KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 4: Tanggap Insiden Siber

Subtopik 4.1: Apa itu Insiden Siber?

Disusun oleh:
Ketut Ananda Dharmawati
NIM: 2215091035

Program Studi S1 Sistem Informasi
Jurusan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha

BERSAMA CORPU KIWA TENGEN,
KLUNGKUNG TANGGUH HADAPI SERANGAN SIBER

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLUNGKUNG
2025

KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya modul pembelajaran *"Keamanan Siber untuk ASN dan Masyarakat"* dapat disusun hingga membahas subtopik penting mengenai *"Apa itu Insiden Siber?"*. Di era digital tahun 2025, aktivitas pemerintahan dan masyarakat semakin bergantung pada sistem elektronik, mulai dari pengelolaan data kependudukan, pelayanan publik, hingga transaksi keuangan. Ketergantungan ini membawa kemudahan, tetapi juga membuka peluang bagi berbagai ancaman digital yang dapat mengganggu sistem, mencuri data, bahkan melumpuhkan layanan pemerintahan.

Melalui subtopik ini, diharapkan ASN dan masyarakat Kabupaten Klungkung dapat lebih waspada dan bertanggung jawab dalam menjaga sistem serta data yang mereka gunakan setiap hari. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan subtopik ini. Semoga subtopik ini memberikan manfaat nyata dalam mendukung terwujudnya tata kelola pemerintahan dan kehidupan masyarakat yang lebih aman di era digital.

Kami menyadari bahwa modul ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan modul ajar ini di masa mendatang.

Klungkung, 2025

Penyusun

DAFTAR ISI

Tujuan Pembelajaran

Setelah mempelajari bagian ini, peserta (ASN maupun masyarakat) mampu:

1. Memahami pengertian dan ruang lingkup insiden siber berdasarkan panduan nasional dan praktik internasional.
2. Mengidentifikasi berbagai jenis insiden siber yang umum terjadi di instansi pemerintah dan masyarakat.
3. Menyadari dampak insiden siber terhadap layanan publik, data pribadi, dan reputasi lembaga.
4. Mengetahui tren dan perkembangan ancaman siber di Indonesia pada tahun 2025.
5. Membangun kesadaran untuk melaporkan potensi insiden siber lebih dini guna mencegah kerugian yang lebih besar.

Sasaran Peserta

1. Aparatur Sipil Negara (ASN): Agar memahami jenis dan dampak insiden siber yang mungkin terjadi pada sistem pemerintahan, serta mampu menjaga keamanan data dan layanan publik di lingkungan kerja.
2. Masyarakat Umum Kabupaten Klungkung: Agar mengenali potensi ancaman digital di kehidupan sehari-hari dan memahami pentingnya melindungi data pribadi serta melapor jika menemukan aktivitas siber mencurigakan.

A. Pengantar: Dunia Digital dan Risiko Siber

Pada tahun 2025, digitalisasi telah menjadi tulang punggung aktivitas pemerintahan dan masyarakat. Mulai dari e-Office, sistem perizinan online, hingga layanan kesehatan digital, semuanya terhubung melalui jaringan internet. Namun, di balik kemudahan ini muncul tantangan baru, **insiden siber**.

Insiden siber adalah peristiwa yang mengganggu atau mengancam keamanan sistem digital. Bentuknya bisa berupa peretasan akun, penyebaran *malware*, pencurian data, hingga gangguan layanan publik. Dalam konteks pemerintahan, satu serangan kecil saja bisa berdampak luas: data warga bocor, layanan terganggu, dan kepercayaan masyarakat menurun.

Tren nasional menunjukkan bahwa ancaman ini terus meningkat. Menurut **Badan Siber dan Sandi Negara (BSSN)**, sepanjang tahun 2024 terdapat lebih dari **400 juta upaya serangan siber** yang terdeteksi di Indonesia, sebagian besar menargetkan sektor pemerintahan daerah dan lembaga pendidikan. Pada tahun 2025, jenis serangan menjadi lebih canggih, memanfaatkan kecerdasan buatan (AI) untuk meniru komunikasi resmi atau mengeksploitasi sistem yang tidak diperbarui.

Di tingkat masyarakat, ancaman ini juga nyata. Mulai dari pencurian akun media sosial, penipuan digital, hingga peretasan dompet elektronik. Semua itu menunjukkan bahwa keamanan siber bukan hanya urusan teknis, tapi juga tanggung jawab bersama, antara pemerintah, ASN, dan warga digital. Oleh karena itu, memahami “apa itu insiden siber” menjadi fondasi penting untuk melangkah ke tahap berikutnya: mengenali tanda-tandanya, mengetahui cara menanganinya, dan berkolaborasi dalam menjaga keamanan digital daerah.

