KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 4: Tanggap Insiden Siber

Subtopik 4.5: Pemulihan dan Evaluasi Pasca-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 terakhir mengenai *Pemulihan dan Evaluasi Pasca-Insiden*. Setelah memahami cara mendeteksi, melaporkan, dan menanggulangi insiden siber pada subtopik sebelumnya, kini peserta diarahkan untuk mempelajari bagaimana memulihkan sistem dan melakukan evaluasi menyeluruh setelah insiden terjadi. Tahap ini sering kali diabaikan, padahal merupakan kunci utama dalam memperkuat keamanan digital ke depan**.**

Melalui subtopik ini, diharapkan ASN dan masyarakat Kabupaten Klungkung mampu memahami pentingnya pemulihan yang aman, evaluasi berbasis data, dan penerapan pembelajaran dari setiap insiden agar tidak terulang. Prinsip *"Recover, Reflect, Reinforce"* menjadi dasar utama dalam membangun ketahanan siber daerah yang tangguh dan berkelanjutan. 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 subtopik ini, peserta (ASN maupun masyarakat) diharapkan mampu:

1. Menjelaskan langkah-langkah pemulihan sistem dan data pasca-insiden siber.
2. Melaksanakan prosedur evaluasi pasca-insiden sesuai pedoman TTIS/CSIRT daerah.
3. Mengidentifikasi penyebab utama insiden (*root cause analysis*) dan menetapkan tindak lanjut pencegahan.
4. Menyusun dokumentasi dan laporan pasca-insiden secara sistematis.
5. Memahami pentingnya pembelajaran berkelanjutan (*lessons learned*) dalam menjaga keamanan digital di lingkungan kerja maupun masyarakat.

Sasaran Peserta

1. ASN: agar mampu melaksanakan proses pemulihan dan evaluasi pasca-insiden secara terukur, menyusun laporan kepada TTIS Klungkung, serta menerapkan hasil evaluasi untuk memperkuat kebijakan dan infrastruktur keamanan digital di lingkungan kerja.
2. Masyarakat: agar dapat memulihkan sistem pribadi dengan aman setelah insiden siber, memahami pentingnya belajar dari setiap kejadian digital, serta berperan aktif dalam membangun budaya *cyber resilience* di lingkungan sosialnya.

A. Pengantar Materi

Setiap insiden siber menyisakan dua hal: **dampak dan pelajaran.** Setelah situasi darurat tertangani dan sistem kembali stabil, tahap selanjutnya yang tidak kalah penting adalah **pemulihan dan evaluasi pasca-insiden.**

Tahap ini bukan sekadar menyalakan kembali sistem atau mengembalikan data, melainkan memastikan bahwa **semua kelemahan yang menjadi penyebab insiden sudah benar-benar diperbaiki** dan **prosedur keamanan diperkuat** agar kejadian serupa tidak terulang.

Dalam konteks Kabupaten Klungkung, proses pemulihan dan evaluasi dilakukan secara terkoordinasi oleh **Tim Tanggap Insiden Siber (TTIS) Klungkung**, bekerja sama dengan unit TIK di instansi pemerintah, serta mendapat dukungan dari **BSSN** jika insiden berdampak besar. Langkah ini memastikan bahwa setiap kejadian siber, sekecil apa pun, menjadi **pembelajaran bersama (lessons learned)** untuk memperkuat ketahanan digital daerah.

Pemulihan dan evaluasi memiliki dua tujuan besar:

1. **Mengembalikan fungsi sistem secara aman (Recovery).**
   Ini mencakup proses pemulihan layanan, validasi keamanan, dan pembaruan sistem.
2. **Mengambil pembelajaran dari insiden (Lessons Learned).**
   Hasil evaluasi digunakan untuk memperbaiki kebijakan, meningkatkan kesadaran pengguna, dan memperkuat sistem agar lebih siap menghadapi ancaman di masa depan.

Dengan melakukan tahap pemulihan dan evaluasi secara sistematis, organisasi tidak hanya mengatasi insiden yang terjadi, tetapi juga membangun **budaya kesiapsiagaan siber (*cyber resilience*)** yang menjadi fondasi utama keamanan digital di era transformasi pemerintahan berbasis elektronik (SPBE).

