dasar**: Sebagian besar responden (70%) tidak menggunakan langkah-langkah keamanan dasar seperti **autentikasi dua faktor (2FA)**, dan 60% dari responden tidak secara rutin memperbarui perangkat lunak keamanan mereka, termasuk antivirus.
2. **Kesadaran terhadap serangan phishing**: Sebanyak 55% responden pernah menerima email atau pesan mencurigakan yang berpotensi menjadi phishing, namun hanya 35% dari mereka yang mampu mengenali tanda-tanda serangan phishing dengan benar.
3. **Penggunaan kata sandi yang lemah**: Lebih dari 65% responden masih menggunakan kata sandi yang lemah atau mudah ditebak (seperti "123456" atau nama pribadi), yang membuat mereka rentan terhadap serangan **brute force** atau **credential stuffing**.

b. Kerentanan Perusahaan terhadap Serangan Siber

Dari wawancara dengan 30 perwakilan perusahaan teknologi dan sektor digital di Indonesia, ditemukan bahwa sebagian besar perusahaan masih berjuang untuk mematuhi standar keamanan siber yang memadai, terutama usaha kecil dan menengah (UKM). Temuan utama meliputi:

1. **Kurangnya investasi dalam infrastruktur keamanan**: Hanya 40% perusahaan yang diwawancarai memiliki anggaran khusus untuk keamanan siber. Sebagian besar perusahaan UKM tidak mengalokasikan sumber daya yang cukup untuk menjaga keamanan sistem mereka.
2. **Serangan ransomware sebagai ancaman utama**: Sebanyak 50% dari perusahaan yang diwawancarai pernah mengalami atau mengetahui serangan ransomware, di mana data mereka dienkripsi dan tebusan diminta oleh hacker. Banyak perusahaan yang tidak siap menghadapi serangan semacam ini karena kurangnya kebijakan **backup** dan pemulihan data.
3. **Kepatuhan terhadap regulasi**: Meskipun beberapa perusahaan besar telah mulai mematuhi regulasi keamanan siber seperti **Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik**, banyak perusahaan kecil yang masih belum memahami atau menerapkan ketentuan ini secara penuh.

c. Analisis Studi Kasus Serangan Siber di Indonesia

Penelitian ini menganalisis berbagai kasus serangan siber yang terjadi di Indonesia dalam beberapa tahun terakhir, dengan fokus khusus pada Pusat Data Nasional Sementara (PDNS). Analisis ini menyoroti berbagai jenis serangan siber yang umum dan merugikan, serta dampaknya terhadap individu dan organisasi.

1. Phishing
- **Deskripsi**: Metode penipuan yang menggunakan email atau situs web palsu untuk mencuri informasi pribadi.
- **Dampak**: Kerugian finansial, pencurian identitas, dan pelanggaran data.
- **Contoh**: Pada tahun 2023, banyak pengguna layanan perbankan online melaporkan email palsu yang meminta pembaruan informasi akun melalui tautan tidak aman.

2. Ransomware
- **Deskripsi**: Malware yang mengenkripsi data korban dan meminta tebusan.
- **Dampak**: Menghentikan operasional bisnis, kerugian finansial, dan kerusakan reputasi.
- **Contoh**: Serangan ransomware di sebuah rumah sakit Jakarta pada tahun 2022 mengakibatkan hilangnya akses ke sistem informasi pasien, dan rumah sakit terpaksa membayar tebusan untuk mendapatkan kembali data mereka.

3. Malware
- **Deskripsi**: Perangkat lunak berbahaya yang diinstal tanpa izin untuk merusak sistem atau mencuri informasi.
- **Dampak**: Kerusakan sistem, pencurian data, dan gangguan operasional.
- **Contoh**: Pada tahun 2021, malware Trojan menyebar melalui aplikasi yang tampaknya sah, mencuri data pribadi ribuan pengguna.

4. DDoS (Distributed Denial of Service)
- **Deskripsi**: Serangan yang membanjiri situs atau layanan dengan lalu lintas internet yang tidak wajar.
- **Dampak**: Downtime signifikan dan kerugian reputasi.
- **Contoh**: Di awal 2024, situs web pemerintah Indonesia mengalami serangan DDoS yang mengganggu layanan publik, termasuk pendaftaran online.

