

Keamanan Jaringan



Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN 2023

Rangkuman Modul 2: Keamanan Cyber dalam Organisasi

Pentingnya Keamanan Siber dalam Organisasi





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

Ilustrasi

Untuk menghadapi risiko kebakaran, organisasi menempatkan detektor asap dan alarm kebakaran di lokasi strategis, melakukan latihan kebakaran secara teratur, dan membeli asuransi.

Demikian pula, organisasi harus mengidentifikasi risiko keamanan dan mengelolanya.

Beberapa Jenis Dampak Bisnis

	Database server is down due to a Distributed Denial of Service (DDoS) attack	Business operations are disrupted due to problems related to suppliers, infrastructure malfunction, etc.
	Extra hours required to recover from mass malware infection	Cost of doing business increases
	Business is fined by local authority due to breach of customer information	Not able to deliver services based on contract. Or, not being able to comply with regulations
	Security incident causing customers to perceive that the organization is not serious about protecting customer information	Image or brand of the organization was affected

Mengelola Risiko

Mitigasi

Mitigasi atau mengurangi risiko dengan menerapkan kontrol keamanan.

Transfer

Mentransfer risiko sehingga ditangani oleh entitas lain seperti Asuransi.

Meningkatkan Kesiapan Keamanan Siber

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

2. Pendekatan komprehensif untuk manajemen risiko harus melibatkan orang-orang di seluruh organisasi untuk meningkatkan kualitas pengambilan keputusan untuk mengelola risiko.
3. Upaya ini akan membutuhkan organisasi untuk menginvestasikan sumber daya (yaitu uang, waktu dan personel) dan mengembangkan program keamanan cyber yang komprehensif.
4. Pada akhirnya, manajemen puncak organisasi bertanggung jawab untuk memastikan keamanan organisasi.

Ancaman Keamanan untuk Organisasi

- Denial Of Service Attack
- Malware
- Identity Theft
- Web Defacement

Cara Mengurangi Risiko Serangan Cyber



Technical Controls to Detect & Prevent

(e.g. firewalls, spam filters, intrusion detection system and antivirus software)



Education and training of our employees

especially when dealing with phishing and how to develop web application securely



Ensuring that network providers have capabilities to support us when we are under attack

Quiz

Which one of the following is not considered good practice when managing passwords?

- ☒ the password should be sent in plaintext by email
- ☐ the password should be long and complex enough to make it difficult for someone else to guess
- ☐ the password should be stored and transmitted securely
- ☐ the password should not be shared with others

Upon infection, what a malware does is dependent on the

- ☒ Payload
- ☐ Trojan
- ☐ Worm
- ☐ Exploit Kit

Tricking users to give away their login credentials is an example of

- ☒ Phishing
- ☐ Denial of Service
- ☐ Malware
- ☐ Password Sniffing

In risk management, implementing counter measures such as a firewall or running security awareness campaigns are an example of

- ☐ Risk Analysis
- ☒ Risk Mitigation
- ☐ Risk Assessment
- ☐ Risk Transfer

In an organization, positive security culture and awareness can be achieved by which of the following approach?

- ☐ Monitoring network activities
- ☐ Vulnerability and Patch Management
- ☒ Security Awareness Campaigns
- ☐ Risk Management

Impersonating a user to gain access to systems accessible to that user is an example of

- ☐ Email Theft
- ☒ Identity Theft
- ☐ Email Spoofing
- ☐ Social Engineering

Which of the following is not affected by a web defacement incident?

- ☐ Information Integrity
- ☐ Information Availability
- ☐ Organization's reputation
- ☒ Server uptime

The primary impact of a distributed denial of service attack is on which of the following security objectives

- ☐ Safety
- ☐ Confidentiality
- ☐ Integrity
- ☒ Availability