B. Definisi Insiden Siber

Secara sederhana, **insiden siber** adalah setiap kejadian yang mengganggu, mengancam, atau melanggar kerahasiaan, integritas, dan ketersediaan data atau sistem digital. Dengan kata lain, insiden siber terjadi ketika ada aktivitas yang **tidak semestinya**

dalam sistem komputer, jaringan, atau aplikasi, baik karena kesalahan manusia, serangan, maupun kegagalan teknis.

Menurut **Badan Siber dan Sandi Negara (BSSN)**, insiden siber mencakup berbagai hal seperti:

a. Akses ilegal terhadap sistem atau data.
b. Gangguan layanan akibat serangan (*denial of service*).
c. Penyebaran perangkat lunak berbahaya (*malware, ransomware*).
d. Kebocoran atau penyalahgunaan data pribadi.
e. Penyusupan atau manipulasi sistem informasi pemerintah.

Sedangkan dalam standar internasional **ISO/IEC 27035:2023**, insiden siber didefinisikan sebagai: "Satu atau lebih kejadian keamanan informasi yang dapat menimbulkan dampak signifikan terhadap operasi organisasi, keamanan data, atau reputasi."

Dengan dua rujukan ini, dapat disimpulkan bahwa **insiden siber tidak selalu berarti peretasan besar**, tapi juga bisa berupa hal sederhana seperti:

a. Email mencurigakan yang menipu pegawai untuk mengklik tautan palsu.
b. File penting tiba-tiba tidak dapat diakses karena terenkripsi.
c. Aplikasi layanan publik berhenti berfungsi akibat gangguan sistem.
d. Data login bocor karena penggunaan kata sandi yang sama di banyak akun.

Mengapa Penting Memahami Insiden Siber?

Bagi ASN dan masyarakat, memahami definisi insiden siber bukan sekadar pengetahuan teknis, tapi bagian dari **kesiapsiagaan digital**. Tanpa pemahaman yang baik, sebuah insiden kecil, seperti email phishing atau file rusak, bisa berkembang menjadi masalah besar yang mengancam data pribadi, reputasi instansi, bahkan stabilitas layanan publik.

Dengan mengenali sejak dini apa yang disebut "insiden siber", setiap individu dapat:

a. Mengambil langkah cepat untuk mencegah kerusakan lebih lanjut.
b. Melapor dengan benar ke unit yang berwenang, seperti **Tim Tanggap Insiden**

Siber (TTIS) Klungkung.

c. Berkontribusi dalam menjaga ekosistem digital daerah yang aman dan terpercaya.

C. Klasifikasi Umum Insiden Siber

Insiden siber dapat terjadi dalam berbagai bentuk. Tidak semuanya melibatkan peretasan langsung, ada juga yang disebabkan oleh kesalahan manusia, gangguan sistem, atau kelalaian keamanan. Berikut klasifikasi umum insiden siber yang perlu dipahami ASN dan masyarakat:

1. Gangguan Teknis (System Disruption)

Gangguan ini disebabkan oleh kesalahan sistem atau serangan yang membuat layanan digital tidak berfungsi sebagaimana mestinya. Contohnya:

a. Website pelayanan publik tiba-tiba tidak bisa diakses.
b. Sistem administrasi data mengalami *crash* karena *overload*.
c. Aplikasi perizinan daring berhenti bekerja akibat gangguan server.

Dampaknya mungkin terlihat kecil di awal, tetapi bisa menimbulkan kepanikan dan menghambat pelayanan masyarakat.

2. Penyusupan dan Akses Ilegal (Unauthorized Access)

Ini adalah bentuk insiden paling umum di lingkungan pemerintahan. Pelaku berusaha masuk ke sistem tanpa izin, baik dengan mencuri kata sandi, memanfaatkan celah keamanan, atau melalui *phishing*. Contohnya:

a. Akun admin sistem SPBE diretas karena *password* lemah.
b. Akses jaringan internal digunakan oleh pihak luar tanpa izin.
c. Data warga diambil oleh oknum dengan cara menyusup ke sistem instansi.

Akses ilegal dapat mengancam keamanan data publik dan merusak reputasi lembaga pemerintah.

