KOMDIGI | BLSDM KOMDIGI YOGYAKARTA

YOUR DATA, YOUR SECURITY!

2026

Laporan Keamanan Siber 2025 & Proyeksi 2026

Global · ASEAN · Indonesia

Table Of Contents

01
Pendahuluan

Latar Belakang

Perkembangan teknologi digital telah membawa perubahan besar dalam berbagai aspek kehidupan, mulai dari sektor ekonomi, pemerintahan, hingga layanan publik. Aktivitas masyarakat kini semakin bergantung pada internet dan sistem digital yang memberikan kemudahan, efisiensi, serta akses informasi yang lebih cepat dalam berbagai bidang.

Namun di balik manfaat tersebut, transformasi digital juga meningkatkan risiko terhadap ancaman keamanan siber. Infrastruktur digital seperti sistem keuangan, layanan pemerintahan, dan platform komunikasi menjadi target berbagai serangan siber yang semakin kompleks dan terorganisir.

Secara global, jumlah serangan siber terus meningkat setiap tahunnya, baik dari segi frekuensi maupun dampaknya terhadap sistem digital. Salah satu bentuk serangan yang paling umum adalah Distributed Denial of Service (DDoS) yang bertujuan melumpuhkan layanan dengan membanjiri sistem menggunakan lalu lintas data dalam jumlah besar, serta berbagai bentuk fraud atau penipuan digital seperti phishing dan pencurian data yang dapat menimbulkan kerugian bagi individu maupun organisasi.

EVOLUSI ANCAMAN SIBER

Perjalanan evolusi ancaman siber mencerminkan akselerasi teknologi itu sendiri. Apa yang dulu membutuhkan tim ahli teknis yang besar dan waktu berbulan-bulan kini dapat direplikasi oleh individu tanpa keahlian khusus dalam hitungan menit, berkat proliferasi alat berbasis AI. Perubahan ini membuat batas antara pengguna biasa dan pelaku ancaman semakin tipis, sehingga setiap inovasi teknologi membawa risiko baru yang harus terus dipahami dan diantisipasi.

Fase: Eksplorasi (1990-an)
Virus dan worm menyebar via disket dan email, dengan motivasi ketenaran di komunitas hacker.

Fase: Kriminalisasi (2000-an)
Internet massal menjadi lahan subur untuk botnet, spam, dan pencurian identitas.

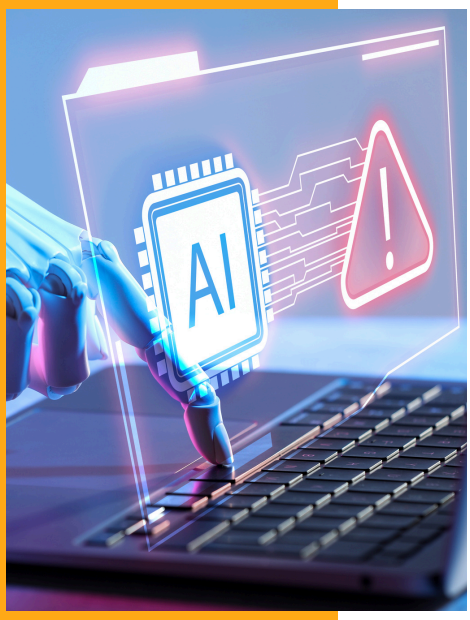
Fase: Eskalasi Negara (2010-an)
Serangan ke infrastruktur negara dan kebocoran data masif terjadi semakin sering.

Fase: Demokratisasi (2020-2022)
Pandemi COVID-19 mempercepat digitalisasi, memunculkan Ransomware-as-a-Service.

Fase: AI Warfare (2023-2030)
AI menjadi senjata utama, meningkatkan serangan phishing dan ransomware yang mengkhawatirkan.

MASALAH KEAMANAN SIBER DI TAHUN 2025

Generative AI telah menjadi titik infleksi terbesar dalam sejarah keamanan siber. Untuk pertama kalinya, teknologi yang sama digunakan secara masif di kedua sisi: oleh penyerang untuk melancarkan serangan yang lebih canggih dan murah, sekaligus oleh defender untuk mendeteksi dan merespons ancaman lebih cepat.



AI Sebagai Senjata Penyerang

- Penjahat siber menggunakan AI untuk membuat pesan phishing yang sangat meyakinkan dan dipersonalisasi dalam ratusan bahasa secara otomatis.
- Penyerang menciptakan deepfake video dan audio untuk penipuan Business Email Compromise (BEC).
- Penyerang bisa mengembangkan malware yang bermutasi secara otomatis untuk menghindari deteksi antivirus.
- Menggunakan AI untuk mengidentifikasi celah keamanan dalam sistem target secara massal dan lebih cepat dari sebelumnya.

AI Sebagai Perisai Pertahanan

Di sisi defensif, organisasi yang mengadopsi AI dalam sistem keamanan mereka membuktikan keunggulan yang signifikan. Data IBM 2025 menunjukkan organisasi dengan AI-driven security mampu memperpendek breach lifecycle hingga 80 hari dan menghemat rata-rata USD 1,9 juta per insiden dibanding organisasi tanpa automasi.

02
Global

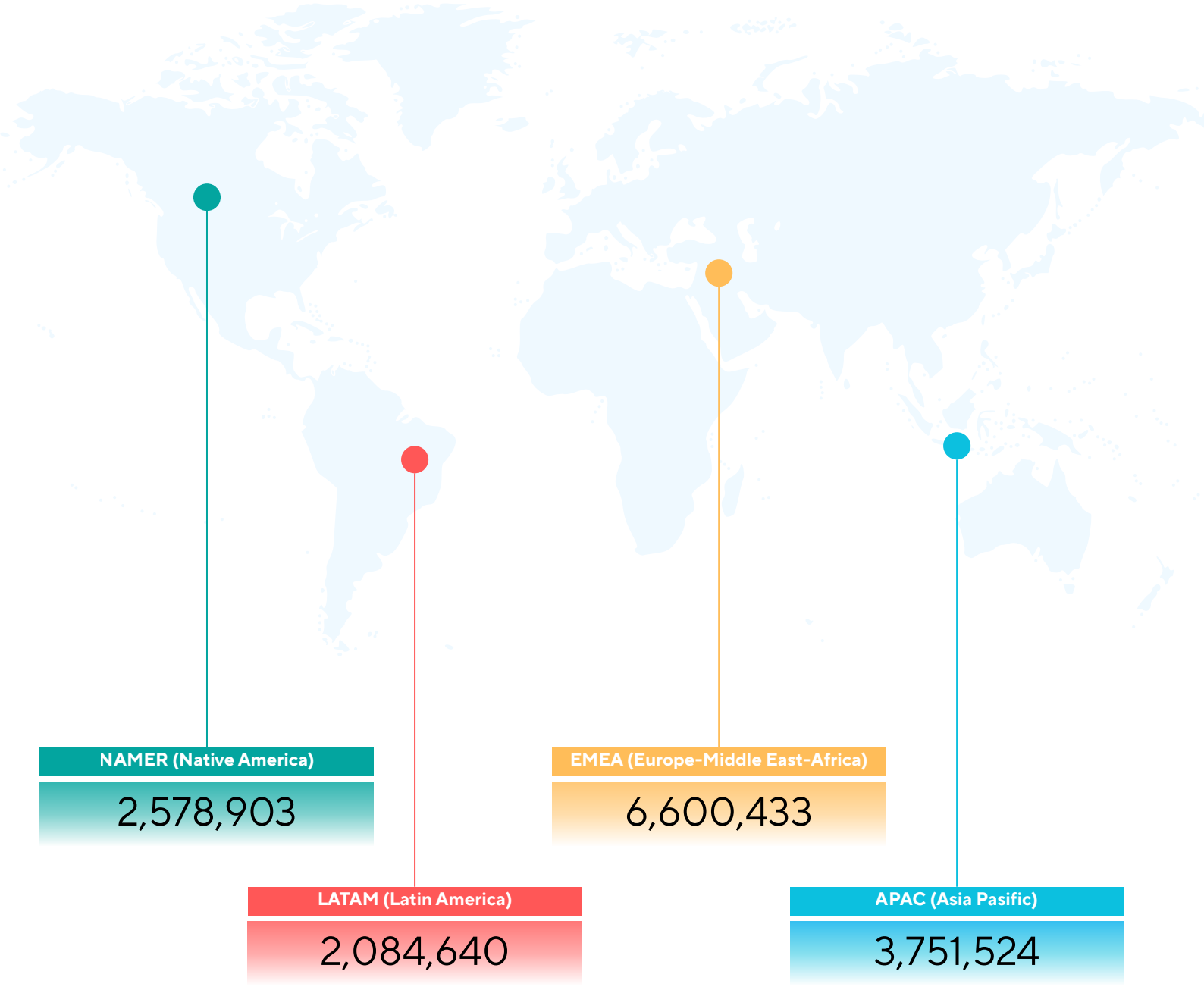
TEMUAN SERANGAN GLOBAL DAN REGIONAL

Tahun 2025

Serangan DDoS Global

Total Serangan

16,151,434



Sumber : NetScout DDoS Threat Intelligence Report Issue 15 & 16

TEMUAN TAHUN 2025

Serangan Global DDoS

- Serangan Distributed Denial of Service (DDoS) secara global terus mengalami peningkatan yang signifikan. Tercatat lebih dari 8 juta serangan DDoS terjadi di 203 negara, yang menunjukkan semakin besarnya risiko operasional bagi organisasi dan perusahaan yang bergantung pada infrastruktur digital.

Serangan DDoS Pada World Economic Forum Februari 2025

- Selama pembukaan hingga penutupan acara, terdeteksi lebih dari 1.400 serangan DDoS dengan berbagai skala dan metode serangan. Peristiwa ini menunjukkan bahwa acara internasional berskala besar juga dapat menjadi target serangan siber yang bertujuan mengganggu layanan digital dan infrastruktur komunikasi.

Kejahatan Siber Dengan Bantuan AI

- Beberapa kasus kejahatan siber kini memanfaatkan kecerdasan buatan (AI) sebagai alat bantu serangan. Contohnya adalah penipuan menggunakan teknologi deepfake untuk meniru wajah atau suara seseorang, serta penggunaan platform AI seperti ChatGPT atau Claude untuk membantu menyusun kode serangan. Selain itu, pelaku juga dapat mengembangkan sistem AI sendiri untuk memantau target dan menjalankan serangan secara otomatis.