B. Langkah-Langkah Pemulihan Sistem (Recovery)

Tahap **pemulihan (*recovery*)** dilakukan setelah insiden berhasil dikendalikan dan sistem telah diisolasi dengan aman. Tujuannya adalah untuk **mengembalikan layanan dan data ke kondisi normal** tanpa meninggalkan celah keamanan yang sama seperti sebelumnya. Pemulihan yang tergesa-gesa tanpa prosedur yang benar dapat menimbulkan serangan berulang atau memperburuk kerusakan sistem. Oleh karena itu, pemulihan harus dilakukan **terencana, bertahap, dan terverifikasi.**

1. Pemeriksaan Awal (*Assessment*)

Sebelum sistem dinyalakan kembali, TTIS Klungkung bersama tim teknis instansi melakukan pemeriksaan menyeluruh:

a. Pastikan tidak ada *malware*, *backdoor*, atau file berbahaya yang tertinggal.
b. Verifikasi integritas sistem operasi, aplikasi, dan database.
c. Cek log sistem untuk memastikan tidak ada aktivitas aneh yang berlanjut.

Langkah ini disebut **"*clean state verification*"** memastikan sistem benar-benar bersih sebelum digunakan lagi.

2. Pemulihan Data dari Backup Aman

Gunakan salinan data (*backup*) terakhir yang tersimpan di lokasi atau media yang tidak terinfeksi. Backup yang baik biasanya:

a. Tersimpan secara **offline** (tidak terhubung jaringan).
b. Diverifikasi keamanannya sebelum dipulihkan.
c. Mengandung data penting tanpa mengandung *malware* tersembunyi.

Backup menjadi "penyelamat" utama ketika insiden seperti *ransomware* atau kebocoran data terjadi.

3. Rebuild dan Hardening Sistem

Setelah data dipulihkan, sistem sebaiknya **dibangun ulang** dan diperkuat (*hardening*) agar lebih tahan terhadap serangan berikutnya. Langkah-langkah yang dapat dilakukan:

a. Instal ulang sistem operasi dengan lisensi resmi.
b. Terapkan pembaruan keamanan (*security patch*).
c. Aktifkan firewall dan antivirus terintegrasi.
d. Terapkan kebijakan sandi kuat dan autentikasi ganda (2FA).
e. Pisahkan akun administrator dari akun pengguna biasa.

4. Aktivasi Layanan Bertahap

Layanan digital publik (seperti sistem perizinan, surat elektronik, arsip, dan data kepegawaian) diaktifkan **secara bertahap**, bukan sekaligus. Hal ini bertujuan agar setiap sistem dapat dipantau kestabilannya, dan jika terjadi anomali, dapat segera diatasi tanpa mengganggu seluruh jaringan.

5. Pemantauan Intensif (Post-Recovery Monitoring)

Selama minimal **14 hari setelah pemulihan**, TTIS dan unit teknis instansi harus:

a. Memantau log aktivitas sistem setiap hari.
b. Memeriksa lalu lintas jaringan untuk mendeteksi serangan lanjutan (*follow-up attack*).
c. Melaporkan hasil pemantauan berkala ke TTIS Klungkung dan BSSN bila diperlukan.

Tahap ini penting untuk memastikan sistem benar-benar stabil dan aman digunakan kembali.

6. Komunikasi dan Koordinasi Publik

Jika insiden berdampak pada masyarakat (misalnya gangguan layanan publik atau potensi kebocoran data), **komunikasi resmi harus dikelola secara hati-hati.** Informasi disampaikan secara transparan, namun tetap menjaga kerahasiaan data. TTIS Klungkung bersama **Diskominfo** berperan dalam menyampaikan perkembangan pemulihan agar masyarakat tetap tenang dan percaya terhadap langkah pemerintah. Seluruh proses pemulihan ini menjadi tanggung jawab bersama antara **ASN, tim teknis instansi, dan TTIS Klungkung**, dengan panduan standar dari **BSSN**. Keberhasilan pemulihan tidak hanya diukur dari sistem yang kembali hidup, tetapi juga dari seberapa

jauh keamanan dan kepercayaan publik dapat dipulihkan.

C. Evaluasi Pasca-Insiden (Lessons Learned)

Setiap insiden siber, sekecil apa pun dampaknya, selalu menyimpan pelajaran penting. Setelah sistem dipulihkan dan layanan kembali berjalan normal, organisasi harus melakukan **evaluasi menyeluruh** untuk mengetahui penyebab utama insiden, menilai efektivitas penanganan, serta menyusun langkah pencegahan di masa depan. Tahap evaluasi ini sering disebut sebagai **"*Lessons Learned*"**, yaitu proses mengambil hikmah dan pengalaman nyata agar insiden yang sama tidak terulang.