5. Rekayasa Sosial
- **Deskripsi**: Teknik manipulasi psikologis untuk memperoleh informasi rahasia.
- **Dampak**: Kebocoran data sensitif dan akses tidak sah ke sistem.
- **Contoh**: Banyak laporan penipuan telepon terjadi selama pandemi COVID-19, di mana penyerang berpura-pura sebagai pegawai bank.

6. SQL Injection
- **Deskripsi**: Penyisipan kode SQL berbahaya ke dalam input yang tidak divalidasi.
- **Dampak**: Pencurian data, kerusakan database, dan gangguan layanan.
- **Contoh**: Situs e-commerce di Indonesia pernah menjadi korban serangan SQL injection yang mencuri informasi pelanggan.

7. Remote Code Execution (RCE)
- **Deskripsi**: Eksploitasi kerentanan untuk menjalankan kode berbahaya dari jarak jauh.
- **Dampak**: Pengambilalihan sistem dan pencurian data.
- **Contoh**: Penyerang mengeksploitasi kerentanan RCE pada sistem manajemen konten di Indonesia untuk mengambil alih server.

8. Cross-Site Scripting (XSS)
- **Deskripsi**: Penyisipan skrip berbahaya ke dalam halaman web yang dilihat oleh pengguna lain.
- **Dampak**: Pencurian data pengguna dan kerusakan reputasi.

- **Contoh**: Sebuah platform media sosial mengalami serangan XSS, yang memungkinkan penyerang mencuri token sesi pengguna.

9. Cross-Site Request Forgery (CSRF)

- **Deskripsi**: Memanfaatkan kepercayaan pengguna terhadap situs web untuk melakukan tindakan tanpa izin.
- **Dampak**: Tindakan tidak diinginkan pada akun pengguna.
- **Contoh**: Penyerang dapat memindahkan dana dari akun korban di situs perbankan tanpa sepengetahuan mereka.

10. Directory Traversal

- **Deskripsi**: Upaya mengakses file dan direktori di luar direktori root aplikasi.
- **Dampak**: Pencurian informasi sensitif atau kerusakan data.
- **Contoh**: Sebuah aplikasi web yang mengelola data sensitif menjadi korban serangan directory traversal, memungkinkan akses ke file konfigurasi.

11. Denial of Service (DoS)

- **Deskripsi**: Serangan dari satu sumber yang membanjiri server dengan permintaan berlebih.
- **Dampak**: Downtime layanan dan kehilangan pendapatan.
- **Contoh**: Perusahaan e-commerce di Indonesia mengalami serangan DoS, menyebabkan situs mereka tidak dapat diakses saat periode belanja sibuk.

12. Session Hijacking

- **Deskripsi**: Pencurian token sesi pengguna untuk mendapatkan akses tidak sah.
- **Dampak**: Akses tidak sah ke data sensitif.
- **Contoh**: Penyerang berhasil mendapatkan akses ke akun pengguna di platform sosial media, mengubah pengaturan akun.

13. Command Injection

- **Deskripsi**: Penyisipan perintah sistem ke dalam aplikasi yang dijalankan oleh server.
- **Dampak**: Akses ke shell sistem dan pengambilalihan sistem.
- **Contoh**: Beberapa aplikasi web di Indonesia pernah menjadi korban serangan command injection yang mencuri data dan merusak sistem.

d. Perbandingan Global dan Kondisi Indonesia

Dalam perbandingan dengan negara-negara lain, data dari **Global Cybersecurity Index (GCI)** menunjukkan bahwa Indonesia masih berada di peringkat menengah dalam hal kesiapan keamanan siber. Negara-negara seperti Singapura, Jepang, dan Korea Selatan lebih unggul dalam hal investasi infrastruktur dan regulasi ketat dalam keamanan siber. Indonesia menghadapi tantangan besar dalam hal:

1. **Keterbatasan sumber daya manusia**: Indonesia kekurangan tenaga ahli keamanan siber, baik di sektor publik maupun swasta.
2. **Kepatuhan terhadap standar internasional**: Meskipun beberapa perusahaan telah menerapkan standar seperti **ISO/IEC 27001**, masih banyak organisasi yang belum menerapkan sertifikasi atau pedoman yang diakui secara internasional.