3. Kebocoran Data (Data Breach)

Terjadi ketika informasi sensitif, seperti NIK, dokumen resmi, atau data

kepegawaian, tersebar tanpa izin. Contohnya:

a. File berisi data ASN dibagikan di media sosial.
b. Database aplikasi publik diunduh secara ilegal.
c. Email berisi dokumen penting bocor ke pihak luar.

Kebocoran data menjadi salah satu isu paling serius karena menyangkut kepercayaan masyarakat terhadap pemerintah.

4. Penyalahgunaan Sistem (System Misuse)

Kadang, insiden siber tidak berasal dari serangan luar, tetapi dari dalam organisasi. Contohnya:

a. Pegawai menggunakan akun dinas untuk kepentingan pribadi.
b. Data instansi digunakan untuk tujuan politik atau bisnis.
c. Modifikasi sistem dilakukan tanpa prosedur keamanan yang benar.

Jenis insiden ini sering diabaikan, padahal berpotensi menimbulkan dampak hukum dan etik bagi ASN.

5. Serangan Siber terhadap Infrastruktur Pemerintah (Cyber Attack on Critical Infrastructure)

Serangan ini menargetkan sistem vital daerah seperti jaringan informasi, data pelayanan publik, atau situs resmi pemerintah. Contohnya:

a. Serangan *ransomware* yang mengenkripsi seluruh server pemerintahan daerah.
b. Website resmi disusupi konten provokatif (*defacement*).
c. Aplikasi pelayanan publik menjadi sasaran *botnet attack*.

Serangan jenis ini dapat mengganggu pelayanan masyarakat luas dan membutuhkan respons cepat dari tim keamanan siber.

D. Dampak Langsung dan Tidak Langsung dari Insiden Siber

Sebuah insiden siber bukan hanya sekadar gangguan teknis. Ia bisa menimbulkan efek berantai, mulai dari kerugian pribadi, gangguan pelayanan publik, hingga hilangnya kepercayaan masyarakat. Bagi ASN dan masyarakat, memahami dampak ini sangat

penting agar kita menyadari betapa vitalnya menjaga keamanan digital sehari-hari.

1. Dampak Langsung

Dampak langsung adalah konsekuensi yang muncul segera setelah insiden terjadi. Biasanya terlihat jelas dan mudah diidentifikasi.

- a. Gangguan Operasional

Layanan digital yang terganggu, seperti e-Office, SIMPEG, atau aplikasi perizinan online, membuat proses pelayanan publik berhenti sementara. Contoh: Sistem perizinan daring tidak bisa diakses selama beberapa jam karena serangan *DDoS*.

- b. Kehilangan Data atau Akses

Ketika data penting terhapus, terenkripsi (*ransomware*), atau diambil oleh pihak tidak sah, instansi kehilangan kontrol terhadap aset digitalnya. Bagi masyarakat, kehilangan akses ke akun e-commerce atau perbankan digital bisa berakibat langsung pada kerugian finansial.

- c. Kerugian Finansial

Insiden seperti pencurian dana digital, pembayaran palsu, atau biaya pemulihan sistem dapat menyebabkan kerugian nyata. Di Indonesia, laporan BSSN tahun 2024 mencatat **kerugian ekonomi akibat kejahatan siber mencapai lebih dari Rp 14 triliun**.

- d. Penyebaran Informasi Palsu (Hoaks)

Setelah sistem diretas, pelaku sering memanfaatkan celah itu untuk menyebarkan berita palsu dengan mengatasnamakan instansi. Hal ini dapat menimbulkan kepanikan di masyarakat dan merusak kredibilitas lembaga pemerintah.

2. Dampak Tidak Langsung

Dampak tidak langsung muncul setelah beberapa waktu dan sering kali lebih sulit dipulihkan karena menyangkut kepercayaan dan reputasi.

- a. Hilangnya Kepercayaan Publik

Ketika data pribadi warga bocor, masyarakat menjadi ragu untuk menggunakan

layanan digital pemerintah. Kepercayaan yang rusak sulit diperbaiki, bahkan jika sistem sudah dipulihkan.

- b. Penurunan Produktivitas ASN

ASN yang terdampak insiden sering harus menunggu pemulihan sistem, melakukan laporan, dan audit keamanan. Akibatnya, waktu kerja terbuang dan beban mental meningkat karena tekanan tanggung jawab publik.

- c. Dampak Psikologis dan Sosial

Korban insiden siber, baik ASN maupun warga, dapat mengalami stres, ketakutan, dan kehilangan rasa aman. Misalnya, ketika foto pribadi disebarkan tanpa izin atau akun media sosial digunakan untuk menipu orang lain.

