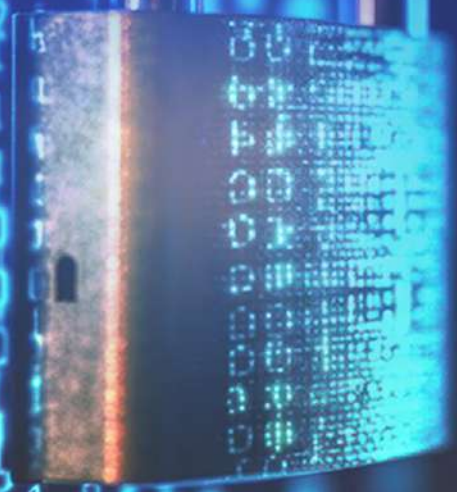
KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 1: Pengenalan Keamanan Siber

Subtopik 1.1: Apa itu Keamanan Siber?



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. Perkembangan teknologi digital telah membawa banyak manfaat bagi pelayanan publik dan kehidupan sehari-hari. Namun, di sisi lain, ancaman siber seperti penipuan daring, pencurian data, hingga serangan pada sistem pemerintahan juga semakin meningkat. Oleh sebab itu, pemahaman dasar tentang apa itu keamanan siber menjadi penting, baik bagi Aparatur Sipil Negara (ASN) maupun masyarakat.

Subtopik ini diharapkan dapat menjadi panduan praktis yang mudah dipahami dalam memperkenalkan konsep dasar keamanan siber. Dengan bekal pemahaman awal ini, diharapkan peserta mampu lebih waspada, bijak, dan terampil dalam menjaga keamanan data pribadi maupun data pemerintah. 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 bagian ini, peserta (ASN maupun masyarakat) mampu:

1. Menjelaskan definisi keamanan siber dengan bahasa sederhana.
2. Menguraikan secara singkat perkembangan keamanan siber di Indonesia sebagai konteks pentingnya perlindungan data.
3. Memahami ruang lingkup keamanan siber dalam kehidupan sehari-hari dan birokrasi.
4. Merefleksikan peran pribadi dalam meningkatkan keamanan siber, baik sebagai ASN maupun masyarakat.

Sasaran Peserta

1. ASN: agar memahami tugas menjaga data pemerintahan sekaligus menyadari posisi strategis pemda dalam ekosistem keamanan siber nasional.
2. Masyarakat: agar lebih bijak dalam menjaga data pribadi, menghindari interaksi digital berisiko, serta mampu merefleksikan langkah kecil untuk meningkatkan keamanan digital sehari-hari.

A. Definisi Keamanan Siber

Apa itu Keamanan Siber? Keamanan siber adalah segala upaya untuk melindungi perangkat, jaringan, dan informasi yang kita gunakan dalam kehidupan sehari-hari maupun pekerjaan agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Informasi yang dimaksud bisa berupa data pribadi, seperti nomor identitas dan akun media sosial, maupun data penting milik pemerintah, seperti dokumen administrasi dan arsip layanan publik.

Dengan adanya keamanan siber, kerahasiaan informasi tetap terjaga, keaslian data tidak berubah, dan sistem pelayanan dapat digunakan kapan saja tanpa gangguan. Tiga hal ini dikenal dengan istilah **"CIA"**:

1. **Confidentiality (Kerahasiaan):** hanya pihak yang berhak yang boleh mengakses data.
2. **Integrity (Integritas):** data harus tetap asli dan tidak boleh dimanipulasi.
3. **Availability (Ketersediaan):** informasi dan layanan tetap tersedia saat dibutuhkan.

Dalam kehidupan sehari-hari, bentuk keamanan siber bisa sesederhana:

1. Mengunci ponsel dengan PIN atau sidik jari.
2. Tidak sembarangan mengklik tautan dari pesan mencurigakan.
3. Menyimpan dokumen resmi di tempat aman dan hanya mengunggah pada aplikasi atau website resmi pemerintah.

Bagi ASN, keamanan siber berarti menjaga sistem dan data yang dikelola pemerintah agar tetap aman, sehingga pelayanan kepada masyarakat tidak terganggu. Sementara bagi masyarakat, keamanan siber membantu melindungi diri dari penipuan, pencurian identitas, atau kebocoran data pribadi.

Dengan demikian, keamanan siber **bukan hanya urusan teknis para ahli IT**, melainkan tanggung jawab bersama seluruh lapisan masyarakat dan aparatur pemerintah.

B. Sejarah Singkat Keamanan Siber di Indonesia

Kesadaran tentang keamanan siber di Indonesia mulai meningkat sejak tahun 2010-an ketika kasus peretasan dan kebocoran data publik semakin sering terjadi. Untuk memperkuat pertahanan digital nasional, pemerintah membentuk **Badan Siber dan Sandi Negara (BSSN) pada tahun 2017**, yang bertugas menyusun kebijakan, standar, dan strategi nasional di bidang siber. Sejak saat itu, isu keamanan siber bukan hanya urusan teknis, tetapi sudah menjadi bagian penting dari pembangunan nasional, termasuk di tingkat pemerintah daerah.

C. Ruang Lingkup Keamanan Siber

Keamanan siber tidak hanya berbicara soal komputer atau hacker, tetapi mencakup seluruh aktivitas digital yang kita lakukan sehari-hari, baik di kantor maupun di rumah. Ada empat ruang lingkup utama yang perlu diperhatikan:

1. **Perangkat**

   Semua alat yang digunakan untuk mengakses dunia digital: HP, komputer kantor, laptop pribadi, bahkan perangkat pintar seperti CCTV atau smart TV.

