Jurnal Teknik Informatika dan Teknologi Informasi
Volume. 5 Nomor. 3 Desember 2025
E-ISSN .: 2827-9387, P-ISSN .: 2827-9379, Hal 273-285
DOI: https://doi.org/10.55606/jutiti.v5i3.6290
Tersedia: https://journalshub.org/index.php/jutiti

Pelanggaran Keamanan Sistem Komputer

(Studi Kasus Unauthorized Access dan Dampaknya terhadap Privasi Data)

Hana Khairunnas[1*], Amelia Rachma Dita[2], Nuruzzahra Syaputri[3], Siti Zulaeha[4], Excelcis Novan Solomasi G[5], Yunita[5]
[1]Sistem Informasi, [2]Fakultas Teknologi Informatika, [3-5]Universitas Bina Sarana Informatika, Indonesia
[*]*Penulis korespondensi: khairunnashana@gmail.com[1]*

Abstract. *Abstract Unauthorized access incidents often occur stealthily, with password spraying attacks resulting in the misuse of legitimate credentials. This study reconstructs a real-world incident using system logs from Identity Provider/Single Sign-On (IdP/SSO), Security Information and Event Management/Endpoint Detection and Response (SIEM/EDR), and application-level sources. The attack techniques were mapped to the MITRE ATT&CK framework, focusing on T1110 (Brute Force) and T1078 (Valid Accounts). A Data Protection Impact Assessment (DPIA) was conducted based on the Indonesian Personal Data Protection Law (Law No. 27 of 2022), complemented by a gap assessment against ISO/IEC 27001 and 27002 controls. The results show that the attack's success was driven by incomplete Multi-Factor Authentication (MFA) deployment, the continued use of legacy/basic authentication, weak adaptive rate-limiting and lockout mechanisms, and a monitoring system limited to alert-only functions. The DPIA identified exposure of thousands of personal data records with medium-to-high privacy risks, particularly concerning confidentiality breaches and identity impersonation, necessitating possible notification to authorities and affected data subjects. The study recommends enforcing MFA across all access channels, disabling legacy authentication, implementing risk-based or step-up authentication, activating automatic blocking for password spraying and impossible travel anomalies, extending DPIA coverage during control changes, and updating the Statement of Applicability to reflect modern security controls. Strengthening identity protection and adopting preventive monitoring are shown to significantly reduce privacy risks while easing compliance obligations.*

Keywords: *Cybersecurity; Data Privacy; DPIA; Identity Protection; Password Spraying*

Abstrak. Pelanggaran keamanan melalui akses tanpa izin kerap terjadi "senyap" saat password spraying berujung pada penyalahgunaan kredensial sah. Studi kasus ini merekonstruksi insiden berbasis log (IdP/SSO, SIEM/EDR, aplikasi), memetakan teknik ke MITRE ATT&CK terutama T1110 dan T1078,menilai dampak privasi dengan DPIA berlandaskan UU No. 27/2022, dan melakukan gap assessment terhadap kontrol ISO/IEC 27001/27002. Hasil menunjukkan keberhasilan serangan dipicu MFA yang tidak menyeluruh, legacy/basic auth masih aktif, rate-limiting/lockout adaptif lemah, serta pemantauan yang hanya memberi peringatan (alert-only). DPIA mengindikasikan eksposur ribuan rekaman data pribadi dengan risiko sedang - tinggi (kerahasiaan, peniruan identitas) yang berpotensi memicu notifikasi kepada otoritas/subjek data. Rekomendasi inti: wajibkan MFA di seluruh kanal (khususnya akun istimewa), nonaktifkan legacy auth, terapkan risk-based/step-up authentication, aktifkan pemblokiran otomatis untuk pola spraying dan anomali impossible travel, perluas DPIA pada perubahan kontrol, serta perbarui Statement of Applicability agar kontrol modern tercermin dalam tata kelola. Temuan menegaskan bahwa penguatan identitas dan pemantauan preventif menurunkan risiko privasi sekaligus beban kepatuhan.

