KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 4: Tanggap Insiden Siber

Subtopik 4.3: Langkah Awal Jika Mengalami Insiden

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 ini *Langkah Awal Jika Mengalami Insiden Siber*. Setelah memahami pengertian dan tanda-tanda insiden pada dua subtopik sebelumnya, kini fokus pembelajaran diarahkan pada apa yang harus dilakukan segera ketika insiden benar-benar terjadi. Dalam praktiknya, banyak kerugian besar terjadi bukan karena serangannya terlalu canggih, tetapi karena tindakan awal yang lambat atau keliru**.**

Melalui subtopik ini, ASN dan masyarakat Kabupaten Klungkung diharapkan mampu bertindak cepat, tepat, dan terkoordinasi dengan mengikuti tiga tahapan utama penanganan insiden: Lapor – Isolasi – Recovery. Pendekatan ini sesuai dengan pedoman Badan Siber dan Sandi Negara (BSSN, 2024) dan praktik terbaik Computer Security Incident Response Team (CSIRT) tingkat nasional. 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

KATA PENGANTAR ii

DAFTAR ISI iii

Tujuan Pembelajaran 4

Sasaran Peserta 4

A. Pengantar: Apa Itu Etika Digital dan Mengapa Penting di Tahun 2025 5

B. Jenis Pelanggaran Etika Digital: Hoaks, Disinformasi, dan Ujaran Kebencian 5

C. Etika Digital bagi ASN: Netralitas, Integritas, dan Tanggung Jawab Bermedia Sosial .. 5

D. Etika Digital bagi Masyarakat: Tanggung Jawab, Literasi, dan Etika Komunikasi di Media Sosial 9

E. Studi Kasus dan Praktik Baik: Hoaks dan Etika Digital di Indonesia & Klungkung 11

F. Prinsip Etika Digital untuk ASN dan Masyarakat 13

G. Dampak Pelanggaran Etika Digital & Konsekuensi Hukum (Hoaks dan Ujaran Kebencian) ..... **Error! Bookmark not defined.**

H. Strategi Membangun Budaya Etika Digital di Lingkungan ASN & Masyarakat ..... **Error! Bookmark not defined.**

Pertanyaan Reflektif 15

DAFTAR PUSTAKA 16

Tujuan Pembelajaran

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

1. Menjelaskan pentingnya langkah awal tanggap insiden siber.
2. Melakukan pelaporan insiden secara benar melalui kanal resmi CSIRT Klungkung atau BSSN.
3. Menerapkan tindakan isolasi untuk mencegah penyebaran serangan.
4. Melakukan pemulihan awal (recovery) dengan prosedur yang aman dan terdokumentasi.
5. Berkoordinasi dengan tim teknis dan keamanan siber untuk memastikan sistem kembali normal dan aman digunakan.

Sasaran Peserta

1. ASN: Agar mampu mengambil langkah cepat dan tepat saat terjadi insiden siber, melapor melalui kanal resmi TTIS Klungkung atau BSSN, serta menjaga bukti digital dan koordinasi sesuai prosedur keamanan instansi.
2. Masyarakat: Agar dapat mengenali insiden siber di lingkungan pribadi, melakukan tindakan awal seperti memutus koneksi dan mengganti sandi, serta melapor ke kanal resmi tanpa menimbulkan kepanikan atau menyebarkan informasi yang belum pasti.

A. Prinsip Umum Penanganan Awal Insiden

Ketika insiden siber terjadi, hal terpenting bukanlah mencari siapa yang salah, melainkan **bagaimana merespons dengan cepat dan benar** agar dampaknya tidak meluas. Penanganan awal yang tepat dapat mencegah gangguan sistem semakin parah dan membantu proses pemulihan berjalan lebih mudah.

Dalam praktik tanggap insiden, dikenal prinsip **"3L" Lapor, Isolasi, dan Recovery.** Ketiga langkah ini menjadi panduan dasar yang wajib dipahami oleh setiap ASN dan masyarakat ketika menghadapi serangan siber, baik di lingkungan kerja maupun pribadi.