Lonjakan Serangan Ransomware Global

- Sepanjang tahun 2025, ransomware tetap menjadi ancaman paling dominan. Banyak kelompok ransomware seperti LockBit, Lynx, dan Virlock menyerang berbagai sektor mulai dari perusahaan teknologi, pendidikan, hingga pemerintahan. Serangan ini biasanya menggunakan metode double extortion, yaitu mengenkripsi data sekaligus mencuri data untuk memeras korban.

Serangan Siber Semakin Berpusat Pada Sektor-Sektor Vital

- Serangan siber saat ini semakin banyak menargetkan sektor-sektor penting yang memiliki peran vital dalam kehidupan masyarakat dan perekonomian. Infrastruktur kritis seperti sektor energi, keuangan, kesehatan, transportasi, serta layanan pemerintahan menjadi sasaran utama karena sistem digital yang digunakan dalam sektor tersebut menyimpan data penting dan mendukung operasional layanan publik.

NEGARA DENGAN KEKUATAN SIBER PALING MENGANCAM

Rusia

Kelompok kriminal siber canggih yang didukung dan berafiliasi dengan negara

Cina

Operasi spionase siber berskala besar yang terorganisir

Amerika Serikat

Unit siber elit dengan tenaga ahli dan profesional terbaik di dunia

Korea Utara

Kejahatan siber bermotif finansial dan aksi gangguan terhadap sistem strategis

Iran

Operasi siber yang menargetkan sektor energi dan pertahanan nasional

India

Komunitas peretas etis (ethical hacker) yang terus berkembang pesat

Ukraina

Pertahanan siber masa perang yang tangguh dan aktif

Israel

Unit siber militer tingkat lanjut dengan teknologi ofensif dan defensif mutakhir

Inggris

Tenaga kerja siber terampil didukung pertahanan siber nasional yang kuat

Brasil

Komunitas peretas dengan pengaruh luas di tingkat regional maupun internasional

Sumber : CloudSEK Top 10 Countries Hit Hardest by Cybercrime in 2025

NEGARA DENGAN SERANGAN SIBER TERBANYAK PADA TAHUN 2025

01 Amerika Serikat — 31.020
Sektor : Keuangan · Kesehatan · Lembaga Federal
Penyerang : LockBit, Black Basta, Royal

02 India — 13.883
Sektor : Fintech · Perbankan Online · Platform Publik
Penyerang : Phishing massal

03 Prancis — 7.622
Sektor : Portal Pemerintah · Media · Perbankan
Penyerang : DDoS, Hacktivist

04 Jerman — 7.144
Sektor : Manufaktur · Otomotif · Teknik
Penyerang : Spionase industri APT

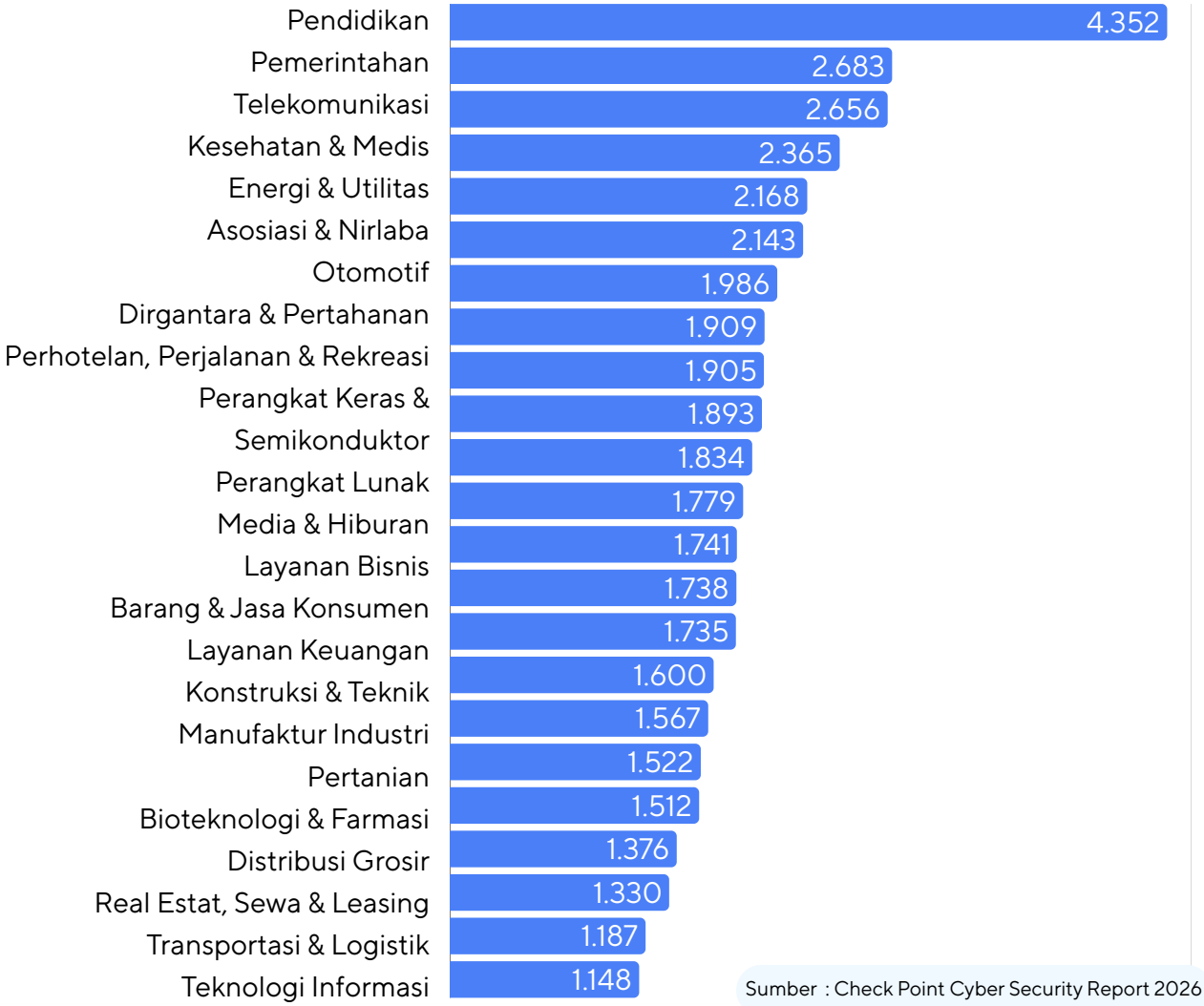
05 Inggris — 2.622
Sektor : Perbankan · Telekomunikasi · Ritel
Penyerang : Phishing, Ransomware

06 Kanada — 2.581
Sektor : Kesehatan · Pendidikan · Energi
Penyerang : Ransomware lintas batas

Data di atas menunjukkan jumlah serangan yang dilaporkan. Volume insiden bervariasi tergantung pada kebijakan pengungkapan dan transparansi pelaporan, yang berarti angka yang dilaporkan tidak selalu mencerminkan keseluruhan skala serangan yang telah dicoba.

Sumber : CloudSEK Top 10 Countries Hit Hardest by Cybercrime in 2025

SEKTOR YANG RENTAN TERHADAP SERANGAN SIBER DI KANCAH GLOBAL



Sumber : Check Point Cyber Security Report 2026

Berdasarkan Check Point Cyber Security Report 2026, Pada tahun 2025 sektor Pendidikan menjadi target serangan siber tertinggi secara global dengan rata-rata 4.352 serangan per minggu, jauh melampaui sektor lainnya. Tingginya angka ini didorong oleh infrastruktur keamanan yang umumnya kurang memadai serta besarnya volume data pengguna yang tersimpan.

Sektor Pemerintahan (2.683), Telekomunikasi (2.656), dan Kesehatan & Medis (2.365) menyusul di posisi berikutnya. Ketiganya menjadi incaran utama karena menyimpan data sensitif bernilai tinggi. Sementara sektor Energi & Utilitas (2.168) turut menjadi perhatian serius mengingat dampak serangan yang berpotensi mengganggu layanan publik secara luas.

National Cyber Security Index

Top 10 Rankings

NCSI (National Cyber Security Index) yang dikembangkan oleh e-Governance Academy Estonia adalah tolok ukur komprehensif kesiapan keamanan siber nasional. Indeks ini menilai kebijakan, infrastruktur, kapabilitas respons insiden, dan program edukasi publik suatu negara.

Nilai Digital Development Level (tingkat perkembangan digital keseluruhan) Czechia (Ceko) memimpin dengan skor 98.33 meski skor DDL-nya bukan yang tertinggi di antara top-10. Ini membuktikan bahwa kesiapan keamanan siber lebih ditentukan oleh fokus kebijakan dan implementasi daripada kekayaan teknologi semata. Estonia di posisi ketiga menjadi model global: setelah menjadi korban serangan siber besar Rusia pada 2007, Estonia justru bertransformasi menjadi salah satu ekosistem digital paling aman di dunia.

Rank	Negara	Skor NCSI	Skor DDL
1	**Czechia**	98,33	72,93
2	**Canada**	96,67	78,14
3	**Estonia**	96,67	82,56
4	**Finland**	95,83	85,76
5	**Lithuania**	95,00	75,53
6	**Moldova**	94,17	62,66
7	**Belgium**	94,17	73,55
8	**Hungary**	93,33	67,88
9	**Albania**	92,50	62,34
10	**Romania**	92,50	64,57

Sumber : ncsi.ega.ee (2025)

Regulasi Internasional

- **NATO Cyber Defence Pledge (2025)**: NATO resmi mengklasifikasikan serangan siber besar sebagai casus belli yang dapat memicu respons kolektif, mendorong seluruh anggotanya untuk meningkatkan anggaran pertahanan siber.
- **EU Cyber Resilience Act (2024-2025)**: Uni Eropa mewajibkan standar keamanan siber untuk semua produk dengan elemen digital yang dijual di pasar Eropa, memperluas regulasi jauh melampaui NIS2 Directive.
- **US National Cybersecurity Strategy 2023-2025**: Amerika Serikat memprioritaskan keamanan infrastruktur kritis, meningkatkan kapabilitas ofensif, dan mendorong liability bagi vendor software yang mengabaikan keamanan.
- **Global Cybercrime Treaty (2024)**: Perjanjian kejahatan siber global pertama di bawah naungan PBB mulai dirundingkan, mencerminkan urgensi kerja sama internasional dalam melawan kejahatan siber lintas batas.

