Jurnal Finansial dan Evaluasi Pasar Modal
Volume: 1, Nomor: 2, Agustus (2026), 138 - 149
Website: https://ejournal.lppnusantara.com/index.php/jfep/article/view/904
EISSN: 3124-7067; DOI: https://doi.org/10.65244/jfep.v1i2.904

ANALISIS KRITIS TERHADAP KELEMAHAN DESAIN DATABASE DALAM MENINGKATKAN RISIKO KEBOCORAN DATA DAN MENURUNKAN INTEGRITAS SISTEM INFORMASI

Abel Bangun [1], Muhammad Irwan Padli Nasution [2]
Program Studi Manajemen, Fakultas Ekonomi Bisnis Islam, Universitas Islam Negeri Sumatera Utara
Corresponding Author: abelbangun144@gmail.com, irwannst@uinsu.ac.id

Info Artikel
Submitted: *04 Mei 2026*
Revised : *09 Juni 2026*
Accepted: *19 Juni 2026*
Published: *25 Juni 2026*

Keywords: *Database Design, Data Breach, Information System Integrity, Database Security, SQL Injection, Database Normalization, Security by Design.*

Kata Kunci*: Desain Database, Kebocoran Data, Integritas Sistem Informasi, Keamanan Database, SQL Injection, Normalisasi Database, Security by Design.*

Abstract
This study critically examines database design weaknesses in the context of modern information system security. Poor database design is one of the primary factors that increase data breach risks and degrade information system integrity in organizations. Through a Systematic Literature Review (SLR) of 35 scientific articles published between 2015 and 2024, this research identifies and classifies database design weaknesses into five main categories: (1) normalization and relational structure weaknesses, (2) insufficient access control and authentication, (3) lack of data encryption, (4) absence of audit trails and logging, and (5) inadequate backup and recovery procedures. Analysis results show that 78% of studied data breach cases were caused by weaknesses at the database design layer, not solely from external attacks. This study concludes that a Security by Design approach in database design is fundamental for protecting organizational data assets and maintaining user trust.

Abstrak
Penelitian ini mengkaji secara kritis kelemahan desain database dalam konteks keamanan sistem informasi modern. Desain database yang buruk merupakan salah satu faktor utama yang meningkatkan risiko kebocoran data dan menurunkan integritas sistem informasi pada organisasi. Melalui metode tinjauan literatur sistematis (Systematic Literature Review/SLR) terhadap 35 artikel ilmiah yang dipublikasikan antara tahun 2015 hingga 2024, penelitian ini mengidentifikasi dan mengklasifikasikan kelemahan desain database ke dalam lima kategori utama: (1) kelemahan normalisasi dan struktur relasional, (2) kurangnya kontrol akses dan autentikasi, (3) minimnya enkripsi data, (4) absennya audit trail dan logging, serta (5) ketiadaan prosedur backup dan recovery yang memadai. Hasil analisis menunjukkan bahwa 78% kasus kebocoran data yang diteliti disebabkan oleh kelemahan pada lapisan desain database, bukan semata-mata dari serangan eksternal. Penelitian ini menyimpulkan bahwa pendekatan Security by Design dalam perancangan database merupakan langkah fundamental untuk melindungi aset data organisasi dan menjaga kepercayaan pengguna. Implikasi praktis dari penelitian ini mencakup rekomendasi penerapan framework database security yang komprehensif mulai dari tahap perencanaan, implementasi, hingga pemeliharaan sistem.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Publisher: Lembaga Penerbit Penelitian Nusantara

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat telah menjadikan data sebagai salah satu aset paling berharga bagi organisasi di berbagai sektor. Dalam konteks ini, database berperan sebagai komponen utama dalam sistem informasi yang bertugas menyimpan, mengelola, dan menyediakan data secara terstruktur untuk mendukung berbagai proses bisnis dan pengambilan keputusan (Coronel & Morris, 2019). Kualitas sistem informasi secara keseluruhan sangat bergantung pada bagaimana database dirancang, dikelola, dan diamankan secara menyeluruh.

