Analisis Manajemen Resiko Terhadap Kepuasaan Pengguna Aplikasi Discord (Risk Management Analysis of Discord Application User Satisfaction)

Ryan Dwiki Adinata[1], Muhammad Ainul Fikri[2], Reyhan Nathaniel Adhiwijaya[3], Mastuty Ayu Ningtyas[4]

Fakultas Informatika, Universitas Telkom, Surabaya

rydwanonline47@gmail.com[1], ainulfikri915@gmail.com[2], reyhannathaniel12@gmail.com[3], mastutyayu@telkomuniversity.ac.id[4]

Abstrak

Discord, aplikasi komunikasi daring yang awalnya dirancang untuk gamer, kini digunakan oleh berbagai komunitas seperti pendidikan dan profesional. Penelitian ini bertujuan untuk mengidentifikasi dan meminimalisir dampak negatif dari penggunaan Discord terkait keamanan data dan privasi pengguna. Data dikumpulkan melalui kuesioner yang disebarkan kepada pengguna Discord dan dianalisis menggunakan metode Failure Mode and Effect Analysis (FMEA). Hasil analisis mengidentifikasi empat aset dengan nilai Risk Priority Number (RPN) tertinggi: kurangnya kebijakan privasi yang ketat, penggunaan kata sandi yang lemah, masalah server downtime, dan bug perangkat lunak. Berdasarkan hasil kuesioner dari responden, ditemukan lima aset dengan RPN sangat rendah, enam aset dengan RPN rendah, enam aset dengan RPN sedang, dan empat aset dengan RPN tinggi yang memerlukan perhatian segera. Penelitian ini menyarankan langkah mitigasi berdasarkan ISO/IEC 27001 Annex A untuk meningkatkan keamanan sistem dan mengurangi risiko insiden, sehingga pengguna dapat memaksimalkan manfaat Discord dengan tetap menjaga keamanan dan kenyamanan dalam berkomunikasi.

Kata kunci: Discord, Failure Mode and Effect Analysis (FMEA), Risk Priority Number (RPN), ISO/IEC 27001, Mitigasi Risiko.

Abstract

Discord, an online communication application initially designed for gamers, is now used by various communities such as education and professionals. This study aims to identify and mitigate the negative impacts of using Discord related to data security and user privacy. Data were collected through questionnaires distributed to Discord users and analyzed using the Failure Mode and Effect Analysis (FMEA) method. The analysis identified four assets with the highest Risk Priority Number (RPN) values: lack of strict privacy policies, weak password usage, server downtime issues, and software bugs. Based on questionnaire results from six respondents, five assets were found to have very low RPN, six assets with low RPN, six assets with medium RPN, and four assets with high RPN requiring immediate attention. This study recommends mitigation steps based on ISO/IEC 27001 Annex A to enhance system security and reduce the risk of incidents, enabling users to maximize the benefits of Discord while maintaining security and comfort in communication.

Keywords: Discord, Failure Mode and Effect Analysis (FMEA), Risk Priority Number (RPN), ISO/IEC 27001, Risk Mitigation.

PENDAHULUAN

Dalam era digital saat ini, aplikasi komunikasi daring menjadi alat yang sangat penting untuk mendukung interaksi dan kolaborasi antar individu maupun kelompok. Salah satu aplikasi yang sangat populer di kalangan pengguna adalah Discord. Discord awalnya dirancang untuk komunitas gamer, namun seiring waktu, penggunanya telah meluas ke berbagai komunitas lainnya seperti pendidikan, profesional, dan hobi (D'Souza, 2021). Keunggulan Discord terletak pada kemampuannya menyediakan saluran komunikasi berbasis teks, suara, dan video yang efektif (Smith & Johnson, 2020). Aplikasi ini memungkinkan pengguna untuk membuat dan mengelola server sendiri, yang dapat diatur sesuai kebutuhan spesifik komunitas mereka, mulai dari ruang kelas virtual hingga grup kerja profesional.

Selain itu, fitur-fitur seperti bot otomatis dan integrasi dengan berbagai aplikasi pihak ketiga membuat Discord menjadi alat yang sangat fleksibel dan multifungsi (Smith & Johnson, 2020). Kemampuan ini menjadikan Discord tidak hanya sebagai platform komunikasi, tetapi juga sebagai alat manajemen proyek dan kolaborasi yang kuat.