03
Asia Tenggara

ANCAMAN DI WILAYAH INDONESIA

Malware & Botnet

Mirai Botnet mendominasi deteksi malware BSSN pada 2025, diikuti Remcos RAT (Remote Access Trojan) dan Generic Trojan. Botnet ini tidak hanya mencuri data tetapi juga merekrut perangkat korban termasuk router rumahan dan perangkat IoT untuk melancarkan serangan DDoS terhadap target lain.

Penelitian AwanPintar.id mencatat 133,4 juta serangan di Indonesia hanya pada semester pertama 2025, dengan DDoS dan eksploitasi CVE sebagai metode dominan.

Social Engineering & Deepfake

Laporan BSSN 2025 menekankan lonjakan serangan social engineering yang memanfaatkan AI generatif, termasuk deepfake voice dan video palsu tokoh publik. Modus ini terutama menargetkan departemen keuangan perusahaan, pegawai pemerintah, dan nasabah perbankan digital.

BSSN juga melakukan cyber patrol untuk mendukung Satgas PASTI OJK dalam memberantas aktivitas keuangan ilegal digital.

Ransomware & Phishing Berbasis AI

BSSN mengidentifikasi ransomware dan phishing berbasis AI sebagai dua ancaman paling merusak bagi ekosistem finansial dan pemerintahan Indonesia. Sebuah bank regional Asia Tenggara harus menghentikan layanan digital selama lebih dari 48 jam akibat serangan ransomware, menimbulkan kerugian miliaran rupiah dan kepanikan nasabah. Phishing berbasis AI kini membuat email penipuan hampir tidak dapat dibedakan dari komunikasi resmi, bahkan oleh sistem keamanan profesional.

ANCAMAN KHAS ASIA TENGGARA 2025

Pada tahun 2025, Asia Tenggara menghadapi berbagai ancaman seperti kejahatan siber, terorisme, perdagangan manusia, serta dampak perubahan iklim juga menjadi tantangan bagi negara-negara yang tergabung dalam *Association of Southeast Asian Nations*. Oleh karena itu, kerja sama regional diperlukan untuk menjaga keamanan dan stabilitas kawasan.

Scam-as-a-Service

Fenomena paling meresahkan di Asia Tenggara adalah berkembangnya 'Scam-as-a-Service' layanan penipuan siber terorganisir yang dioperasikan dari kompleks perbudakan siber (cyber slavery) di wilayah perbatasan Myanmar, Kamboja, dan Laos. Operasi ini mempekerjakan ribuan korban perdagangan manusia untuk melancarkan penipuan digital berskala masif ke seluruh kawasan dan global.

Serangan Infrastruktur Finansial Digital

Dengan adopsi layanan keuangan digital yang pesat, sektor fintech menjadi target prioritas. Lebih dari 50% konsumen di Thailand, Filipina, Malaysia, Indonesia, dan Singapura melaporkan pernah menghadapi skema penipuan siber setidaknya sekali per minggu angka yang mencerminkan betapa masifnya eksposur risiko di level individu.

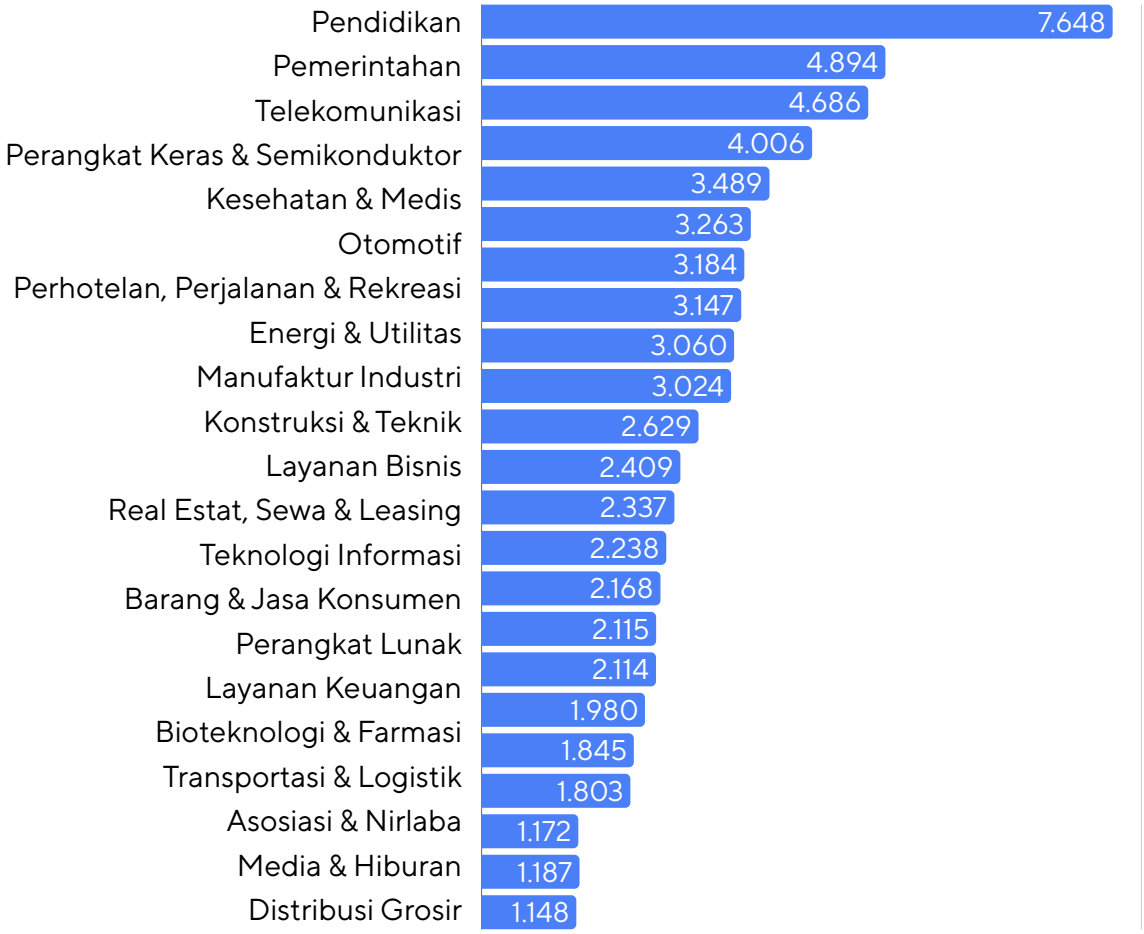
QR Code Exploitation

Serangan berbasis QR code yang sebelumnya marak di China mulai menyebar ke seluruh Asia Tenggara pada 2025. Pengguna diarahkan ke situs phishing atau mengunduh malware melalui QR code yang dipasang di tempat umum, menggantikan QR code resmi. Kaspersky melaporkan lonjakan 40% serangan berbasis QR code di kawasan ASEAN pada semester pertama 2025.

Spionase Siber Geopolitik

Ketegangan geopolitik di Laut China Selatan semakin memperparah ancaman spionase siber. Hacker yang terhubung dengan pemerintah China dilaporkan meningkatkan serangan terhadap negara-negara ASEAN sebesar 20% pada 2024-2025, menargetkan server pemerintah untuk mencuri informasi diplomatik dan militer sensitif di Thailand, Malaysia, Vietnam, Indonesia, dan Myanmar.

SEKTOR YANG RENTAN TERHADAP SERANGAN SIBER DI KAWASAN ASIA TENGGARA



Sumber : Check Point Cyber Security Report 2026

Berdasarkan Check Point Cyber Security Report 2026, Pada tahun 2025 Pendidikan menjadi sektor yang paling banyak diserang dengan 7.648 serangan per minggu, jauh melampaui sektor lainnya. Disusul Pemerintahan (4.894), Telekomunikasi (4.686), dan Perangkat Keras & Semikonduktor (4.006) yang masuk dalam kelompok teratas karena menyimpan data strategis bernilai tinggi.

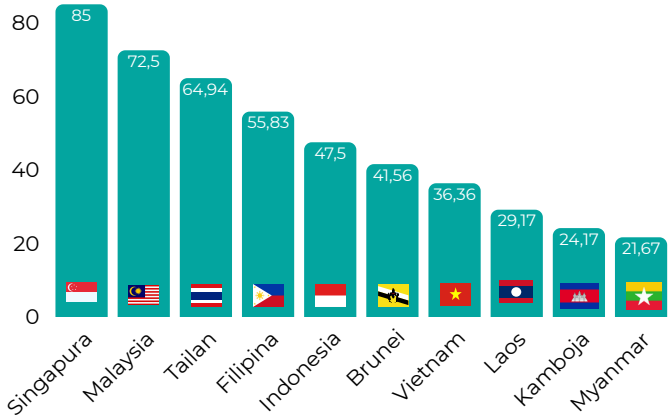
Sektor Kesehatan & Medis, Otomotif, Energi & Utilitas, hingga Manufaktur Industri berada di kisaran 3.000–3.500 serangan per minggu, mencerminkan bahwa infrastruktur kritis pun tidak luput dari ancaman. Mayoritas sektor lainnya berada di rentang 1.000–2.700 serangan per minggu angka yang tetap menunjukkan tingkat ancaman serius bagi setiap organisasi.

INDEKS KEAMANAN SIBER NASIONAL
KAWASAN ASIA TENGGARA

Kawasan Asia Tenggara terus memperkuat upaya menjaga ruang digitalnya. Pertumbuhan teknologi yang cepat membuat negara-negara di wilayah ini menghadapi tantangan baru, mulai dari serangan siber hingga perlindungan data. Kerja sama regional menjadi kunci untuk membangun lingkungan digital yang lebih aman.

- Berdasarkan National Cyber Security Index (NCSI) negara Singapura merupakan negara dengan Indeks keamanan siber tertinggi di Asia Tenggara yang disusul oleh Malaysia.
- Negara lain berada dibawah nilai 65 seperti Tailan, Filipina, Indonesia, dan lainnya. Hal ini membuktikan bahwa keamanan siber di Kawasan Asia Tenggara masih perlu pentingkatan agar keamanan masyarakat dan sektor penting dapat terjaga dengan baik.

Indeks Keamanan Siber Nasional



Sumber : ncsi.ega.ee (2025)

Regulasi Siber Tingkat Asia Tenggara

Kerjasama regional sangat penting dalam menghadapi tantangan siber, dengan ASEAN berperan signifikan dalam memfasilitasi diskusi dan kolaborasi antar negara anggotanya. Langkah-langkah penting seperti pembentukan pusat keamanan siber dan pelatihan bersama telah diambil untuk meningkatkan kapasitas dan kesiapan menghadapi ancaman siber.