Namun demikian, masih banyak organisasi yang menghadapi permasalahan serius akibat desain database yang kurang optimal. Kelemahan dalam perancangan database, seperti tidak diterapkannya normalisasi dengan baik, kurangnya kontrol akses, serta minimnya mekanisme keamanan berlapis, dapat menyebabkan berbagai risiko serius termasuk redundansi data, inkonsistensi informasi, hingga kebocoran data (Elmasri & Navathe, 2016; Connolly & Begg, 2015). Dalam era digital saat ini, kebocoran data menjadi ancaman yang semakin meningkat seiring dengan berkembangnya metode dan teknik serangan siber yang semakin canggih.

Penelitian terbaru menunjukkan bahwa kelemahan dalam sistem database modern sering kali dimanfaatkan melalui serangan seperti SQL Injection dan eksploitasi hak akses yang tidak terkontrol, yang dapat menyebabkan akses ilegal terhadap data sensitif organisasi maupun individu (Riyanti et al., 2024; Tanjung & Nasution, 2024). Selain itu, kurangnya penerapan sistem keamanan yang terintegrasi sejak tahap desain juga menjadi faktor utama meningkatnya kerentanan terhadap kebocoran data (Iqbal et al., 2024). Hal ini menunjukkan bahwa permasalahan tidak hanya terletak pada penggunaan teknologi, tetapi juga pada perencanaan dan desain database itu sendiri.

Kelemahan desain database tidak hanya berdampak pada aspek keamanan, tetapi juga berpengaruh signifikan terhadap integritas sistem informasi secara keseluruhan. Data yang tidak konsisten, duplikat, atau tidak valid dapat mengurangi keakuratan informasi yang dihasilkan, sehingga berpotensi menimbulkan kesalahan fatal dalam pengambilan keputusan strategis (Silberschatz et al., 2019). Dalam jangka panjang, kondisi ini dapat menurunkan kepercayaan pengguna terhadap sistem serta menghambat kinerja dan daya saing organisasi di pasar global.

Laporan IBM Cost of Data Breach 2023 mencatat bahwa rata-rata biaya yang harus ditanggung organisasi akibat kebocoran data mencapai USD 4,45 juta per insiden, meningkat 15% dalam tiga tahun terakhir. Lebih mengkhawatirkan, sebagian besar insiden tersebut terjadi akibat kelemahan pada lapisan infrastruktur database yang seharusnya dapat dicegah dengan desain yang lebih baik. Fakta ini menggarisbawahi urgensi kajian mendalam tentang hubungan antara kualitas desain database dan risiko kebocoran data.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk: (1) mengidentifikasi dan mengklasifikasikan kelemahan desain database yang paling umum ditemukan dalam praktik, (2) menganalisis hubungan kausal antara kelemahan desain database dengan peningkatan risiko kebocoran data, (3) mengkaji dampak kelemahan desain database terhadap penurunan integritas sistem informasi, serta (4) merumuskan rekomendasi penerapan prinsip Security by Design dalam perancangan database.

2. TINJAUAN PUSTAKA

2.1 Konsep Desain Database

Desain database merupakan proses sistematis dalam mendefinisikan struktur, karakteristik, dan hubungan antar data dalam sebuah sistem manajemen basis data (Database Management System/DBMS). Menurut Coronel dan Morris (2019), desain database yang baik harus memenuhi empat kriteria utama: integritas data, konsistensi data, efisiensi penyimpanan, dan kemudahan pemeliharaan. Proses desain database umumnya melibatkan tiga tahapan utama, yaitu desain konseptual menggunakan Entity-Relationship Diagram (ERD), desain logis yang mencakup normalisasi, dan desain fisik yang mempertimbangkan aspek implementasi pada platform DBMS tertentu.

Normalisasi merupakan salah satu konsep fundamental dalam desain database relasional. Proses ini bertujuan untuk mengurangi redundansi data dan ketergantungan yang tidak diinginkan antar atribut dalam sebuah relasi (Elmasri & Navathe, 2016). Normalisasi dilakukan secara bertahap melalui serangkaian bentuk normal (Normal Form), mulai dari First Normal Form (1NF) hingga Boyce-Codd Normal Form (BCNF) atau bahkan Third Normal Form (3NF) yang merupakan standar minimum yang umumnya diterapkan dalam praktik industri.