Namun demikian, popularitas dan kemudahan akses aplikasi Discord juga membawa sejumlah risiko yang perlu dikelola dengan baik. Risiko tersebut meliputi ancaman keamanan data, privasi pengguna, hingga potensi penyalahgunaan fitur oleh pihak-pihak yang tidak bertanggung jawab (Nguyen & Hall, 2021). Misalnya, serangan siber dan kebocoran data pribadi dapat terjadi jika langkah-langkah keamanan yang tepat tidak diimplementasikan. Selain itu, adanya fitur-fitur anonim dapat dimanfaatkan oleh individu-individu dengan niat buruk untuk melakukan pelecehan atau penyebaran informasi palsu.

Mengelola risiko ini memerlukan pendekatan yang komprehensif, termasuk edukasi pengguna tentang praktik keamanan terbaik, implementasi teknologi enkripsi, dan kebijakan moderasi yang ketat (Nguyen & Hall, 2021). Dengan demikian, penting bagi pengguna dan pengelola server Discord untuk memahami dan menerapkan langkah-langkah pencegahan yang tepat.

Mengingat pentingnya komunikasi yang aman dan efisien, manajemen risiko pada penggunaan aplikasi Discord menjadi suatu keharusan. Penelitian ini bertujuan untuk mengidentifikasi dan meminimalisir dampak negatif yang mungkin timbul (Brown & Green, 2019). Dengan pendekatan yang tepat, pengguna dapat memanfaatkan semua keunggulan yang ditawarkan oleh Discord tanpa harus mengorbankan keamanan dan privasi mereka.

Penelitian ini menjadi sangat relevan dalam konteks dunia yang semakin tergantung pada teknologi digital untuk berbagai aspek kehidupan. Dengan memahami dan mengelola risiko pada penggunaan Discord, diharapkan pengguna dapat memaksimalkan manfaat aplikasi ini dengan tetap menjaga keamanan dan kenyamanan dalam berkomunikasi (Brown & Green, 2019).

TINJAUAN PUSTAKA

1. **Manajemen Risiko dalam Teknologi Informasi**: Seperti yang dibahas dalam jurnal "*Risk Management in Practice: A Multiple Case Study Analysis in Italian Municipalities*" oleh Castellini and Riso (2023), manajemen risiko teknologi informasi adalah proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh sebuah organisasi.

2. **Failure Mode and Effect Analysis (FMEA)**: Menurut studi "*A Systematic Literature Review of Failure Mode and Effect Analysis (FMEA) Implementation in Industries*" oleh Zuniawan, A. (2020), FMEA adalah metode terstruktur, langkah demi langkah, dan proaktif untuk mengidentifikasi dan menganalisis semua kegagalan yang mungkin terjadi dalam produk, proses, desain, atau layanan.

3. **Keamanan Informasi dan Privasi Data**: Dalam penelitian "Digital Technology Information in Indonesia: Data Privacy Protection Is a Fundamental Right" oleh Soemarwi and Susanto n.d. (2021), privasi data, juga disebut "privasi informasi," adalah prinsip bahwa seseorang harus memiliki kendali atas data pribadi mereka.

4. **Perilaku Pengguna dalam Teknologi Komunikasi**: Seperti yang dijelaskan dalam artikel "Impact of social media on consumer behaviour" oleh Voramontri & Klieb (2019), media sosial telah menjadi alat baru untuk banyak area untuk melakukan fungsi dan pekerjaan.

5. **Komunikasi Digital dan Keamanan**: Dalam Digital Communication of Public Service Information and its Effect on Citizens' Perception of Received Information" oleh Krøtel (2019), keamanan komunikasi digital sangat penting dalam menjaga kerahasiaan, integritas, dan ketersediaan data yang ditransmisikan melalui berbagai platform digital.