1. **Lapor:** Setiap kejadian yang diduga sebagai insiden siber harus segera dilaporkan ke kanal resmi, seperti **Tim Tanggap Insiden Siber (TTIS) Klungkung** atau **CSIRT Klungkung**. Pelaporan dini memungkinkan pihak berwenang melakukan analisis cepat dan memberikan panduan penanganan yang aman.
2. **Isolasi:** Setelah laporan dibuat, langkah berikutnya adalah **menghentikan penyebaran serangan** dengan memutus koneksi internet, menonaktifkan jaringan internal, atau memisahkan perangkat yang terinfeksi. Tahapan ini penting agar kerusakan tidak menjalar ke sistem lain.
3. **Recovery:** Setelah situasi terkendali, dilakukan **pemulihan sistem dan data** dengan tetap menjaga bukti digital untuk investigasi lebih lanjut. Pemulihan awal meliputi pembersihan perangkat, penggantian sandi, serta pemulihan layanan yang terdampak secara bertahap.

Prinsip 3L ini juga menekankan pentingnya **ketenangan dan koordinasi.** Dalam situasi insiden, tindakan tergesa-gesa seperti menghapus file, memformat ulang perangkat, atau menyebarkan kabar belum pasti justru dapat memperburuk keadaan. ASN dan masyarakat perlu memahami bahwa setiap insiden siber memiliki nilai pembelajaran untuk memperkuat ketahanan digital di masa depan.

B. Langkah 1 – Lapor (Reporting)

Langkah pertama dalam menghadapi insiden siber adalah **melapor dengan cepat**

ke pihak yang berwenang di tingkat daerah. Pelaporan yang tepat waktu dan melalui jalur resmi memungkinkan tim tanggap insiden melakukan investigasi awal dan menekan dampak yang lebih luas.

Di Kabupaten Klungkung, **Tim Tanggap Insiden Siber (TTIS)** berperan sebagai **garda pertama** yang menerima laporan insiden dari ASN maupun masyarakat. Jika insiden dinilai berdampak besar atau membutuhkan dukungan teknis lanjutan, barulah **TTIS Klungkung berkoordinasi dengan BSSN (Badan Siber dan Sandi Negara)** di tingkat nasional.

1. Tujuan Pelaporan

Pelaporan insiden dilakukan untuk:

a. Mengaktifkan mekanisme penanganan cepat di tingkat daerah.
b. Mencegah meluasnya dampak serangan pada sistem lain.
c. Menyediakan data awal dan bukti bagi investigasi forensik digital.
d. Menjadi dasar evaluasi keamanan siber di masa mendatang.

2. Alur Pelaporan Resmi (Tingkat Daerah ke Nasional)

a. Masyarakat dan ASN**:** Melaporkan insiden ke **TTIS/CSIRT Klungkung** sebagai pintu pertama penanganan.
b. TTIS Klungkung: Melakukan verifikasi, mitigasi awal, dan bila diperlukan, **meneruskan laporan ke BSSN** untuk pendampingan teknis dan koordinasi nasional.

Kanal Pelaporan Resmi Klungkung

Tingkat	Pihak	Kanal	Kontak
Daerah (Utama)	**TTIS / CSIRT Klungkung**	Website resmi	https://csirtklungkung.klungkungkab.go.id
		Hotline	0366 5551705

3. Informasi Minimal yang Perlu Disampaikan

Informasi	Penjelasan
Waktu kejadian	Tanggal dan jam ketika insiden terdeteksi
Sistem/Akun terdampak	Aplikasi, server, atau akun yang bermasalah
Gejala awal	Misalnya tidak bisa login, muncul pesan aneh, atau file hilang
Tindakan sementara	Langkah awal yang sudah dilakukan (misalnya memutus jaringan)
Bukti digital	Screenshot, log aktivitas, atau email mencurigakan (tidak dihapus)

4. Etika Pelaporan

a. **Tenang dan terkoordinasi**: jangan menyebarkan kabar insiden di media sosial.
b. **Laporkan langsung ke TTIS/CSIRT daerah**, bukan ke forum publik.
c. **Jaga kerahasiaan data dan bukti digital** agar investigasi tidak terganggu.

