HUMANITIS: Jurnal Humaniora, Sosial dan Bisnis
Vol. 2 No. 7 Juli 2024, hal. 759-762 e-ISSN: 2988-6287

MANAJEMEN KEAMANAN CYBER DI PERUSAHAAN

Yesta Sadha Saputra[1*], Rizki Nur Wakhid[2], Raihan Gading Rabbani[3], Ammar Wildan[4], Arif Bentar Suganda Heriyanto[5],Tubagus Hedi Saepudin[6]
[1]Teknik, Teknik industri, Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia
Email: [1]202210215079@mhs.ac.id, [2]202210215077@msh.ac.id, [3]202210215088@mhs.ac.id, [4]202210215101@msh.ac.id, [5]202210215089@msh.ac.id, [6]tubagus.hedi@dsn.ubhara.ac.id

Abstract

Cyber security has become an increasingly important issue in the era of modern technology. In recent years, we have seen an increase in the number and complexity of cyber attacks that threaten computer systems and data around the world. Attacks such as data theft, malware attacks, hacking, and DDoS attacks have resulted in financial losses, imagery, and business operations. The chosen qualitative approach allows researchers to explore subtle and complex aspects of complex situations such as corporate security and security management. The objective of this qualitatively descriptive research is to gain a deeper understanding of how effective security management affects corporate safety. It can undermine customer confidence, brand value, and relationships with business partners and other stakeholders. Therefore, security management should take proactive action to avoid security issues that could damage the Company's reputation.

Keywords: *management of securities, Company, Cyber Crime, Technology.*

Abstrak

Keamanan cyber telah menjadi masalah yang semakin penting di era teknologi modern. Dalam beberapa tahun terakhir, kami telah melihat peningkatan jumlah dan kompleksitas serangan cyber yang mengancam sistem komputer dan data di seluruh dunia. Serangan seperti pencurian data, serangan malware, peretasan, dan serangan DDoS telah mengakibatkan kerugian finansial, citra, dan operasi bisnis Pendekatan kualitatif yang dipilih memungkinkan peneliti untuk mengeksplorasi aspek yang halus dan kompleks dari situasi yang kompleks seperti manajemen sekuriti dan keamanan perusahaanTujuan dari penelitian deskriptif kualitatif ini adalah untuk mendapatkan pemahaman yang lebih mendalam tentang bagaimana manajemen sekuriti efektif berdampak pada keamanan perusahaanKerusakan reputasi perusahaan dapat terjadi karena kehilangan data atau pelanggaran keamanan. Ini dapat merusak kepercayaan pelanggan, nilai merek, dan hubungan dengan mitra bisnis dan pemangku kepentingan lainnya. Oleh karena itu, manajemen sekuriti harus mengambil tindakan proaktif untuk menghindari masalah keamanan yang dapat merusak reputasi Perusahaan.

Kata Kunci: Manajemen Sekuriti, Perusahaan, Kejahatan Siber, Teknologi.

PENDAHULUAN

Keamanan *cyber* telah menjadi masalah yang semakin penting di era teknologi modern. Dalam beberapa tahun terakhir, kami telah melihat peningkatan jumlah dan kompleksitas serangan *cyber* yang mengancam sistem komputer dan data di seluruh dunia. Serangan seperti pencurian data, serangan malware, peretasan, dan serangan DDoS telah mengakibatkan kerugian finansial, citra, dan operasi bisnis. Penelitian ini bertujuan untuk mempelajari elemen penting yang terkait dengan keamanan *cyber* di era digital karena tingkat ancaman ini yang tinggi. Para peneliti dan

praktisi di bidang keamanan informasi terus bekerja keras untuk mengembangkan strategi yang lebih baik untuk melindungi data dan sistem komputer dari serangan siber (Susanto et al., 2023).

