Jurnal Sinabis
https://jsinabis.upnjatim.ac.id/index.php/jsinabis
ISSN (Online): XXXX-XXX
Volume 1 Nomor 4 Agustus 2025

Cybersecurity and Data Protection in the Government Sector Keamanan Siber dan Perlindungan Data Pada Sektor Pemerintahan

Fii Nuuraa Mirzanda
Universitas Pembangunan Nasional "Veteran" Jawa Timur, Indonesia
21042010194@student.upnjatim.ac.id

ABSTRAK

Keamanan Siber serta Perlindungan Data merupakan suatu hal yang krusial dalam sektor pemerintahan di mana data sensitif dan informasi publik menjadi target utama serangan siber. Penelitian ini bertujuan untuk menganalisis tantangan dan strategi yang diterapkan dalam melindungi sistem informasi pemerintah dari ancaman siber. Metologi yang digunakan mencakup kajian literatur dan analisis kebijakan yang ada serta kasus kasus mengenai insiden keamanan siber di lembaga pemerintahan. Hasil penelitian menunjukkan bahwa meskipun banyak upaya telah dilakukan, seperti peningkatan infrastruktur TI dan pelatihan pegawai, masih terdapat kelemahan dalam koordinasi antarinstansi dan pemahaman tentang risiko yang ada. Kesimpulan dari penelitian ini menekankan pentingnya pendekatan holistik dalam keamanan siber, yang meliputi kolaborasi lintas sektor, peningkatan kesadaran, serta penerapan teknologi canggih untuk menjaga integritas dan kerahasiaan data pemerintah.

Kata Kunci: Keamanan Siber, Sektor Pemerintahan, Perlindungan Data, Ancaman Siber, Kebijakan.

ABSTRACT

Cybersecurity and data protection are crucial in the government sector, where sensitive data and public information are primary targets for cyber attacks. This study aims to analyze the challenges and strategies implemented to protect government information systems from cyber threats. The methodology used includes a literature review and analysis of existing policies, as well as case studies on cybersecurity incidents in government institutions. The research findings indicate that although many efforts have been made, such as improving IT infrastructure and employee training, there are still weaknesses in inter-agency coordination and understanding of existing risks. The conclusion of this study emphasizes the importance of a holistic approach to cybersecurity, which includes cross-sector collaboration, increased awareness, and the implementation of advanced technologies to maintain the integrity and confidentiality of government data.

Keywords: Cybersecurity, Government Sector, Data Protection, Cyber Threats, Policy.

PENDAHULUAN

Perkembangan teknologi informasi membawa dampak yang sangat besar bagi segala aspek kehidupan manusia, sementara itu pengguna internet terus meningkat tetapi masih banyak yang tidak menyadari pentingnya perlindungan data pribadi. Lebih dari 30% pengguna internet di Indonesia belum sadar bahwa pentingnya membangun keamanan data privasi untuk mencegah terjadinya data pribadi yang dapat memungkinkan diambil oleh pihak yang tidak bertanggung jawab.Data perlu dijaga baik kerahasiaannya maupun ketersediaannnya khususnya bagi anak dan remaja, dimana data pribadi dan orang tua serta keluarga juga bisa terungkap jika tidak dipahami bagaimana untuk mengamankan data tersebut (Deanna Durbin Hutagalung, 2022).

Keamanan merupakan bagian terpenting dalam sistem informasi karena informasi hanya diserahkan pada bagian golongan tertentu. Jadi, pentingnya melakukan pencegahan agar tidak salah dipergunakan oleh golongan golongan yang tidak memiliki hak dalam kepentingan. Oleh karena itu dibutuhkan suatu keamanan komputer agar informasi dapat terjaga dengan baik

(Ika Yusnita Sari, 2020) Di zaman yang serba digital seperti saat ini sangat penting untuk memahami apa itu keamanan siber dan bagai-mana menggunakannya di dunia yang tidak dapat ada tanpa teknologi dan koneksi jaringan. Tanpa adanya bentuk perlindungan yang memadai, kemungkinan file, data pribadi dan aset virtual penting lainnya mungkin bisa dalam keadaan bahaya. Cyber Security merupakan proses mempertahankan diri dari serangan siber pada jaringan, perangkat lunak dan data sensitive. Serangan ini dapat diklasifikasikan sebagai eksploitasi sumber daya, akses tidak sah ke sistem, seperti serangan ransomware untuk mengenkripsi data dengan tujuan untuk pemerasan. (Yose Indarta, 2022) Bahaya yang terkait dengan ancaman siber sangat tinggi. Keamanan siber sangat penting untuk semua organisasi termasuk kalangan diusia remaja sekolah, tidak hanya untuk organisasi komersial dan pemerintah.