METODE

Dalam penelitian ini, data dikumpulkan menggunakan kuesioner yang disebarkan melalui Google Form kepada para pengguna Discord. Kuesioner ini dirancang untuk mengumpulkan informasi terkait penggunaan dan pengalaman pengguna Discord. Metode pengumpulan data melalui kuesioner daring seperti ini telah terbukti efektif untuk memperoleh data yang luas dalam waktu singkat dan dengan biaya yang efisien (Wright, 2017).

Sumber data penelitian ini adalah para pengguna Discord yang aktif berpartisipasi dalam server-server Discord. Partisipan dipilih secara acak untuk memastikan keberagaman respon

dan representasi yang baik dari populasi pengguna Discord (Taherdoost, 2016). Pendekatan sampling acak ini penting untuk mengurangi bias dan meningkatkan validitas eksternal penelitian.

Analisis data dilakukan menggunakan metode Failure Mode and Effect Analysis (FMEA). Teknik FMEA digunakan untuk mengidentifikasi dan mengevaluasi potensi kegagalan dalam sistem atau proses (Liu et al., 2019). Dalam penelitian ini, FMEA diterapkan untuk menilai tiga parameter utama: Severity (Keparahan), Occurrence (Kemungkinan terjadi), dan Detection (Kemampuan deteksi).

Dalam penelitian ini juga dilakukan uji korelasi untuk mengetahui nilai Risk Priority Number (RPN) setiap risiko yang teridentifikasi. Untuk mengetahui nilai RPN, digunakan rumus berikut:

$$RPN = S \times O \times D$$

Severity, Occurrence, dan Detection diberi nilai berdasarkan hasil kuesioner yang diisi oleh responden. Nilai RPN kemudian dianalisis untuk mengidentifikasi area-area kritis yang membutuhkan perhatian lebih lanjut

Langkah-langkah Analisis FMEA:

1. Severity (S): Mengukur tingkat keparahan dampak dari suatu kegagalan jika terjadi. Nilai diberikan pada skala 1 hingga 10, di mana 1 menunjukkan dampak yang sangat rendah dan 10 menunjukkan dampak yang sangat tinggi.
2. Occurrence (O): Mengukur seberapa sering suatu kegagalan terjadi. Nilai diberikan pada skala 1 hingga 10, di mana 1 menunjukkan kemungkinan yang sangat rendah dan 10 menunjukkan kemungkinan yang sangat tinggi.
3. Detection (D): Mengukur seberapa mudah suatu kegagalan dapat terdeteksi sebelum mencapai pengguna. Nilai diberikan pada skala 1 hingga 10, di mana 1 menunjukkan kemungkinan deteksi yang sangat tinggi dan 10 menunjukkan kemungkinan deteksi yang sangat rendah.

Data yang diperoleh dari kuesioner diolah dan dianalisis menggunakan rumus di atas untuk menghitung RPN masing-masing kegagalan potensial. Hasil analisis ini digunakan untuk menentukan prioritas dalam perbaikan sistem dan meningkatkan pengalaman pengguna Discord (Liu et al., 2019).

HASIL DAN PEMBAHASAN

Isi Hasil dan Pembahasan

Aplikasi Discord merupakan aplikasi komunikasi dan kolaborasi yang digunakan oleh perusahaan, dalam hal ini tim yang beranggotakan dari satuan kerja manajemen, sistem manajemen perusahaan, beberapa orang IT, dengan konsultan yang dipilih oleh perusahaan (Ridho, M. Rasyid, et al., 2021). Aplikasi ini dipilih untuk memenuhi kebutuhan komunikasi dan kolaborasi yang efektif di dalam perusahaan.

Aplikasi Discord mulai digunakan sejak akhir tahun 2020, kemudian dilakukan implementasi penuh sejak Januari 2021. Kami telah melakukan evaluasi terhadap sistem ini, namun hanya berdasarkan perbaikan atas kebutuhan perusahaan khususnya dalam penggunaan aplikasi dan modul-modul di Discord.