01

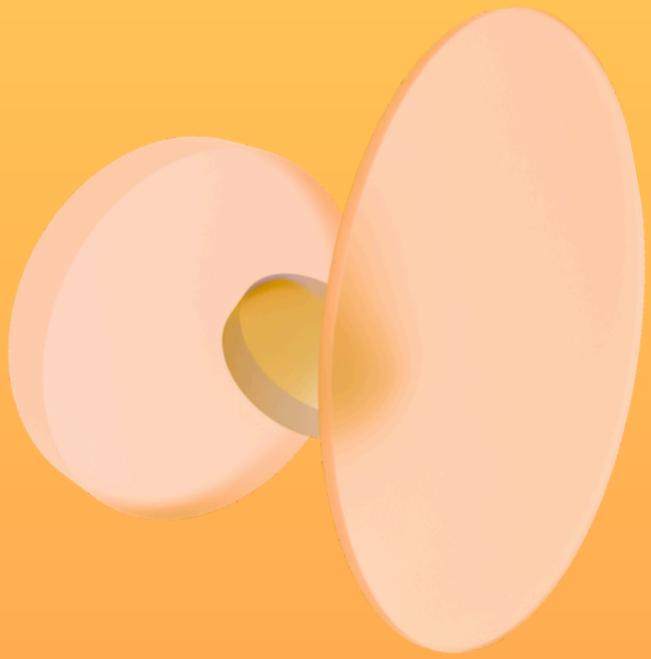
ASEAN Cybersecurity Cooperation Strategy 2021-2025

Strategi ini memiliki lima dimensi utama : (1) Meningkatkan Kerja Sama Kesiapan Siber, (2) Memperkuat Koordinasi Kebijakan Siber Regional, (3) Meningkatkan Kepercayaan di Ruang Siber, (4) Pengembangan Kapasitas di Tingkat Regional, dan (5) Kerja Sama Internasional.

02

ASEAN Regional CERT Framework

Pada 10 Juni 2024, seluruh 10 negara anggota ASEAN menandatangani dua kesepakatan baru: ASEAN Cybersecurity Emergency Response Team (CERT) Framework yang bersifat legally binding dan ASEAN Cybersecurity Capacity Building Programme (ACCP). ASEAN CERT mulai beroperasi secara fisik pada 16 Oktober 2024 di Singapura, menjadikannya CERT regional pertama di kawasan ini



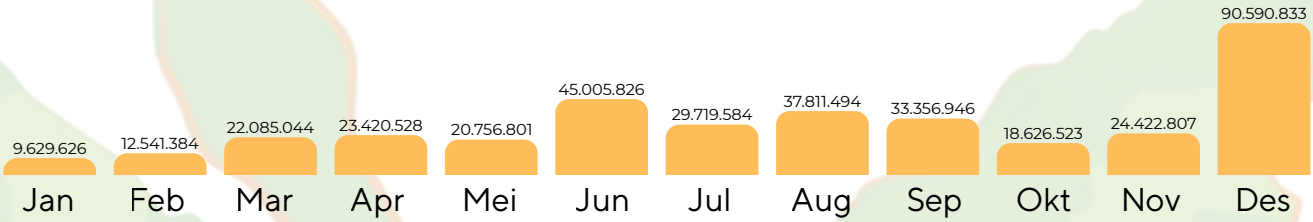
04
Nasional

JUMLAH SERANGAN DI WILAYAH INDONESIA

133,4 jt
Serangan Semester 1
Jan-Jun 2025

234,5 jt
Serangan Semester 2
Jul-Des 2025

+75,76%
Lonjakan S2 vs S1
15 serangan/detik



Awal tahun relatif aman

Januari–Februari mencatat serangan paling sedikit (9,6–12,5 jt). Periode ini jadi jendela ideal untuk konsolidasi sistem keamanan.

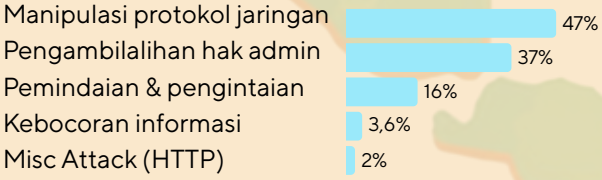
Dua puncak ancaman

Juni (45 jt) dan Desember (90,6 jt) menjadi dua bulan dengan ancaman tertinggi. Keduanya bertepatan dengan musim liburan nasional.

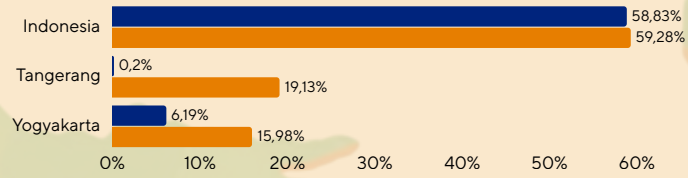
Lonjakan Desember ekstrem

Serangan di Desember hampir dua kali lipat puncak sebelumnya. Momen belanja akhir tahun diduga menjadi faktor pemicunya.

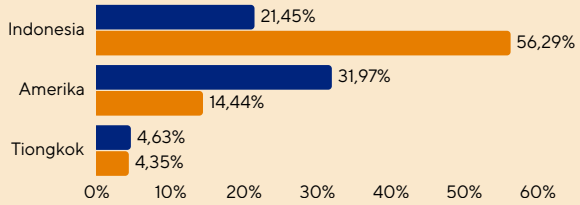
JENIS SERANGAN YANG DOMINAN



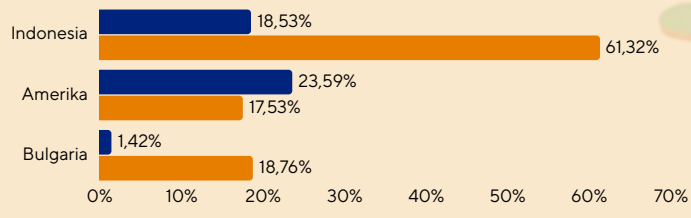
KOTA DENGAN SERANGAN TERBANYAK



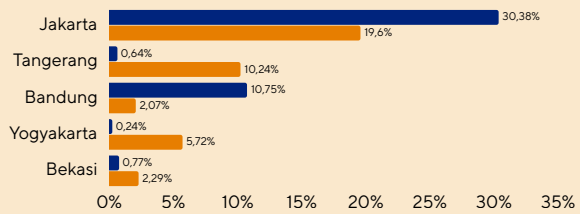
NEGARA PENGIRIM SPAM TERBANYAK



NEGARA PENGIRIM MALWARE TERBANYAK



DAERAH PENYERANG DI INDONESIA



KETERANGAN

SEMESTER 1

SEMESTER 2

Sumber : AwanPintar, BSSN

TIMELINE ANOMALI & KEJADIAN PENTING 2025

Januari 2025

Malware tertinggi tahun ini: **43,46%**. Kampanye distribusi malware masif di awal tahun.

Feb–Mar 2025

Spam melonjak tajam (+18–20% vs 2024). Kerinci & Klaten muncul sebagai hotspot baru domestik.

April–Juni 2025

Spam & malware mulai melandai. Pekanbaru muncul sebagai daerah paling diserang (26,32%).

Juli 2025

Spam meledak: 36,34% — puncak tertinggi tahun. Kampanye spam global terkoordinasi menargetkan Indonesia.

Agustus 2025

Eksploitasi CVE puncak: **33,23%**. OSV terbesar: 42.622 kerentanan baru (48,57% dari S2). Zero-day mulai aktif.

Sep–Nov 2025

Tangerang & Yogyakarta melonjak sebagai titik baru. Serangan menyebar ke luar Pulau Jawa (Bengkulu).

Desember 2025

Puncak absolut: 90,6 juta serangan dalam 1 bulan. DDoS masif + CVE puncak 34,48% + musim transaksi digital.

2026 — Proyeksi

Perluasan 5G & internet murah berpotensi perbesar permukaan serangan IoT. Kewaspadaan mendesak.

SEKTOR TERDAMPAK TAHUN 2025

Infrastruktur Kritis & IoT

Risiko Kritis

Januari–Februari mencatat serangan paling sedikit (9,6–12,5 jt). Periode ini jadi jendela ideal untuk konsolidasi sistem keamanan.

Pemerintah & Layanan Publik

Risiko Kritis

Admin privilege gain dominan: 2,76% (S1) → 70,45% (S2). DoublePulsar backdoor 92–99%. Target utama ransomware & pencurian data massal.

Keuangan & Perbankan

Risiko Kritis

Fortinet SSL VPN (CVSS 9.8) aktif S2. SQL Server Port 1433 jadi target konstan. Regulasi OJK & BI wajibkan kepatuhan CVE/CVSS.

Telekomunikasi & ISP

Risiko Tinggi

Indonesia sumber spam 21,45% (S1) → 56,29% (S2). SNMP lonjak 18%. VoIP/SIP 2× lipat. Infrastruktur dijadikan zombie botnet global.

Teknologi & Cloud

Risiko Tinggi

Log4Shell (CVSS 10.0) & WebLogic (CVSS 9.8) aktif penuh S1 & S2. React Server Components mulai diserang. SysAid & Infoblox jadi target berulang.

Pendidikan & Riset

Risiko Tinggi

Yogyakarta naik 5,48% sebagai sumber serangan (S2). S1: Klaten & Semarang baru. Infrastruktur kampus lemah, target botnet & recon.

Kesehatan

Risiko Menengah

Data pasien jadi sasaran pencurian kredensial. Webmin (CVE-2024-14007) & backdoor Trojan sebagai pintu masuk ransomware.

Energi & Industri

Risiko Menengah

Balikpapan (IKN + energi) masuk radar S1. Siemens & Rockwell Automation CVSS tinggi. ICS/SCADA mulai jadi sasaran aktor negara.

E-Commerce & Retail

Risiko Menengah

Spam Juli 36,34% + Des 90,6 jt serangan saat transaksi puncak. Phishing kartu kredit. DDoS saat Harbolnas & libur akhir tahun.