2.2 Konsep Keamanan Database

Keamanan database merujuk pada mekanisme perlindungan yang diterapkan untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data dalam sebuah sistem basis data. Konsep CIA Triad ini menjadi landasan fundamental dalam membangun sistem keamanan database yang komprehensif (Stallings, 2018). Dalam praktiknya, keamanan database melibatkan berbagai lapisan perlindungan, mulai dari kontrol akses berbasis peran (Role-Based Access Control/RBAC), enkripsi data, audit logging, hingga pemantauan aktivitas database secara real-time.

Penelitian Hadi dan Kurniawan (2023) menunjukkan bahwa mayoritas pelanggaran keamanan database terjadi bukan karena kecanggihan serangan, melainkan karena celah yang terdapat dalam desain sistem itu sendiri. Fenomena ini sering disebut sebagai 'security debt', yakni akumulasi kerentanan keamanan yang timbul akibat keputusan desain yang tidak mempertimbangkan aspek keamanan sejak awal pengembangan sistem.

2.3 Integritas Sistem Informasi

Integritas sistem informasi mengacu pada kemampuan sistem untuk memastikan bahwa data yang tersimpan, diproses, dan ditransmisikan akurat, lengkap, dan konsisten setiap saat. Menurut Laudon dan Laudon (2020), integritas sistem informasi dipengaruhi oleh tiga faktor utama: kualitas desain database, mekanisme validasi input, dan prosedur kontrol perubahan data. Ketika integritas sistem informasi terganggu, organisasi dapat menghadapi konsekuensi serius mulai dari keputusan bisnis yang salah hingga pelanggaran regulasi data.

Framework COBIT 2019 yang dikembangkan oleh ISACA menyebutkan bahwa integritas informasi merupakan salah satu prinsip tata kelola teknologi informasi yang paling kritis. Organisasi yang gagal menjaga integritas sistem informasinya berisiko mengalami kerugian finansial, kerusakan reputasi, dan tuntutan hukum. Dalam konteks regulasi, General Data Protection Regulation (GDPR) di Eropa dan Undang-Undang Pelindungan Data Pribadi (UU PDP) di Indonesia mewajibkan organisasi untuk menerapkan langkah-langkah teknis yang memadai untuk menjaga integritas dan keamanan data pribadi.

3. METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan Systematic Literature Review (SLR) yang dikombinasikan dengan analisis kritis terhadap studi kasus. Metode SLR dipilih karena kemampuannya dalam mengumpulkan, mengevaluasi, dan mensintesis hasil penelitian secara sistematis dan reproducible, sehingga menghasilkan temuan yang komprehensif dan dapat dipertanggungjawabkan secara ilmiah (Kitchenham & Charters, 2007). Pendekatan ini memungkinkan peneliti untuk mengidentifikasi pola, tren, dan kesenjangan dalam literatur yang berkaitan dengan kelemahan desain database.

3.2 Prosedur Pengumpulan Data

Pengumpulan data dilakukan melalui pencarian terstruktur pada lima database akademik utama: IEEE Xplore, ACM Digital Library, Springer Link, Scopus, dan Google Scholar. Pencarian dilakukan menggunakan kombinasi kata kunci dalam Bahasa Indonesia dan Bahasa Inggris, meliputi: 'database design weakness', 'data breach', 'database security', 'SQL injection', 'data integrity', 'kelemahan database', dan 'kebocoran data'. Periode publikasi dibatasi antara tahun 2015 hingga 2024 untuk memastikan relevansi dengan perkembangan teknologi terkini.

Kriteria inklusi yang diterapkan mencakup: (1) artikel yang dipublikasikan di jurnal atau prosiding yang telah melalui proses peer review, (2) penelitian yang secara spesifik membahas kelemahan desain database dan implikasinya terhadap keamanan data, (3) studi kasus nyata yang didokumentasikan dengan metodologi yang jelas, dan (4) artikel yang tersedia dalam teks penuh. Sebaliknya, kriteria eksklusi meliputi artikel opini tanpa dukungan empiris, penelitian yang berfokus pada perangkat keras jaringan, serta duplikasi publikasi.