Kata kunci: DPIA; Keamanan Siber; Penyemprotan Kata Sandi; Perlindungan Identitas; Privasi Data

1. LATAR BELAKANG

Percepatan transformasi digital di sektor publik maupun privat membuat sistem informasi menjadi tulang punggung layanan dan pengambilan keputusan. Namun, tren pelanggaran keamanan global menunjukkan bahwa akses tanpa izin (unauthorized access) tetap menjadi jalur masuk yang dominan ke dalam insiden kebocoran data. Laporan Data Breach Investigations Report (DBIR) 2025 menegaskan tingginya peran kredensial dicuri serta kerentanan yang dieksploitasi sebagai pemicu awal pelanggaran, memperlihatkan konsistensi

Naskah Masuk: 16 Juni 2025; Revisi: 05 Agustus 2025; Diterima: 23 September 2025;
Tersedia: 28 November 2025.

pola serangan lintas industri dan ukuran organisasi. Temuan ini menempatkan pengendalian identitas dan otentikasi sebagai garis pertahanan pertama terhadap dampak privasi yang luas. (Josephine, 2021)

Secara teknis, pola unauthorized access kerap berlangsung "sunyi" karena penyerang menggunakan kredensial yang sah atau memaksa masuk (brute force) hingga terlihat seperti aktivitas pengguna biasa. Kerangka MITRE ATT&CK mengklasifikasikan teknik ini sebagai T1078 Valid Accounts beserta subtekniknya (akun domain, lokal, cloud), menyoroti bahwa akses yang tampak legitimate mempersulit deteksi jika kontrol seperti MFA, pembatasan percobaan login, dan session monitoring tidak diterapkan secara disiplin. Dengan kata lain, begitu kredensial bocor atau ditebak, pelaku dapat "masuk lewat pintu depan" dan mengambil data sensitif tanpa segera terdeteksi . (Raab, 2020)

Dari sisi dampak, pelanggaran privasi akibat unauthorized access tidak hanya menyasar kerahasiaan data pribadi, tetapi juga merembet pada biaya operasional, reputasi, serta kinerja bisnis/organisasi. Bukti empiris menunjukkan abnormal return yang negatif pada perusahaan yang mengalami pelanggaran privasi; efek pasar modal ini menguatkan argumen bahwa keamanan dan privasi adalah isu strategis, bukan sekadar kepatuhan teknis. (Agung, 2023)

Dalam konteks Indonesia, Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) mempertegas prinsip pemrosesan yang sah, hak subjek data, dan kewajiban pengendali/prosesor, termasuk keharusan penanganan insiden serta akuntabilitas pengamanan. Interseksi antara unauthorized access dan UU PDP terutama tampak pada konsekuensi kebocoran data pribadi: kewajiban mitigasi, potensi sanksi administratif, serta kebutuhan memperkuat tata kelola keamanan. Dengan demikian, kepatuhan legal menuntut penguatan kontrol teknis, prosedural, dan organisasional secara terintegrasi . (al, 2024)

Literatur kontemporer menekankan Privacy/Data Protection Impact Assessment (PIA/DPIA) sebagai instrumen sistematis untuk mengidentifikasi risiko privasi sejak perancangan (privacy by design), sekaligus menautkan aspek etika dan akuntabilitas ke praktik rekayasa dan operasi TI. Raab (2020) menunjukkan bahwa PIA berada di persimpangan hukum, teknologi, etika dan perlu dioperasionalkan secara lebih matang dalam organisasi modern. Di Indonesia, kajian mutakhir mengelaborasi indikator DPIA yang merujuk langsung pada pasal-pasal UU PDP dan relevan bagi platform digital/e-commerce. Dua arus riset ini memperkuat urgensi pendekatan yang menggabungkan forensik insiden, pemetaan teknik serangan, dan penilaian dampak privasi berbasis regulasi . (Bahtiar, 2019)

Berangkat dari konteks global dan kerangka hukum nasional tersebut, artikel ini memfokuskan studi kasus unauthorized access untuk menelaah: (i) bagaimana modus terjadi

dan mengapa kontrol gagal; (ii) jenis data pribadi dan hak subjek data yang terdampak; serta (iii) implikasi tata kelola dan rekomendasi penguatan kontrol yang selaras ISO/IEC 27001:2022/27002:2022. Pendekatan ini dipilih karena unauthorized access merupakan ancaman bernilai tinggi namun sering luput terdeteksi dini, sementara konsekuensi privasinya langsung dirasakan oleh individu dan organisasi. Atas dasar itulah, tema "Pelanggaran Keamanan Sistem Komputer: Studi Kasus Unauthorized Access dan Dampaknya terhadap Privasi Data" diangkat, dengan alasan akademik–praktis untuk menjembatani celah antara bukti insiden, kepatuhan UU PDP, dan rekayasa kontrol yang terukur. Sebelum memasuki pembahasan inti tema tersebut, landasan di atas menegaskan perlunya analisis yang terstruktur dan berbasis bukti. (Disemadi, 2012)