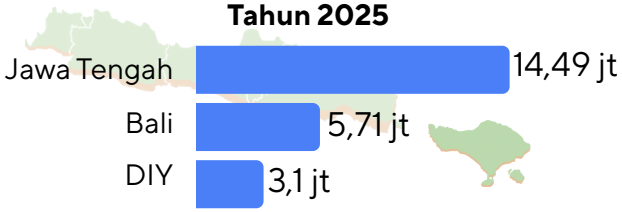
Sumber :Sumber data: AwanPintar, BSSN

Ancaman Siber di DIY, Jawa Tengah & Bali

Data insiden, jenis serangan, dan perkembangan pertahanan siber wilayah

Setiap detik, rata-rata 15 serangan siber menghantam sistem digital Indonesia, Daerah Istimewa Yogyakarta, Jawa Tengah, dan Bali, tiga wilayah dengan kepadatan layanan publik, industri, dan pariwisata, menghadapi ancaman siber yang terus tumbuh dalam skala dan kecanggihan. Buku ini menyajikan data, fakta, dan langkah mitigasi yang perlu diketahui semua pihak.

Jumlah Serangan yang Dilaporkan pada Tahun 2025



- Jawa Tengah 14,49 jt, tertinggi karena banyaknya infrastruktur digital pemda dan industri yang tersebar di 35 kab/kota
- Bali 5,71 jt, target empuk karena ekosistem pariwisata digital (reservasi hotel, OTA) yang menyimpan data sensitif wisatawan asing
- DIY 3,1 jt, lebih rendah tapi tetap rentan, terutama server perguruan tinggi dan sistem pemda

Linimasa kejadian penting 2025–2026

- **28 Juli 2025**

  Rakor Keamanan Informasi Jateng di Solo

  Diskominfo Jateng melaporkan 1.853 insiden di semester I 2025. Seluruh Kepala Diskominfo se-Jateng hadir membahas strategi mitigasi bersama.

- **7 Agt 2025**

  3,64 miliar anomali Jan–Jul 2025

  BSSN menyatakan angka hampir menyamai total 5 tahun terakhir. Mayoritas serangan berbasis malware (83,68%). Jateng dan Bali masuk wilayah tersering terserang.

- **27 Agt 2025**

  Forum Keamanan Siber Nasional di Bali

  Kemenko Polkam menggelar forum di Bali karena posisi strategisnya sebagai hub pariwisata global dan ekosistem siber yang berkembang. Membahas kedaulatan digital.

- **14 Okt 2025**

  Pionir CSIRT pertama di Indonesia

  Kota Yogyakarta ditetapkan sebagai kota pertama yang memiliki Tim Tanggap Insiden Siber (CSIRT) di tingkat kabupaten/kota. BSSN mendorong pembentukan UU Keamanan Siber.

D.I Yogyakarta
Sektor Terdampak

- Pendidikan & Riset
- Pemerintahan
- Keuangan
- Pariwisata
- Layanan Publik

Jawa Tengah
Sektor Terdampak

- Pemerintahan
- Industri & Perusahaan
- UMKM
- Kesehatan
- Transportasi

Bali
Sektor Terdampak

- Pariwisata
- Perhotelan & Resort
- Keuangan
- E-commerce
- Imigrasi

Regulasi Keamanan Siber Di Indonesia

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP).

UU PDP mewajibkan pengendali data dan prosesor data untuk menerapkan langkah langkah keamanan yang memadai untuk melindungi data pribadi dari risiko keamanan, termasuk kebocoran, kehilangan, dan penyalahgunaan.

Peraturan Presiden

- Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV).
- Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

Peraturan Badan Siber dan Sandi Negara (BSSN)

- Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber 2024-2028.
- Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber. Laporan Ancaman Digital di Indonesia
- Nomor 8 Tahun 2023 tentang Pelindungan Infrastruktur Informasi Vital (IIV) Panduan ini menekankan pentingnya identifikasi, penilaian, dan mitigasi kerentanan.

Peraturan di Sektor Khusus

- Peraturan Bank Indonesia (PBI) Nomor 2 tahun 2024 tentang Keamanan SIstem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, Serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia.
- POJK Nomor 11 tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.
- SEOJK Nomor 20 Tahun 2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum.

05
Perbandingan

01 INTERNASIONAL — GLOBAL

ESKALASI ANCAMAN SIBER KE DIMENSI GEOPOLITIK, MILITER, DAN INFRASTRUKTUR KRITIS LINTAS BENUA

2025	2026
Ransomware Black Rift Lumpuhkan infrastruktur energi AS, Asia & Eropa. Kerugian ditaksir $1,2 triliun serangan terbesar sektor energi global sepanjang sejarah.	**AI sebagai mesin serangan** AI otomatisasi seluruh rantai eksploitasi: memindai CVE, menulis payload, beradaptasi real-time terhadap pertahanan.
Malware ICS air bersih Eropa 6 juta warga Jerman & Belanda kehilangan suplai air bersih. Biaya pemulihan sistem mencapai €4 miliar.	**CVE tereksploitasi dalam 48 jam** 50–61% kerentanan baru dieksploitasi dalam 2 hari sejak diumumkan jauh lebih cepat dari siklus patching organisasi.
Jepang MirrorFace & DDoS masif 46 entitas termasuk Mizuho Bank & Japan Airlines diserang. Spionase semikonduktor dan kedirgantaraan oleh aktor negara Tiongkok.	**Siber sebagai Pemicu Perang NATO** Serangan siber besar kini alasan sah aktivasi Pasal 5 NATO eskalasi formal ke dimensi militer dan pertahanan kolektif.
Jamming satelit Asia-Pasifik GPS & internet lumpuh 7 jam, berdampak pada penerbangan, pelayaran, dan perdagangan lintas negara (Mei 2025).	**Cybercrime-as-a-Service meluas** Teknologi serangan diperjualbelikan seperti SaaS. Siapapun tanpa keahlian teknis kini dapat melancarkan serangan canggih.
EduNet 82 juta data pelajar bocor Platform pendidikan global diretas April 2025. Data 82 juta pelajar di 15+ negara terekspos.	**Serangan rantai pasok dominan** Satu celah vendor memicu efek domino ke ribuan organisasi model serangan industrial yang terstruktur & terspesialisasi.

Kesimpulan :

Perang siber global sudah lebih dari sekadar kejahatan digital biasa sekarang menjadi alat politik yang terorganisir antar negara. Cara pertahanan tradisional sudah tidak cukup untuk mengatasi kecepatan otomatisasi AI dan jaringan kejahatan siber yang beroperasi terus-menerus, sepanjang waktu, serta melintasi batas negara.

02

ASIA TENGGARA — ASEAN

DIGITALISASI TERCEPAT DI DUNIA, KAPASITAS PERTAHANAN SIBER PALING TIMPANG ANTARNEGARANYA

2025	2026
Singapura serangan UNC3886 Hacker Tiongkok eksploitasi zero-day di firewall, router & virtualisasi infrastruktur kritis Singapura (1 Juli 2025). Operasi spionase data strategis nasional.	**Serangan rantai pasok ancaman #1** Group-IB: integrasi cloud antar perusahaan jadi vektor masuk utama. Satu vendor diretas sama dengan seluruh ekosistem pelanggannya terdampak.
Rumah sakit Bangkok lumpuh 2 hari Ransomware membuat layanan darurat offline penuh 2 hari (Juni 2025), sektor kesehatan menjadi target prioritas baru di kawasan ASEAN.	**Lazarus, Scattered Spider aktif** Kelompok APT global mengeksploitasi integrasi antarperusahaan untuk memperluas jangkauan serangan ke ekosistem terhubung di ASEAN.
Phishing masif sektor keuangan Keuangan, pemerintahan, militer & telekomunikasi jadi sasaran kampanye phishing terkoordinasi di seluruh ASEAN sepanjang 2025.	**Manufaktur OT target baru** Modernisasi perangkat OT yang terhubung internet tanpa keamanan memadai membuka celah besar di sektor manufaktur dan utilitas.
Penipuan digital $37 miliar Kerugian fraud siber di Asia Tenggara mencapai $37 miliar/tahun, digerakkan jaringan Scam-as-a-Service lintas batas terorganisir.	**Disparitas kapasitas antar-negara** Singapura & Malaysia maju, Myanmar & Kamboja minim sumber daya. Disparitas ini dimanfaatkan peretas sebagai basis operasi.
Vietnam data RS bocor di dark web 112.000 data pasien RS Hong Ngoc dijual di dark web sinyal eskalasi serangan ke sektor layanan publik sensitif.	**Ancaman kecepatan mesin (APAC)** Palo Alto & Cisco peringatkan serangan berbasis AI di APAC kini bergerak di kecepatan mesin melampaui kemampuan respons manusia.

Kesimpulan :

Asia Tenggara berada di titik paling rentan: pertumbuhan digital tercepat di dunia, namun kapasitas pertahanan siber paling timpang. Kawasan ini menjadi laboratorium eksperimen bagi APT state-sponsored maupun sindikat kriminal terorganisir global dan kesenjangan antarnegara justru memperburuk posisi keamanan kolektif ASEAN.

03 INDONESIA

KRISIS SIBER AKTIF: VOLUME SERANGAN REKOR, REGULASI TERTINGGAL, ANCAMAN AI AKSELERASI RISIKO 2026

2025	2026
BPJS Kesehatan 40 juta data bocor April 2025: data 40 juta peserta BPJS Kesehatan terekspos salah satu kebocoran data publik terbesar dalam sejarah Indonesia.	**5 miliar anomali per tahun (BSSN)** 500 juta anomali dalam 3 bulan terakhir menyerang 700 entitas K/L & pemda. Kepala BSSN: "kita sedang berperang di ruang siber setiap hari."
Bank Sentral Indonesia lumpuh 12 jam Phishing massal menargetkan pegawai internal Bank Indonesia menyebabkan sistem digital lumpuh penuh selama 12 jam (Mei 2025).	**14,9 juta serangan web diblokir** Kaspersky KSN blokir 14,9 juta serangan di Indonesia sepanjang 2025 (~40.848/hari). 22,4% pengguna internet Indonesia terpapar ancaman peringkat ke-84 dunia.
Indonesia sumber DDoS #1 dunia Laporan Cloudflare Q3 2025: Indonesia dinobatkan sumber serangan DDoS terbesar di dunia, didominasi Mirai Botnet yang menguasai perangkat IoT warga (CCTV, DVR, router).	**AI perkuat ancaman di semua sektor** Fortinet & Kaspersky peringatkan AI menjadi katalisator serangan di perbankan, e-commerce, manufaktur, dan energi "gelombang ketiga kejahatan siber."
Deepfake & rekayasa sosial masif Video AI palsu Presiden Prabowo, BTS palsu pembajak OTP, dan APK penipuan PT Taspen menguras rekening lansia serangan social engineering terakselerasi AI.	**Darurat regulasi — RUU KKS belum ada** RUU Keamanan & Ketahanan Siber dan lembaga PDP mandiri belum terbentuk. Tanpa payung hukum, penegakan perlindungan infrastruktur kritis tetap lemah.
367 juta serangan ditahun2025 Turun dari 2,49 miliar H1 2024 (efek Pemilu), namun kualitas serangan makin canggih dan tertarget. Mayoritas (83,68%) berbasis malware (BSSN).	**Krisis SDM keamanan siber** Laporan Fortinet Global Skills Gap 2025: Indonesia kekurangan operator kompeten keamanan siber modern memperlebar gap antara ancaman dan kemampuan bertahan.

