Strategi Pengelolaan Risiko dan Keamanan Informasi pada Platform E-Bisnis: Studi Kasus Tokopedia (Tokopedia: Bagaimana Platform Ini Menangani Insiden Kebocoran Data pada Tahun 2020, Termasuk Langkah Mitigasi dan Perbaikan Sistem Keamanannya)

Marsyanada
Universitas 17 Agustus 1945 Surabaya
email: marsyndaa05@gmail.com

Article Info

Article history:

Received : 28 - 09, 2024
Revised : 27 - 10, 2024
Accepted : 04 - 11, 2024

Keywords:

Data Security;
Online Sales Transaction;
Tokopedia;
Data Encryption.

ABSTRACT

The data leak incident experienced by Tokopedia in 2020 is an important reminder of the need for effective risk management and information security strategies on e-business platforms. This article discusses the mitigation measures taken by Tokopedia, including system security enhancements, user education, and collaboration with cybersecurity agencies. Using a qualitative approach through case study analysis, this article reviews the incident chronology, evaluation of mitigation measures, and recommendations for more proactive risk management. The findings show that while Tokopedia's mitigation measures were successful in improving security, further investment in proactive technologies such as two-factor authentication (2FA) and end-to-end encryption is required. The article concludes with recommendations for other e-business platforms to minimize the risk of data leakage and maintain customer trust.

Corresponding Author:

Marsyanada
Universitas 17 Agustus 1945 Surabaya
Email: marsyndaa05@gmail.com

1. PENDAHULUAN

Era digital telah mengubah lanskap dunia bisnis secara signifikan, dengan banyak perusahaan beralih ke platform berbasis elektronik atau e-bisnis untuk memperluas jangkauan pasar mereka. Perkembangan teknologi yang pesat memungkinkan proses transaksi yang lebih efisien dan mudah diakses oleh konsumen di seluruh dunia (Zuech & Yardley, 2010). Namun, kemajuan ini juga membawa tantangan besar, khususnya dalam hal risiko dan keamanan informasi. Salah satu insiden yang menonjol dalam konteks ini adalah kebocoran data yang terjadi pada Tokopedia pada tahun 2020, yang mengungkap lebih dari 91 juta akun pengguna (Tokopedia, 2020). Insiden ini mencerminkan betapa rentannya platform e-bisnis terhadap ancaman cyber dan bagaimana kebocoran data dapat merusak reputasi perusahaan serta kepercayaan pelanggan.

Kejadian tersebut tidak hanya menyoroti pentingnya memiliki sistem keamanan yang kuat, tetapi juga menunjukkan bahwa risiko keamanan informasi adalah tantangan yang harus dikelola dengan serius oleh perusahaan-perusahaan yang bergerak di sektor e-bisnis. Dalam dunia yang semakin terhubung, perlindungan data menjadi prioritas utama yang tidak bisa diabaikan. Tokopedia, sebagai salah satu platform e-commerce terbesar di Indonesia, segera mengambil langkah-langkah strategis untuk mengatasi insiden tersebut dan memperbaiki sistem keamanan mereka guna mencegah kebocoran lebih lanjut. Langkah-langkah ini penting

tidak hanya untuk pemulihan perusahaan, tetapi juga untuk memastikan perlindungan yang lebih baik bagi data pelanggan dan untuk menjaga kepercayaan publik.

Penelitian ini akan mengulas langkah-langkah yang diterapkan Tokopedia untuk mengelola risiko dan meningkatkan keamanan informasi setelah kebocoran data tersebut. Studi ini bertujuan untuk memberikan wawasan mengenai pendekatan mitigasi risiko yang dapat diterapkan oleh platform e-bisnis lainnya, sehingga mereka dapat belajar dari pengalaman Tokopedia dan mengembangkan strategi yang lebih baik dalam mengelola risiko dan melindungi data pelanggan mereka.

2. TINJAUAN PUSTAKA

Pengelolaan risiko dan keamanan informasi dalam e-bisnis merupakan topik yang semakin penting dalam era digital yang berkembang pesat. Perusahaan-perusahaan berbasis elektronik menghadapi tantangan besar dalam menjaga integritas dan kerahasiaan data pelanggan mereka. Untuk itu, pengelolaan risiko dan keamanan informasi harus mencakup berbagai strategi yang komprehensif, mulai dari penerapan kebijakan keamanan hingga adopsi teknologi canggih yang dapat melindungi data sensitif. Salah satu pedoman yang sering digunakan dalam mengelola keamanan informasi adalah ISO 27001 (International Organization for Standardization (ISO), 2013), yang merupakan standar internasional untuk sistem manajemen keamanan informasi (ISMS). Standar ini memberikan kerangka kerja yang membantu organisasi untuk melindungi data melalui kebijakan, prosedur, dan kontrol yang sistematis. Selain itu, NIST Cybersecurity Framework juga digunakan sebagai referensi untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari ancaman siber (National Institute of Standards and Technology (NIST), 2018).