Melapor melalui TTIS Klungkung bukan hanya prosedur, tetapi wujud **tanggung jawab digital bersama** untuk menjaga keamanan informasi daerah. TTIS menjadi penghubung antara masyarakat, ASN, dan pemerintah pusat dalam memastikan setiap insiden ditangani secara profesional.

C. Langkah 2 – Isolasi (Containment)

Setelah laporan insiden disampaikan ke **TTIS Klungkung**, langkah berikutnya yang harus segera dilakukan adalah **isolasi**. Tujuan isolasi adalah **menghentikan penyebaran serangan**, **menjaga bukti digital tetap utuh**, dan **melindungi sistem lain yang belum terdampak**.

Langkah ini tidak bertujuan memperbaiki sistem secara langsung, tetapi **menahan dampak agar tidak semakin meluas**. Dalam konteks pemerintahan daerah, tindakan isolasi biasanya dilakukan **bersama tim teknis atau TTIS Klungkung** dengan panduan dari BSSN jika diperlukan.

1. Tujuan Isolasi

a. Menghentikan aktivitas serangan sebelum menjalar ke sistem lain.
b. Melindungi jaringan internal dan data penting dari kerusakan lanjutan.
c. Menjaga bukti digital agar bisa digunakan untuk analisis forensik.

2. Langkah Isolasi untuk ASN

Apabila insiden terjadi di lingkungan kerja instansi:

a. **Putus sementara koneksi internet atau jaringan lokal (LAN)** pada perangkat yang dicurigai.
b. **Nonaktifkan sistem layanan publik** yang terdampak, misalnya aplikasi perizinan, kepegawaian, atau arsip digital, untuk mencegah kebocoran data.
c. **Jangan hapus file mencurigakan**, log sistem, atau email yang menjadi sumber insiden. Data tersebut diperlukan oleh TTIS untuk analisis.
d. **Segera koordinasikan dengan TTIS Klungkung atau admin TIK instansi** agar langkah teknis dilakukan secara aman.

3. Langkah Isolasi untuk Masyarakat

Jika insiden terjadi pada perangkat pribadi atau akun media sosial:

a. **Matikan koneksi internet atau data seluler** untuk menghentikan aktivitas mencurigakan.
b. **Jangan gunakan akun atau perangkat yang terkena insiden** untuk transaksi atau komunikasi sampai dinyatakan aman.
c. **Ubah kata sandi dari perangkat lain** yang bersih dan belum terinfeksi.
d. Laporkan kejadian ke **TTIS Klungkung** melalui kanal resmi agar tim dapat memberikan panduan lanjutan.

4. Hal yang Harus Dihindari

a. **Jangan panik dan jangan langsung memperbaiki sistem sendiri.** Perbaikan tanpa panduan bisa menghapus bukti digital penting.
b. **Jangan menyebarkan informasi insiden ke media sosial**, karena dapat menimbulkan kepanikan dan mengganggu proses penanganan.

c. **Jangan menyalakan ulang perangkat berulang kali**, karena dapat mengubah jejak digital yang sedang dianalisis.

5. Peran TTIS Klungkung dalam Tahap Isolasi

TTIS Klungkung berfungsi memberikan **bimbingan teknis dan dukungan langsung** kepada ASN maupun masyarakat. Tim ini akan:

a. Menilai tingkat keparahan insiden.
b. Memberi instruksi isolasi sesuai standar keamanan BSSN.
c. Melakukan koordinasi dengan perangkat daerah terkait untuk menahan penyebaran.
d. Menyimpan log atau bukti digital dengan prosedur forensik.