3.3 Proses Seleksi dan Analisis

Dari total 312 artikel yang diidentifikasi melalui pencarian awal, dilakukan proses seleksi bertahap menggunakan metode PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). Setelah penghapusan duplikat dan skrining berdasarkan judul dan abstrak, tersisa 87 artikel yang kemudian diseleksi lebih lanjut berdasarkan kriteria inklusi/eksklusi. Proses ini menghasilkan 35 artikel yang memenuhi seluruh kriteria dan dijadikan bahan analisis utama dalam penelitian ini.

Analisis dilakukan menggunakan pendekatan tematik induktif, di mana tema-tema utama diidentifikasi secara organik dari data yang ada. Setiap artikel dianalisis menggunakan

matriks ekstraksi data yang mencakup: jenis kelemahan database yang diidentifikasi, konteks implementasi, metode penelitian yang digunakan, temuan utama, dan rekomendasi yang diberikan. Hasil ekstraksi kemudian disintesis untuk menghasilkan klasifikasi komprehensif tentang kelemahan desain database dan dampaknya.

Tabel 1. Distribusi Artikel berdasarkan Database Sumber dan Tahun Publikasi

Database Sumber	2015-2017	2018-2020	2021-2022	2023-2024	Total
IEEE Xplore	3	4	3	2	12
ACM Digital Library	1	2	3	2	8
Springer Link	2	2	2	1	7
Scopus	1	1	2	2	6
Google Scholar	0	1	1	0	2
Total	**7**	**10**	**11**	**7**	**35**

4. HASIL PENELITIAN

4.1 Klasifikasi Kelemahan Desain Database

Berdasarkan analisis terhadap 35 artikel yang menjadi korpus penelitian ini, teridentifikasi lima kategori utama kelemahan desain database yang paling sering ditemukan. Kategori-kategori ini tidak berdiri sendiri, melainkan saling berinteraksi dan memperburuk satu sama lain, menciptakan ekosistem kerentanan yang kompleks dalam sebuah sistem informasi.

Kategori pertama adalah Kelemahan Normalisasi dan Struktur Relasional, yang ditemukan dalam 28 dari 35 artikel (80%). Kelemahan ini mencakup redundansi data yang

berlebihan akibat normalisasi yang tidak lengkap, ketergantungan fungsional yang tidak teridentifikasi, serta penggunaan atribut bernilai ganda (multi-valued attributes) yang menyulitkan pemrosesan query. Redundansi data tidak hanya membuang kapasitas penyimpanan, tetapi juga membuka peluang terjadinya anomali pembaruan yang dapat merusak konsistensi data.

Kategori kedua adalah Kelemahan Kontrol Akses dan Autentikasi, yang ditemukan dalam 30 dari 35 artikel (86%). Ini merupakan kategori paling kritis yang meliputi penggunaan akun database dengan hak akses berlebihan (excessive privileges), kurangnya segregasi peran pengguna, lemahnya mekanisme autentikasi, serta tidak adanya penerapan prinsip least privilege. Banyak aplikasi yang ditemukan menggunakan akun database tunggal dengan hak akses penuh (superuser), padahal seharusnya setiap komponen aplikasi hanya memiliki akses minimal yang dibutuhkan.

Kategori ketiga adalah Minimnya Enkripsi Data, yang teridentifikasi dalam 25 dari 35 artikel (71%). Kelemahan ini mencakup penyimpanan data sensitif dalam format plaintext, penggunaan algoritma enkripsi yang sudah usang atau lemah, serta tidak adanya enkripsi pada koneksi antara aplikasi dan database server. Data seperti kata sandi, nomor kartu kredit, dan informasi identitas pribadi seringkali disimpan tanpa enkripsi yang memadai, menjadikannya target empuk bagi penyerang.

Kategori keempat adalah Absennya Audit Trail dan Logging, yang ditemukan dalam 22 dari 35 artikel (63%). Tanpa mekanisme pencatatan aktivitas yang komprehensif, organisasi tidak dapat mendeteksi pelanggaran keamanan secara dini, mengidentifikasi sumber kebocoran data, atau memenuhi persyaratan kepatuhan regulasi. Penelitian menunjukkan bahwa rata-rata waktu yang dibutuhkan untuk mendeteksi pelanggaran keamanan database tanpa audit trail yang memadai mencapai 277 hari.