- d. Biaya Pemulihan dan Reputasi

Pemulihan pasca-serangan sering kali memerlukan waktu lama dan biaya besar, terutama untuk mengganti sistem, meningkatkan keamanan, dan mengedukasi pegawai. Lebih parah lagi, reputasi lembaga bisa tercoreng di mata publik dan media.

E. Contoh Kasus Insiden Siber di Indonesia (2023–2025)

Insiden siber di Indonesia semakin meningkat dari tahun ke tahun, seiring dengan pesatnya transformasi digital di pemerintahan dan masyarakat. Data Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa **pada tahun 2024 terjadi lebih dari 400 juta anomali serangan siber**, termasuk upaya *phishing*, *ransomware*, dan kebocoran data pribadi di sektor publik maupun swasta. Berikut adalah beberapa contoh kasus yang dapat menjadi pembelajaran penting bagi ASN dan masyarakat.

1. Kebocoran Data e-HAC Kementerian Kesehatan (2023)

Salah satu kasus besar yang sempat ramai adalah kebocoran data pada aplikasi **Electronic Health Alert Card (e-HAC)** milik Kementerian Kesehatan.

🔍 **Dampak:** Lebih dari 1,3 juta data pengguna, termasuk nama, NIK, dan riwayat perjalanan, bocor di forum daring.

📌 **Penyebab utama:** Pengelolaan server tanpa enkripsi memadai dan lemahnya pengawasan pihak ketiga (vendor).

💡 **Pelajaran:** ASN perlu memastikan data yang dikumpulkan melalui aplikasi publik disimpan dengan sistem terenkripsi dan tidak dibagikan kepada pihak luar tanpa izin resmi.

2. Serangan Ransomware pada Sistem Pemerintahan Daerah (2024)

Pada pertengahan 2024, beberapa **pemerintah daerah di Indonesia**, termasuk salah satu dinas di Jawa Timur dan Sulawesi Selatan, dilaporkan menjadi korban serangan *ransomware*.

🔍 **Dampak:** Sistem administrasi perizinan lumpuh selama beberapa hari, dan pelaku meminta tebusan dalam bentuk mata uang kripto.

📌 **Penyebab utama:** Tidak adanya *backup data* rutin dan keterlambatan dalam melakukan pembaruan sistem keamanan.

💡 **Pelajaran:** ASN harus menerapkan kebiasaan *backup* data berkala dan melakukan update sistem sesuai panduan keamanan CSIRT.

3. Kebocoran Data SIM Card Nasional (2023)

Kejadian ini menimpa salah satu operator besar di Indonesia, di mana **data registrasi SIM card pengguna bocor dan diperjualbelikan di forum internasional**.

🔍 **Dampak:** Ratusan juta data NIK dan nomor telepon terekspos, membuka peluang penyalahgunaan untuk *phishing* dan penipuan digital.

📌 **Penyebab utama:** Lemahnya kontrol terhadap basis data pusat dan belum optimalnya enkripsi data pribadi.

💡 **Pelajaran:** ASN dan masyarakat tidak boleh menyepelekan penyimpanan data pribadi; selalu pastikan nomor identitas dan kontak tidak dibagikan ke situs atau aplikasi yang tidak resmi.

4. Penipuan Digital Mengatasnamakan Instansi Pemerintah (2024–2025)

Kasus lain yang meningkat signifikan adalah munculnya **akun media sosial palsu**

dan situs tiruan (fake domain) yang mengatasnamakan instansi pemerintah daerah, termasuk dinas perizinan dan bantuan sosial.

🔍 **Dampak:** Banyak masyarakat tertipu dan menyerahkan data pribadi atau uang kepada akun palsu tersebut.

📌 **Penyebab utama:** Minimnya verifikasi identitas akun resmi pemerintah dan kurangnya literasi digital masyarakat.

💡 **Pelajaran:** ASN dan masyarakat harus selalu memeriksa situs resmi (.go.id) atau akun terverifikasi, serta melapor ke CSIRT Klungkung jika menemukan akun mencurigakan.

5. Kasus Kebocoran Data MyPertamina (2025)

Pada awal 2025, sempat muncul laporan kebocoran **data pengguna aplikasi MyPertamina**, yang berisi nama, NIK, dan riwayat transaksi bahan bakar.