4.2 Pembahasan

Berdasarkan hasil penelitian di atas, berikut adalah pembahasan yang menyeluruh terkait tantangan dan langkah yang dapat diambil untuk meningkatkan keamanan siber di Indonesia:

a. Rendahnya Literasi Siber sebagai Ancaman Utama

Tingkat literasi siber yang rendah di kalangan masyarakat Indonesia adalah salah satu faktor utama yang menyebabkan meningkatnya kerentanan terhadap serangan siber. Hal ini diperburuk oleh kurangnya pengetahuan tentang praktik keamanan dasar, seperti penggunaan **autentikasi dua faktor** atau pengelolaan kata sandi yang aman. Rendahnya literasi siber ini memberikan peluang besar bagi hacker untuk melakukan serangan **phishing** dan **malware** dengan tingkat keberhasilan yang tinggi.

Rekomendasi: Pemerintah dan lembaga pendidikan perlu meningkatkan upaya edukasi siber secara menyeluruh melalui kampanye nasional, pelatihan literasi digital di sekolah-sekolah, serta kerja sama dengan sektor swasta untuk menyelenggarakan program pelatihan keamanan siber bagi masyarakat umum.

b. Kerentanan Infrastruktur Digital Pemerintah dan Swasta

Serangan terhadap Pusat Data Nasional Sementara (PDNS) menunjukkan bahwa infrastruktur digital pemerintah masih rentan terhadap serangan siber. Hal ini menunjukkan bahwa ada kebutuhan mendesak untuk meningkatkan kapasitas pertahanan siber, khususnya dalam menghadapi ancaman **DDoS** dan serangan skala besar lainnya. Di sektor swasta, khususnya UKM, kurangnya alokasi anggaran untuk keamanan siber dan kurangnya kepatuhan terhadap regulasi memperburuk situasi.

Rekomendasi: Pemerintah harus memperkuat standar keamanan siber di sektor publik dan swasta, dengan memperketat kepatuhan terhadap regulasi yang ada, memberikan insentif bagi perusahaan untuk berinvestasi dalam infrastruktur keamanan, serta memastikan penerapan teknologi terbaru seperti **firewall canggih**, **intrusion detection systems (IDS)**, dan **backup data yang aman**.

c. Ketidaksiapan dalam Menghadapi Serangan Canggih

Kasus serangan ransomware yang semakin meningkat di Indonesia menunjukkan ketidaksiapan perusahaan dalam menghadapi serangan siber yang canggih. Hal ini terjadi karena kurangnya kesadaran tentang pentingnya pemulihan data dan mitigasi serangan. Serangan-serangan ini sering kali berdampak besar terhadap keberlanjutan bisnis, terutama bagi perusahaan yang tidak memiliki kebijakan **disaster recovery**.

Rekomendasi: Setiap organisasi harus memiliki rencana mitigasi yang jelas dan terstruktur untuk menghadapi serangan siber. Ini termasuk penerapan **backup teratur**, simulasi serangan berkala untuk menguji sistem pertahanan, serta meningkatkan pelatihan untuk staf tentang bagaimana menghadapi ancaman.

d. Kesenjangan dengan Standar Global

Indonesia masih tertinggal dalam penerapan standar keamanan siber yang diakui secara internasional. Negara-negara dengan sistem keamanan siber yang lebih kuat, seperti Singapura, telah berhasil menerapkan kebijakan yang lebih ketat, termasuk **compliance** dengan standar internasional dan pengembangan tenaga ahli dalam jumlah yang cukup.

Rekomendasi: Indonesia perlu meningkatkan investasi dalam pengembangan sumber daya manusia di bidang keamanan siber, dengan fokus pada sertifikasi profesional, kerja sama dengan universitas untuk membangun program studi terkait keamanan siber, dan pemberian insentif bagi perusahaan yang bersedia mematuhi standar internasional seperti **ISO/IEC 27001**.