Penelitian sebelumnya menunjukkan bahwa teknologi keamanan yang canggih memiliki peran yang sangat penting dalam mengurangi risiko keamanan siber (Bada et al., 2019). Salah satu teknologi utama yang banyak diterapkan adalah autentikasi dua faktor (2FA), yang memberikan lapisan tambahan perlindungan selain kata sandi. Dengan 2FA, pengguna harus melalui dua tahap verifikasi sebelum mendapatkan akses, yang secara signifikan mengurangi kemungkinan akses tidak sah (Anderson, 2010). Selain itu, enkripsi data juga merupakan komponen penting dalam melindungi informasi yang dikirimkan atau disimpan oleh platform e-bisnis. Data yang terenkripsi hanya dapat diakses oleh pihak yang memiliki kunci enkripsi yang sah, sehingga mengurangi risiko kebocoran data (Jeon et al., 2012). Teknologi lain yang juga semakin populer adalah deteksi anomali berbasis machine learning (ML), yang memungkinkan sistem untuk mengidentifikasi perilaku tidak biasa dalam lalu lintas data atau aktivitas pengguna. Dengan menggunakan algoritma pembelajaran mesin, sistem dapat mendeteksi potensi ancaman dengan lebih cepat dan akurat dibandingkan dengan metode tradisional (Zuech & Yardley, 2010).

Studi kasus pada insiden serupa, seperti kebocoran data yang dialami oleh Equifax pada tahun 2017, memberikan pelajaran berharga mengenai pentingnya respons cepat dan penanganan yang tepat dalam mengurangi dampak dari kebocoran data. Dalam insiden tersebut, lebih dari 147 juta data pengguna terekspos akibat kelemahan dalam sistem keamanan perusahaan. Penanganan yang lambat dan kurangnya transparansi dalam memberi tahu pelanggan mengenai kebocoran tersebut memperburuk dampak yang ditimbulkan (Equifax, 2017; Symantec, 2017). Hal ini menunjukkan bahwa respons yang cepat dan jelas sangat penting dalam menjaga kepercayaan pelanggan dan mencegah kerusakan reputasi yang lebih besar. Oleh karena itu, selain meningkatkan sistem keamanan, perusahaan juga perlu memiliki rencana tanggap darurat yang efektif dan prosedur komunikasi yang jelas (Clark et al., 2014).

Penelitian juga menyoroti peran penting edukasi pengguna dalam mengurangi risiko terkait rekayasa sosial (social engineering), salah satu metode yang sering digunakan oleh peretas untuk memperoleh akses tidak sah ke dalam sistem. Rekayasa sosial melibatkan manipulasi psikologis terhadap individu untuk mengeksploitasi kelemahan manusia, seperti meminta informasi sensitif melalui email atau panggilan telepon palsu. Oleh karena itu, pelatihan yang rutin bagi karyawan dan pengguna mengenai cara mengenali upaya rekayasa sosial dan kebiasaan pengamanan yang baik dapat membantu mencegah terjadinya serangan yang berbasis pada kelalaian manusia.

Secara keseluruhan, pendekatan yang terintegrasi antara teknologi canggih, kebijakan yang kuat, respons yang cepat terhadap insiden, dan edukasi yang berkelanjutan merupakan kunci untuk mengelola risiko dan meningkatkan keamanan informasi dalam e-bisnis. Perusahaan harus selalu siap mengadaptasi pendekatan-pendekatan ini untuk menghadapi ancaman yang terus berkembang di dunia maya.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan analisis studi kasus (Sugiyono, 2017). Sumber data sekunder meliputi laporan media, pernyataan resmi dari Tokopedia, dan literatur terkait keamanan informasi. Analisis difokuskan pada kronologi insiden kebocoran data Tokopedia, langkah-langkah mitigasi yang diambil, serta evaluasi efektivitas strategi tersebut.

4. HASIL DAN PEMBAHASAN

4.1. Kronologi Insiden Kebocoran Data Tokopedia

Pada Mei 2020, data lebih dari 91 juta akun Tokopedia dilaporkan bocor dan dijual di forum daring. Informasi yang bocor mencakup nama pengguna, email, dan kata sandi yang di-hash. Meskipun tidak ada data afinansial yang dilaporkan bocor, insiden ini tetap menjadi peringatan serius akan celah keamanan di sistem e-bisnis (Tokopedia, 2020).