Langkah isolasi ini merupakan **titik kritis** dalam penanganan insiden siber. Kecepatan dan ketepatan pada tahap ini menentukan apakah serangan bisa dihentikan lebih awal atau justru berkembang menjadi gangguan besar. Karena itu, **koordinasi dengan TTIS Klungkung menjadi keharusan utama** setiap kali terjadi insiden di lingkungan ASN maupun masyarakat.

D. Langkah 3 – Pemulihan Awal (Recovery)

Setelah insiden berhasil dikendalikan dan sistem diisolasi dengan aman, tahap berikutnya adalah **pemulihan (*recovery*)**. Tahap ini bertujuan untuk **mengembalikan sistem dan data ke kondisi normal** sekaligus memastikan **keamanan baru telah diperkuat** agar insiden serupa tidak terulang. Pemulihan awal dilakukan secara **bertahap dan terkoordinasi**, biasanya di bawah pendampingan **TTIS Klungkung**, terutama jika insiden melibatkan sistem pemerintahan daerah atau data publik.

1. Tujuan Pemulihan Awal

a. Mengembalikan fungsi layanan digital, sistem kerja, atau perangkat terdampak.
b. Memastikan seluruh malware, akses ilegal, atau celah keamanan telah dihapus.
c. Melindungi data agar tidak kembali bocor atau terinfeksi.
d. Memulihkan kepercayaan pengguna terhadap sistem digital.

2. Langkah Recovery untuk ASN

Apabila insiden terjadi di lingkungan kerja instansi:

a. **Gunakan backup data terakhir yang sudah diverifikasi aman** oleh TTIS atau admin TIK.
b. **Perbarui sistem keamanan (*security patch*)** dan pastikan seluruh perangkat lunak resmi.
c. **Ganti seluruh password dan kredensial akses** (terutama akun admin, email dinas, dan portal kerja).
d. **Lakukan uji fungsi sistem (*testing*)** sebelum kembali dioperasikan penuh.
e. **Koordinasikan dengan TTIS Klungkung** untuk memastikan sistem benar-benar bersih dan stabil.

3. Langkah Recovery untuk Masyarakat

Jika insiden terjadi di perangkat pribadi atau akun digital:

a. **Lakukan pemindaian antivirus menyeluruh** dengan aplikasi keamanan terpercaya.
b. **Pulihkan data dari salinan cadangan (*backup*)** yang disimpan di media eksternal atau cloud aman.
c. **Perbarui semua aplikasi dan sistem operasi** ke versi terbaru.
d. **Ubah seluruh kata sandi** dan aktifkan **verifikasi dua langkah (2FA)** untuk akun penting seperti email, media sosial, dan dompet digital.
e. **Konsultasikan dengan TTIS Klungkung** jika masih ditemukan aktivitas mencurigakan.

4. Dokumentasi dan Evaluasi

Setelah pemulihan selesai, penting untuk membuat **laporan pasca-insiden**. Dokumentasi ini menjadi dasar evaluasi dan pembelajaran agar kasus serupa tidak terjadi kembali. Isi laporan biasanya mencakup:

a. Kronologi singkat insiden dan langkah yang dilakukan.
b. Sistem atau akun yang terdampak.

c. Data yang berhasil dipulihkan dan yang hilang.
d. Rekomendasi peningkatan keamanan dari TTIS.
e. Dokumentasi dikirim ke **TTIS Klungkung** sebagai bagian dari arsip daerah dan koordinasi rutin dengan BSSN.

5. Peran TTIS Klungkung dalam Tahap Recovery

Pada tahap ini, TTIS Klungkung akan:

a. Melakukan **verifikasi keamanan pasca-pemulihan**.
b. Memberikan panduan teknis pemulihan data dan sistem.
c. Menyusun **laporan pasca-insiden daerah (*Incident Post-Mortem Report*)** untuk disampaikan ke BSSN.
d. Memberikan rekomendasi peningkatan sistem keamanan bagi ASN dan masyarakat.