Kategori kelima adalah Ketiadaan Prosedur Backup dan Recovery yang Memadai, teridentifikasi dalam 19 dari 35 artikel (54%). Kelemahan ini tidak hanya berdampak pada ketersediaan data, tetapi juga pada integritas data setelah terjadinya insiden. Backup yang tidak konsisten, tidak terenkripsi, atau tidak diuji secara reguler dapat membuat proses pemulihan menjadi tidak efektif ketika benar-benar dibutuhkan.

Tabel 2. Ringkasan Kategori Kelemahan Desain Database dan Frekuensi Temuan

No.	Kategori Kelemahan	Sub-Kategori Utama	Frekuensi (n=35)	Persentase
1	Normalisasi & Struktur Relasional	Redundansi, anomali data	28	80%
2	Kontrol Akses & Autentikasi	Excessive privileges, SQL Injection	30	86%
3	Enkripsi Data	Plaintext storage, algoritma lemah	25	71%
4	Audit Trail & Logging	Tidak ada pencatatan aktivitas	22	63%
5	Backup & Recovery	Backup tidak konsisten/terenkripsi	19	54%

4.2 Dampak terhadap Risiko Kebocoran Data

Analisis terhadap studi kasus yang terdokumentasi dalam literatur menunjukkan korelasi yang kuat antara kelemahan desain database dan insiden kebocoran data nyata. Dari 23 studi kasus kebocoran data yang teridentifikasi dalam korpus penelitian ini, 18 kasus (78%) memiliki akar penyebab yang dapat ditelusuri kembali ke kelemahan pada lapisan desain database.

SQL Injection tetap menjadi vektor serangan yang paling merusak dan paling sering ditemukan, dengan 15 dari 23 studi kasus melibatkan kerentanan ini. Yang memprihatinkan, kerentanan SQL Injection pada dasarnya dapat sepenuhnya dicegah melalui praktik desain yang baik, termasuk penggunaan parameterized queries, stored procedures, dan validasi input yang ketat pada lapisan database. Fakta bahwa serangan ini masih berhasil menunjukkan bahwa masih banyak sistem yang dibangun tanpa mempertimbangkan keamanan sejak tahap desain.

Kelemahan kontrol akses menjadi faktor amplifikasi yang signifikan dalam menentukan dampak dari suatu insiden keamanan. Sistem yang menggunakan akun database dengan hak akses berlebihan terbukti mengalami kebocoran data dengan volume 3,7 kali lebih besar dibandingkan sistem yang menerapkan prinsip least privilege dengan baik. Hal ini menunjukkan bahwa meskipun serangan berhasil dilakukan, dampaknya dapat dibatasi secara signifikan melalui desain kontrol akses yang tepat.

5. PEMBAHASAN

5.1 Analisis Komparatif dengan Penelitian Terdahulu

Temuan penelitian ini secara umum sejalan dengan hasil penelitian terdahulu, namun juga mengungkapkan beberapa aspek baru yang belum banyak dibahas dalam literatur. Penelitian Riyanti et al. (2024) yang berfokus pada sistem informasi akademik di perguruan tinggi menemukan bahwa 82% sistem yang diteliti memiliki kelemahan pada lapisan kontrol akses, sebuah angka yang konsisten dengan temuan dalam penelitian ini (86%). Namun, penelitian tersebut kurang membahas dimensi integritas data sebagai konsekuensi dari kelemahan desain, sesuatu yang menjadi kontribusi penting dari penelitian ini.

Berbeda dengan penelitian Tanjung dan Nasution (2024) yang cenderung melihat masalah keamanan database dari perspektif serangan eksternal, penelitian ini mengambil sudut pandang yang lebih holistik dengan menekankan bahwa sebagian besar kerentanan bersumber dari kelemahan desain internal. Pendekatan ini konsisten dengan konsep 'shift-left security' yang semakin mendapat perhatian dalam komunitas pengembangan perangkat lunak modern, di mana pertimbangan keamanan harus dimulai sejak fase paling awal dalam siklus pengembangan sistem.

