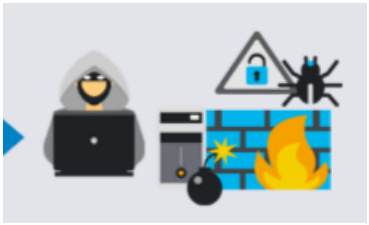
KEAMANAN JARINGAN
(SUMMARY MODUL 2 CYBER SECURITY IN THE ORGANIZATION)

Nadya Indah Trisnawati
(3122640034)
LJ D4 IT B

PROGRAM STUDI TEKNIK INFORMATIKA
DEEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2023/2024

1. **Mengapa Organisasi Memerlukan Keamanan Siber ?**

Alasan utamanya adalah ancaman yang mengeksploitasi kerentanan dapat merugikan atau mengganggu aktivitas bisnis.



Untuk menghadapi risiko kebakaran, organisasi menempatkan detektor asap dan alarm kebakaran di lokasi strategis, melakukan latihan kebakaran rutin, dan membeli asuransi.
Demikian pula, organisasi harus mengidentifikasi risiko keamanan dan mengelolanya.

Beberapa Jenis Dampak Usaha :

Insiden keamanan dapat memengaruhi bisnis dalam beberapa cara:

Server basis data mati karena serangan Distributed Denial of Service (DDoS).	Operasi bisnis terganggu karena masalah yang terkait dengan pemasok, Kerusakan infrastruktur, dll.
Diperlukan jam ekstra untuk pulih dari infeksi malware massal	Biaya melakukan bisnis meningkat
Bisnis didenda oleh otoritas lokal karena pelanggaran informasi pelanggan	Tidak dapat memberikan layanan berdasarkan kontrak. Atau, tidak mampu mematuhi peraturan
Insiden keamanan yang menyebabkan pelanggan merasa bahwa organisasi tidak serius dalam melindungi informasi pelanggan	Citra atau merek organisasi terpengaruh

- Pada data terbagi menjadi 2 yaitu :
  1. Data in storage mengacu pada data yang disimpan dalam media penyimpanan seperti hard disk, solid state drive (SSD), atau cloud storage. Data yang disimpan dalam media ini dapat diakses kapan saja, asalkan perangkat penyimpanannya terhubung ke perangkat yang membutuhkan data tersebut.
  2. data movement mengacu pada proses memindahkan data dari satu lokasi ke lokasi lain. Proses ini dapat terjadi di dalam perangkat, antara perangkat, atau melalui jaringan komputer. Data movement dapat terjadi dalam berbagai bentuk, seperti transfer file, streaming video, atau pengiriman email.
- CSI merupakan singkatan dari "Cybersecurity Incident Response" atau Respons Insiden Keamanan Siber. Konsep CSI terdiri dari lima tahap yaitu "Identify, Protect, Detect, Respond, dan Recover" yang masing-masing memiliki peran penting dalam menangani insiden keamanan siber:
  1. Identify (Identifikasi): Tahap ini bertujuan untuk mengidentifikasi insiden keamanan siber.
  2. Protect (Perlindungan): Tahap ini bertujuan untuk melindungi sistem dari ancaman yang mungkin terjadi.
  3. Detect (Deteksi): Tahap ini bertujuan untuk mendeteksi insiden keamanan siber secepat mungkin.
  4. Respond (Tanggapan): Tahap ini bertujuan untuk merespons insiden keamanan siber dengan cepat dan efektif.
  5. Recover (Pemulihan): Tahap ini bertujuan untuk memulihkan sistem keamanan siber setelah insiden terjadi.

- Threat impact atau dampak ancaman dalam konteks keamanan siber adalah kerugian atau konsekuensi negatif yang terjadi ketika suatu sistem atau jaringan mengalami serangan atau insiden keamanan. Dampak ancaman dapat berdampak pada berbagai aspek, seperti keuangan, operasional, dan reputasi organisasi atau individu. Oleh karena itu, penting untuk mencegah dan menanggapi ancaman dengan cepat dan efektif untuk meminimalkan dampak negatifnya.
- Vulnerabilities atau kerentanan dalam konteks keamanan siber adalah celah atau kelemahan dalam sistem, aplikasi, atau infrastruktur yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan atau insiden keamanan siber. Kerentanan dapat terjadi karena berbagai faktor, seperti kesalahan desain, kegagalan pengembangan perangkat lunak, atau kurangnya pembaruan keamanan. Berikut adalah pengertian kerentanan dalam beberapa konteks:
    1. Kerentanan sistem: Kerentanan pada sistem komputer dapat terjadi karena kelemahan pada sistem operasi, layanan jaringan, atau perangkat keras.
    2. Kerentanan aplikasi: Aplikasi perangkat lunak seringkali memiliki kerentanan yang dapat dimanfaatkan oleh penyerang untuk mendapatkan akses ke sistem atau data.
    3. Kerentanan infrastruktur: Infrastruktur keamanan siber, seperti firewall, router, atau switch, juga dapat memiliki kerentanan yang dapat dimanfaatkan oleh penyerang untuk menyerang sistem atau jaringan.
- Risk atau risiko dalam konteks keamanan siber adalah kemungkinan terjadinya kerugian atau konsekuensi negatif akibat dari serangan atau insiden keamanan siber. Risiko dapat berasal dari berbagai sumber, seperti kerentanan sistem atau jaringan, kelemahan keamanan dalam aplikasi, atau serangan siber yang dilakukan oleh penyerang.
    1. Reduce, atau mengurangi risiko dalam konteks keamanan siber adalah tindakan untuk mengurangi kemungkinan terjadinya serangan atau insiden keamanan siber, sehingga dapat meminimalkan dampak negatifnya.
- Weakest link atau "lemahnya tautan" dalam konteks keamanan siber adalah orang atau elemen dalam sistem yang menjadi sumber kerentanan atau titik lemah yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan atau insiden keamanan siber. Contoh dari weakest link dalam keamanan siber yang berkaitan dengan orang atau manusia antara lain adalah:
    1. Password yang lemah: Orang seringkali menggunakan password yang lemah atau mudah ditebak.
    2. Kurangnya pelatihan keamanan siber: Orang seringkali tidak memiliki kesadaran yang cukup tentang keamanan siber dan dapat membuat kesalahan, seperti membuka email dari pengirim yang tidak dikenal atau mengklik tautan yang mencurigakan.
    3. Ketergantungan pada teknologi: Orang seringkali mengandalkan teknologi keamanan, seperti firewall atau antivirus, untuk melindungi sistem dan data mereka, tanpa menyadari bahwa mereka sendiri dapat menjadi target serangan siber.