Dengan menyelesaikan tahap pemulihan secara benar dan terkoordinasi, ASN maupun masyarakat bukan hanya memulihkan sistem, tetapi juga **memperkuat ketahanan digital daerah**. Setiap insiden yang ditangani dengan baik menjadi **pelajaran berharga** untuk membangun **Klungkung yang Aman Siber**: siap, tanggap, dan resilien menghadapi ancaman digital masa depan.

E. Studi Kasus

Kasus: Serangan Phishing pada Akun Email Dinas (2025)

Pada awal tahun 2025, salah satu pegawai di lingkungan Pemerintah Kabupaten Klungkung menerima email dengan subjek **"Pembaruan Data ASN SPBE"** yang tampak dikirim dari domain resmi pemerintah. Tanpa menyadari bahwa email tersebut palsu, pegawai tersebut mengklik tautan di dalam pesan dan memasukkan akun serta kata sandinya.

Beberapa jam kemudian, akun email dinasnya digunakan untuk mengirimkan pesan serupa ke seluruh rekan kerja di instansi tersebut. Aktivitas ini terdeteksi oleh tim IT karena adanya lonjakan pengiriman email mencurigakan dari satu akun pegawai.

Langkah Penanganan (Penerapan Prinsip 3L)

1. **Lapor**

   Pegawai yang akunnya disusupi segera melapor ke **TTIS Klungkung** dan bagian TIK instansinya. Laporan disampaikan lengkap dengan tangkapan layar (screenshot) email mencurigakan dan waktu kejadian. TTIS kemudian mencatat insiden tersebut sebagai **phishing terarah (targeted phishing)** dan segera memberikan panduan penanganan ke unit terkait.

2. **Isolasi**

   Tim IT instansi langsung **memutus sementara akses email pegawai tersebut**, serta **menonaktifkan tautan berbahaya** di seluruh server surat elektronik internal. Semua pegawai diimbau **tidak membuka email serupa** dan segera mengganti kata sandi masing-masing. TTIS Klungkung melakukan verifikasi bahwa tidak ada data penting yang bocor.

3. **Recovery**

   Setelah sistem dinyatakan aman, akun pegawai tersebut **diaktifkan kembali** dengan kata sandi baru dan pengamanan tambahan berupa ***Two-Factor Authentication*** **(2FA)**. TTIS Klungkung juga memberikan **briefing singkat** kepada seluruh ASN mengenai cara mengenali phishing dan kewajiban melapor cepat bila terjadi kejadian serupa.

Hasil dan Pembelajaran

Penanganan cepat dan koordinasi yang baik antara pegawai, tim IT, dan TTIS Klungkung membuat insiden ini **tidak berkembang menjadi kebocoran data**. Kasus ini menjadi **contoh nyata pentingnya pelaporan dini dan isolasi cepat**, serta menunjukkan bagaimana prosedur 3L dapat mencegah kerugian yang lebih besar di lingkungan pemerintahan daerah.

Pelajaran utama:

> **“Satu klik bisa jadi masalah besar, tapi satu laporan cepat bisa menyelamatkan sistem.”**

F. Rekomendasi Praktis untuk ASN dan Masyarakat

Penanganan insiden siber tidak berhenti setelah sistem pulih. Diperlukan kebiasaan baru dan langkah pencegahan agar kejadian serupa tidak terulang. Berikut beberapa rekomendasi praktis yang dapat diterapkan oleh ASN dan masyarakat di Klungkung untuk memperkuat ketahanan siber daerah.

1. Untuk ASN

a. **Lapor cepat, jangan tunda.** Setiap tanda atau kejadian mencurigakan segera dilaporkan ke **TTIS Klungkung** melalui kanal resmi, meskipun tampak sepele.
b. **Simpan bukti digital.** Jangan menghapus email, log, atau file mencurigakan sebelum tim teknis melakukan pemeriksaan.
c. **Pisahkan akun pribadi dan akun dinas.** Gunakan perangkat kerja hanya untuk urusan kedinasan.
d. **Perbarui sistem secara rutin.** Pastikan komputer, aplikasi, dan antivirus selalu menggunakan versi terbaru.
e. **Ikuti pelatihan keamanan siber.** ASN dianjurkan mengikuti sosialisasi atau simulasi tanggap insiden minimal dua kali dalam setahun.