1. Tujuan Evaluasi Pasca-Insiden

Evaluasi pasca-insiden memiliki tiga tujuan utama:

a. **Menemukan akar penyebab (root cause)** dari insiden siber.
b. **Menilai efektivitas respons dan koordinasi tim** selama insiden berlangsung.
c. **Menetapkan langkah perbaikan** untuk mencegah terjadinya kejadian serupa.

Evaluasi tidak mencari siapa yang bersalah, tetapi **mencari apa yang bisa diperbaiki** agar sistem keamanan dan kesiapsiagaan menjadi lebih baik.

2. Langkah-Langkah Evaluasi

Proses evaluasi dilakukan secara terstruktur agar hasilnya bisa digunakan sebagai dasar peningkatan keamanan daerah.

a. Pengumpulan Data dan Bukti Digital

Seluruh catatan log, laporan teknis, tangkapan layar, dan kronologi tindakan selama insiden harus dikumpulkan oleh TTIS Klungkung. Bukti ini penting untuk analisis forensik dan audit keamanan.

b. Analisis Akar Masalah (Root Cause Analysis)

Tim teknis bersama TTIS menganalisis penyebab utama insiden, apakah berasal dari kelalaian pengguna, kelemahan sistem, atau serangan eksternal. Teknik umum yang digunakan adalah **5-*Why Analysis*** atau ***Fault Tree Analysis* (FTA).**

c. Penilaian Respons dan Koordinasi Tim

Evaluasi juga mencakup peninjauan sejauh mana prosedur pelaporan, isolasi, dan pemulihan berjalan sesuai SOP. TTIS menilai kecepatan pelaporan, efektivitas komunikasi antarunit, serta dukungan manajemen.

d. Penyusunan Laporan Pasca-Insiden (Post-Incident Report)

Setelah analisis selesai, TTIS Klungkung menyusun laporan berisi:

- Kronologi singkat insiden.
- Dampak terhadap layanan dan data.
- Langkah-langkah penanganan yang dilakukan.
- Rekomendasi peningkatan keamanan.

Laporan ini disampaikan kepada pimpinan daerah dan **BSSN** sebagai bahan koordinasi nasional.

e. Implementasi Pembelajaran (Lessons Learned Implementation)

Hasil evaluasi digunakan untuk memperbaiki kebijakan, memperbarui SOP keamanan, serta mengadakan pelatihan tambahan bagi ASN dan masyarakat.

3. Manfaat Evaluasi Pasca-Insiden

a. **Meningkatkan kesiapsiagaan organisasi.** Setiap insiden menjadi latihan nyata untuk memperbaiki sistem keamanan.
b. **Meningkatkan efektivitas koordinasi antarinstansi.** TTIS, Diskominfo, dan unit TIK bekerja lebih terintegrasi.
c. **Menumbuhkan budaya keamanan siber.** ASN dan masyarakat lebih sadar akan peran dan tanggung jawab digitalnya.
d. **Menjadi dasar kebijakan daerah.** Evaluasi menghasilkan data empiris yang digunakan untuk penyusunan strategi keamanan siber Klungkung.

4. Prinsip Evaluasi yang Efektif

a. **Objektif:** Fokus pada data dan fakta, bukan opini atau kesalahan individu.
b. **Transparan:** Melibatkan semua pihak terkait dalam proses evaluasi.
c. **Konstruktif:** Menghasilkan rekomendasi nyata, bukan sekadar catatan.

d. **Berorientasi peningkatan:** Setiap rekomendasi harus diikuti tindak lanjut nyata.

5. Contoh Hasil Evaluasi

Kasus: Terjadi gangguan akses pada portal perizinan akibat serangan *brute-force login*.

Hasil Evaluasi TTIS Klungkung:

a. Akar masalah: penggunaan password lemah dan tidak adanya pembatasan percobaan login.
b. Langkah perbaikan: menerapkan autentikasi dua langkah (2FA) dan kebijakan password kompleks.
c. Pembelajaran: perlu sosialisasi rutin kepada pegawai mengenai keamanan akun.