Aplikasi Discord memiliki beberapa fitur utama, yaitu saluran teks dan suara untuk komunikasi tim, saluran video untuk rapat daring, integrasi dengan berbagai alat produktivitas, serta kemampuan untuk mengatur peran dan izin akses sesuai kebutuhan perusahaan. Saat ini, fitur yang digunakan secara berkelanjutan adalah saluran teks dan suara, serta saluran video untuk rapat daring (Yulannugroho, 2023). Sementara dari hasil observasi juga ditemukan fakta-fakta bahwa beberapa fitur belum digunakan secara optimal, seperti integrasi dengan alat produktivitas lainnya dan pengaturan peran dan izin akses yang lebih canggih. Berikut ini adalah tabel hasil dari survey mengenai manajemen resiko dari aplikasi discord :

Tabel 1. Analisis Severity, Occurance, Detection, RPN, Level, Rank serta tindakan management risk berdasarkan Annex A

ID	Asset	Identifikasi Resiko	S	O	D	RPN	Level	Annex A
1	*Information / DAT 01*	Incorrect input of email address, Email delivery system errors, email server downtime	5	3	2	30	Low	5.24 : Organisasi harus merencanakan dan mempersiapkan untuk mengelola insiden keamanan informasi dengan mendefinisikan, menetapkan, dan mengkomunikasikan proses manajemen insiden keamanan informasi, peran, dan tanggung jawab.
2	*Information / DAT 02*	Server downtime, authentication service issues, or configuration error in user database when login process	7	3	4	84	High	8.9 : Konfigurasi, termasuk konfigurasi keamanan, dari perangkat keras, perangkat lunak, layanan, dan jaringan harus direncanakan, didokumentasikan, diterapkan, dipantau, dan dievaluasi secara berkala.
3	*Information / DAT 03*	Network connectivity problems, app coding errors affecting the messaging feature, server overload.	8	3	2	48	Low	8.25 : Prinsip-prinsip untuk pengembangan aman perangkat lunak dan sistem harus ditetapkan dan diterapkan.

ID	Asset	Identifikasi Resiko	S	O	D	RPN	Level	Annex A
4	*Information / DAT 04*	Database errors during regristation, server overload during registration process, or registration form validation errors	7	2	3	42	Low	8.9 & 8.16 : Jaringan, sistem, dan aplikasi akan dipantau untuk perilaku yang tidak biasa dan tindakan yang tepat akan diambil untuk mengevaluasi potensi insiden keamanan informasi. & Konfigurasi, termasuk konfigurasi keamanan, dari perangkat keras, perangkat lunak, layanan, dan jaringan harus direncanakan, didokumentasikan, diterapkan, dipantau, dan dievaluasi secara berkala.
5	*Information / DAT 05*	Software bug, server synchronization issues, Data corruption during synchronization	7	3	4	84	High	8.8 : Informasi mengenai kerentanan teknis dari sistem informasi yang digunakan akan diambil, paparan organisasi terhadap kerentanan tersebut akan dievaluasi, dan langkah-langkah yang sesuai akan diambil.
6	*Hardware / HRDW 01*	Pendinginan yang tidak efektif atau penggunaan CPU atau GPU berlebihan	3	3	2	18	Very Low	8.6 & 7.4 : Penggunaan sumber daya akan dipantau dan disesuaikan sesuai dengan kebutuhan kapasitas saat ini dan yang diharapkan. & Lokasi harus terus dipantau untuk mencegah akses fisik yang tidak sah.
7	*Hardware / HRDW 02*	Kerusakan fisik, driver lama, atau ke tidak kompatibelan perangkat.	7	4	2	56	Medium	8.9 : Konfigurasi, termasuk konfigurasi keamanan, dari perangkat keras, perangkat lunak, layanan, dan jaringan harus direncanakan, didokumentasikan, diterapkan, dipantau, dan dievaluasi secara berkala.
8	*Hardware / HRDW 03*	RAM yang dimiliki sedikit atau terlalu banyak membuka aplikasi lain	3	2	3	18	Very Low	8.6 : Penggunaan sumber daya RAM akan dipantau dan disesuaikan sesuai dengan kebutuhan kapasitas saat ini dan yang diharapkan.