2. Untuk Masyarakat

a. **Laporkan ke TTIS Klungkung lebih dulu.** Jika akun, perangkat, atau data pribadi terdampak, hubungi TTIS sebelum membuat laporan ke kanal nasional.
b. **Gunakan password kuat dan verifikasi dua langkah (2FA).** Hindari penggunaan kata sandi yang sama di berbagai akun.

c. **Lakukan backup data berkala.** Simpan salinan data penting di media eksternal atau cloud yang aman.
d. **Hindari menyebarkan informasi insiden ke publik.** Jangan membagikan tangkapan layar atau kabar insiden di media sosial tanpa izin TTIS.
e. **Edukasi keluarga dan lingkungan.** Ajak anggota keluarga untuk mengenali cara melapor dan menjaga keamanan perangkat pribadi.

3. Untuk TTIS / Pemerintah Daerah

a. **Perkuat jalur komunikasi satu pintu.** Pastikan masyarakat dan ASN mengetahui cara melapor ke TTIS.
b. **Lakukan simulasi insiden berkala.** Minimal dua kali setahun agar semua perangkat daerah siap menghadapi insiden nyata.
c. **Bangun sistem monitoring aktif.** Gunakan alat pemantau aktivitas jaringan dan sistem agar anomali bisa terdeteksi lebih cepat.
d. **Berbagi pembelajaran.** Setelah insiden ditangani, TTIS perlu menyampaikan hasil evaluasi dan pembelajaran kepada instansi lain di Klungkung sebagai referensi pencegahan.

Dengan menerapkan rekomendasi ini secara disiplin, baik ASN maupun masyarakat akan menjadi bagian dari **rantai pertahanan siber daerah** yang saling mendukung. Ketika setiap orang tahu cara melapor, menahan, dan memulihkan insiden, maka seluruh ekosistem digital Klungkung akan menjadi **lebih tangguh dan resilien** menghadapi ancaman siber.

Pertanyaan Reflektif

1. Ketika sistem atau akun Anda tiba-tiba tidak bisa diakses dan muncul aktivitas mencurigakan, langkah apa yang paling pertama harus dilakukan sebelum mencoba memperbaikinya sendiri?
2. Mengapa penting untuk melapor terlebih dahulu ke TTIS Klungkung dan tidak langsung menyebarkan informasi insiden ke media sosial?
3. Dalam situasi darurat siber, bagaimana Anda memastikan proses isolasi dilakukan dengan benar tanpa menghapus bukti digital yang diperlukan untuk investigasi?
4. Setelah proses recovery selesai, langkah apa yang sebaiknya dilakukan ASN atau masyarakat untuk memastikan sistem benar-benar aman digunakan kembali?
5. Apa manfaat mencatat kronologi dan tindakan yang dilakukan selama penanganan insiden bagi proses evaluasi keamanan di masa depan?
6. Bagaimana Anda, sebagai ASN atau anggota masyarakat digital Klungkung, dapat membantu membangun budaya lapor cepat dan tanggap siber di lingkungan kerja atau komunitas Anda?

DAFTAR PUSTAKA

Aditya Putra, F. (2022). Tata Kelola Ekosistem Berbagi Informasi Keamanan Siber pada Information Sharing and Analysis Center (ISAC) Sektor Pemerintah Daerah di Indonesia. *Info Kripto*, *16*(1), 23–32. https://doi.org/10.56706/ik.v16i1.39

Arafat, M., & Wirasto, A. T. E. (2024). Kebijakan Kriminal dalam Penanganan Siber di Era Digital: Studi Kasus di Indonesia. *Equality : Journal of Law and Justice*, *1*(2), 220–241. https://doi.org/10.69836/equality-jlj.v1i2.170