Kesimpulan :

Indonesia menghadapi krisis siber yang bukan lagi potensi, melainkan realitas aktif. Volume serangan mendekati rekor historis, kerugian finansial terus membesar, sementara kerangka hukum dan kapasitas SDM keamanan siber masih jauh dari memadai terutama menghadapi ancaman yang kini diakselerasi AI secara masif di 2026.

06
Panduan Aksi

PANDUAN AKSI INDIVIDU

Sebagian besar insiden siber terjadi akibat kebiasaan digital yang kurang waspada bukan karena sistem yang canggih. Checklist berikut dapat langsung Anda terapkan hari ini, tanpa memerlukan keahlian teknis khusus.

Keamanan Kata Sandi

- Gunakan kata sandi minimal 12 karakter, kombinasi huruf besar, kecil, angka, dan simbol
- Gunakan kata sandi berbeda untuk setiap akun penting
- Aktifkan Password Manager (Bitwarden, 1Password) agar tidak perlu hafal semua
- Ganti kata sandi secara berkala, minimal setiap 6 bulan

Autentikasi Dua Faktor (2FA)

- Aktifkan 2FA di semua akun penting: email, perbankan, media sosial
- Pilih aplikasi autentikator (Google Authenticator, Authy) dibanding SMS OTP yang bisa disadap
- Simpan kode backup 2FA di tempat aman (offline)
- Jangan pernah berikan kode OTP kepada siapapun, termasuk yang mengaku pihak bank

Mengenali Phishing & Deepfake

- Periksa alamat email pengirim secara teliti — bukan hanya nama tampilan
- Jangan klik link mencurigakan; arahkan kursor terlebih dulu untuk melihat URL asli
- Waspadai pesan yang menciptakan urgensi palsu ("Akun Anda diblokir, klik sekarang!")
- Verifikasi identitas lewat saluran resmi terpisah sebelum transfer uang atau klik tautan
- Video/audio mencurigakan? Cari tanda deepfake: gerakan bibir tidak sinkron, pencahayaan aneh

Keamanan Perangkat

- Selalu perbarui sistem operasi & aplikasi jangan tunda pembaruan keamanan
- Pasang antivirus/antimalware dan jalankan pemindaian rutin
- Ubah kata sandi default router dan perangkat IoT (CCTV, smart TV) di rumah
- Nonaktifkan fitur yang tidak digunakan: Bluetooth, lokasi, kamera jika tidak diperlukan
- Lakukan backup data secara rutin ke media terpisah (3-2-1 rule)

Media Sosial & Privasi

- Atur privasi akun ke "hanya teman" atau "private" pada platform media sosial
- Jangan tampilkan nomor telepon, alamat rumah, atau tanggal lahir lengkap secara publik
- Waspada terhadap kuis/permainan online yang meminta data pribadi
- Cabut izin aplikasi pihak ketiga yang tidak lagi digunakan dari pengaturan akun

Wi-Fi & Jaringan

- Hindari transaksi perbankan di Wi-Fi publik tanpa VPN terpercaya
- Gunakan enkripsi WPA3 atau WPA2 pada router rumah, bukan WEP/WPS
- Buat jaringan tamu (guest network) terpisah untuk perangkat IoT rumah
- Periksa daftar perangkat yang terhubung ke Wi-Fi Anda secara berkala

Ingat: Tidak Ada Sistem yang 100% Aman : Langkah-langkah tersebut meningkatkan hambatan bagi penyerang. Semakin banyak lapisan keamanan, semakin tinggi biaya serangan, sehingga peretas lebih memilih target yang lebih mudah.

PANDUAN AKSI ORGANISASI

Ancaman siber tidak hanya menyasar perusahaan besar. UKM dan organisasi kecil justru menjadi target favorit karena keamanan yang umumnya lebih lemah namun menyimpan data bernilai. Berikut langkah yang dapat diambil tanpa anggaran besar.

Prioritas Pertama

1 Inventarisasi Aset Digital
Buat daftar semua perangkat, akun cloud, aplikasi, dan data penting yang dimiliki organisasi. Anda tidak bisa melindungi apa yang tidak Anda ketahui.

2 Audit Akun & Akses
Hapus akun karyawan yang sudah keluar. Terapkan prinsip "least privilege" beri akses hanya sesuai kebutuhan pekerjaan.

3 Aktifkan 2FA di Semua Akun Bisnis
Email kantor, Google Workspace, Microsoft 365, akun cloud, dan media sosial bisnis wajib menggunakan autentikasi dua faktor.

4 Backup Data 3-2-1
Simpan **3** salinan data di **2** media berbeda, dengan **1** salinan tersimpan di lokasi terpisah (cloud + hard disk eksternal).

Prioritas Kedua

5 Buat Kebijakan Keamanan Siber
Tulis aturan penggunaan perangkat, Wi-Fi, dan data yang wajib diikuti semua karyawan. Tidak perlu panjang satu halaman sudah cukup.

6 Latih Karyawan Kenali Phishing
Lakukan simulasi phishing dan edukasi rutin. Manusia adalah lapisan pertahanan terpenting sekaligus yang paling rentan.

7 Pasang Firewall & Antivirus Endpoint
Gunakan solusi keamanan endpoint di seluruh perangkat kantor. Banyak solusi gratis tersedia untuk UKM (Windows Defender, ClamAV).

8 Buat Rencana Respons Insiden
Siapkan prosedur: siapa yang dihubungi, apa yang dilakukan, bagaimana memulihkan sistem jika terjadi serangan. Latih seluruh tim.

"Biaya rata-rata serangan siber pada UKM Indonesia adalah Rp 850 juta — jauh lebih mahal daripada investasi keamanan dasar yang hanya memerlukan Rp 5–50 juta per tahun."

Tools Gratis

- Google Workspace Security (gratis untuk akun Gmail)
- Bitwarden — Password Manager open source
- Have I Been Pwned — cek kebocoran data
- VirusTotal — scan file/URL mencurigakan
- Cloudflare — proteksi DDoS gratis

Nomor Darurat Siber

- BSSN Hotline: 117 ext 8
- Aduan BSSN: aduan@bssn.go.id
- Kominfo: 159
- Aduan Konten: aduankonten.id
- Polisi Siber: patrolisiber.id

PANDUAN AKSI ORGANISASI

Kecepatan respons menentukan seberapa besar kerugian yang ditimbulkan. Ikuti panduan berikut jika Anda menduga sistem atau akun Anda telah dibobol.

Tingkat Kewaspadaan & Tindakan

KRITIS

Ransomware / Data Terenkripsi / Akun Keuangan Dibobol

Lakukan segera: Cabut koneksi internet perangkat yang terinfeksi. Hubungi BSSN (117 ext 8). Jangan bayar tebusan tanpa konsultasi ahli. Isolasi sistem, laporkan ke OJK jika menyangkut keuangan. Aktifkan rencana backup pemulihan.

TINGGI

Akun Email/Media Sosial Dibajak / Data Pribadi Bocor

Lakukan segera: Ganti kata sandi dari perangkat bersih. Aktifkan 2FA. Hubungi platform untuk pemulihan akun. Periksa riwayat login/aktivitas mencurigakan. Beritahu kontak terpercaya agar tidak merespons pesan mencurigakan dari akun Anda.

SEDANG

Menerima Email/Pesan Phishing / Klik Link Mencurigakan

Lakukan segera: Jangan masukkan data apapun. Tutup halaman. Jalankan scan antivirus. Ganti kata sandi akun yang mungkin terpapar. Laporkan ke platform dan aduankonten.id. Periksa apakah ada transaksi tidak dikenal.

WASPADA

Aktivitas Tidak Biasa / Login dari Lokasi Asing / Perangkat Lambat

Lakukan segera: Periksa riwayat login akun. Cabut sesi aktif lain. Perbarui sistem & aplikasi. Jalankan scan malware. Monitor transaksi keuangan. Tingkatkan pengaturan keamanan akun.

Contoh Skenario Penyerangan

Skenario: Email Phishing BEC

Tanda Bahaya

Email dari "atasan" atau "bank" meminta transfer dana segera dengan alasan mendesak. Nama pengirim benar tapi alamat email sedikit berbeda (@gmail.com bukan domain kantor).

Tindakan Tepat

Hubungi atasan/bank via telepon atau saluran resmi lain untuk verifikasi. Jangan transfer sebelum konfirmasi verbal langsung.

Skenario: Penipuan Modus Keluarga

Tanda Bahaya

Seseorang mengaku anggota keluarga dengan nomor baru, minta transfer uang darurat. Mungkin menggunakan foto profil yang dicuri dari media sosial.

Tindakan Tepat

Hubungi nomor asli keluarga tersebut untuk konfirmasi. Buat "kata kode keluarga" yang hanya diketahui anggota asli.

Skenario: APK Palsu / Smishing

Tanda Bahaya

Pesan berisi link download APK yang mengaku dari kurir, bank, atau instansi pemerintah. Setelah diinstal, aplikasi meminta izin akses SMS dan kontak.

Tindakan Tepat

Jangan instal APK di luar Play Store/App Store. Hapus segera jika terlanjur. Ganti seluruh kata sandi perbankan dari perangkat lain.