4.2. Langkah Mitigasi yang Diterapkan

Tokopedia segera mengambil langkah-langkah berikut (Tokopedia, 2020):

a) Peningkatan Keamanan Sistem:
- Memperbarui algoritma hashing untuk meningkatkan keamanan kata sandi pengguna.
- Melakukan audit menyeluruh terhadap sistem keamanan.

b) Edukasi Pengguna:
- Mengimbau pengguna untuk mengganti kata sandi secara berkala.
- Memberikan panduan tentang praktik keamanan daring yang baik.

c) Kolaborasi dengan Pihak Ketiga:
- Bekerja sama dengan lembaga keamanan siber untuk menyelidiki insiden tersebut.
- Mengadopsi teknologi deteksi ancaman berbasis AI untuk memantau aktivitas mencurigakan.

4.3. Evaluasi Keberhasilan Langkah Mitigasi

Langkah-langkah mitigasi yang diambil oleh Tokopedia setelah kebocoran data pada tahun 2020 menunjukkan perbaikan yang signifikan dalam sistem keamanan mereka. Beberapa tindakan yang diimplementasikan mencakup pembaruan protokol keamanan, penguatan enkripsi data, dan peningkatan deteksi anomali berbasis kecerdasan buatan. Tokopedia juga melakukan audit internal untuk menilai kelemahan yang ada dalam sistem mereka dan mengidentifikasi potensi celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Hasil dari langkah-langkah mitigasi ini adalah penurunan jumlah insiden keamanan yang terdeteksi dalam periode pasca insiden, yang menunjukkan keberhasilan dalam meningkatkan ketahanan terhadap ancaman siber.

Namun, insiden kebocoran data tersebut juga mengungkapkan pentingnya investasi yang lebih besar dalam teknologi keamanan proaktif. Meskipun langkah-langkah mitigasi yang diambil Tokopedia sudah cukup efektif, kebocoran data yang terjadi menunjukkan bahwa pendekatan yang lebih komprehensif masih dibutuhkan untuk mengantisipasi ancaman yang terus berkembang. Salah satu area yang masih memerlukan perhatian adalah implementasi firewall cerdas yang dapat mendeteksi dan menanggulangi ancaman secara lebih otomatis dan dinamis. Teknologi firewall cerdas menggunakan kecerdasan buatan untuk memantau lalu lintas data dan secara real-time mengidentifikasi pola yang mencurigakan, sehingga memberikan perlindungan yang lebih baik terhadap serangan berkelanjutan (Alicea & Alsmadi, 2021; Anwar et al., 2021; Bringhenti et al., 2023). Selain itu, penerapan enkripsi ujung-ke-ujung (*end-to-end encryption*) yang lebih kuat pada seluruh proses transaksi dan komunikasi pengguna dapat memberikan lapisan perlindungan tambahan yang lebih maksimal terhadap potensi kebocoran data.

Salah satu langkah mitigasi yang telah terbukti efektif adalah penerapan autentikasi dua faktor (2FA). Autentikasi dua faktor telah diimplementasikan oleh Tokopedia sebagai bagian dari upaya berkelanjutan mereka untuk meningkatkan keamanan. Penelitian dan pengalaman dari platform serupa menunjukkan bahwa penerapan 2FA dapat secara signifikan mengurangi risiko akses tidak sah ke dalam akun pengguna, bahkan jika kata sandi pengguna terkompromikan. Dengan memanfaatkan dua metode verifikasi (misalnya, kata sandi dan kode verifikasi yang dikirimkan ke ponsel pengguna), 2FA menambah lapisan perlindungan yang sulit ditembus oleh peretas. Sebagai contoh, platform-platform besar seperti Google, Facebook, dan Apple juga telah mengimplementasikan 2FA secara luas (Dmitrienko et al., 2014; Gupta, 2017) untuk meningkatkan keamanan pengguna mereka.Perbandingan dengan platform serupa yang telah berhasil mengimplementasikan 2FA menunjukkan bahwa Tokopedia berada di jalur yang tepat dalam mengurangi risiko akses yang tidak sah dan melindungi data pengguna. Meskipun implementasi 2FA bukanlah solusi tunggal untuk semua ancaman keamanan, pengadopsiannya secara luas memberikan hasil yang positif dalam meningkatkan ketahanan

terhadap serangan phishing dan brute-force attack.Secara keseluruhan, meskipun langkah-langkah mitigasi yang diambil Tokopedia setelah insiden kebocoran data telah menunjukkan kemajuan yang signifikan dalam memperkuat sistem keamanan, insiden tersebut juga menyoroti perlunya upaya yang lebih besar dan berkelanjutan dalam investasi teknologi keamanan canggih dan penguatan sistem perlindungan data. Oleh karena itu, Tokopedia dan platform e-bisnis lainnya perlu terus berinovasi dan menyesuaikan diri dengan tren teknologi terbaru dalam upaya menjaga integritas dan kepercayaan pelanggan mereka.