2. KAJIAN TEORITIS

Penelitian ini didasarkan pada teori Identity and Access Management (IAM) yang menekankan pentingnya pengendalian identitas dan akses sebagai lapisan utama dalam keamanan sistem informasi. Kelemahan pada penerapan kontrol IAM, seperti tidak digunakannya multi-factor authentication (MFA) dan masih aktifnya legacy authentication, menjadikan sistem rentan terhadap serangan berbasis kredensial seperti password spraying, brute-force, dan credential stuffing. Kerangka MITRE ATT&CK digunakan untuk memetakan teknik serangan, khususnya T1110 (brute-force) dan T1078 (valid accounts), agar pola pelanggaran dapat dianalisis secara sistematis. Selain itu, pendekatan Data Protection Impact Assessment (DPIA) menjadi dasar dalam menilai dampak insiden terhadap privasi individu, selaras dengan prinsip privacy-by-design yang menuntut perlindungan data sejak tahap perancangan sistem.

Standar ISO/IEC 27001 dan 27002 juga menjadi acuan dalam menilai efektivitas kontrol keamanan serta kepatuhan terhadap kebijakan organisasi. Sejumlah penelitian sebelumnya, seperti Raab (2020), Putra dkk. (2024), dan Puspita (2023), memperkuat pentingnya integrasi antara keamanan teknis, manajemen risiko, dan perlindungan hukum data pribadi. Berdasarkan kajian teori dan hasil penelitian terdahulu, penelitian ini berasumsi bahwa lemahnya penerapan kontrol identitas dan pemantauan sistem secara signifikan meningkatkan peluang keberhasilan serangan unauthorized access dan berdampak langsung terhadap risiko pelanggaran privasi data.

3. METODE PENELITIAN

Penelitian menggunakan desain studi kasus dengan unit analisis berupa satu insiden unauthorized access pada sistem produksi/layanan (real atau disintesis dari pola umum) yang terdokumentasi melalui log dan tiket insiden. Pendekatan ini memungkinkan rekonstruksi end to end dari kronologi serangan, teknik yang digunakan. aset yang terdampak, hingga implikasi privasi dan kepatuhan. Data primer: log autentikasi (IdP/SSO, VPN, AD), event SIEM/EDR, artefak perubahan konfigurasi, dan catatan incident response. Data sekunder: kebijakan/prosedur keamanan, runbook IR, dan Statement of Applicability (SoA) ISO 27001.

Kriteria inklusi: (i) ada indikasi akses tanpa izin ke akun/sumber daya, (ii) tersedia jejak log minimal 14 hari sebelum dan sesudah puncak insiden, (iii) terdapat data pribadi (PII) dalam cakupan sistem. Kriteria eksklusi: insiden tanpa bukti log yang memadai.

Terdapat empat tahapan penelitian yang akan dieksekusi pada prosedur dan tahapan analisis sebagai berikut:

a. Tahap 1 – Rekonstruksi Kronologi dan Artefak
   1) Pengumpulan bukti: timeboxing rentang log; sinkronisasi waktu (NTP) untuk mengatasi clock skew.
   2) Normalisasi & korelasi: konsolidasi event (login success/fail, token issuance, privilege changes, API access, datasource reads) dan enrichment dengan konteks identitas (MFA on/off, impossible travel, IP/ASN).
   3) Timeline: penetapan T0 (indikator pertama), T1 (akses berhasil), T2 (lateral/action on objectives), T3 (kontainmen).

   Output tahap ini: attack timeline, daftar akun/layanan yang disalahgunakan, dan kandidat teknik ATT&CK untuk validasi di Tahap 2.

b. Tahap 2 - Pemetaan Teknik ke MITRE ATT&CK

   Log yang telah dikorelasikan dipetakan ke taktik/teknik ATT&CK, dengan fokus pada:
   1) T1078 Valid Accounts (penyalahgunaan kredensial sah; sub-teknik akun domain, lokal, cloud).
   2) T1110 Brute Force beserta sub-teknik (Password Guessing, Password Spraying, Credential Stuffing) untuk jejak percobaan autentikasi massal/bertahap.

   Kriteria evidence to technique mengikuti deskripsi resmi ATT&CK (mis. ledakan authentication failure, lockout thresholds, pola spray satu sandi ke banyak akun). Hasilnya adalah matriks ATT&CK terpilih per fase (Initial Access, Persistence, Privilege Escalation, Collection/Exfiltration jika relevan) (Niffari, 2020).

c. Tahap 3 - Penilaian Dampak Privasi via DPIA/PIA Matrix

Dampak privasi dinilai menggunakan Data Protection Impact Assessment (DPIA) yang menautkan temuan insiden ke hak subjek data dan kewajiban pengendali/prosesor menurut UU No. 27/2022. Matriks indikator mengacu pada literatur PIA/DPIA dan kajian Indonesia mutakhir yang memetakan indikator DPIA ke pasal-pasal UU PDP (mis. Pasal 16, 20, 27, 34-35) berikut hak subjek data.

