Nama : Muhammad Yusuf
NIM : 122140193
Dosen Pengampu : Andika Setiawan, S.Kom.,M.Cs.

DRPL RC

Pengantar Keamanan Siber Untuk OJK Institute

1. Definisi Keamanan Siber
   Keamanan siber adalah praktik melindungi komputer, jaringan, aplikasi perangkat lunak, sistem kritis, dan data dari potensi ancaman dan gangguan digital. Organisasi bertanggung jawab untuk mengamankan data guna menjaga kepercayaan pelanggan dan memenuhi kepatuhan terhadap peraturan.

2. Pentingnya Keamanan Siber
   Bisnis di berbagai sektor menggunakan sistem digital untuk menyediakan layanan efisien dan menjalankan operasi bisnis yang hemat biaya. Keamanan siber menjadi penting untuk melindungi aset digital, mencegah biaya pelanggaran, memelihara kepatuhan terhadap peraturan, dan mengurangi ancaman siber yang terus berkembang.

3. Jenis Ancaman & Serangan Siber
   Meliputi malware, phishing, serangan Denial-of-Service (DoS), serangan Man-in-the-Middle, dan Zero-Day Exploits.

4. Bagaimana Keamanan Siber Bekerja
   Organisasi menerapkan strategi keamanan siber dengan melibatkan spesialis keamanan siber yang membuat kerangka kerja keamanan siber komprehensif dan melibatkan edukasi kepada karyawan mengenai praktik terbaik keamanan.

5. Komponen Keamanan Siber
   Termasuk keamanan jaringan (NETWORK SECURITY), kriptografi, keamanan ujung ke ujung, serta perlindungan data dan privasi.

6. Ancaman Siber yang Nyata
   Ancaman siber dapat memiliki dampak fisik, psikologis, ekonomi, dan politik. Perlindungan dari serangan siber bukanlah ilmu sulap, melainkan memerlukan langkah-langkah konkret dan pemahaman yang mendalam.

7. Tantangan dan Resiko Terkini
   Termasuk tantangan dalam mengelola data pribadi, risiko dari pihak ketiga (vendor), serta tantangan dalam menghadapi serangan siber yang semakin kompleks.

8. Budaya Digital dan Perlindungan Data
   Membangun budaya digital yang aman, nyaman, dan berkelanjutan melalui pemahaman, edukasi, dan kepatuhan terhadap regulasi perlindungan data.

9. Tata Kelola, Manajemen Krisis, dan Perlindungan Diri
   Pentingnya tata kelola yang baik, manajemen krisis yang efektif, serta perlindungan diri yang komprehensif melalui berbagai komponen keamanan seperti konsultasi keamanan, uji keamanan, respons insiden, dan perlindungan asuransi.

Rangkuman ini memberikan gambaran luas tentang topik keamanan cyber yang mencakup definisi, pentingnya, jenis-jenis ancaman, bagaimana cara kerjanya, komponen-komponennya, tantangan yang dihadapi, dan langkah-langkah untuk mengatasinya.