🔍 **Dampak:** Data pengguna dijual di *dark web* dan berpotensi digunakan untuk rekayasa sosial (*social engineering*).

📌 **Penyebab utama:** Kerentanan API (antarmuka sistem) dan kurangnya pengujian keamanan pada pembaruan aplikasi.

💡 **Pelajaran:** Pengelola sistem pemerintah maupun swasta wajib melakukan *penetration testing* rutin dan audit keamanan digital.

F. Upaya Pencegahan Insiden Siber bagi ASN dan Masyarakat

Pencegahan adalah benteng pertama dalam menghadapi ancaman siber. Sebagian besar serangan digital sebenarnya bisa dihindari jika pengguna memiliki **kedisiplinan, kesadaran, dan kebiasaan aman dalam beraktivitas online.** ASN dan masyarakat sama-sama memiliki peran penting dalam menjaga ruang digital Klungkung tetap aman dan terpercaya.

1. Meningkatkan Literasi Keamanan Digital

Kesadaran dimulai dari pengetahuan. ASN dan masyarakat perlu memahami bentuk ancaman digital seperti *phishing*, *malware*, atau kebocoran data, agar tidak

mudah menjadi korban.

📘 **Langkah praktis:**

a. Ikuti pelatihan keamanan siber dari **BSSN** atau **CSIRT Klungkung** secara berkala.
b. Baca panduan keamanan digital dari situs resmi pemerintah seperti https://bssn.go.id.
c. Hindari sumber informasi yang tidak kredibel atau bersifat sensasional.

🧩 **Tujuan:** agar setiap pengguna digital di Klungkung menjadi "filter keamanan" pertama sebelum teknologi bekerja.

2. Gunakan Password Kuat dan Unik

Password yang lemah adalah pintu termudah bagi peretas. Gunakan kombinasi huruf besar, kecil, angka, dan simbol. Hindari nama anak, tanggal lahir, atau kata umum seperti "123456".

🔐 **Tips cepat:**

a. Gunakan **password manager** (contoh: *Bitwarden, Google Password Manager*).
b. Ganti password setiap 3–6 bulan sekali.
c. Aktifkan **verifikasi dua langkah (2FA)** pada akun penting, termasuk email dinas dan media sosial.

3. Waspadai Email dan Pesan Mencurigakan

Serangan *phishing* masih menjadi cara paling populer untuk mencuri data ASN dan masyarakat. Biasanya dikemas dalam bentuk email atau pesan yang seolah berasal dari lembaga resmi.

⚠️ **Tanda-tanda umum phishing:**

a. Menggunakan domain mirip instansi asli (contoh: @klungkungkab.co bukan .go.id).
b. Mengandung permintaan data pribadi atau tautan mencurigakan.
c. Mengandung pesan mendesak seperti "akun Anda akan diblokir".

📍 **Langkah aman:** Jangan pernah mengklik tautan atau mengunduh lampiran tanpa

verifikasi sumbernya.

4. Amankan Perangkat dan Jaringan

Perangkat digital seperti ponsel dan laptop kini menjadi aset kerja dan pribadi sekaligus. Keamanan perangkat berarti melindungi seluruh data di dalamnya.

🧱 **Langkah perlindungan:**

a. Pasang antivirus atau *endpoint security* yang selalu diperbarui.
b. Aktifkan penguncian otomatis dan sidik jari.
c. Hindari mengakses akun penting menggunakan Wi-Fi publik tanpa VPN.
d. Gunakan jaringan internet resmi atau pribadi untuk urusan pekerjaan ASN.

5. Rutin Melakukan Backup Data

Serangan siber seperti *ransomware* sering membuat data tidak dapat diakses. Backup berkala memastikan data tetap aman meski sistem utama diserang.

💾 **Rekomendasi:**

a. ASN: backup dokumen kerja ke **server instansi atau cloud pemerintah (drive.go.id)**.
b. Masyarakat: gunakan penyimpanan terpercaya seperti **Google Drive** atau **OneDrive**.
c. Simpan salinan offline di media penyimpanan terenkripsi.

6. Laporkan Insiden Secara Cepat dan Tepat

Keterlambatan laporan sering memperburuk dampak insiden. Setiap ASN atau warga yang menemukan indikasi kebocoran, peretasan, atau situs palsu harus segera melapor ke kanal resmi.

📞 **Saluran pelaporan resmi:**

CSIRT Klungkung: https://csirtklungkung.klungkungkab.go.id

🧭 **Manfaat laporan cepat:**

Mencegah penyebaran serangan, mempercepat pemulihan, dan melindungi data publik lainnya.