   Jika perangkat tidak aman (misalnya tidak di-update, tidak memakai password, atau terinfeksi malware), maka data di dalamnya bisa dicuri atau dipalsukan.

2. **Data**

   Data adalah aset paling berharga. Untuk pemerintah, ini termasuk **dokumen resmi, NIK, KK, arsip pelayanan publik, data keuangan daerah, dan laporan internal**.

   Untuk masyarakat, data bisa berupa **akun media sosial, password email, foto pribadi, hingga data keuangan di aplikasi bank digital**.

   Data yang bocor bisa disalahgunakan untuk penipuan, pemerasan, atau penyebaran hoaks.

3. **Layanan Publik Digital**

Saat ini banyak pelayanan pemerintah berbasis aplikasi dan website, seperti pendaftaran sekolah online, layanan kesehatan, hingga administrasi kependudukan.

Jika sistem ini diserang atau diretas, pelayanan bisa terhenti, bahkan menimbulkan kerugian besar bagi masyarakat.

Contoh: website layanan publik down akibat serangan siber, sehingga warga tidak bisa mengakses layanan penting.

4. **Interaksi Sosial Digital**

Aktivitas komunikasi sehari-hari melalui WhatsApp, email, Instagram, atau Facebook juga termasuk ruang lingkup keamanan siber.

Banyak serangan justru berawal dari interaksi sosial ini: pesan palsu, tautan berbahaya, akun palsu yang menyamar sebagai teman atau pejabat.

Keamanan dalam bersosialisasi digital sama pentingnya dengan keamanan data, karena kebocoran sering dimulai dari hal yang terlihat sepele.

D. Studi Kasus Nyata di Indonesia

1. **Kebocoran Data Dukcapil (2021)**

Data kependudukan yang berisi NIK, KK, dan alamat warga dilaporkan bocor dan diperjualbelikan di forum gelap.

Dampaknya: masyarakat merasa tidak aman, muncul risiko penipuan menggunakan identitas palsu.

Pelajaran: data kependudukan yang dikelola ASN adalah aset strategis negara, sehingga pengamanan berlapis wajib dilakukan.

2. **Kasus Penipuan Online via SMS/WA (2022–2024)**

Ribuan masyarakat Indonesia menjadi korban SMS/WA palsu yang mengatasnamakan bank, BPJS, atau layanan kurir.

Contoh: korban diminta mengklik tautan untuk “cek paket” lalu tanpa sadar memasang aplikasi palsu yang mencuri data perbankan.

Pelajaran: masyarakat perlu berhati-hati terhadap pesan mencurigakan, meskipun terlihat resmi.

3. **Peretasan Akun Media Sosial Pejabat Publik (2023)**

   Beberapa akun pejabat pemerintah diretas dan digunakan untuk menyebarkan informasi palsu.

   Dampaknya bukan hanya kerugian pribadi, tetapi juga bisa merusak citra lembaga pemerintah.

   Pelajaran: keamanan akun media sosial sama pentingnya dengan keamanan data kantor.

Dari studi kasus nyata yang terjadi di Indonesia terlihat bahwa **ASN maupun masyarakat sama-sama rentan terkena ancaman siber**, hanya bentuknya berbeda: ASN pada data pemerintahan, masyarakat pada data pribadi.

E. Kenapa Harus Dipahami ASN & Masyarakat?

1. **Peran ASN**

   ASN adalah pengelola dan penjaga sistem pemerintahan digital. Jika ASN lalai, data sensitif instansi dapat bocor dan merugikan ribuan masyarakat.

   Pemahaman keamanan siber membuat ASN lebih waspada dalam menggunakan perangkat kantor, mengelola akun, serta memberikan pelayanan publik yang aman.

2. **Peran Masyarakat**

   Masyarakat adalah pengguna layanan digital sekaligus target empuk bagi penipu online.

   Dengan memahami keamanan siber, masyarakat bisa lebih berhati-hati dalam menyimpan data pribadi, menghindari jebakan link palsu, serta melaporkan insiden ke pihak berwenang.

Kesimpulannya: **Keamanan siber adalah tanggung jawab bersama.** ASN menjaga sistem dan data publik, sementara masyarakat menjaga data pribadi dan berhati-hati dalam interaksi digital.

Pertanyaan Reflektif

1. Dari berbagai contoh ruang lingkup keamanan siber (perangkat, data, layanan publik digital, dan interaksi sosial), mana yang paling sering Anda gunakan dalam kehidupan sehari-hari? Apakah sudah aman?
2. Jika keamanan siber dianggap sebagai tanggung jawab bersama, langkah kecil apa yang bisa Anda lakukan mulai hari ini untuk melindungi data pribadi maupun data instansi?

DAFTAR PUSTAKA

Asyrofi, M. F., & Nugraha, I. G. D. (2025). Cybersecurity Of Work From Anywhere Model For Government : A Systematic Literature Review. *International Journal of Electrical, Computer, and Biomedical Engineering*, *3*(1), 117–141. https://doi.org/10.62146/ijecbe.v3i1.113

Badan Siber dan Sandi Negara. (2023). *Strategi Keamanan Siber Nasional Republik Indonesia*. Jakarta: BSSN. https://bssn.go.id

Khoironi, S. C. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. *Jurnal Studi Komunikasi Dan Media, 24*(1), 37–50. https://doi.org/10.31445/jskm.2020.2945

National Institute of Standards and Technology. (2022). *Cybersecurity framework*. https://www.nist.gov/cyberframework