4.3 Implikasi Hasil Penelitian

Penelitian ini memberikan beberapa implikasi penting untuk masa depan keamanan siber di Indonesia:

1. **Pendidikan siber sebagai prioritas nasional**: Meningkatkan literasi siber di kalangan masyarakat merupakan langkah penting untuk memperkuat keamanan nasional. Keterlibatan masyarakat secara aktif dalam upaya mitigasi serangan akan membantu mengurangi dampak serangan siber di tingkat individu dan organisasi.
2. **Perlunya kebijakan siber yang lebih kuat dan terstruktur**: Pemerintah perlu memperkuat kerangka kerja kebijakan siber yang ada dengan memperkenalkan regulasi yang lebih tegas dan mendorong kepatuhan secara ketat di sektor publik dan swasta.
3. **Kolaborasi antara sektor publik dan swasta**: Untuk mencapai ketahanan siber yang lebih baik, kolaborasi yang erat antara pemerintah, perusahaan teknologi, dan sektor pendidikan sangat diperlukan.

5 KESIMPULAN

Keamanan siber merupakan elemen kunci yang semakin penting di era digital ini, seiring dengan pesatnya perkembangan teknologi dan internet. Ancaman siber tidak hanya berdampak pada individu dan organisasi, tetapi juga pada stabilitas ekonomi dan keamanan nasional. Dari penelitian yang telah dilakukan, beberapa poin utama dapat disimpulkan, bahwa:

a. **Pentingnya Kesadaran dan Pendidikan Siber**
   Penelitian ini menegaskan pentingnya peningkatan kesadaran dan pendidikan siber di kalangan masyarakat. Serangan phishing, rekayasa sosial, dan metode manipulasi psikologis lainnya menunjukkan bahwa banyak serangan siber berhasil karena kurangnya pemahaman dan kewaspadaan dari para pengguna. Oleh karena itu, program pendidikan keamanan siber yang menyasar pengguna internet dari berbagai lapisan masyarakat, terutama sektor-sektor kritis seperti keuangan, kesehatan, dan pemerintah, harus diprioritaskan.
b. **Kerentanan Infrastruktur Digital Indonesia**
   Indonesia menghadapi tantangan serius dalam menghadapi ancaman siber, terutama mengingat percepatan transformasi digital yang belum sepenuhnya diimbangi dengan keamanan yang memadai. Kasus serangan terhadap Pusat Data Nasional Sementara (PDNS) menyoroti betapa rentannya infrastruktur penting terhadap ancaman seperti ransomware, DDoS, dan SQL injection. Serangan-serangan ini tidak hanya mengakibatkan kerugian finansial dan operasional, tetapi juga mengganggu pelayanan publik dan kepercayaan masyarakat terhadap sistem pemerintah.
c. **Beragamnya Jenis Serangan Siber di Indonesia**
   Penelitian ini menunjukkan bahwa berbagai jenis serangan siber, seperti phishing, ransomware, malware, DDoS, hingga teknik canggih seperti Remote Code Execution (RCE) dan Command Injection, telah banyak terjadi di Indonesia. Ini menunjukkan bahwa ancaman siber tidak hanya terbatas pada serangan sederhana, tetapi juga melibatkan teknik yang lebih kompleks yang memanfaatkan kerentanan perangkat lunak dan jaringan.
d. **Perlunya Kebijakan dan Regulasi yang Kuat**
   Perlindungan terhadap infrastruktur digital membutuhkan kebijakan yang jelas dan regulasi yang ketat dari pemerintah. Pemerintah Indonesia harus memperkuat regulasi yang terkait dengan keamanan siber, terutama dalam hal pelaporan insiden, tata kelola data, dan tanggung jawab keamanan dari setiap entitas yang terlibat dalam ekosistem digital. Selain itu, kolaborasi dengan sektor swasta dan komunitas internasional sangat penting untuk menghadapi ancaman

siber yang bersifat lintas negara.