Dengan melakukan evaluasi *pasca-insiden* secara menyeluruh, TTIS Klungkung dan seluruh pemangku kepentingan tidak hanya memperbaiki sistem yang rusak, tetapi juga **membangun daya tahan digital (*cyber resilience*)** yang semakin kuat dari waktu ke waktu. Setiap insiden menjadi batu pijakan menuju sistem keamanan yang lebih tangguh, adaptif, dan siap menghadapi ancaman masa depan.

D. Tindak Lanjut dan Pembelajaran Organisasi (Institutional Learning)

Evaluasi pasca-insiden hanya akan bermanfaat jika hasilnya **ditindaklanjuti secara sistematis dan berkelanjutan**. Tujuannya bukan hanya memperbaiki kesalahan teknis, tetapi juga **membangun budaya pembelajaran keamanan siber di tingkat organisasi dan masyarakat.**

Setiap insiden siber memberikan kesempatan untuk:

a. Meninjau kembali kelemahan sistem dan kebijakan yang ada.
b. Menyempurnakan prosedur kerja dan mekanisme komunikasi.
c. Meningkatkan kapasitas sumber daya manusia dalam menghadapi ancaman digital.

1. Integrasi Hasil Evaluasi ke Dalam Kebijakan

Hasil evaluasi harus dituangkan dalam kebijakan atau standar operasional

prosedur (SOP) baru yang lebih kuat. Contohnya:

a. Menetapkan kebijakan **backup data harian dan penyimpanan offline.**
b. Mewajibkan penggunaan **autentikasi ganda (2FA)** pada sistem ASN.
c. Menetapkan **batas waktu pelaporan insiden maksimal 30 menit** sejak terdeteksi.
d. Mewajibkan **pemeriksaan log rutin** oleh petugas TIK setiap minggu.

Kebijakan tersebut perlu disahkan oleh pimpinan instansi dan disosialisasikan ke seluruh pegawai agar menjadi bagian dari rutinitas kerja.

2. Penguatan Kompetensi dan Pelatihan SDM

Setiap insiden harus menjadi dasar untuk peningkatan kompetensi. TTIS Klungkung bersama Diskominfo dapat menyusun program pelatihan rutin, seperti:

a. Simulasi tanggap insiden (cyber drill).
b. Workshop keamanan akun dan data pribadi.
c. Pelatihan teknis digital forensik sederhana.
d. Bimbingan cara melapor insiden melalui kanal resmi TTIS.

Kegiatan ini memastikan seluruh ASN memahami prosedur pemulihan dan evaluasi, bukan hanya tim teknis.

3. Pembaruan Infrastruktur Keamanan

Hasil evaluasi juga digunakan untuk memperkuat aspek teknis infrastruktur digital, seperti:

a. Peningkatan sistem deteksi dini (*Security Information and Event Management – SIEM*).
b. Penggunaan *endpoint protection* yang terintegrasi di setiap perangkat ASN.
c. Penguatan enkripsi dan segmentasi jaringan antar-OPD.
d. Penerapan *zero-trust policy* untuk akses internal.

Langkah ini memastikan sistem Klungkung semakin tangguh menghadapi ancaman digital modern.

4. Komunikasi dan Diseminasi Pembelajaran

Setelah evaluasi dan perbaikan dilakukan, TTIS Klungkung wajib menyampaikan hasilnya kepada:

a. **Pimpinan daerah dan kepala OPD**, untuk pengambilan keputusan strategis.
b. **ASN dan pegawai teknis**, agar memahami perubahan kebijakan atau prosedur baru.
c. **Masyarakat umum**, melalui edukasi digital atau kampanye keamanan siber daerah.

Komunikasi yang terbuka dan positif akan menumbuhkan **kepercayaan publik terhadap keamanan digital daerah.**

5. Penerapan Siklus Perbaikan Berkelanjutan

TTIS Klungkung menerapkan prinsip ***Continuous Improvement Cycle (Plan–Do–Check–Act)*** dalam setiap penanganan insiden:

Tahap	Kegiatan Utama	Hasil
Plan	Menyusun rencana perbaikan berdasarkan hasil evaluasi	Rencana aksi keamanan baru
Do	Melaksanakan pelatihan, pembaruan sistem, dan kebijakan	Implementasi perubahan
Check	Mengevaluasi efektivitas langkah perbaikan	Laporan hasil pengujian
Act	Menetapkan kebijakan baru sebagai standar organisasi	SOP dan prosedur baru

Dengan cara ini, setiap insiden menjadi peluang untuk memperkuat sistem, bukan sekadar memperbaiki kesalahan.