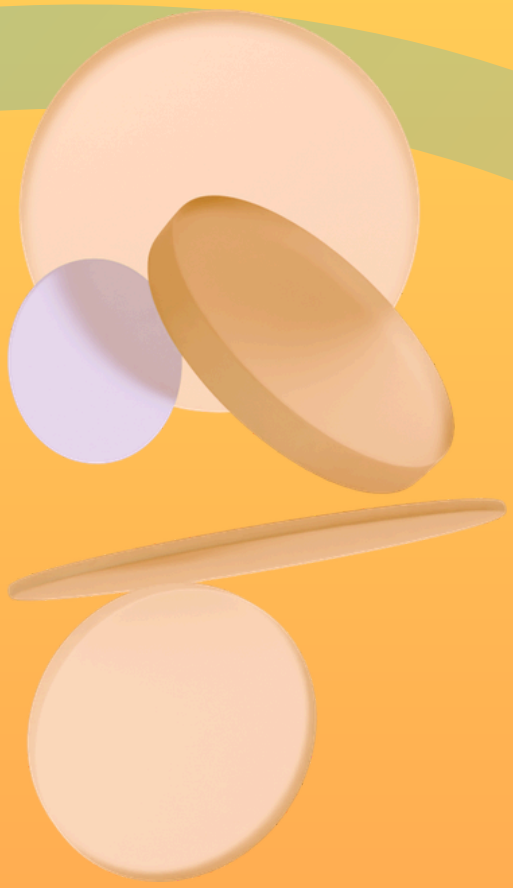
Skenario: Video Deepfake Meminta Dana

Tanda Bahaya

Video call atau video yang dikirim menampilkan wajah pejabat/tokoh publik/atasan yang meminta bantuan keuangan. Sinkronisasi bibir tidak sempurna.

Tindakan Tepat

Verifikasi lewat saluran resmi. Minta lawan bicara melakukan gerakan tidak terduga (misalnya sentuh hidung) — deepfake real-time belum sempurna.



07

Peran KOMDIGI & BLSDM KOMDIGI

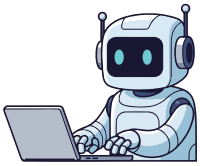
TINDAKAN KOMDIGI DI RUANG SIBER

Sebagai kementerian yang bertanggung jawab atas tata kelola ruang digital nasional, KOMDIGI tampil sebagai garda terdepan dalam menghadapi lonjakan ancaman siber sepanjang 2025. Tiga agenda prioritas dijalankan secara simultan: pemberantasan konten kriminal digital (judol & pinjol ilegal), penanganan ancaman kecerdasan buatan (deepfake & AI generatif), serta perlindungan kelompok rentan khususnya anak-anak melalui regulasi pembatasan usia di media sosial.

Menghadapi Deepfake & Ancaman AI di Ruang Digital Indonesia

Sepanjang 2025, teknologi kecerdasan buatan (AI) generatif berubah menjadi senjata siber yang menyasar langsung warga Indonesia. Deepfake manipulasi video dan audio berbasis AI digunakan untuk penipuan finansial, pembajakan OTP, hingga konten asusila berbasis foto nyata. Komdigi merespons dengan serangkaian tindakan regulatif dan teknis yang mencakup tekanan kepada platform global hingga langkah pemblokiran.

DEEPFAKE — DARI FENOMENA GLOBAL KE ANCAMAN LOKAL



Lonjakan 550%

Data dari Sensity AI menunjukkan bahwa dalam lima tahun terakhir, terdapat peningkatan sebesar 550% dalam konten deepfake secara global. Wamenkomdigi Nezar Patria memperingatkan bahwa angka sebenarnya kemungkinan jauh lebih tinggi, mengingat semakin meluasnya aksesibilitas aplikasi pembuat deepfake.

90% untuk Kejahatan

Dari semua konten deepfake yang beredar, 90% dimanfaatkan untuk tujuan berbahaya mayoritas berupa penipuan digital. Di Indonesia, modus deepfake video tokoh publik dan audio palsu digunakan untuk membobol rekening dan membajak OTP.

Modus di Indonesia

Video AI palsu mengatasnamakan pejabat publik beredar luas. APK penipuan berkedok instansi negara menguras rekening lansia. Deepfake suara dipakai dalam penipuan Business Email Compromise (BEC) yang menyasar keuangan perusahaan.

Sepanjang 2025–2026, KOMDIGI menjalankan tiga lini pertahanan siber sekaligus:

(1) Pemberantasan konten kriminal digital dengan 2,8 juta takedown dan tekanan keuangan yang berhasil menekan transaksi judi sebesar 57%;

(2) Penanganan ancaman AI generatif melalui tekanan regulatif ke platform global dan pemblokiran layanan yang tidak patuh; serta

(3) Perlindungan anak melalui PP TUNAS dan pembatasan usia 16 tahun yang menjadikan Indonesia pelopor non-Barat. Keberhasilan agenda ini bergantung pada percepatan RUU KKS, investasi SDM siber, dan kolaborasi penuh dengan seluruh pemangku kepentingan.

AKSI KOMDIGI TAHUN 2025-2026

LINIMASA KETERLIBATAN KOMDIGI 2025

JANUARI 2025
Kick Off Digital Talent Scholarship 2025

BPSDM KOMDIGI meluncurkan DTS 2025 di Digital Talent Center Cikarang,menargetkan 100.000 talenta digital nasional dengan modul keamanan siber dan AI

18 FEBRUARI 2025
Safer Internet Day & Perlindungan Anak Digital

Kolaborasi KOMDIGI–Google Indonesia memperingati Safer Internet Day 2025. Menkomdigi Meutya Hafid menekankan pentingnya perlindungan anak di ruang digital 9,17% pengguna internet Indonesia berusia di bawah 12 tahun.

21 FEBRUARI 2025
Sinergi Strategis KOMDIGI–BSSN

Menkomdigi Meutya Hafid dan Kepala BSSN Nugroho Sulistyo Budi menetapkan tiga pilar kolaborasi nasional. Arahan Presiden Prabowo: keamanan siber adalah prioritas nasional.

27 FEBRUARI 2025
Kolaborasi Industri – Cyber Safe Kids

Wamenkomdigi Nezar Patria menghadiri Cyber Security Trend & Outlook 2025 bersama Palo Alto Networks. KOMDIGI menyiapkan program sertifikasi keamanan untuk K/L dan pemda dengan pendekatan security by design.

6 MARET 2025
Kolaborasi RCS – MWC Barcelona 2025

KOMDIGI, Telkomsel, dan Google umumkan kolaborasi pengamanan komunikasi digital melalui RCS dengan fitur verifikasi bisnis, proteksi phishing, dan deteksi pola pesan mencurigakan berbasis AI.

JUNI – SEPTEMBER 2025
DTS Menjangkau Seluruh Indonesia

Program DTS hadir di berbagai daerah termasuk Rembang (307 peserta): pelajar SMK mengikuti Basic Cyber Security, ASN dalam Government Transformation Academy, dan wirausaha dalam Digital Entrepreneurship Academy.

9 AGUSTUS 2025
Pengungkapan Kerugian Siber Rp 476 Miliar

Wamen Nezar Patria mengungkap kerugian finansial kejahatan siber dan 1,2 juta laporan penipuan digital. KOMDIGI bersinergi dengan Bareskrim Polri untuk tindak lanjut spam dan scam lintas batas.

NOVEMBER 2025
Penegakan Kedaulatan Digital – Isu Cloudflare

KOMDIGI menemukan mayoritas situs judi online menggunakan infrastruktur Cloudflare. Dirjen Alexander Sabar mengirim surat teguran resmi dan ultimatum
14 hari kepada Cloudflare dan 24 PSE untuk mematuhi regulasi Indonesia.

23 NOVEMBER 2025
Program Roketin Generasi Tunas Digital

KOMDIGI bersama MyRepublic Indonesia meluncurkan program literasi keamanansiber pelajar. Menkomdigi: "Generasi Tunas Digital adalah aset terbesar bangsa."

28 Maret 2026
Pembatasan Umur Pada Sosial Media

Pemerintah Indonesia secara resmi menerapkan pembatasan umur media sosial untuk anak di bawah 16 tahun mulai 28 Maret 2026. Kebijakan ini, berdasarkan Peraturan Menteri Komunikasi dan Digital (Permenkomdigi) Nomor 9 Tahun 2026 dan PP TUNAS, mewajibkan platform menonaktifkan akun anak di bawah usia tersebut untuk melindungi mereka dari konten negatif.

KERJA SAMA INTERNASIONAL

Partisipasi Aktif ASEAN Cybersecurity

KOMDIGI aktif dalam ASEAN Cybersecurity Cooperation, bermitra dengan negara ASEAN, dan mendukung operasionalisasi ASEAN CERT yang mulai aktif di Singapura sejak Oktober 2024. Indonesia turut dalam pertukaran intelijen ancaman regional.

Kerja Sama Strategis AS–Indonesia

Penguatan kerja sama kebijakan siber bilateral antara Indonesia dan AS, mencakup pertukaran praktik terbaik pertahanan siber dan pengembangan kapasitas tenaga ahli keamanan siber nasional.

Prioritas KOMDIGI Menuju 2026

REGULASI
Mendorong penyelesaian RUU Keamanan & Ketahanan Siber ser ta pembentukan lembaga PDP mandiri yang memperkuat penegakan perlindungan infrastruktur kritis.

AI & TALENTA
Memperluas AI Talent Factory ke lebih banyak universitas; mendorong adopsi *AI-driven security di seluruh sektor kritis pemerintahan.*

IOT & 5G
Perluasan 5G berpotensi memperbesar permukaan serangan IoT. KOMDIGI menyiapkan kerangka keamanan perangkat IoT nasional.

ZERO BLANKSPOT
Akselerasi Zero Blankspot harus diiringi sistem deteksi dini dan manajemen keamanan informasi di seluruh wilayah termasuk 8.065 desa bersinyal rendah.

BLSDM KOMDIGI YOGYAKARTA

Pusat Talenta Digital Wilayah Jateng–DIY–Bali

Balai Pelatihan Sumber Daya Manusia Komunikasi dan Digital (BLSDM) Komdigi Yogyakarta memiliki peran strategis sebagai ujung tombak pengembangan kompetensi keamanan siber di tingkat daerah. Wilayah kerjanya mencakup tiga provinsi yang dalam IMDI 2025 berhasil melampaui rata-rata nasional Jawa Tengah (51,19), DI Yogyakarta (51,13), dan Bali (48,22) membuktikan bahwa intervensi pelatihan yang konsisten menghasilkan ekosistem digital yang lebih tangguh. BLSDM Yogyakarta menjalankan peran ini melalui tiga jalur utama: program pelatihan berjenjang, workshop tematik keamanan siber berseri, dan kemitraan strategis lintas sektor.

