MATERI 1

Pada 10 Desember 2025, Kementerian Sekretariat Negara menggelar forum keamanan siber yang dihadiri 484 peserta membahas ancaman digital terkini. Forum mengungkap bahwa **anomali trafik mencapai 216,5 juta events per bulan**, menunjukkan masifnya aktivitas mencurigakan yang harus dipantau. Ancaman siber kini semakin canggih dengan memanfaatkan **AI untuk menghindari deteksi**, munculnya **RaaS (Ransomware as a Service)** yang memudahkan siapa saja meluncurkan serangan, serta **phishing yang jauh lebih sulit diidentifikasi**. Ditemukan pula beberapa **aset server berisiko tinggi dengan skor 67-73** dan **kebocoran akun dari domain setneg.go.id** yang memerlukan penanganan serius.

Sepanjang 2025, Kemensetneg menghadapi berbagai insiden kritis mulai dari **command injection di Januari**, **serangan DDoS intensif di Februari**, hingga ancaman paling serius berupa **backdoor pada server di September-Oktober** yang memberikan akses persisten kepada penyerang. Setiap insiden ditangani dengan langkah spesifik seperti isolasi host, penghapusan file berbahaya, **blocking IP Command & Control**, **reset password paksa**, penerapan **Multi-Factor Authentication (MFA)**, dan pemberian security awareness kepada pengguna. Tim SOC melakukan monitoring real-time untuk deteksi dini dan respons cepat terhadap setiap anomali.

Untuk memperkuat pertahanan, Kemensetneg menerapkan **strategi berlapis** yang komprehensif mencakup optimalisasi **firewall dan WAF**, implementasi **rate limiting**, hardening sistem, serta pemantauan log proaktif untuk deteksi pola scanning. Yang paling fundamental adalah adopsi **framework cybersecurity internasional** (NIST, Defense in Depth) dengan tiga pilar: **People** (awareness & training), **Process** (governance & compliance), dan **Technology** (Zero Trust architecture). Pendekatan holistik ini menegaskan bahwa keamanan siber tidak cukup hanya mengandalkan teknologi, tetapi harus didukung **SDM kompeten** dan **proses terstruktur** untuk menghadapi landscape ancaman yang terus berkembang.

MATERI 2

.Deputi V Bidang Koordinasi Komunikasi dan Informasi Kemenko Polkam RI menyampaikan presentasi tentang **"Peningkatan Koordinasi Keamanan Siber dalam Penyelenggaraan Pertahanan Semesta"** yang mengangkat lima poin krusial. Pertama, **ancaman siber meningkat signifikan** dengan modus yang semakin terorganisir untuk kepentingan ekonomi, spionase, dan sabotase. Kedua, **kesiapan keamanan siber nasional belum merata** dengan kesenjangan besar antar instansi dari segi infrastruktur, SDM, dan kebijakan. Ketiga, **koordinasi lintas K/L masih lemah** padahal ancaman siber bersifat lintas sektoral yang memerlukan respons terkoordinasi. Keempat, pentingnya **pendekatan pertahanan semesta di ruang siber** sebagai tanggung jawab seluruh elemen bangsa, bukan hanya BSSN atau unit IT. Kelima, **penguatan kapasitas berkelanjutan** menjadi keharusan mengingat ancaman berevolusi sangat cepat.

Presentasi mengidentifikasi **empat pilar utama kerentanan** di era otomatisasi digital. **End-User Digital** rentan terhadap eksploitasi data melalui aplikasi yang meminta izin akses berlebihan. **Pabrikan Tertanam** menghadapi risiko dari sensor dan software IoT yang bisa dimanfaatkan penyerang untuk mengakses data bahkan mengendalikan perangkat. **Ekosistem Terhubung** menciptakan celah baru dimana sistem terintegrasi (tiket elektronik, manajemen lalu lintas, logistik) bisa diakses melalui satu titik lemah. Yang paling kritis adalah **Risiko Kritis** dengan peringatan bahwa **"satu gangguan siber dapat melumpuhkan seluruh sistem transportasi nasional"**—seperti kasus ransomware di negara lain yang melumpuhkan bandara dan pelabuhan selama berhari-hari dengan dampak ekonomi triliunan rupiah.