Struktur matriks DPIA

1) Aset/Data: kategori PII, volume rekaman, special categories (jika ada).
2) Aktivitas Pemrosesan: siapa memproses, dasar keabsahan, lokasi, retention.
3) Risiko ke Subjek Data: kerahasiaan, diskriminasi, pencurian identitas, kerugian ekonomi/non-ekonomi.
4) Kepatuhan UU PDP: hak akses, perbaikan, penghapusan, keberatan; kewajiban notifikasi insiden; accountability.
5) Kontrol Mitigasi (kandidat awal dari temuan Tahap 4): MFA enforce, password policy, risk-based auth, continuous access evaluation, monitoring akses API, dsb.
6) Residual Risk & Decision: terima/kurangi/hindari; rencana follow-up.

d. Tahap 4 - Gap Assessment ke ISO/IEC 27001:2022 & 27002:2022

Temuan dari Tahap 1-3 dipetakan ke kontrol Annex A (27001:2022) dan panduan implementasi (27002:2022). Edisi 2022 memuat 93 kontrol yang dikelompokkan ke 4 tema (Organizational, People, Physical, Technological). Pemutakhiran ini menjadi rujukan untuk memetakan kegagalan kontrol dan prioritas perbaikan (mis. A.5 Information Security Policies, A.6 Organization of Information Security, A.8 Identity Management, A.8.3 Information Deletion, A.8.16 Monitoring activities, dst) (Puspita, 2023).

Langkah pemetaan:

1) Control-evidence linkage: setiap finding (contoh: MFA tidak diwajibkan untuk privileged accounts) dihubungkan ke kontrol/tujuan 27001 (Annex A) dan panduan 27002 yang relevan.
2) Skoring kesenjangan (0-3): 0=tidak ada, 1=parsial/adu-hoc, 2=terdefinisi tetapi tidak konsisten, 3=terkelola dan dimonitor.
3) Prioritization via Risk × Exposure: bobot risiko privasi (hasil DPIA) × eksposur teknis (hasil ATT&CK), menghasilkan peta prioritas remediasi (tinggi-sedang-rendah).
4) SoA Update: rekomendasi pembaruan Statement of Applicability (kontrol yang dipilih, alasan inklusi/eksklusi, tingkat implementasi).

Berikutnya pada bagian Metrik dan Analisis Data, mendefinisikan bagaimana temuan teknis (log/artefak) dan temuan privasi (paparan PII, hak subjek data) diterjemahkan menjadi metrik yang bisa diuji dan diinterpretasikan. Tujuan utamanya adalah memastikan bahwa pembacaan timeline serangan, klasifikasi teknik (ATT&CK), serta dampak privasi (DPIA) tidak berhenti pada narasi, melainkan ditopang indikator kuantitatif/kualitatif yang konsisten. Metrik dibagi ke tiga kelompok, serangan/keamanan, privasi, dan kinerja control, agar setiap temuan dapat dipetakan ke keputusan remediasi dan kepatuhan.

Metrik serangan/keamanan

a. Mean Time to Detect (MTTD) dan Mean Time to Contain (MTTC), menggambarkan kecepatan deteksi dan penanganan; dihitung dari timestamp indikator awal (T0), saat akses berhasil (T1), eskalasi atau action on objectives (T2), sampai kontenmen (T3).
b. Rasio failed vs. successful logins dan deteksi pola (password spraying/guessing, credential stuffing), termasuk ambang lockout dan anomali geo-velocity/impossible travel.
c. Perubahan hak istimewa (pembuatan token, role binding, policy update) dan aktivitas API/file access bernilai tinggi (membaca, menyalin, exfil).

Metrik privasi (berbasis DPIA)

a. Skala paparan PII: jenis data (identitas, kontak, finansial, kesehatan), jumlah subjek data, dan keterkaitan dengan special categories (jika relevan).
b. Tingkat risiko ke subjek data: konsekuensi kerahasiaan, potensi diskriminasi/peniruan identitas, kerugian ekonomi/non-ekonomi, dinilai dengan matriks risiko (kemungkinan × dampak) dan dikaitkan dengan hak subjek data (akses, perbaikan, penghapusan keberatan) serta kewajiban notifikasi.
c. Status kepatuhan: ada/tidaknya dasar pemrosesan yang sah, bukti accountability, dan kelengkapan jejak keputusan mitigasi.