Menurut analisis yang lebih baru oleh Australian Cyber Security center (ACSC), ada 59.806 laporan kejahatan dunia maya antara juli 2019 dan juni 2020, atau rata-rata 164 kejahatan dunia maya setiap tahun. Cyber Security juga menjadi masalah yang serius di Indonesia dengan kebocoran data yang sering terjadi di Indonesia selama 2020-2021. Menurut riset Trend Micro, Indeks Risiko Siber (CRI) Indonesia untuk tahun 2020 adalah 0,26, yang menunjukan tingkat bahaya yang moderat. Sebaliknya, turun menjadi - 0,12 pada tahun 2021, menunjukan bahwa bahayanya meningkat walau belum dalam resiko tinggi. (Wahyu Tisno Atmojo, 2021).

METODE PELAKSANAAN

Penelitian ini menggunakan metode pendekatan kualitatif untuk mengkaji literatur dan sumber sekunder yang relevan mengenai Siber dan Keamanan Data pada Sektor Pemerintahan. Literatur yang digunakan meliputi jurnal akademis, serta dari berbagai lembaga pemerintahan. Pendekatan ini membantu memahami secara mendalam teori dan konsep yang berkaitan dengan Siber dan Keamanan Data pada Sektor Pemerintah tanpa menggunakan data kuantitatif langsung.

HASIL DAN PEMBAHASAN

Penelitian ini mengidentifikasi berbagai ancaman siber yang dihadapi oleh sektor pemerintahan, yang memiliki dampak serius terhadap keamanan data dan operasional lembaga. Berikut adalah penjelasan lebih rinci

mengenai beberapa ancaman tersebut:

a. Serangan Malware
   Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mengakses sistem tanpa izin. Dalam konteks pemerintahan, malware dapat digunakan untuk :
   a) Mengambil alih system : Penyerang dapat memasukkan malware ke dalam sistem untuk mengendalikan data dan fungsi kritis.
   b) Menginfeksi jaringan : Malware dapat menyebar melaluijaringan, menyebabkan gangguan operasional yang luas.
b. Phishing
   Phishing adalah metode penipuan di mana penyerang mencoba untuk mendapatkan informasi sensitif, seperti kata sandi atau data keuangan, dengan menyamar sebagai entitas terpercaya. Ancaman ini sangat berbahaya di sektor pemerintahan karena :
   a) Targeting pegawai : Pegawai pemerintah mungkin menjadi target serangan ini, yang dapat mengakibatkan kebocoran informasi rahasia.
   b) Metode yang sulit dikenali : Phishing sering kali dilakukan melalui email atau pesan yang terlihat sah, membuatnya sulit untuk diidentifikasi.
c. Ransomware
   Ransomware adalah jenis malware yang mengenkripsi data pengguna dan meminta tebusan untuk mendekripsinya. Di sektor pemerintahan, serangan ransomware dapat mengakibatkan:
   a) Gangguan layanan public : Ketika sistem pemerintah terinfeksi, layanan yang penting bagi masyarakat dapat terhenti.
   b) Kehilangan data penting : Jika data tidak dapat dipulihkan, informasi krusial dapat hilang, yang berdampak pada pengambilan keputusan dan pelayanan publik.
d. Kebocoran Data
   Insiden kebocoran data, di mana informasi sensitif publik atau internal bocor ke pihak luar, menunjukkan kerentanan sistem informasi pemerintah. Kebocoran ini dapat disebabkan oleh:
   a) Kesalahan manusia: Prosedur keamanan yang tidak diikuti atau kesalahan dalam pengelolaan data dapat menyebabkan kebocoran.
   b) Serangan siber : Penyerang dapat mengeksploitasi celah keamanan untuk mencuri data, yang dapat digunakan untuk kepentingan politik atau ekonomi, seperti pemerasan atau spionase.