Ancaman terhadap objek penting dan keamanan file terus meningkat.Serangan malware, peretasan, dan serangan jaringan yang kompleks adalah beberapa contoh kegagalan keamanan sistem digital yang dieksploitasi oleh penjahat *cyber* yang semakin mahir dan mahir. Selain itu, dengan semakin banyaknya informasi yang dikirim dan disimpan secara elektronik, masalah keamanan file menjadi semakin sulit. Oleh karena itu, diperlukan analisis menyeluruh tentang ancaman yang dihadapi dalam dunia digital serta solusi yang dapat diterapkan untuk meningkatkan keamanan *cyber*. Studi kasus serangan yang pernah terjadi dan tindakan yang diambil untuk mengatasinya sangat penting untuk memahami kompleksitas dan kesulitan yang dihadapi dalam pengamanan objek dan file penting (Soesanto et al., 2023)

Keamanan bisnis mencakup tindakan proaktif seperti membuat kebijakan, memberikan instruksi kepada karyawan tentang prosedur keamanan, dan menggunakan teknologi keamanan seperti firewall dan antivirus. Tindakan responsif juga termasuk, seperti mengamati dan menemukan aktivitas yang mencurigakan. Berbagai faktor, seperti strategi bisnis, orientasi pembelajaran, kemampuan manajemen, dan manajemen, dapat memengaruhi keamanan perusahaan. Tujuan utamanya adalah untuk menghindari pencurian atau pencurian data, melindungi reputasi perusahaan, mematuhi peraturan dan kebijakan, dan memastikan operasi lancar (Irawan et al., 2024)

Ada banyak *framework cyber security* yang dapat digunakan. Namun, penulis menyarankan untuk menggunakan *NIST Cybersecurity Framework*, yang diterbitkan oleh *National Institute of Standart and Technology (NIST)* dan *NIST Special Publication 800-53. Framework* ini menyediakan pedoman untuk meningkatkan keamanan siber dan mengurangi ancaman. Selain itu, menggunakan struktur ini memiliki beberapa keuntungan, seperti mudah untuk digunakan dan dapat menghemat uang dengan memilih proses yang paling sesuai dengan kebutuhan bisnis (Tan & Soewito, 2022)

METODE PENELITIAN

Tujuan dari penelitian deskriptif kualitatif ini adalah untuk mendapatkan pemahaman yang lebih mendalam tentang bagaimana manajemen sekuriti efektif berdampak pada keamanan perusahaan. Pendekatan kualitatif yang dipilih memungkinkan peneliti untuk mengeksplorasi aspek yang halus dan kompleks dari situasi yang kompleks seperti manajemen sekuriti dan keamanan perusahaan. Penelitian ini didasarkan pada konsep dan teori yang relevan dari bidang manajemen sekuriti, keamanan bisnis, dan teori organisasi. Tinjauan pustaka akan menemukan penelitian sebelumnya yang relevan dalam publikasi nasional dan internasional.

HASIL DAN PEMBAHASAN

Peran dan tanggung jawab manajemen sekuriti dalam mengelola risiko keamanan.

Manajemen sekuriti memainkan peran penting dalam menjaga perusahaan aman dengan mengelola risiko yang terkait. Manajemen sekuriti bertanggung jawab atas banyak hal, seperti membuat kebijakan keamanan yang jelas, mengidentifikasi ancaman dan kerentanan yang mungkin, dan menerapkan kontrol keamanan yang tepat untuk mengelola risiko. Selain itu,

manajemen sekuriti juga harus memastikan bahwa karyawan memahami praktik keamanan yang baik melalui pelatihan dan pendidikan yang tepat.Selain itu, mereka harus memastikan bahwa teknologi keamanan yang diperlukan, seperti *firewall* dan sistem deteksi intrusi, telah *diinstal* dan dipertahankan untuk melindungi sistem informasi perusahaan Anda dari serangan.
Dampak positif dari manajemen sekuriti yang efektif terhadap keseluruhan operasional perusahaan.

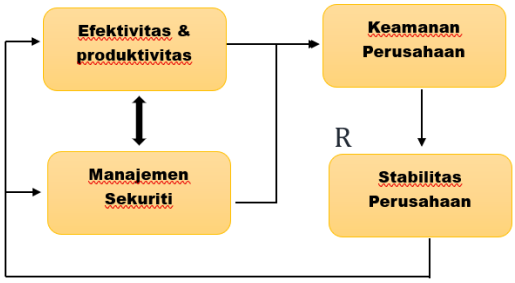
Manajemen sekuriti yang efektif meningkatkan kepercayaan pelanggan dan mitra bisnis. Di era di mana keamanan data menjadi semakin penting bagi pemangku kepentingan eksternal seperti pelanggan dan mitra bisnis, sertifikasi keamanan atau kepatuhan terhadap standar keamanan tertentu dapat memberikan keunggulan kompetitif yang signifikan. Dengan manajemen sekuriti yang baik, bisnis juga dilindungi dari berbagai bahaya keamanan. Perusahaan dapat mengurangi risiko hukuman atau denda karena pelanggaran keamanan atau privasi data dengan menerapkan kontrol keamanan yang tepat dan mematuhi standar keamanan yang berlaku.