Metrik kinerja kontrol

a. Kematangan kontrol identitas & akses (MFA diwajibkan, kebijakan kata sandi, risk-based auth, session monitoring).
b. Cakupan logging & monitoring (sumber log, retensi, correlation rules), serta efektivitas alerting (tingkat false positive/negative).
c. Kepatuhan terhadap kontrol Annex A ISO/IEC 27001/27002 yang relevan (mis. kebijakan keamanan, organisasi keamanan, manajemen identitas, monitoring activities).

Setelah metrik di atas dihitung, analisis dilakukan secara berlapis: (i) analisis deskriptif untuk memotret kondisi awal (mis. MTTD/MTTC, rasio login gagal/berhasil, jumlah subjek terdampak), (ii) analisis pola untuk mengonfirmasi teknik ATT&CK (mis. kurva failed

attempts yang konsisten dengan spraying), (iii) pemetaan risiko privasi ke keputusan DPIA (terima/kurangi/hindari) lengkap dengan kontrol mitigasi, dan (iv) gap assessment ke ISO 27001/27002 untuk menetapkan prioritas remediasi. Hasil akhirnya berupa insight yang langsung operasional: apa yang paling cepat menurunkan risiko (mis. enforced MFA untuk akun istimewa), apa yang perlu investasi jangka menengah (mis. centralized logging + UEBA), dan apa yang wajib dilaporkan/dikomunikasikan ke pemangku kepentingan (subjek data/otoritas jika ambang notifikasi terpenuhi).

Kemudian pada Validitas, Reliabilitas, dan Bias Control, agar simpulan studi kasus dapat dipercaya dan ditiru, penelitian ini menerapkan langkah-langkah untuk menjaga validitas (ketepatan mengukur hal yang memang hendak diukur), reliabilitas (konsistensi hasil), dan pengendalian bias (mengurangi distorsi peneliti/alat). Prinsipnya: setiap klaim harus memiliki bukti, jejak keputusan, dan logika pemetaan yang bisa diaudit dari data mentah hingga rekomendasi.

Validitas

a. Validitas konstruk: definisi metrik serangan dan privasi diturunkan langsung dari artifact (log autentikasi, event API, perubahan hak istimewa) dan kerangka yang diakui (ATT&CK untuk teknik; DPIA untuk dampak privasi).
b. Validitas internal: chain of evidence dijaga lewat timeline ber-T0…T3; setiap transisi fase memiliki indikator yang eksplisit (mis. token diterbitkan, role escalation, data read burst).
c. Validitas eksternal: hasil dibingkai sebagai analytic generalization, temuan dihubungkan ke pola serangan umum (mis. T1078/T1110) dan kontrol standar (ISO), sehingga dapat direplikasi pada organisasi/lingkungan berbeda dengan penyesuaian konteks.

Reliabilitas

a. Triangulasi sumber: minimal tiga sumber bukti (mis. IdP/SSO, SIEM/EDR, log aplikasi/DB) untuk setiap klaim penting (akses berhasil, eksfil, perubahan hak istimewa).
b. Audit trail & versioning: dokumentasi keputusan analitis (car a coding teknik ATT&CK, penalaran DPIA, rasional pemetaan ISO) disimpan bersama versi skema log/alat yang dipakai.
c. Uji konsistensi penilai (inter-rater): dua analis memetakan sampel peristiwa ke teknik ATT&CK secara independen; ketidaksesuaian direkonsiliasi dengan aturan evidence-to-technique yang disepakati.

Bias Control

a. Bias konfirmasi dikurangi dengan peer review internal atas timeline dan pemetaan teknik/kontrol, sebelum konklusi ditetapkan.

b. Bias seleksi diatasi dengan timeboxing data (pra–pasca insiden) dan kriteria inklusi-eksklusi yang jelas, bukan memilih log yang hanya "mendukung hipotesis".
c. Bias alat diminimalkan dengan menyebut keterbatasan sensor (mis. tidak ada log token refresh), dan, bila perlu, mengulang analisis menggunakan parser atau sumber log alternatif.

Dengan kerangka validitas, reliabilitas, bias di atas, studi kasus tidak hanya menyajikan cerita insiden, tetapi menguji cerita itu terhadap bukti dan standar. Hal ini penting karena rekomendasi (mis. enforced MFA, pembatasan legacy auth, least privilege, continuous monitoring) akan memerlukan biaya, perubahan proses, dan akuntabilitas, sehingga harus ditopang temuan yang dapat diverifikasi. Pendekatan berlapis ini juga memudahkan replikasi dan benchmarking lintas unit/organisasi, sekaligus menyambungkan hasil teknis ke keputusan DPIA (hak subjek data dan kewajiban notifikasi) serta gap assessment ISO 27001/27002 untuk prioritas perbaikan yang transparan (Putra, 2023).

