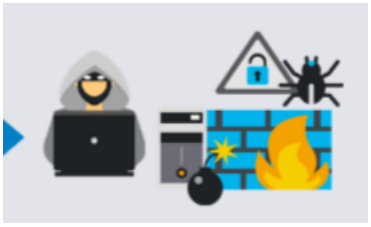
KEAMANAN JARINGAN
(SUMMARY MODUL 2 CYBER SECURITY IN THE ORGANIZATION)

Fifin Nur Rahmawati
Dosen : Dr. Ferry Astika Saputra ST, M.Sc
3122640040
D4 LJ-Teknik Informatika

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

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

1. Mitigasi
   Mitigasi atau kurangi risiko dengan menerapkan kontrol keamanan.
2. Transfer
   Mentransfer risiko sehingga ditangani oleh entitas lain seperti Asuransi

Meningkatkan Kesiapan Keamanan Siber

Menyadari tingkat dan kemungkinan risiko memungkinkan organisasi untuk lebih proaktif dan siap.

Pada akhirnya, manajemen puncak organisasi bertanggung jawab untuk memastikan keamanan

Pendekatan komprehensif untuk manajemen risiko harus melibatkan orang-orang di seluruh organisasi untuk meningkatkan kualitas pengambilan keputusan untuk mengelola risiko.

Upaya ini akan membutuhkan organisasi untuk menginvestasikan sumber daya (yaitu uang, waktu dan personel) dan mengembangkan program keamanan cyber yang komprehensif

Cara Mengurangi Risiko Serangan Cyber