5.2 Implikasi terhadap Integritas Sistem Informasi

Hubungan antara kelemahan desain database dan integritas sistem informasi bersifat multidimensional. Pada level paling mendasar, normalisasi yang tidak sempurna menyebabkan anomali data yang secara langsung mengancam integritas faktual informasi. Ketika data yang sama disimpan di lebih dari satu lokasi dalam database tanpa mekanisme sinkronisasi yang tepat, inkonsistensi data menjadi tidak terhindarkan seiring waktu.

Pada level yang lebih kompleks, kurangnya mekanisme audit trail menciptakan situasi di mana organisasi tidak dapat memverifikasi keakuratan historis datanya. Ini menjadi masalah serius dalam konteks regulasi seperti GDPR dan UU PDP, yang mengharuskan organisasi untuk

dapat menunjukkan bahwa data yang mereka kelola akurat dan diproses secara sah. Tanpa audit trail yang komprehensif, pembuktian kepatuhan menjadi hampir mustahil dilakukan.

Aspek yang sering luput dari perhatian adalah dampak psikologis dari pelanggaran integritas data terhadap kepercayaan pengguna. Penelitian Martinez et al. (2022) menunjukkan bahwa kepercayaan pengguna terhadap sebuah sistem informasi mengalami penurunan rata-rata 67% setelah terjadinya insiden kebocoran data yang signifikan, dan hanya 23% pengguna yang sepenuhnya memulihkan kepercayaan mereka bahkan setelah organisasi mengumumkan langkah-langkah perbaikan. Ini menggarisbawahi bahwa biaya dari kelemahan desain database tidak hanya bersifat finansial dan teknis, tetapi juga menyangkut aset reputasi yang jauh lebih sulit untuk dipulihkan.

5.3 Pendekatan Security by Design sebagai Solusi

Sintesis dari temuan penelitian ini mengarah pada sebuah kesimpulan yang mendasar: kelemahan desain database sebagian besar dapat dicegah melalui penerapan konsisten pendekatan Security by Design (SbD) dalam seluruh tahapan pengembangan sistem informasi. Pendekatan ini, sebagaimana didefinisikan oleh OWASP (Open Web Application Security Project), melibatkan integrasi pertimbangan keamanan ke dalam setiap tahapan desain, mulai dari pemodelan ancaman (threat modeling), perancangan arsitektur keamanan, hingga pengujian keamanan yang komprehensif.

Dalam konteks desain database secara spesifik, penerapan SbD mencakup: (1) pemodelan ancaman terhadap data sensitif sebelum fase desain dimulai, (2) perancangan skema kontrol akses yang mengimplementasikan prinsip least privilege secara konsisten, (3) integrasi mekanisme enkripsi sebagai bagian dari skema database, bukan sebagai lapisan tambahan yang ditempelkan kemudian, (4) perancangan skema audit logging yang komprehensif, dan (5) perencanaan prosedur backup dan recovery sebagai bagian integral dari arsitektur sistem, bukan sebagai renungan belakangan.

Penerapan SbD membutuhkan perubahan paradigma dalam cara organisasi memandang keamanan database. Keamanan tidak boleh lagi dipandang sebagai overhead yang menghambat kecepatan pengembangan, melainkan sebagai investasi yang menghasilkan manfaat jangka panjang. Penelitian menunjukkan bahwa biaya untuk memperbaiki kerentanan keamanan yang ditemukan pada fase desain adalah 30 kali lebih murah dibandingkan memperbaikinya setelah sistem diproduksi, dan 100 kali lebih murah dibandingkan memperbaikinya setelah terjadinya insiden keamanan.

6. KESIMPULAN

Penelitian ini berhasil mengidentifikasi dan menganalisis lima kategori utama kelemahan desain database yang berkontribusi terhadap peningkatan risiko kebocoran data dan penurunan integritas sistem informasi. Temuan ini memiliki implikasi penting bagi para perancang sistem, pengembang perangkat lunak, dan pengambil keputusan di bidang teknologi informasi.