Kemenko Polkam menekankan pentingnya **pendekatan proaktif dan preventif** melalui penguatan arsitektur keamanan, implementasi standar internasional, pengujian penetrasi berkala, dan membangun kesadaran di semua level. **Koordinasi lintas sektor menjadi kunci utama** dimana BSSN harus bekerja sama erat dengan Kementerian Perhubungan, Kementerian BUMN, dan operator infrastruktur untuk membangun **sistem deteksi dan respons terintegrasi**. Kesimpulannya, keamanan siber bukan lagi isu teknis IT semata tetapi menjadi **isu strategis nasional** yang memerlukan implementasi **pertahanan semesta di ruang siber** dengan melibatkan seluruh elemen bangsa untuk membangun **ketahanan siber nasional yang kuat dan berkelanjutan.**

MATERI 3

Rindy, Ketua Tim Pengawasan Kepatuhan Ruang Digital dan Ketua CSIRT Sektor TIK dengan berbagai sertifikasi internasional (CEH, ECSA, ISO 27001/27701 Auditor, ECPC-A, Professional DPO), menyampaikan materi tentang regulasi dan privasi data pribadi. Data menunjukkan **urgensi perlindungan data pribadi** dengan penetrasi internet mencapai **80,66% atau 229 juta pengguna di 2025**, berbanding lurus dengan lonjakan kasus pelanggaran dari 3 kasus (2019) menjadi 46 kasus (2023), dimana **89,8% adalah kebocoran data pribadi**. Berdasarkan **Pasal 46 Ayat (2) UU PDP**, pengendali wajib melaporkan kegagalan PDP dalam **waktu 3x24 jam** kepada subjek data dan lembaga, mencakup data yang terungkap, kronologi kejadian, upaya pemulihan, dan langkah mitigasi dampak. Presentasi menekankan **Data Centric Security** dengan pendekatan berlapis mulai dari data sebagai pusat hingga infrastruktur terluar untuk memastikan perlindungan menyeluruh.

Penanganan kebocoran data mengikuti **sembilan fase Data Breach Handling**: identifikasi breach, menghentikan penyebaran dan investigasi, tindakan perbaikan preventif, pelaporan ke otoritas, identifikasi dampak dan mitigasi, identifikasi subjek data terdampak, merespon subjek data, hingga dokumentasi dan evaluasi. **Root cause** kegagalan PDP yang paling sering terjadi adalah **lemahnya akses kredensial** (tidak ada MFA, penyimpanan password di browser, tanpa VPN), **konfigurasi software tidak aman** (API lemah, bisa di-brute force), dan **mekanisme verifikasi tidak efektif**. Masalah lain termasuk software tidak terupdate, phishing, data tidak terenkripsi/tanpa masking, dan manajemen BCP buruk. **Pilar People** menjadi **Security Weakest Link** yang harus diperkuat melalui awareness, training, MFA,

anti-malware, bijak menggunakan free WiFi, update software berkala, backup rutin, dan tidak menyimpan password di browser.

Sanksi pelanggaran PDP sangat berat dan terbagi dua kategori. **Sanksi Administratif** meliputi peringatan tertulis, penghentian kegiatan pemrosesan, penghapusan data, dan **denda administratif maksimal 2% pendapatan tahunan**. **Sanksi Pidana** jauh lebih serius: memperoleh/mengumpulkan data secara melawan hukum **pidana 5 tahun dan/atau denda Rp5 miliar**, mengungkapkan data **pidana 4 tahun dan/atau denda Rp4 miliar**, menggunakan data orang lain **pidana 5 tahun dan/atau denda Rp5 miliar**, serta membuat/memalsu data pribadi **pidana 6 tahun dan/atau denda Rp6 miliar**. Sanksi tegas ini menunjukkan keseriusan pemerintah dalam melindungi data pribadi warga negara dan memberikan efek jera bagi pelanggar, mengingat kegagalan PDP berdampak pada **incompliance** (sanksi, gugatan, rusaknya reputasi, hilangnya customer trust) versus **compliance** yang memberikan nilai kompetitif dan perluasan pasar.