Strategi Perlindungan yang diterapkan berbagai strategi telah diimplementasikan untuk melindungi sistem informasi pemerintah. Ini termasuk:

a. Peningkatan Infrastruktur TI: Investasi dalam perangkat keras dan perangkat lunak yang lebih aman.
b. Pelatihan Pegawai : Program pendidikan untuk meningkatkan kesadaran keamanan siber di kalangan pegawai.
c. Pengembangan Kebijakan Keamanan : Pembuatan kebijakan yang jelas dan komprehensif untuk mengatur keamanan data.

Kelemahan yang Ditemukan Meskipun berbagai upaya telah dilakukan, terdapat kelemahan yang signifikan, seperti:

a. Kurangnya Koordinasi Antarinstansi : Banyak lembaga yang bekerja secara terpisah, sehingga menghambat respon cepat terhadap insiden keamanan.
b. Pemahaman yang Terbatas tentang Risiko : Beberapa pegawai masih kurang memahami

pentingnya praktik keamanan siber, yang dapat menyebabkan kesalahan manusia.

Rekomendasi untuk Perbaikan Dari analisis tersebut, beberapa rekomendasi dapat diberikan :

a. Meningkatkan Kolaborasi Lintas Sektor : Mengembangkan jaringan kerjasama antara lembaga pemerintah dan sektor swasta untuk berbagi informasi dan praktik terbaik.
b. Mengimplementasikan Teknologi Canggih : Menggunakan alat analitik dan kecerdasan buatan untuk mendeteksi dan merespons ancaman lebih cepat.
c. Kampanye Kesadaran Keamanan : Meluncurkan kampanye berkelanjutan untuk mendidik pegawai dan publik tentang pentingnya keamanan siber.

KESIMPULAN

Hasil dari kajian literatur ini menegaskan bahwa Keamanan siber dan perlindungan data di sektor pemerintahan merupakan aspek yang sangat penting, mengingat tingginya risiko serangan yang dapat mengancam integritas, kerahasiaan, dan ketersediaan data publik. Artikel ini mengungkapkan bahwa sektor pemerintahan menghadapi berbagai ancaman, termasuk malware, phishing, dan ransomware, yang dapat mengakibatkan kebocoran data sensitif dan gangguan layanan publik.

Meskipun banyak langkah telah diambil untuk meningkatkan infrastruktur keamanan, seperti pelatihan pegawai dan pengembangan kebijakan keamanan, masih terdapat kelemahan dalam koordinasi antarinstansi dan pemahaman tentang risiko yang ada. Oleh karena itu, diperlukan pendekatan yang lebih holistik dan terintegrasi, yang meliputi:

a. Kolaborasi Lintas Sektor : Membangun jaringan kerjasama antara lembaga pemerintah dan sektor swasta untuk berbagi informasi dan praktik terbaik.
b. Penerapan Teknologi Canggih : Menggunakan alat analitik dan kecerdasan buatan untuk mendeteksi dan merespons ancaman secara lebih efektif.
c. Kampanye Kesadaran Keamanan : Meluncurkan inisiatif berkelanjutan untuk mendidik pegawai dan masyarakat tentang pentingnya keamanan siber.

Dengan langkah-langkah tersebut diharapkan sektor pemerintahan dapat memperkuat pertahanannya terhadap ancaman siber, sehingga mampu melindungi data dan sistem informasi yang vital bagi kepentingan publik. Keberhasilan dalam mengatasi tantangan ini akan berkontribusi pada peningkatan kepercayaan masyarakat terhadap institusi pemerintah

DAFTAR PUSTAKA

Herdiana, Y., Munawar, Z., & Putri, N. I. (2021). Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT: Information Communication & Technology, 21*(1), 42-52.

Silalahi, F. D. (2022*). Keamanan Cyber (Cyber Security).* Penerbit Yayasan Prima Agus Teknik, 1-285.

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

Anjani, N. H. (2021). Perlindungan Keamanan Siber di Indonesia.

Gunawan, I. (2021). Analisis Keamanan Data Pada Website Dengan Wireshark. *JES (Jurnal Elektro Smart), 1*(1), 16-19.