Chotimah, H. C. (2019). Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency. *JURNAL POLITICA*, *10*(2), 113–128. https://doi.org/10.22212/ jp.v10i1.1447

Christy Natalia, M., & Anindya Wijayanti, R. (2024). Analisis Kemampuan Security Incident Response PT XXX dalam Mengelola Insiden Siber. *Info Kripto*, *18*(1), 31–38. https://doi.org/10.56706/ik.v18i1.98

Dinata, A. C., & Syafaat, A. (2025). Peran BSSN dalam Menangani Ancaman Siber di Indonesia. *Jurnal Kebijakan Keamanan Nasional*, *01*(01), 14–28. https://www.academia.edu/130321206/Peran_BSSN_dalam_Menangani_Ancaman_Siber_di_Indonesia

Firmansyah, M., & Yuswanto, A. (2022). Manajemen Pengetahuan Penanganan Insiden Keamanan Informasi Pada Security Operation Center Di Pemerintah Provinsi Dki Jakarta Knowledge Management for Information Security Incident Handling At Security Operation Center of Jakarta Provincial Government. *Jurnal Inovasi Aparatur*, *4*(2), 441–452.

Khotimah, H., Bimantoro, F., Kabanga, R. S., & Widiartha, I. B. K. (2022). Implementasi Security Information And Event Management (SIEM) Pada Aplikasi Sms Center Pemerintah Daerah Provinsi Nusa Tenggara Barat. *Jurnal Begawe Teknologi Informasi (JBegaTI)*, *3*(2), 213–219. https://doi.org/10.29303/jbegati.v3i2.752

Prabaswari, Alfikri, M., & Ahmad, I. (2022). Evaluasi Implementasi Kebijakan

Pembentukan Tim Tanggap Insiden Siber pada Sektor Pemerintah. *Matra Pembaruan, Jurnal Inovasi Kebijakan*, *6*(1), 1–13. https://doi.org/10.21787/mp.6.1.2022.1-14

Sembiring, F., & Pattihahuan, F. M. (2024). PERAN BADAN SIBER DAN SANDI NEGARA DALAM KASUS SERANGAN SIBER YANG MENGAKIBATKAN KEBOCORAN DATA PRIBADI PUSAT DATA NASIONAL SEMENTARA 2 (PDNS2). *Jurnal Gloria Justitia*, *2*, 116–134. https://doi.org/10.25170/gloriajustitia.v5i1.6807

Sitanggang, A. S., Darmawan, F., & Manurung, D. S. (2024). Hukum Siber dan Penegakan Hukum di Indonesia: Tantangan dan Solusi Memerangi Kejahatan Siber. *Jurnal Pendidikan Dan Teknologi Indonesia*, *4*(3), 79–83. https://doi.org/10.52436/1.jpti.409

Sutra, S. M., & Haryanto, A. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan. *Global Political Studies Journal*, *7*(1), 56–69. https://doi.org/10.34010/gpsjournal.v7i1

Syawaluddin, A. S., H, A. F. P., & A, M. P. (2025). Cyber Security Dan Ketahanan Nasional: Tantangan Dan Solusi Di Era Digital. *Jurnal Media Akademik (JMA)*, *3*(6), 3031–5220. https://doi.org/10.62281

Tommy, S., & Nasution, M. I. P. (2025). EVALUASI MANAJEMEN RISIKO KEAMANAN SIBER PADA INFRASTRUKTUR DIGITAL PEMERINTAH : STUDI KASUS PUSAT DATA NASIONAL (PDN) Prodi Manajemen , Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Sumatera Utara I . Pendahuluan Dalam era transformasi dig. *Jurnal Manajemen Ekonomi Dan Bisnis (JMEB)*, *04*(01), 1–26. https://doi.org/10.61715

Yusron, M. (2025). Pembinaan peningkatan kapasitas SDM tim tanggap insiden siber pemerintah daerah Provinsi Banten. *Jurnal Cahaya Nusantara*, *1*(2), 3093–8113. https://jurnal.cahayapublikasi.com/index.php/jcn