MATERI 4

Nunil Pantjawati, Direktur Kebijakan Tata Kelola Keamanan Siber dan Sandi BSSN, menyampaikan materi tentang peran strategis PSE pengelola **Infrastruktur Informasi Vital (IIV)** dalam konteks **transformasi digital pemerintahan** yang mencakup tiga pilar: **Digital ID, Digital Payment, dan Data Exchange**. Berdasarkan **Perpres 82/2022 Pasal 1**, IIV adalah sistem yang memanfaatkan TI/Sistem Elektronik di **delapan sektor strategis**: Administrasi Pemerintahan, Kesehatan, Transportasi, Keuangan, ESDM, TIK, Pangan, dan Pertahanan. **Landscape keamanan siber 2025** menunjukkan ancaman dominan berupa **malware, ransomware, Advanced Persistent Threat (APT)**, dan data breach, dengan **279 insiden belum ditindaklanjuti** dan **532 insiden sudah ditindaklanjuti**. Yang krusial, presentasi menampilkan **interdependensi antar sektor** dimana gangguan pada satu sektor dapat berdampak **cascading** ke sektor lain—misalnya blackout listrik akan melumpuhkan transportasi, sistem keuangan, dan komunikasi secara bersamaan.

Pemerintah telah menerbitkan **hierarki regulasi komprehensif** mulai dari UUD 1945, UU ITE No. 38/2008, PP PSTE No. 71/2019, **Perpres 47/2023 dan 82/2022** tentang strategi keamanan siber nasional, hingga berbagai PerBSSN (PerBSSN 8/2020, 5/2021, 7/2023, 8/2023, 7/2024, 8/2024) yang mengatur sistem pengamanan, manajemen risiko, dan manajemen krisis siber. IIV memiliki tiga komponen utama: **Objek/Infra Vital** (infrastruktur fisik), **Cyber Space** (aplikasi dan data), dan **SE (IT/OT)** yang mencakup Information Technology dan Operational Technology. Pelindungan IIV bertujuan: (1) melindungi keberlangsungan penyelenggaraan secara **aman, andal, dan terpercaya**, (2) mencegah gangguan/kerusakan akibat serangan siber, (3) meningkatkan kesiapan menghadapi insiden dan mempercepat pemulihan, karena jika terjadi gangguan/kehancuran IIV dampaknya dapat menimbulkan **krisis ekonomi dan sosial**.

Penyelenggaraan pelindungan IIV mengikuti **sembilan langkah strategis** berdasarkan PerBSSN 7/2023: identifikasi SE yang menjadi IIV, penetapan IIV oleh K/L Sektor, penerapan standar keamanan (PerBSSN 4/2021 dan 8/2020), penerapan kerangka kerja

pelindungan IIV, **pengukuran tingkat kematangan kamsiber minimal 1 kali/tahun** (PerBSSN 10/2023), penerapan manajemen risiko, pengelolaan insiden siber (PerBSSN 1/2024 dan 2/2024), berbagi informasi, dan peningkatan kapasitas SDM (PerBSSN 9/2023). **Tugas PSE Penyelenggara IIV** mencakup: membentuk **TTIS Organisasi** (Tim Tanggap Insiden Siber), melaksanakan kesiapan terhadap insiden siber dengan incident response plan dan drill, melaporkan hasil identifikasi IIV dan manajemen risiko kepada K/L, menerapkan compliance terhadap standar keamanan secara mandatory, melakukan maturity assessment dan self-assessment untuk improvement berkelanjutan, menyelenggarakan forum berbagi informasi, serta melakukan **kerja sama internasional** untuk berbagi threat intelligence mengingat ancaman siber bersifat transnasional

MATERI 5

Cybersecurity Management untuk ATMAS (Air Traffic Management Automation System)

Identifikasi & Monitoring Keamanan Siber

Tahap awal dimulai dengan **identifikasi aset IT/OT** berdasarkan CANSO 2023, mencakup **primary assets** (radar, ADS-B, komunikasi VHF/HF) dan **primary information assets** (hardware, storage, network devices, firewall). Untuk **monitoring 24/7**, diterapkan **Managed Service SIEM** dengan **SOC (Security Operation Center)** yang mengintegrasikan berbagai tools seperti **EDR, WAF, NGFW**, serta layanan **Incident Response, Vulnerability Assessment, Penetration Testing**, dan **Digital Forensic**.