Kesimpulan pertama yang dapat ditarik adalah bahwa kelemahan desain database bersifat sistemis dan multidimensional. Tidak ada satu kelemahan tunggal yang dapat diidentifikasi sebagai penyebab tunggal insiden keamanan; sebaliknya, kerentanan cenderung muncul dari interaksi kompleks antara berbagai kelemahan desain yang saling memperburuk satu sama lain. Ini mengimplikasikan bahwa pendekatan perbaikan yang bersifat parsial atau reaktif tidak akan efektif dalam jangka panjang.

Kesimpulan kedua adalah bahwa sebagian besar insiden kebocoran data yang diteliti (78%) dapat dicegah melalui praktik desain database yang lebih baik. Ini merupakan temuan yang sekaligus mengkhawatirkan dan menggembirakan: mengkhawatirkan karena menunjukkan bahwa kerugian besar yang dialami organisasi seharusnya tidak perlu terjadi, tetapi menggembirakan karena menunjukkan bahwa masalah ini dapat diatasi dengan pengetahuan dan komitmen yang tepat.

Kesimpulan ketiga adalah bahwa penerapan pendekatan Security by Design dalam perancangan database merupakan strategi paling efektif untuk mengatasi kelemahan-kelemahan yang teridentifikasi. Investasi dalam desain yang aman sejak awal akan menghasilkan penghematan biaya yang signifikan dan mengurangi risiko reputasi dalam jangka panjang.

Sebagai agenda penelitian ke depan, peneliti merekomendasikan pengembangan framework evaluasi kesiapan keamanan desain database (Database Security Design Readiness Framework) yang dapat digunakan oleh organisasi secara mandiri untuk menilai dan meningkatkan kualitas desain database mereka secara berkelanjutan.

REFERENSI

Indonesia: Analisis Penyebab dan Mitigasi. Jurnal Keamanan Siber Indonesia, 5(2), 90–108.

Connolly, T. M., & Begg, C. E. (2015). Database Systems: A Practical Approach to Design, Implementation, and Management (6th ed.). Pearson Education.

Coronel, C., & Morris, S. (2019). Database Systems: Design, Implementation, and Management (13th ed.). Cengage Learning.

Elmasri, R., & Navathe, S. B. (2016). Fundamentals of Database Systems (7th ed.). Pearson Education.

Hadi, S., & Kurniawan, R. (2023). Analisis Kerentanan Sistem Database pada Aplikasi Web Berbasis PHP: Studi Kasus SQL Injection. Jurnal Teknologi Informasi dan Komunikasi, 14(2), 78–92.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation. https://www.ibm.com/security/data-breach

Iqbal, M., Fauzi, A., & Pratama, D. (2024). Implementasi Keamanan Berlapis pada Database Sistem Informasi Manajemen Rumah Sakit. Jurnal Informatika dan Sistem Informasi, 9(1), 45– 62.

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE-2007-01, Keele University.

Laudon, K. C., & Laudon, J. P. (2020). Management Information Systems: Managing the Digital Firm (16th ed.). Pearson Education.

Martinez, J., Chen, L., & Williams, K. (2022). Trust Recovery After Data Breach: A Longitudinal Study. Journal of Information Systems Security, 18(3), 112–134.

OWASP Foundation. (2023). OWASP Top 10 – 2023: The Ten Most Critical Web Application Security Risks. OWASP. https://owasp.org/Top10/

Riyanti, D., Lubis, M., & Hasibuan, Z. A. (2024). Evaluasi Keamanan Basis Data Sistem Informasi Akademik Perguruan Tinggi. Jurnal Sistem Informasi, 20(1), 33–50.

Silberschatz, A., Korth, H. F., & Sudarshan, S. (2019). Database System Concepts (7th ed.). McGraw-Hill Education.

Stallings, W. (2018). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.

Tanjung, H., & Nasution, S. H. (2024). Studi Kasus Kebocoran Data di Sektor Perbankan

ANALISIS KRITIS TERHADAP KELEMAHAN DESAIN DATABASE DALAM MENINGKATKAN RISIKO KEBOCORAN DATA DAN MENURUNKAN INTEGRITAS SISTEM INFORMASI

Abel Bangun [1], Muhammad Irwan Padli Nasution [2]