PROGRAM PELATIHAN

Digital Talent Scholarship (DTS) — Lintas Kota/Kabupaten

Program pelatihan keliling yang membawa kurikulum keamanan siber, AI, dan literasi digital ke kota/kabupaten di bawah wilayah kerja BLSDM Yogyakarta. Diselenggarakan berkolaborasi dengan pemerintah daerah dan institusi pendidikan setempat.

Target: Wirausaha, Pelajar, ASN, UMKM, dan Masyarakat

Kolaborasi: Pemda, SMK, Universitas, dan lainnya

PROGRAM PELATIHAN

Micro skill — Self-learning

Micro skill adalah pelatihan berbasis self-learning (belajar mandiri) untuk meningkatkan kompetensi digital secara cepat dan fleksibel, sering kali bagian dari program Digital Talent Scholarship (DTS). Secara umum, ini merujuk pada keterampilan kecil, spesifik, dan modular yang dapat dipelajari dengan cepat

Target: Wirausaha, Pelajar, ASN, UMKM, dan Masyarakati

PROGRAM WORKSHOP

Workshop/Seminar - Hybrid/Offline

Balai Pelatihan Sumber Daya Manusia Komunikasi dan Digital (BLSDM Komdigi) Yogyakarta (sebelumnya dikenal sebagai BPTIKP/BPSDMP) rutin mengadakan berbagai workshop dan pelatihan offline yang fokus pada pengembangan talenta digital.

Contohnya: Workshop AI-Security

KOLABORASI

Sinergi Lintas Sektor

BLSDM membangun ekosistem kolaborasi yang mencakup: perguruan tinggi (Univ. Amikom, STMM MMTC), komunitas siber (Cyberkarta), pemerintah daerah, institusi pendidikan menengah, serta organisasi pariwisata menciptakan jaring pengaman digital yang menjangkau dari sekolah hingga desa wisata.

Informasi mengenai pelaksanaan pelatihan, workshop, atau acara lainnya dapat diakses melalui media sosial BLSDM atau melalui aplikasi/website BLSDM dan Digital Talent Scholarship.

- bpsdm.komdigi.go.id/upt/yogyakarta
- digitalent.komdigi.go.id
- blsdm.komdigi.yogyakarta
- +6281391000404

TINGKATKAN SKILL & KESADARAN SIBER

Tingkatkan pengetahuan Anda untuk melindungi keamanan digital melalui pelatihan gratis dari Digital Talent Scholatship yang diselenggarakan oleh Kementerian Digital (KOMDIGI).

Belajar Mandiri Microskill

Perlindungan Data Diri

Tips Melindungi Diri Dari Ancaman Phising dan Malware di Era Digital

Daftar Sekarang ↗

Pentingnya Menjaga Keamanan Digital: Perlindungan Diri di Dunia Maya

Daftar Sekarang ↗

Ancaman Pembobolan Akun Pribadi dan Pencegahannya

Daftar Sekarang ↗

Mengamankan Diri dari Kejahatan Siber

Daftar Sekarang ↗

Kenali Tanda-Tandanya dan Lindungi Data Pribadi

Daftar Sekarang ↗

Keamanan Digital

Dasar-dasar Keamanan AI

Daftar Sekarang ↗

Introduction to Cyber Security and Career Awareness

Daftar Sekarang ↗

Seberapa Aman Informasi Anda dari Ancaman Digital

Daftar Sekarang ↗

SCAN UNTUK INFORMASI PELATIHAN LAINNYA

https://digitalent.komdigi.go.id

Mengapa memilih Microskill?

- Pembelajaran mandiri yang gratis dan fleksibel
- Materi yang singkat, praktis, dan relevan
- Cocok untuk pelajar, mahasiswa, profesional, dan orang tua
- Meningkatkan literasi digital serta kesiapsiagaan siber
- Sertifikat yang diakui setelah menyelesaikan kursus

#Jaga Data dan Informasi #Jadi Jagoan Digital

08
Kesimpulan

KESIMPULAN

Transformasi digital pada tahun 2025 memberikan manfaat besar di berbagai sektor, namun juga meningkatkan ancaman siber. Serangan kini terorganisir dan canggih, menggunakan teknologi seperti AI, baik oleh penjahat maupun pertahanan.

Secara global, ancaman siber menjadi isu strategis terkait geopolitik, ekonomi, dan keamanan nasional. Infrastruktur kritis seperti energi, keuangan, kesehatan, dan pemerintahan menjadi target utama karena dampaknya yang besar. Di Asia Tenggara, digitalisasi pesat tanpa kesiapan keamanan menjadikan wilayah ini rentan terhadap serangan seperti scam, phishing, dan spionase siber.

Di Indonesia, ancaman siber mencapai krisis aktif, dengan tingginya serangan dan kejahatan berbasis AI, serta terbatasnya regulasi dan sumber daya manusia. Data menunjukkan serangan meningkat, dengan sektor pemerintahan, pendidikan, dan infrastruktur digital sebagai sasaran utama.

TANTANGAN UTAMA

Generative AI telah menjadi titik infleksi terbesar dalam sejarah keamanan siber teknologi yang sama digunakan oleh penyerang untuk serangan yang lebih canggih, dan oleh defender untuk deteksi yang lebih cepat. Sektor Pendidikan, Pemerintahan, dan Telekomunikasi menjadi yang paling rentan secara konsisten baik di tingkat global maupun kawasan Asia Tenggara.

Rekomendasi Strategis

01 **Segera sahkan RUU Keamanan & Ketahanan Siber**
Payung hukum nasional yang komprehensif sangat diperlukan untuk memperkuat penegakan perlindungan infrastruktur kritis dan data pribadi warga.

02 **Investasi SDM keamanan siber secara masif**
Menutup kesenjangan kompetensi melalui pelatihan, sertifikasi, dan pembentukan CSIRT di seluruh kabupaten/kota, mengacu pada keberhasilan Kota Yogyakarta sebagai pionir pertama.

03 **Adopsi AI-driven security di sektor kritis**
Organisasi dengan keamanan berbasis AI terbukti mampu mempersingkat siklus insiden hingga 80 hari dan menghemat rata-rata USD 1,9 juta per kejadian.

04 **Edukasi literasi digital masyarakat**
Kampanye nasional tentang keamanan siber, pengenalan deepfake, dan rekayasa sosial berbasis AI untuk mengurangi eksposur individu terhadap ancaman phishing dan penipuan digital.

GLOSARIUM

APT (Advanced Persistent Threat)	:	Serangan siber canggih yang dilakukan secara diam-diam dalam jangka panjang, biasanya disponsori negara, bertujuan memata-matai atau mencuri data strategis.
BEC (Business Email Compromise)	:	Penipuan yang menargetkan perusahaan dengan cara meretas atau memalsukan email eksekutif untuk mengelabui karyawan agar mentransfer uang.
Botnet	:	Jaringan ratusan atau jutaan perangkat (komputer, router, kamera CCTV) yang sudah terinfeksi malware dan dikendalikan dari jarak jauh oleh penjahat siber.
CVE (Common Vulnerabilities & Exposures)	:	Sistem penomoran standar internasional untuk mendaftar dan mengidentifikasi celah keamanan yang ditemukan dalam perangkat lunak atau perangkat keras.
CVSS (Common Vulnerability Scoring System)	:	Sistem skor dari 0.0 hingga 10.0 untuk mengukur seberapa berbahaya sebuah celah keamanan. Skor di atas 9.0 dianggap kritis.
DDoS (Distributed Denial of Service)	:	Serangan yang membanjiri server atau website dengan lalu lintas palsu dari banyak sumber secara bersamaan, sehingga layanan menjadi lambat atau lumpuh total.
Deepfake	:	Konten video, audio, atau gambar palsu yang dibuat menggunakan kecerdasan buatan (AI) untuk meniru tampilan atau suara seseorang secara sangat meyakinkan.
Double Extortion	:	Taktik ransomware di mana penjahat tidak hanya mengenkripsi data korban, tetapi juga mencurinya dan mengancam akan mempublikasikannya jika tebusan tidak dibayar.
Exploit / Eksploitasi	:	Teknik atau kode yang memanfaatkan celah keamanan (vulnerability) dalam perangkat lunak untuk mendapatkan akses tidak sah ke sistem.
ICS/SCADA	:	Sistem kontrol industri yang digunakan untuk mengoperasikan infrastruktur fisik seperti pembangkit listrik, pengolahan air, pabrik, dan kilang minyak.
IoT (Internet of Things)	:	Perangkat fisik sehari-hari yang terhubung ke internet, seperti kamera CCTV, smart TV, kulkas pintar, atau router rumahan.
Malware	:	Perangkat lunak berbahaya yang dirancang untuk merusak, mencuri data, atau mengendalikan perangkat tanpa izin pengguna. Mencakup virus, worm, trojan, spyware, dll.
Phishing	:	Teknik penipuan digital yang mengelabui korban agar menyerahkan informasi sensitif (kata sandi, data kartu kredit) melalui email, SMS, atau website palsu.
Ransomware	:	Jenis malware yang mengenkripsi seluruh data korban dan meminta tebusan (biasanya dalam kripto) untuk memberikan kunci dekripsinya.
Social Engineering (Rekayasa Sosial)	:	Manipulasi psikologis terhadap manusia untuk membocorkan informasi rahasia atau melakukan tindakan yang menguntungkan penyerang, bukan mengeksploitasi teknologi.
Zero-day	:	Celah keamanan yang belum diketahui oleh vendor atau belum ada perbaikannya (patch), sehingga sangat berbahaya karena tidak ada perlindungan yang tersedia.

Tim Penyusun

Your Data Your Security 2026

Laporan Keamanan Siber 2025 & Proyeksi 2026

Global · ASEAN · Indonesia

Penanggung Jawab/ Person In Charge

Rahmanita Febrianti Rusmaningtyas

Penulis Naskah/ Writers

Rhizky Dwi Mertani / Magang BLSDM Komdigi Yogyakarta

Pendesain/ Designer

Rhizky Dwi Mertani / Magang BLSDM Komdigi Yogyakarta

Pengolah Data/ Data Processor

Rhizky Dwi Mertani / Magang BLSDM Komdigi Yogyakarta

Penyunting/ Editor

Rahmanita Febrianti Rusmaningtyas

Instansi

BLSDM Komdigi Yogyakarta

KOMDIGI | BLSDM KOMDIGI YOGYAKARTA

Jl. Imogiri Barat No.km 5, Tanjung, Bangunharjo, Kec. Sewon, Kabupaten Bantul, Daerah Istimewa Yogyakarta 55188