KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 1: Pengenalan Keamanan Siber

Subtopik 1.2: Pentingnya Keamanan Siber untuk PemDa & Masyarakat

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. Keamanan siber bukan lagi isu teknis yang hanya dipahami oleh tenaga IT. Di era digital, seluruh layanan publik, administrasi pemerintah daerah, hingga aktivitas masyarakat sehari-hari sangat bergantung pada sistem digital. Oleh karena itu, memahami pentingnya keamanan siber menjadi hal mendasar bagi ASN maupun masyarakat.

Subtopik ini akan menjelaskan mengapa keamanan siber memiliki peran strategis, baik dalam menjaga keberlangsungan pemerintahan daerah maupun melindungi masyarakat dari kerugian pribadi. 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 subtopik 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 mengikuti pembelajaran pada subtopik ini, peserta diharapkan mampu:

1. Menjelaskan urgensi keamanan siber bagi pemerintah daerah dalam menjaga layanan publik dan data strategis.
2. Menguraikan pentingnya keamanan siber bagi masyarakat dalam melindungi identitas pribadi, finansial, dan aktivitas digital.
3. Mengidentifikasi dampak yang mungkin terjadi jika keamanan siber diabaikan, baik pada level pemerintah daerah maupun masyarakat.
4. Merefleksikan peran masing-masing dalam memahami urgensi keamanan siber.

Sasaran Peserta

1. ASN: agar memahami bahwa keamanan siber adalah aspek vital dalam tata kelola pemerintahan dan pelayanan publik, bukan hanya urusan teknis.
2. Masyarakat: agar menyadari bahwa keamanan siber melindungi identitas pribadi, finansial, dan meningkatkan kepercayaan pada layanan digital.

A. Urgensi Keamanan Siber bagi Pemerintah Daerah

1. **Menjaga Keberlanjutan Layanan Publik**

Pemerintah daerah kini mengandalkan sistem digital untuk hampir seluruh layanan. Administrasi kependudukan, perizinan, bantuan sosial, kesehatan, hingga pendidikan dilakukan lewat aplikasi. Jika terjadi serangan siber, pelayanan bisa terhenti, menimbulkan antrian panjang, keresahan masyarakat, bahkan potensi konflik sosial.

Misalnya, gangguan sistem kependudukan bisa membuat masyarakat tidak dapat mencetak KTP atau KK, yang berimbas pada akses layanan lain seperti kesehatan dan pendidikan. Dampak lain: turunnya produktivitas ASN karena layanan manual harus kembali dijalankan.

2. **Perlindungan Data Pemerintah sebagai Aset Strategis**

Data pemerintah bukan sekadar angka, tapi cerminan identitas dan hak masyarakat. Kebocoran data bukan hanya soal kerugian teknis, tetapi juga **keamanan nasional**. Data keuangan, tata ruang, dan perencanaan pembangunan jika jatuh ke tangan yang salah dapat digunakan untuk sabotase, manipulasi kebijakan, atau penyalahgunaan anggaran.

Misalnya, data aset daerah yang bocor bisa dimanfaatkan untuk kepentingan komersial atau kriminal. Data perencanaan pembangunan yang disalahgunakan dapat menimbulkan spekulasi politik atau ekonomi.

3. **Mendukung Kebijakan Nasional & Reputasi Pemda**

Pemda adalah perpanjangan tangan pemerintah pusat dalam menjalankan kebijakan nasional, termasuk di bidang keamanan siber. Kegagalan pemda menjaga data dan layanan digital dapat menurunkan reputasi pemerintah secara keseluruhan.

Pemda yang berhasil menjaga keamanan digital akan mendapat **kepercayaan lebih besar dari warganya**. Pemda yang sering mengalami insiden

digital berisiko dianggap tidak profesional, bahkan bisa kehilangan dukungan publik.

B. Urgensi Keamanan Siber bagi Masyarakat

1. **Melindungi Identitas Pribadi sebagai Hak Dasar**

   Identitas digital masyarakat sama pentingnya dengan identitas fisik. Jika NIK, rekening bank, atau akun digital diretas, masyarakat tidak hanya kehilangan uang, tapi juga bisa menjadi korban **pinjaman online ilegal**, **penyalahgunaan identitas**, bahkan **tindak kriminal**.

2. **Mencegah Kerugian Ekonomi & Psikologis**

   Kerugian akibat kejahatan siber tidak hanya materi, tapi juga menimbulkan trauma. Korban penipuan online sering mengalami tekanan psikologis: malu, takut, bahkan enggan melaporkan ke aparat karena khawatir disalahkan. Ini menunjukkan bahwa keamanan siber berdampak langsung pada **kesejahteraan mental dan sosial masyarakat**.

3. **Membangun Kepercayaan terhadap Layanan Digital**

   Digitalisasi hanya berhasil jika masyarakat percaya data mereka aman. Tanpa kepercayaan, masyarakat enggan menggunakan aplikasi pemerintah atau layanan digital.

   Contoh: jika warga merasa aplikasi kesehatan rawan bocor, mereka lebih memilih layanan tatap muka meski lebih sulit. Ini menghambat visi pemerintah untuk mewujudkan **Smart City** atau **Smart Regency**.