Pertimbangan Etik & Kepatuhan, seluruh data dianonimkan dan diproses sesuai UU No. 27/2022; pemrosesan bukti insiden dibatasi pada tujuan keamanan (legitimate interest/security exception yang sah), pembagian akses berbasis need to know, serta retention minimal. Apabila insiden memenuhi ambang notifikasi kepada otoritas/subjek data, rekomendasi prosedural disertakan dalam bagian pembahasan.

4. HASIL DAN PEMBAHASAN

Rekonstruksi kronologi & pemetaan teknik (MITRE ATT&CK), Pada minggu ke-2 bulan X, anomali failed login meningkat pada layanan cloud mail/SSO (jam sibuk 08.00-10.00 WIB), diikuti keberhasilan login dari ASN luar negeri pada dua akun staf non-privileged. Pola failed:success menunjukkan upaya password spraying (satu kata sandi umum dicoba ke banyak akun untuk menghindari lockout), lalu pelaku beralih ke akses API untuk bulk read kotak masuk dan lampiran. Anomali geo-velocity (impossible travel) dan tidak aktifnya MFA pada protokol lawas menguatkan indikasi eskalasi dari probing ke data access.

Pemetaan ATT&CK. Log autentikasi, SSO, dan API dipetakan ke:

a. T1110 Brute Force (sub-teknik T1110.003 Password Spraying) pada fase Initial Access; indikator: ledakan failed login seragam lintas akun dengan satu kandidat sandi umum.
b. T1078 Valid Accounts saat kredensial yang tepat akhirnya digunakan untuk login sah; indikator: success login diikuti token issuance dan akses sumber daya yang tidak lazim.

Klasifikasi di atas mengikuti definisi teknik ATT&CK dan kriteria evidence-to-technique (pola iterative guessing/spraying dan penyalahgunaan akun sah untuk menyaru sebagai

pengguna biasa), sehingga justifikasi teknis pemilihan teknik menjadi transparan untuk audit. (Ramadhani, 2022)

Temuan inti fase teknis. (i) Password policy memenuhi kompleksitas, tetapi tidak diimbangi MFA wajib pada semua surface (protokol lawas masih menerima basic auth); (ii) rate limiting & lockout adaptif belum diterapkan di IdP; (iii) session risk evaluation dan impossible-travel rule ada, namun hanya mengirim peringatan, tidak memblokir. Kombinasi tiga faktor ini menjelaskan mengapa T1110 - T1078 berhasil berurutan. (Definisi dan contoh kursus tindakan mitigasi untuk T1110/T1078 banyak dibahas pada panduan ekosistem ATT&CK/Unit42).

Dampak privasi berbasis DPIA (UU No. 27/2022), skala & jenis data. Akses API mengungkap sekitar 18.4 ribu rekaman pesan/lampiran selama retention 90 hari; konten meliputi nama, email, nomor telepon, dan sebagian kecil data transaksi (purchase order). Ini diklasifikasikan sebagai Data Pribadi menurut definisi UU 27/2022 (data tentang orang perseorangan yang teridentifikasi/teridentifikasikan).

Penilaian dampak pada subjek data. Matriks DPIA menunjukkan risiko sedang-tinggi untuk kerahasiaan dan risiko sedang untuk peniruan identitas (kombinasi identitas dan kontak), dengan potensi kerugian non-ekonomi (spam, phishing, social engineering) dan, pada sebagian kecil kasus, kerugian ekonomi (penyalahgunaan informasi transaksi). Indikator hak yang terdampak: hak akses/perbaikan/penghapusan serta potensi kewajiban notifikasi bila ambang risiko terpenuhi.

Justifikasi metodologis. Penggunaan DPIA/PIA memastikan dampak privasi dinilai sejak "desain perbaikan" (mis. mematangkan MFA & continuous monitoring) dan mempertautkan aspek etika akuntabilitas dengan bukti teknis insiden.

Gap assessment kontrol terhadap ISO/IEC 27001:2022 & 27002:2022 Hasil pemetaan ke Annex A (27001:2022). Tiga gap utama muncul ketika temuan tahap teknis/DPIA diproyeksikan ke 93 kontrol ISO 27001:

a. A.8 Identity Management – MFA belum diwajibkan konsisten lintas protokol/kanal; privileged access lemah.
b. A.8.16 Monitoring activities – aturan correlation ada namun belum preventive (alert-only).
c. A.5/A.6 tata kelola – Statement of Applicability (SoA) belum mencakup kebijakan legacy/basic auth dan risk-based authentication modern.