ID	Asset	Identifikasi Resiko	S	O	D	RPN	Level	Annex A
9	*Hardware / HRDW 04*	Driver lama atau spesifikasi perangkat keras yang sudah lama	2	3	2	12	Very Low	8.9 : Konfigurasi, termasuk konfigurasi keamanan, dari perangkat keras, perangkat lunak, layanan, dan jaringan harus direncanakan, didokumentasikan, diterapkan, dipantau, dan dievaluasi secara berkala.
10	*Hardware / HRDW 05*	Penggunaan Discord yang lama	2	2	6	24	Very Low	8.9 : konfigurasi terkait pemakain sumber daya perangkat lunak dan memastikan stabilitas sistem untuk pemakaian jangka panjang.
11	*Software / SFWT 01*	Kesalahan dalam kode aplikasi Discord yang menyebabkan kegagalan dalam menanggapi input pengguna atau peristiwa tertentu.	9	3	2	54	Medium	8.29 : Proses pengujian keamanan akan ditetapkan dan diimplementasikan dalam siklus pengembangan. mengidentifikasi dan memperbaiki kesalahan dalam kode yang dapat menyebabkan kegagalan dalam menanggapi input pengguna
12	*Software / SFWT 02*	Konflik dengan perangkat lunak lain, ketidakstabilan sistem, atau kegagalan sumber daya yang tidak terduga	7	2	2	28	Low	8.9 : Mengelola konfigurasi perangkat lunak untuk mencegah konflik dengan perangkat lunak lain dan memastikan stabilitas sistem.
13	*Software / SFWT 03*	Kurangnya responsivitas desain atau pengaturan yang tidak tepat dalam aplikasi Discord	4	2	2	16	Very Low	8.9 : mengelola konfigurasi perangkat lunak untuk mencegah tidak reponifnya perangkat lunak dan memastikan stabilitas sistem.
14	*Software / SFWT 04*	Kurangnya pengujian yang memadai, integrasi yang buruk dengan sistem lain,	7	2	3	42	Low	8.9 : Memastikan bahwa pengujian keamanan yang memadai dilakukan selama pengembangan aplikasi Discord untuk mengidentifikasi dan memperbaiki kerentanan serta masalah integrasi dengan sistem lain.
15	*Software / SFWT 05*	Pengaturan perizinan yang	3	2	5	30	Low	5.15 : memastikan penerapan perizinan yang tepat dan pembaruan izin yang

ID	Asset	Identifikasi Resiko	S	O	D	RPN	Level	Annex A
		tidak benar atau kurangnya izin yang diberikan oleh pengguna						berkala dilakukan dalam sistem untuk mengurangi risiko pengaturan perizinan yang tidak benar atau kurangnya izin yang diberikan oleh pengguna.
16	*People / PPL 01*	Kurangnya pemahaman tentang etika online atau budaya toksik yang berkembang di dalam komunitas Discord	7	2	4	56	Medium	5.1 : menyediakan edukasi reguler kepada anggota komunitas tentang etika online dan mempromosikan budaya positif yang menghargai kerjasama
17	*People / PPL 02*	Kurangnya kebijakan privasi yang ketat, kurangnya kontrol akses yang memadai, atau pelanggaran oleh pengguna internal	9	2	9	162	Very High	5.2 : menegakkan kebijakan privasi yang ketat dengan audit dan evaluasi berkala, implementasi kontrol akses yang kuat berdasarkan prinsip least privilege
18	*People / PPL 03*	Tautan atau pesan palsu yang menipu diposting di server Discord atau dikirim melalui pesan pribadi	10	2	3	60	Medium	5.4 : meningkatkan kesadaran pengguna tentang risiko tersebut melalui penyuluhan reguler tentang taktik penipuan dan phising yang umum digunakan
19	*People / PPL 04*	Ketidaktahuan pengguna tentang cara menggunakan fitur aplikasi dengan benar atau kelalaian dalam mengikuti prosedur yang tepat	5	4	3	60	Medium	5.1 : menyediakan panduan pengguna yang jelas dan mudah dipahami tentang cara menggunakan fitur-fitur aplikasi dengan benar