5. KESIMPULAN

Insiden kebocoran data Tokopedia pada tahun 2020 memberikan pelajaran penting tentang tantangan yang dihadapi oleh platform e-bisnis dalam menjaga keamanan informasi pengguna. Langkah-langkah mitigasi yang diambil setelah insiden tersebut efektif dalam memperbaiki sistem keamanan dan mengurangi risiko lebih lanjut. Namun, kejadian ini juga menekankan pentingnya pengelolaan risiko dan keamanan informasi dengan pendekatan yang lebih holistik dan proaktif. Strategi mitigasi harus dilengkapi dengan langkah-langkah preventif untuk mengantisipasi potensi ancaman sebelum terjadi.

Berdasarkan evaluasi langkah-langkah yang telah diterapkan dan perbandingan dengan praktik terbaik di industri, ada beberapa rekomendasi yang dapat diikuti oleh platform e-bisnis lainnya. Pertama, platform disarankan mengadopsi kerangka kerja keamanan informasi yang diakui secara internasional, seperti ISO 27001, untuk membantu merancang dan mengimplementasikan kebijakan serta prosedur yang meningkatkan ketahanan terhadap ancaman siber. Kedua, teknologi autentikasi yang lebih kuat seperti biometrik dapat dipertimbangkan untuk memberikan lapisan perlindungan tambahan. Ketiga, audit keamanan secara berkala sangat penting untuk mengidentifikasi celah dalam sistem, termasuk pengujian penetrasi dan analisis kerentanan. Terakhir, edukasi pengguna tentang praktik keamanan daring, seperti menghindari serangan phishing dan pentingnya kata sandi yang kuat, dapat membantu mengurangi risiko akibat kelalaian pengguna. Dengan menerapkan pendekatan ini, platform e-bisnis dapat lebih baik dalam mengelola risiko keamanan, meminimalkan potensi kebocoran data, dan mempertahankan kepercayaan pengguna. Keamanan informasi yang kuat bukan hanya melindungi data pelanggan tetapi juga menjadi fondasi keberlanjutan perusahaan di dunia digital.

DAFTAR PUSTAKA

Alicea, M., & Alsmadi, I. (2021). Misconfiguration in firewalls and network access controls: Literature review. In *Future Internet* (Vol. 13, Issue 11). https://doi.org/10.3390/fi13110283

Anderson, R. J. (2010). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. In *Applied Sciences (Switzerland)* (Vol. 11, Issue 19). https://doi.org/10.3390/app11199183

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *ArXiv Preprint ArXiv:1901.02672*.

Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F., & Yusupov, J. (2023). Automated Firewall Configuration in Virtual Networks. *IEEE Transactions on Dependable and Secure Computing*, *20*(2). https://doi.org/10.1109/TDSC.2022.3160293

Clark, D., Berson, T., & Lin, H. S. (2014). At the nexus of cybersecurity and public policy. *Computer Science and Telecommunications Board. National Research Council, Washington DC: The National Academies Press*.

Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A. R. (2014). On the (in)security of mobile two-factor authentication. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8437*. https://doi.org/10.1007/978-3-662-45472-5_24

Equifax. (2017). *Equifax Data Breach Summar*.

Gupta, C. (2017). The Market's Law of Privacy: Case Studies in Privacy and Security Adoption. *IEEE Security and Privacy*, *15*(3). https://doi.org/10.1109/MSP.2017.57

International Organization for Standardization (ISO). (2013). *Information technology – Security techniques – Information security management systems – Requirements*.

Jeon, W., Kim, J., Nam, J., Lee, Y., & Won, D. (2012). An enhanced secure authentication scheme with anonymity for wireless environments. *IEICE Transactions on Communications*, *95*(7), 2505–2508.

National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical*

Infrastructure Cybersecurity.
Sugiyono, P. D. (2017). Metode penelitian bisnis: pendekatan kuantitatif, kualitatif, kombinasi, dan R&D. *Penerbit CV. Alfabeta: Bandung*, *225*.
Symantec. (2017). *2017 Internet Security Threat Report*.
Tokopedia. (2020). *Pernyataan Resmi mengenai Kebocoran Data pada Mei 2020*.
Zuech, N., & Yardley, P. A. (2010). Machine Vision—Does the Technology Satisfy the Marketplace. A Panel Discussion. In *Machine Vision for Three-Dimensional Scenes* (pp. 399–403). Academic Press.