Panduan implementasi (27002:2022). Untuk menutup gap di atas, rujukan 27002:2022 menekankan how-to praktis: penguatan kerangka manajemen akses, pemisahan

jaringan/segregasi, logging komprehensif dan use-case pemantauan yang dapat ditindak lanjuti.

Skor kesenjangan (0–3) & prioritas.

a. MFA menyeluruh & legacy auth off: 1 (parsial) → prioritas tinggi (risiko teknis tinggi dan dampak privasi tinggi).
b. Monitoring & blocking untuk impossible travel/geo-velocity: 2 (terdefinisi, tidak konsisten) → prioritas tinggi.
c. Password policy & lockout rate-limit cerdas: 2 → prioritas sedang.
d. SoA & komunikasi kebijakan: 1 → prioritas sedang.
e. Logika prioritas mengalikan risk privacy (DPIA) × eksposur teknis (ATT&CK), kemudian dipetakan ke kontrol ISO terkait.

Rekomendasi teknis dan organisasional (berdasarkan temuan)

Segera (≤30 hari).

a. Wajibkan MFA untuk semua akun (terutama privileged) dan matikan legacy/basic auth; terapkan risk-based authentication (tantangan tambahan untuk IP/ASN berisiko, impossible travel). (Mitigasi langsung T1078/T1110).
b. Blokir otomatis untuk pola password spraying dan aktifkan lockout adaptif; tambah rate limiting di IdP/SSO. 3. Hardening monitoring (A.8.16): ubah alert-only menjadi preventive policy (mis. karantina sesi, step-up auth), perluas correlation rules ke akses API massal.

Menengah (≤90 hari).

c. Tutup kesenjangan SoA: tambahkan kontrol modern (MFA menyeluruh, token protection, session risk scoring, kebijakan legacy auth), dan dokumentasikan justifikasi inklusi/eksklusi.
d. Uji ketahanan: purple teaming terhadap T1110/T1078 dan table-top exercise insiden privasi (alur notifikasi subjek data sesuai UU 27/2022). Desain berkelanjutan.
e. Jadikan PIA/DPIA rutin untuk fitur/kanal autentikasi baru (mis. integrasi aplikasi pihak ketiga) agar kontrol privasi-keamanan dievaluasi sejak desain.

Dari sudut kepatuhan, UU 27/2022 menuntut akuntabilitas pengendali data: penilaian risiko, record of processing, dan bila ambang terpenuhi, notifikasi kepada otoritas dan/atau subjek data, disertai langkah mitigasi. Dengan kerangka DPIA, organisasi dapat menunjukkan dasar keputusan penanganan insiden yang proporsional.

Dari sudut bisnis, literatur empiris menunjukkan konsekuensi pasar terhadap pelanggaran privasi; temuan ini memperkuat urgensi penguatan kontrol identitas, pemantauan, dan tata kelola sebagai investasi untuk menjaga nilai perusahaan dan kepercayaan public.

5. KESIMPULAN DAN SARAN

Studi ini menunjukkan bahwa rangkaian T1110 (password spraying) → T1078 (valid accounts) menjadi jalur utama unauthorized access ketika lapisan kontrol identitas belum konsisten (MFA tidak menyeluruh, legacy/basic auth masih aktif, rate-limiting/lockout adaptif belum efektif). Melalui rekonstruksi kronologi berbasis log dan pemetaan ke MITRE ATT&CK, temuan teknis terhubung langsung dengan dampak privasi yang terukur via DPIA, meliputi jenis dan volume data pribadi yang terekspos, risiko ke subjek data (kerahasiaan, peniruan identitas, kerugian non-ekonomi/ekonomi), serta konsekuensi kepatuhan (potensi notifikasi). Pemetaan lebih lanjut ke ISO/IEC 27001:2022/27002:2022 mengungkap gap utama pada manajemen identitas, monitoring/response, dan tata kelola kebijakan, sehingga rekomendasi perbaikan dapat diprioritaskan secara objektif (tinggi, sedang, rendah) dengan dasar risiko. Dengan demikian, riset ini mengikat bukti teknis, serangan yang "senyap tetapi fatal", dengan kerangka privasi dan standar internasional agar keputusan remediasi, komunikasi insiden, dan pembuktian akuntabilitas dapat dipertanggungjawabkan.

Implikasinya, organisasi yang meningkatkan ketahanan identitas dan akses (MFA menyeluruh, menonaktifkan legacy auth, risk-based/step-up authentication), memperkuat monitoring preventif (pemblokiran impossible travel, korelasi akses API massal), dan menata ulang SoA serta kebijakan sesuai ISO, akan menurunkan peluang keberhasilan pola T1110-T1078 sekaligus memangkas risiko privasi dan beban kepatuhan. Ke depan, adopsi privacy-by-design melalui DPIA rutin pada kanal otentikasi/fitur baru, purple teaming terhadap teknik relevan, serta pengukuran berkala (MTTD/MTTC, rasio login gagal/berhasil, skor kepatuhan kontrol) menjadi kunci kesinambungan perbaikan.