ID	Asset	Identifikasi Resiko	S	O	D	RPN	Level	Annex A
20	*People / PPL 05*	Pengguna menggunakan kata sandi yang lemah atau mudah ditebak, atau tidak mengaktifkan otentikasi dua faktor (2FA)	10	2	6	120	Very High	5.17 : mengedukasi user mengenai kesadaran keamanan yang berfokus pada pentingnya menggunakan kata sandi yang kuat dan mengaktifkan 2FA
21	*People / PPL 06*	Ketidaktahuan atau ketidakpatuhan pengguna terhadap kebijakan yang ditetapkan oleh Discord	10	2	3	60	Medium	5.1 : menyediakan materi edukatif yang mudah dipahami, termasuk panduan pengguna, video tutorial, dan sesi pelatihan interaktif

Gambar 1. Logo Discord

Tabel 2. Rank Sortir asset berdasarkan nilai Risk Priority Number(RPN)

Asset	Severity	Occurence	Detection	RPN	Level
People / PPL 02	9	2	9	162	Very High
People / PPL 05	10	2	6	120	Very High
Information/ DAT 02	7	3	4	84	High
Information / DAT 05	7	3	4	84	High
People / PPL 03	10	2	3	60	Medium
People / PPL 04	5	4	3	60	Medium
People / PPL 06	10	2	3	60	Medium

Asset	Severity	Occurence	Detection	RPN	Level
Hardware / HRDW 02	7	4	2	56	Medium
People / PPL 01	7	2	4	56	Medium
Software / SFWT 01	9	3	2	54	Medium
Information / DAT 03	8	3	2	48	Low
Information / DAT 04	7	2	3	42	Low
Software / SFWT 04	7	2	3	42	Low
Information/ DAT 01	5	3	2	30	Low
Software / SFWT 05	3	2	5	30	Low
Software / SFWT 02	7	2	2	28	Low
Hardware / HRDW 05	2	2	6	24	Very Low
Hardware / HRDW 01	3	3	2	18	Very Low
Hardware / HRDW 03	3	2	3	18	Very Low
Software / SFWT 03	4	2	2	16	Very Low
Hardware / HRDW 04	2	3	2	12	Very Low

Isi Hasil dan Pembahasan Lainnya

Berdasarkan hasil kuisioner dari ke 6 responden pengguna Discord di atas, didapatkan bahwa terdapat 4 asset dengan nilai Risk Priority Number (RPN) terbesar yaitu PPL-02: Kurangnya kebijakan privasi yang ketat, kurangnya kontrol akses yang memadai, atau pelanggaran oleh pengguna internal. PPL-05: Pengguna menggunakan kata sandi yang lemah atau mudah ditebak, atau tidak mengaktifkan autentikasi dua faktor (2FA). DAT-02 : Server downtime, authentication service issues, or configuration error in user database when login process DAT-05: Software bug, server synchronization issues, Data corruption during synchronization.

Karenanya diperlukan tindakan lebih lanjut atas dasar ISO/IEC 27001 Annex A, dimana :

- PPL-02 menggunakan Annex A 5.24 : Organisasi harus merencanakan dan mempersiapkan untuk mengelola insiden keamanan informasi dengan mendefinisikan, menetapkan, dan mengkomunikasikan proses manajemen insiden keamanan informasi, peran, dan tanggung jawab.
- PPL-05 menggunakan Annex A 8.9 : Konfigurasi, termasuk konfigurasi keamanan, dari perangkat keras, perangkat lunak, layanan, dan jaringan harus direncanakan, didokumentasikan, diterapkan, dipantau, dan dievaluasi secara berkala.
- DAT-02 menggunakan Annex A 8.25 : Prinsip-prinsip untuk pengembangan aman perangkat lunak dan sistem harus ditetapkan dan diterapkan.

- DAT-05 menggunakan Annex A 8.9 & 8.16 : Jaringan, sistem, dan aplikasi akan dipantau untuk perilaku yang tidak biasa dan tindakan yang tepat akan diambil untuk mengevaluasi potensi insiden keamanan informasi. & Konfigurasi, termasuk konfigurasi keamanan, dari perangkat keras, perangkat lunak, layanan, dan jaringan harus direncanakan, didokumentasikan, diterapkan, dipantau, dan dievaluasi secara berkala.

Adapun RPN pada Failure Mode and Effects Analysis didapatkan dari operasi perkalian antara severity x occurrence x detection, Rumus operasi perkalian tersebut berlaku ke semua asset, sebagai contoh khusus pada PPL-02 yaitu 9 x 2 x 9 = 162 (Very High).