7. Bangun Budaya Keamanan Siber

Keamanan siber tidak cukup dengan teknologi. Ia harus menjadi budaya, terutama di lingkungan ASN dan masyarakat digital.

🏛️ **Praktik budaya aman digital:**

a. Jangan membagikan akun atau password ke rekan kerja.
b. Gunakan perangkat kantor hanya untuk urusan dinas.
c. Ciptakan kebiasaan “berpikir dulu sebelum klik”.
d. Jadikan keamanan digital bagian dari nilai integritas ASN dan perilaku masyarakat cerdas digital.

Pertanyaan Reflektif

1. Ketika Anda melihat sistem kerja daring di instansi tiba-tiba melambat atau tidak bisa diakses, langkah apa yang seharusnya segera dilakukan untuk memastikan hal itu bukan bagian dari serangan siber?
2. Sebagai ASN yang mengelola data publik, bagaimana cara Anda menjaga agar akun kerja dan perangkat dinas tetap aman dari akses tidak sah?
3. Dalam kehidupan sehari-hari, kebiasaan digital apa yang paling sering Anda lakukan tanpa sadar berisiko memicu insiden siber?
4. Ketika menerima pesan mencurigakan dari alamat email yang tampak resmi, apa strategi Anda untuk memverifikasi kebenaran pesan tersebut sebelum membuka tautan atau lampiran di dalamnya?
5. Banyak masyarakat masih berpikir bahwa insiden siber hanya terjadi di instansi besar atau lembaga nasional. Bagaimana Anda menjelaskan bahwa ancaman ini juga relevan bagi perangkat desa, UMKM, atau sekolah di tingkat lokal?
6. Jika Anda menemukan tanda-tanda serangan pada sistem instansi, kepada siapa laporan pertama seharusnya ditujukan, dan mengapa kecepatan laporan menjadi sangat penting dalam penanganan insiden?
7. Sebagai bagian dari komunitas digital di Kabupaten Klungkung, bagaimana Anda dapat berperan aktif dalam membangun budaya tanggap insiden di lingkungan kerja, keluarga, atau masyarakat sekitar?

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2024). *Panduan Respon Insiden Siber untuk Pemerintah Daerah.* Jakarta: BSSN. https://bssn.go.id/panduan-respon-insiden-siber-2024

Basuki, R. A., & Nurhadi, A. (2023). *Analisis kesiapan pemerintah daerah dalam menangani insiden siber menggunakan kerangka NIST. Jurnal Teknologi Informasi dan Keamanan Siber, 6*(2), 88–102. https://jurnal.bssn.go.id/index.php/jtik/article/view/234

European Union Agency for Cybersecurity (ENISA). (2024). *Threat Landscape 2024: Cyber Incidents and Response in the EU.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Kominfo RI. (2024). *Pedoman Penanganan Insiden Siber untuk ASN dan Instansi Pemerintah.* https://kominfo.go.id/content/detail/47258/pedoman-penanganan-insiden-siber

Li, X., Zhang, Y., & Wang, L. (2024). *AI-assisted incident response in smart city networks: A resilience-based approach. Computers & Security, 140*, 103692. https://doi.org/10.1016/j.cose.2024.103692

Mazari, M. A., Rahman, S., & Ullah, I. (2024). *Cyber incident management and response frameworks for developing nations: A systematic review. Journal of Cybersecurity Research and Practice, 5*(2), 45–62. https://www.researchgate.net/publication/381235799_Cyber_Incident_Management_and_Response_Frameworks

Purnama, D., & Santoso, Y. (2024). *Peran CSIRT dalam meningkatkan ketahanan siber pemerintah daerah di Indonesia. Jurnal Keamanan Siber Nasional, 3*(1), 12–25. https://jurnal.bssn.go.id/index.php/jksn/article/view/312

United Nations Office on Drugs and Crime (UNODC). (2023). *Cybercrime and Incident Response in Southeast Asia: Capacity and Collaboration.* Vienna: UN.

https://www.unodc.org/unodc/en/cybercrime/publications.html

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025.* Geneva: WEF. https://www.weforum.org/publications/global-cybersecurity-outlook-2025

Yuliana, D., & Mahendra, B. (2023). *Studi implementasi manajemen insiden siber di instansi pemerintah daerah. Jurnal Sistem Informasi dan Keamanan Digital, 8*(3), 55–70. https://journal.ui.ac.id/j-siskom/article/view/9087