Strategi & Implementasi Keamanan

Penerapan keamanan siber disusun dalam **8 kerangka utama**: Cybersecurity Policy, Network Infrastructure Protection, User Account Management, System Development Life Cycle, Removable Media Control, Software Security Patch Management, Physical Security, dan Response to Cyber Security Incidents. Implementasi fokus pada **8 key points** krusial: **patch otomatis** minimal dua minggu sekali, **MFA (Multi-Factor Authentication)**, **restrict administrative privileges** dengan PAM dan jumphost, **application control**, disable macro berbahaya, user hardening, dan **regular backups** untuk business continuity.

Penilaian & Tools Rekomendasi

Tingkat keamanan dinilai sesuai **ICAO Doc 10084** melalui 5 kategori: penilaian risiko, pengukuran keamanan (FMEA/SWIFT), evaluasi otoritas, pelaporan hasil, dan syarat kontrak pengadaan. **Tools esensial** yang direkomendasikan meliputi **Firewall (EDR/IPS)**, sistem audit, **jumphost** sebagai access control terpusat, monitoring traffic jaringan, **EDR** untuk proteksi endpoint, dan manajemen patch sistematis—semuanya disesuaikan dengan kebijakan nasional dan kompatibilitas sistem existing.

MATERI 6

Panduan Koordinasi dan Operasional CSIRT Sektor Transportasi

Dasar Hukum & Tujuan Pembentukan CSIRT

Panduan ini dibentuk berdasarkan Kepmen Perhubungan KM 116/2024 tentang Tim Tanggap Insiden Siber, Perpres 82/2022 tentang Pelindungan Infrastruktur Informasi Vital, dan Peraturan BSSN 10/2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber. Tujuan utamanya adalah membentuk CSIRT Sektor Transportasi dengan struktur koordinasi jelas, memudahkan alur koordinasi antar unit kerja, memberikan data keamanan siber secara aman, cepat, dan tepat, serta memandu identifikasi IIV (Infrastruktur Informasi Vital), penilaian tingkat kematangan, pelaporan insiden, dan koordinasi insidentil saat terjadi serangan siber pada sistem elektronik kritikal.

Alur Koordinasi Identifikasi IIV & Penilaian Kematangan

Untuk Administrasi Pemerintahan, proses dimulai dari Koordinator TIK Es I & Pemilik SE menerima surat persiapan, dilanjutkan penilaian mandiri menggunakan tools IKAS, hingga verifikasi oleh BSSN dan penetapan SE IIV. Untuk Sektor Transportasi, Penyelenggara Transportasi melakukan identifikasi dan penilaian mandiri, menyampaikan ke Narahubung (Darat/Laut/Udara/Perkeretaapian), diteruskan ke Ketua CSIRT, kemudian diverifikasi BSSN dan disahkan Ketua Pengarah. Proses penilaian tingkat kematangan melibatkan Sekretariat CSIRT, Koordinator TIK, dan Pemilik SE dengan dokumentasi baseline kemampuan organisasi untuk perbaikan berkelanjutan.

Mekanisme Penanganan & Evaluasi Insiden Siber

Di Administrasi Pemerintahan, Service Desk menerima laporan insiden, melakukan forensik awal, diteruskan ke Sekretariat CSIRT dan Ketua CSIRT, kemudian Pemilik SE melakukan mitigasi dan melaporkan hasilnya. Sekretariat CSIRT melakukan validasi, mengisi form evaluasi pasca insiden, dan melaporkan ke BSSN. Di Sektor Transportasi, Nat-CSIRT melakukan monitoring dan menyampaikan insiden ke Ketua CSIRT, yang kemudian berkoordinasi dengan Narahubung dan Penyelenggara Transportasi untuk penanggulangan, pemulihan, dan evaluasi. Seluruh proses dilengkapi dengan kontak resmi seperti cs_digiportasi@kemenhub.go.id, @id_SIRTI, dan @GovCSIRT_ID untuk memastikan koordinasi efektif dalam menghadapi ancaman siber sesuai standar nasional BSSN.