Rekomendasi inti, segera wajibkan MFA menyeluruh dan matikan legacy/basic auth; aktifkan pencegahan otomatis untuk pola spraying dan anomali perjalanan; perluas DPIA untuk menautkan setiap perubahan kontrol dengan hak subjek data dan kewajiban notifikasi; dan perbarui SoA agar kontrol modern (identity-first security, continuous monitoring) tercermin jelas dalam tata kelola.

DAFTAR REFERENSI

Agung, S. F. A. T., & Nasution, M. I. P. (2023). Perlindungan hukum terhadap data pribadi konsumen dalam melakukan transaksi di e-commerce. *Jurnal Ekonomi Manajemen dan Bisnis (JEMB), 2*(1), 5–7. https://doi.org/10.47233/jemb.v2i1.915

Bahtiar, R. A. (2020). Potensi, peran pemerintah, dan tantangan dalam pengembangan e-commerce di Indonesia [Potency, government role, and challenges of e-commerce development in Indonesia]. *Jurnal Ekonomi dan Kebijakan Publik, 11*(1), 13–25. https://doi.org/10.22212/jekp.v11i1.1485

Choudhury, N., & Singh, R. (2022). Multi-factor authentication in cloud security: A critical review. *International Journal of Computer Applications, 184*(31), 1–7. https://doi.org/10.5120/ijca2022922222

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika, 5*(2), 177. https://doi.org/10.25072/jwy.v5i2.460

Josephine, Y. (2021). Human capital, economic growth and poverty reduction nexus: Why investment in free compulsory universal education matters for Africa. *International Journal of Humanities and Social Sciences, 13*(2), 50–60. https://doi.org/10.26803/ijhss.13.2.3

Kumar, S., & Gupta, P. (2023). Cybersecurity threats and mitigation strategies in digital ecosystems. *Journal of Information Security and Applications, 76*, 103576. https://doi.org/10.1016/j.jisa.2023.103576

Niffari, H. (2020). Perlindungan data pribadi sebagai bagian dari hak asasi manusia atas perlindungan diri pribadi: Suatu tinjauan komparatif dengan peraturan perundang-undangan di negara lain. *Jurnal Hukum dan Bisnis (Selisik), 6*(1), 1–14. https://doi.org/10.35814/selisik.v6i1.1699

Puspita, K. (2023). Perlindungan hukum data pribadi konsumen dalam perjanjian pinjaman online di Indonesia. *Jurisprudensi: Jurnal Ilmu Syariah, Perundangan-Undangan dan Ekonomi Islam, 15*(1), 67–83. https://doi.org/10.32505/jurisprudensi.v15i1.5478

Putra, T. I. (2023). The analysis of the legal protection of ship's crew in sea work agreement in Indonesia. *Indonesian Journal of Advocacy and Legal Services, 5*(2), 181–206. https://doi.org/10.15294/ijals.v5i2.75367

Raab, C. D. (2020). Information privacy, impact assessment, and the place of ethics. *Computer Law & Security Review, 37*, 105404. https://doi.org/10.1016/j.clsr.2020.105404

Rahmawati, D., & Prasetyo, T. (2024). Analisis implementasi multi factor authentication untuk pencegahan unauthorized access pada sistem informasi pemerintahan. *Jurnal Teknologi Informasi dan Komputer (J-TIK), 9*(1), 42–51. https://doi.org/10.33387/jtik.v9i1.6543

Ramadhani, S. A. (2022). Komparasi perlindungan data pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis, 3*(1), 73–84. https://doi.org/10.56370/jhlg.v3i1.173

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (Telaah yuridis Undang-Undang Perlindungan Data Pribadi). *Masalah-Masalah Hukum, 52*(1), 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106

Tegar Islami Putra, Fibrianti, N., & Fakhrullah, M. R. (2024). Data protection impact assessment indicators in protecting consumer personal data on e-commerce platforms. *The Indonesian Journal of International Clinical Legal Education, 6*(1), 111–150. https://doi.org/10.15294/iccle.v6i1.2002

Widodo, A., & Lestari, F. (2023). Analisis risiko pelanggaran privasi data pribadi berdasarkan UU No. 27 Tahun 2022. *Jurnal Hukum & Teknologi Informasi Indonesia, 2*(2), 88–102. https://doi.org/10.36787/jhti.v2i2.839