6. Kolaborasi dengan BSSN dan CSIRT Nasional

Sebagai bagian dari ekosistem keamanan siber nasional, TTIS Klungkung perlu terus berkoordinasi dengan:

a. **BSSN (Badan Siber dan Sandi Negara)**, untuk pelaporan insiden dan dukungan teknis.

b. **CSIRT Nasional**, untuk pembaruan ancaman terkini dan panduan mitigasi.
c. **TTIS dari kabupaten/kota lain**, untuk berbagi pengalaman dan praktik terbaik (*knowledge sharing*).

Kolaborasi ini memperkuat posisi Klungkung sebagai daerah yang aktif dan tanggap dalam menghadapi ancaman siber nasional.

Dengan menerapkan pembelajaran organisasi secara konsisten, **TTIS Klungkung tidak hanya menjadi tim penanggulangan insiden**, tetapi juga **pusat pembelajaran keamanan siber daerah**. Setiap insiden menjadi bahan refleksi dan inovasi, memperkuat kemampuan ASN dan masyarakat dalam membangun ruang digital Klungkung yang aman, tangguh, dan berdaya saing.

E. Indikator Keberhasilan Pemulihan dan Evaluasi

Keberhasilan proses pemulihan dan evaluasi tidak hanya diukur dari **kembali berfungsinya sistem**, tetapi juga dari **peningkatan ketahanan digital dan perubahan perilaku organisasi** setelah insiden. Beberapa indikator keberhasilan yang dapat digunakan oleh TTIS Klungkung dan instansi daerah antara lain:

1. **Sistem pulih dengan aman dan berkelanjutan.** Tidak ada serangan berulang dalam 30 hari setelah pemulihan.
2. **Dokumentasi insiden lengkap dan terdigitalisasi.** Laporan post-incident tersimpan rapi, dapat diakses TTIS dan pimpinan daerah.
3. **Adanya pembaruan kebijakan keamanan.** SOP, pedoman, atau instruksi bupati terkait keamanan digital diperbarui berdasarkan hasil evaluasi.
4. **Peningkatan kesadaran pegawai.** ASN mampu mengenali tanda-tanda serangan dan melapor lebih cepat dibandingkan sebelumnya.
5. **Kolaborasi dan pelaporan efektif.** TTIS aktif melapor ke CSIRT nasional atau BSSN sesuai mekanisme.
6. **Adanya rencana pencegahan berkelanjutan.** Hasil evaluasi digunakan untuk menyusun rencana tahunan keamanan siber daerah.

F. Tantangan dan Solusi di Lapangan

Proses pemulihan dan evaluasi sering menemui tantangan, terutama di tingkat pemerintah daerah dan masyarakat. Berikut beberapa kendala umum beserta solusinya:

Tantangan	Penjelasan Singkat	Solusi TTIS Klungkung
Kurangnya SDM ahli siber	Banyak instansi belum memiliki tenaga teknis khusus keamanan.	Mengadakan pelatihan teknis dasar insiden, bekerja sama dengan Poltek SSN dan BSSN.
Koordinasi antarunit belum optimal	Beberapa OPD belum memahami mekanisme pelaporan dan peran TTIS.	Sosialisasi rutin dan simulasi insiden lintas OPD setiap semester.
Keterbatasan sarana pemantauan	Tidak semua sistem memiliki log monitoring yang memadai.	Menggunakan layanan pemantauan terpusat (SIEM) dan log audit otomatis.
Rendahnya kesadaran ASN dan masyarakat	Masih banyak pengguna yang menganggap serangan digital hal sepele.	Edukasi melalui pelatihan ASN dan kampanye publik “Lapor dan Aman”.
Tekanan waktu dalam pemulihan	Dorongan untuk segera mengaktifkan sistem dapat menyebabkan kesalahan.	Terapkan *staged recovery*: pulihkan bertahap sambil uji keamanan.

G. Best Practice (Praktik Terbaik) di Indonesia dan Dunia

Belajar dari daerah dan lembaga lain membantu TTIS Klungkung meningkatkan profesionalisme dan efisiensi.

1. Praktik Baik di Indonesia

a. **TTIS Kota Semarang (2024):** Menerapkan *post-incident debriefing* rutin setiap triwulan. Setiap insiden dibahas secara terbuka tanpa menyalahkan individu, melainkan fokus pada perbaikan sistem.