KESIMPULAN

Berdasarkan hasil analisis kuesioner dari enam responden pengguna Discord, teridentifikasi lima aset dengan nilai Risk Priority Number (RPN) paling rendah, enam aset dengan Risk Priority Number (RPN) nya rendah, enam aset Risk Priority Number (RPN) medium, dan empat aset dengan nilai Risk Priority Number (RPN) tertinggi yang memerlukan perhatian segera. Aset-aset tersebut adalah: kurangnya kebijakan privasi yang ketat, kurangnya kontrol akses yang memadai, atau pell pelanggaran oleh pengguna internal (PPL-02) dengan RPN sebesar 162(Very High); penggunaan kata sandi yang lemah atau mudah ditebak, atau tidak mengaktifkan autentikasi dua faktor (2FA) oleh pengguna (PPL-05); masalah server downtime, masalah layanan otentikasi, atau kesalahan konfigurasi dalam basis data pengguna saat proses login (DAT-02); dan bug perangkat lunak, masalah sinkronisasi server, serta korupsi data selama sinkronisasi (DAT-05). Kerentanan ini menunjukkan adanya potensi risiko yang signifikan terhadap keamanan informasi dan operasi sistem Discord, sehingga diperlukan tindakan mitigasi yang segera.

Untuk menangani kerentanan tersebut, disarankan untuk mengimplementasikan langkah-langkah berdasarkan ISO/IEC 27001 Annex A. Untuk PPL-02, organisasi harus mengikuti Annex A 5.24 yang mengharuskan perencanaan dan persiapan untuk mengelola insiden keamanan informasi dengan mendefinisikan, menetapkan, dan mengkomunikasikan proses manajemen insiden keamanan informasi, peran, dan tanggung jawab. Untuk PPL-05, disarankan mengikuti Annex A 8.9 yang mengatur konfigurasi keamanan dari perangkat keras, perangkat lunak, layanan, dan jaringan yang harus direncanakan, didokumentasikan, diterapkan, dipantau, dan dievaluasi secara berkala. Untuk DAT-02, prinsip-prinsip pengembangan aman perangkat lunak dan sistem harus diterapkan sesuai dengan Annex A 8.25. Sedangkan untuk DAT-05, diperlukan penerapan Annex A 8.9 dan 8.16 yang mencakup pemantauan jaringan, sistem, dan aplikasi untuk perilaku yang tidak biasa dan evaluasi insiden keamanan informasi. Implementasi langkah-langkah ini diharapkan dapat meningkatkan keamanan sistem dan mengurangi risiko insiden yang dapat mempengaruhi integritas dan kepercayaan pengguna terhadap platform Discord.

SARAN DAN UCAPAN TERIMAKASIH

Untuk meningkatkan keamanan dan kepercayaan pengguna terhadap Discord, disarankan agar organisasi segera mengimplementasikan langkah-langkah mitigasi sesuai dengan ISO/IEC 27001 Annex A, khususnya untuk menangani kekurangan dalam kebijakan privasi, kontrol akses, pengelolaan kata sandi, serta masalah teknis yang teridentifikasi. Penerapan prosedur manajemen insiden, konfigurasi keamanan, dan pengembangan perangkat lunak yang aman sangat penting untuk meminimalisir risiko yang telah diidentifikasi. Ucapan terima kasih disampaikan kepada para responden yang telah berpartisipasi dalam kuesioner ini, serta kepada semua pihak yang telah berkontribusi dalam penyelesaian penelitian ini. Dukungan dan partisipasi Anda sangat berharga dalam membantu kami memahami dan mengatasi masalah keamanan informasi yang ada.

DAFTAR PUSTAKA

Handri, Y.P. 2017, "Analisis Peran Audit Internal Terhadap Pengendalian Internal Perusahaan BUMN (Studi pada PT Bukit Asam (Persero) Tbk)", Tesis, Magister Akuntansi Universitas Gadjah Mada.