C. Dampak Jika Keamanan Siber Diabaikan

Level	Dampak Utama	Contoh Nyata
Pemda	Gangguan layanan, rusaknya reputasi, pemborosan anggaran untuk pemulihan	Sistem kependudukan lumpuh, antrean panjang warga.

Level	Dampak Utama	Contoh Nyata
Masyarakat	Pencurian data pribadi, kerugian finansial, trauma psikologis	Penyalahgunaan identitas untuk kejahatan, penipuan via WA bank palsu, hoaks menyebar cepat, menimbulkan kepanikan sosial.
Negara	Turunnya kepercayaan global, terhambatnya transformasi digital, ancaman ketahanan nasional	Indonesia dianggap lemah di bidang siber, kebocoran data nasional dijual di forum gelap, serangan siber bisa jadi alat perang non-militer.

D. Implikasi Strategis Keamanan Siber

Subtopik 1.1 menjelaskan bentuk ancaman teknis seperti phishing, kebocoran data, atau peretasan. Namun, penting dipahami bahwa dampak serangan siber jauh lebih luas daripada sekadar persoalan teknis.

1. **Krisis Kepercayaan Publik**

   Insiden siber bukan hanya masalah teknologi, tetapi juga menyangkut kepercayaan masyarakat. Ketika data bocor, masyarakat kehilangan keyakinan terhadap kemampuan pemerintah melindungi mereka.

2. **Ancaman terhadap Stabilitas Pemerintahan Daerah**

   Gangguan layanan publik digital dapat melumpuhkan aktivitas birokrasi, menurunkan produktivitas ASN, dan menimbulkan keresahan sosial. Hal ini berpotensi mengganggu stabilitas politik dan pemerintahan daerah.

3. **Potensi Krisis Sosial-Ekonomi**

   Kerugian individu akibat penipuan atau pencurian data dapat menumpuk menjadi kerugian kolektif. Jika dibiarkan, hal ini bisa menghambat perkembangan ekonomi digital dan menciptakan krisis sosial yang lebih luas.

Dengan demikian, keamanan siber harus dipahami sebagai bagian dari **kepercayaan publik, keberlanjutan pelayanan, dan stabilitas sosial-ekonomi**, bukan hanya urusan teknis IT.

Pertanyaan Reflektif

1. Jika suatu layanan publik digital (misalnya aplikasi kependudukan atau kesehatan) tiba-tiba berhenti karena serangan siber, menurut Anda apa dampak paling terasa bagi masyarakat?
2. Kepercayaan masyarakat terhadap layanan digital sangat penting. Menurut Anda, apa yang membuat masyarakat bisa merasa yakin atau justru ragu untuk menggunakan layanan tersebut?

DAFTAR PUSTAKA

Badan Siber dan Sandi Negara. (2021). *Laporan Tahunan Keamanan Siber Indonesia.* Jakarta: BSSN. https://bssn.go.id

Fatanah, D. Y., Putri, E. R. D., Z, W. O. A., Faturachman Alputra Sudirman, & Saidin. (2025). ANALISIS BIBLIOMETRIK BIROKASI DIGITAL DAN KEAMANAN DATA DI INDONESIA TAHUN 2023-2024. *Jurnal Ilmu Pemerintahan*, *13*(02), 191–206.

Kementerian Komunikasi dan Digital. (2024). *Laporan Tahunan Keamanan Siber dan Perlindungan Data Pribadi.* https://www.komdigi.go.id

Maharani, M. A., & Atman, W. (2025). Evaluasi Strategi Nasional Keamanan Siber Indonesia dalam Menanggapi Ancaman Digital Indonesia Keamanan Siber sebagai Bagian dari Keamanan Nasional. *Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial Dan Politik*, *2*(3), 344–354. https://doi.org/10.62383/sosial.v2i3.2291

Nikolov, G., Varga, M., Panganiban, A. R., Kullman, K., & Lavigne, V. (2025). Enhancing Cyber Situation Awareness: Visualizing Advanced Persistent Threats as Complex Systems. *Lecture Notes in Computer Science*, *15995 LNCS*, 90–107. https://doi.org/10.1007/978-3-032-00633-2_6

Pratama, F. A., Setiono, S. A., Prayogo, H. A., Budhiyanto, M. N., & Kusuma, A. A. D. P. (2025). Challenges and Strengthening of the Islamic Banking Security System in the Digital Age. *Journal of Legal and Social Changes*, *1*(1), 52–62.

Roumani, Y., & Roumani, Y. F. (2025). Predicting Ransomware Incidents with Time-Series Modeling. *Journal Od Cybersecurity and Privacy*, *5*(61), 1–16. https://doi.org/10.3390/jcp5030061

Satrya, I. Z. (2025). The Influence of Experience , Fear , Awareness of Cyber Attacks on the Acceptance of Banking Technology Moderated by Perceived Benefits in the Development of Digital-Based Banking Services in Indonesia. *Eduvest – Journal of Universal Studies*, *5*(8), 10059–10074.

Surbakti, F. P. S. (2025). Digital Safety Education for the Constituents of West Nusa

Tenggara Electoral District 2. *Jurnal Pengabdian UNDIKMA: Jurnal Hasil Pengabdian & Pemberdayaan Kepada Masyarakat*, *6*(3), 479–487. https://doi.org/10.33394/jpu.v6i3.16374