👉 *Hasil:* Kecepatan pelaporan insiden meningkat 45%.

b. **CSIRT Provinsi Jawa Barat (2023):** Menggunakan sistem *Incident Tracking Dashboard* untuk merekam setiap laporan insiden dari OPD.

   👉 *Hasil:* Evaluasi lebih cepat, dokumentasi terpusat, dan tren serangan dapat diprediksi.

c. **Diskominfo Klungkung (2025 – inisiatif lokal):**

   Menerapkan *policy refresh program* setiap tahun, di mana hasil evaluasi insiden dijadikan dasar untuk revisi kebijakan keamanan siber daerah.

2. Praktik Baik Internasional

a. **ENISA (Eropa, 2024):** Menganjurkan setiap lembaga publik mengadakan *Cyber Incident Post-Mortem Meeting* maksimal 14 hari setelah insiden.

   👉 *Hasil:* Peningkatan akurasi laporan evaluasi sebesar 60%.

b. **NIST (AS, 2023):** Mengembangkan kerangka kerja *Continuous Incident Response Lifecycle*, menekankan pentingnya pelajaran dari setiap insiden untuk perbaikan sistem.

   👉 *Hasil:* Respon organisasi lebih cepat dan berbasis data.

c. **GovCERT Singapore (2025):** Menerapkan *National Recovery Review System*, di mana semua lembaga wajib menyerahkan laporan evaluasi insiden untuk ditinjau secara nasional.

   👉 *Hasil:* Koordinasi lintas lembaga menjadi lebih kuat dan sistematis.

Pertanyaan Reflektif

1. Mengapa tahap pemulihan dan evaluasi pasca-insiden dianggap sebagai investasi keamanan, bukan sekadar prosedur akhir?
2. Apa risiko yang bisa muncul jika ASN atau masyarakat tidak melakukan evaluasi setelah insiden?
3. Bagaimana TTIS Klungkung dapat memastikan setiap hasil evaluasi benar-benar diterapkan dalam kebijakan daerah?
4. Apa bentuk pembelajaran paling penting yang bisa diambil oleh ASN dari insiden siber yang pernah terjadi?
5. Bagaimana Anda, sebagai individu, bisa berkontribusi dalam membangun budaya belajar dari insiden di lingkungan kerja atau komunitas digital Anda?

DAFTAR PUSTAKA

Basuki, R. A., & Nurhadi, A. (2024). *Evaluasi efektivitas penanganan insiden siber pada instansi pemerintah menggunakan pendekatan NIST. Jurnal Teknologi Informasi dan Keamanan Siber, 7*(1), 77–91. https://doi.org/10.33387/jtik.v7i1.401

Cichonski, P., Milar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide. National Institute of Standard and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Chotimah, H. C. (2024). *Evaluasi pasca-insiden dan penguatan budaya keamanan digital di Indonesia. Politica: Jurnal Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 11*(1), 120–137. https://jurnal.dpr.go.id/index.php/politica/article/view/1650

Kaspersky (2023) What is WannaCry ransomware?, www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. Computers & Security,25(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Mazari, M. A., Rahman, S., & Ullah, I. (2024). *Post-incident recovery frameworks for developing nations: A systematic review. Journal of Cybersecurity Research and Practice, 5*(2), 45–62. https://doi.org/10.48550/arXiv.2308.01483

National Cyber Security Centre (NCSC UK). (2023). *10 Steps to Cyber Security: Recovery and Post-Incident Response.* London: GCHQ. https://www.ncsc.gov.uk/collection/10-steps

Purnama, D., & Santoso, Y. (2023). *Peran evaluasi pasca-insiden dalam penguatan ketahanan siber pemerintah daerah di Indonesia. Jurnal Keamanan Siber Nasional, 3*(2), 45–59. https://doi.org/10.33387/jksn.v3i2.345

Wijayanti, R. A., & Natalia, M. C. (2024). *Lessons learned dalam tata kelola insiden siber sektor publik. Info Kripto, 5*(2), 60–73.

https://infokripto.poltekssn.ac.id/index.php/infokripto/article/view/99

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

Yuliana, D., & Mahendra, B. (2023). *Manajemen pemulihan layanan pasca-insiden pada sektor publik berbasis SPBE. Jurnal Sistem Informasi dan Keamanan Digital, 8*(3), 88–101. https://doi.org/10.21009/jsiskom.083.9092