Peran manajemen sekuriti dalam melindungi aset, data, dan reputasi perusahaan. Peran

Manajemen sekuriti sangat penting untuk memastikan bahwa bisnis aman dan bertahan. Mereka bertanggung jawab secara signifikan untuk melindungi aset, data, dan reputasi perusahaan dari bahaya yang dapat mengancam keberlangsungan bisnis dan kepercayaan pemangku kepentingan. Aset perusahaan dilindungi oleh manajemen sekuriti. Melindungi aset ini sangat penting karena merupakan dasar operasi bisnis. Aset ini dapat berupa aset fisik, seperti inventaris, bangunan, dan peralatan, serta aset non-fisik, seperti data, properti kekayaan intelektual, dan informasi rahasia perusahaan. Ancaman seperti pencurian, kerusakan, atau kehilangan aset dapat sangat mengganggu operasi perusahaan. Manajemen sekuriti sangat penting untuk menjaga data perusahaan aman. Sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data, yang merupakan salah satu aset paling berharga dalam bisnis kontemporer.

Selain menjaga aset dan data, manajemen sekuriti juga harus menjaga reputasi perusahaan. Perlindungan aset dan keamanan data sangat penting untuk menjaga kelangsungan bisnis dan reputasi perusahaan. Kerusakan reputasi perusahaan dapat terjadi karena kehilangan data atau pelanggaran keamanan. Ini dapat merusak kepercayaan pelanggan, nilai merek, dan hubungan dengan mitra bisnis dan pemangku kepentingan lainnya. Oleh karena itu, manajemen sekuriti harus mengambil tindakan proaktif untuk menghindari masalah keamanan yang dapat merusak reputasi perusahaan. Selain itu, manajemen sekuriti bertanggung jawab untuk memastikan bahwa bisnis mematuhi semua peraturan dan standar keamanan yang berlaku. Mematuhi peraturan keamanan ini memperkuat kepercayaan pemangku kepentingan dan mengurangi risiko hukum dan keuangan bagi perusahaan. Secara keseluruhan, manajemen sekuriti sangat penting untuk menjaga keamanan, keberlangsungan operasi, dan reputasi bisnis. Mereka memastikan bahwa bisnis dapat beroperasi secara efisien dan aman dalam lingkungan bisnis yang semakin kompleks dan rentan terhadap ancaman keamanan dengan menerapkan pendekatan keamanan yang holistik dan proaktif.

Konsep Pemodelan



KESIMPULAN

Manajemen sekuriti sangat penting untuk menjaga aset, data, dan reputasi perusahaan agar dapat beroperasi dengan aman di lingkungan bisnis yang penuh dengan ancaman keamanan. Ini menjaga keamanan, keberlangsungan operasi, dan reputasi perusahaan. Mereka mencapai hal ini dengan mematuhi peraturan dan standar keamanan yang berlaku dan menggunakan kebijakan, prosedur, dan kontrol keamanan yang tepat. Perlindungan aset dan keamanan data sangat penting untuk menjaga kelangsungan bisnis dan reputasi perusahaan. Kerusakan reputasi perusahaan dapat terjadi karena kehilangan data atau pelanggaran keamanan. Ini dapat merusak kepercayaan pelanggan, nilai merek, dan hubungan dengan mitra bisnis dan pemangku kepentingan lainnya. Oleh karena itu, manajemen sekuriti harus mengambil tindakan proaktif untuk menghindari masalah keamanan yang dapat merusak reputasi perusahaan.

REFERENCES

Irawan, C. R., Fauzi, A., Sanjaya, F., & Ramadhan, A. (2024). *Pengaruh Efektivitas Manajemen Sekuriti Dalam Keamanan Perusahaan*. *3*(1), 59–68.

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2), 186.

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber Di Era Digital. *Journal of Business And Entrepreneurship*, *11*(1), 23. https://doi.org/10.46273/jobe.v11i1.365

Tan, T., & Soewito, B. (2022). Manajemen Risiko Serangan SiberMenggunakan Framework NistCybersecurity Di Universitas Zxc. *Journal of Information System, Applied, Management, Accounting and Research*, *6*(2), 411–422. https://doi.org/10.52362/jisamar.v6i2.781