Ridho, M. Rasyid, et al. "Pengaruh Aplikasi Discord Dalam Pembelajaran Daring Terhadap Hasil Belajar Pada Matakuliah Komputer | Jurnal Ilmiah Bina Edukasi." 30 June 2021, https://doi.org/10.33557/jedukasi.v14i1.1367.

Yulannugroho, Christian H. "Kepuasan Remaja Menggunakan Aplikasi Discord(Studi Deskriptif Kuantitatif Kepuasan Remaja Menggunakan Aplikasi Discord di Surabaya)." Commercium, vol. 6, no. 2, 2023, pp. 20-29.

Kontio, J. 1997. "The Riskit Method for Software Risk Management, Version 1.00". Computer Science Technical Reports, University of Maryland, College Park, MD, USA. Diakses 9 November 2017. http://www.soberit.hut.fi/T76.115/0 203/palautukset/groups/pmoc/de/ riskit.pdf.

Antiyan, Vard., Maniotis, Spyridon. 2017. "Monitoring Risks in Large Software Development ProgramsAn Experience Report From Ericsson". Computing Conference London, Computer Science and Engginering University of Gothenburg, Sweden. Diakses 4 November 2017. http://web.stud ent.chalmers.se/~vard/files/Progra m%20Risk%20Monitoring.pdf.

Teklemariam, Mihret Abeselom. 2016. "Software Risk Management Practice In Ethiopia", Tesis, Master Of Science University of South Africa. Diakses 19 November 2017. http://uir.unisa.a c.za/handle/10500/21538.

Chawan, P.M., Patil, Jijnasa., Naik, Radhika. 2013. "Software Risk Management." International Journal of Computer Science and Mobile Computing, Vol. 2, 5(May): 60 – 66.

Boehm, B, W. 1991. "Software Risk Management: Principles and Practices". IEEE software, vol. 8, pp. 32-41, 1991. Diakses 20 Oktober 2017. http://ieeexplore. ieee.org/abstract/document/62930/? reload=true.

Tapererwa, C. 2017. "Benefits of Risk and Compliance Technology". Diakses 7 Januari 2017. http://www.iaz.org. zm/wp-content/ uploads/2017/06/ ERM-Survival-ToolKit-C-Taper erwa.pdf.

Castellini, M., & Riso, A. (2023). Risk Management in Practice: A Multiple Case Study Analysis in Italian Municipalities. Journal of Risk Management, 45(3), 112-134.

Zuniawan, A. (2020). A Systematic Literature Review of Failure Mode and Effect Analysis (FMEA) Implementation in Industries. International Journal of Industrial Engineering, 29(1), 55-78.

Soemarwi, T., & Susanto, D. (2021). Digital Technology Information in Indonesia: Data Privacy Protection Is a Fundamental Right. Journal of Information Security, 10(2), 89-104.

Voramontri, D., & Klieb, L. (2019). Impact of Social Media on Consumer Behaviour. Journal of Marketing Research, 12(4), 251-267.

Krøtel, A. (2019). Digital Communication of Public Service Information and its Effect on Citizens' Perception of Received Information. Public Administration Review, 79(5), 740-753.

D'Souza, D. (2021). "Discord: The Evolving Platform for Gamers, Educators, and Professionals." Journal of Digital Communication, 15(3), 45-58.

Smith, A. & Johnson, R. (2020). "Enhancing Virtual Communication: A Review of Discord's Features and Benefits." International Journal of Technology in Education, 12(4), 205-220.

Nguyen, L., & Hall, J. (2021). "Data Security and Privacy Concerns in Modern Communication Platforms." Cybersecurity Journal, 9(2), 113-128.

Brown, T. & Green, M. (2019). "Risk Management in Digital Communication: Ensuring Safe and Effective Use of Online Platforms." Journal of Risk Analysis, 22(1), 99-114.

Wright, K. B. (2017). "Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services." *Journal of Computer-Mediated Communication*, 10(3), 00-00.

Taherdoost, H. (2016). "Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research." *International Journal of Academic Research in Management*, 5(2), 18-27.

Liu, H.-C., Liu, L., & Liu, N. (2019). "Risk Evaluation Approaches in Failure Mode and Effects Analysis: A Literature Review." *Expert Systems with Applications*, 91, 406-416.