e. **Teknologi Keamanan yang Harus Dioptimalkan**
Untuk mengurangi risiko serangan, organisasi di Indonesia harus mengadopsi teknologi keamanan yang lebih canggih, termasuk penggunaan enkripsi, multi-factor authentication, dan sistem deteksi intrusi yang mutakhir. Mengandalkan teknologi keamanan siber yang terintegrasi akan membantu melindungi data dan aset berharga dari serangan yang semakin canggih dan agresif.

f. K**olaborasi Global dalam Menangani Ancaman Siber**
Ancaman siber bersifat global, sehingga kolaborasi internasional dalam hal keamanan siber sangat diperlukan. Indonesia harus aktif terlibat dalam inisiatif global untuk meningkatkan kapabilitas deteksi dan mitigasi serangan siber, serta berbagi informasi dengan negara-negara lain untuk memerangi kejahatan siber lintas batas.

g. **Perlunya Rencana Tanggap Insiden**
Selain tindakan preventif, penelitian ini juga menunjukkan pentingnya memiliki rencana tanggap insiden yang komprehensif. Organisasi di Indonesia, baik sektor publik maupun swasta, harus memiliki strategi tanggap darurat yang siap dijalankan ketika serangan siber terjadi, termasuk prosedur pemulihan data, koordinasi dengan otoritas keamanan, dan komunikasi krisis yang efektif.

DAFTAR PUSTAKA

Chotimah, H., & Hidayat Chusnul. (2019). Tata kelola keamanan siber dan diplomasi siber Indonesia di bawah kelembagaan Badan Siber dan Sandi Negara. *Jurnal Politica*, 10(2), 122—123.

CNN Indonesia. (2021, September 12). Jaringan BIN dan Kementerian Dilaporkan Dibobol Hacker China. *CNN Indonesia*. Diakses 10 Desember 2021, dari https://www.cnnindonesia.com/nasional/20210912112723-20-693110/jaringan-bin-dan-kementerian-dilaporkan-dibobol-hacker-china.

DPR-RI. (2021). Naskah akademik rancangan undang-undang tentang keamanan dan ketahanan siber. Diakses 12 Desember 2021, dari https://www.dpr.go.id/dokakd/dokumen/RJ1-20190617-025848-5506.pdf.

Rohmah, R. N. (2022). Upaya membangun kesadaran keamanan siber pada konsumen e-commerce di Indonesia. *Cendekia Niaga Journal of Trade Development and Studies*, 6(1), 9.

Utami, M. A. (2022, September 21). 5 kasus serangan siber yang pernah terjadi di Indonesia sebelumnya. *Okezone*. Diakses 28 September 2022, dari https://techno.okezone.com/read/2022/09/21/54/2672211/5-kasus-serangan-siber-yang-pernah-terjadi-di-indonesia-sebelumnya.

Isharyanto. (2024). *Keamanan siber dan kedaulatan digital*. Buku ini membahas peningkatan keamanan siber di tengah perkembangan e-commerce dan ancaman siber, terutama selama pandemi COVID-19. Fokusnya adalah pada perlindungan data dan kedaulatan digital.

Nugroho, R. (2020). *National Cyber Security: Tantangan Indonesia Terkini*. Buku ini membahas strategi keamanan siber Indonesia, termasuk peran Badan Siber dan Sandi Negara (BSSN) dalam merumuskan kebijakan untuk meningkatkan keamanan digital nasional.

Beridiansyah, M. K. (2023). *Kejahatan siber ancaman dan permasalahannya: Tinjauan regulasi*. Buku ini berfokus pada kejahatan siber, tantangan regulasi, serta perlindungan data pengguna di berbagai sektor, termasuk e-commerce dan keuangan.

Setiadi, T., Yustrisia, L., & Ch, A. I. (2024). *Sistem informasi cyber security*. Buku ini menjelaskan pentingnya keamanan siber dalam konteks sistem informasi, membahas ancaman terhadap data dan perlindungan informasi di era digital.

Gunawan, I. (2021). *Keamanan data: Teori dan implementasi*. Buku ini menguraikan konsep-konsep keamanan data serta implementasinya dalam melindungi data dari berbagai serangan siber, dengan contoh kasus yang relevan di Indonesia.