Commentary

iMedPub Journals
http://www.imedpub.com

American Journal of Computer Science and Engineering Survey

2020
Vol. 8 No.3:13

Cybersecurity and Computer Protection (countermeasures)

Nilam Verma*

Department of Computer Science & Engineering, HR Institute of technology, Pune, India

*Corresponding author: Nilam Verma, Department of Computer Science & Engineering, HR Institute of technology, Pune, India, E-mail: nilam.verma.ak@gmail.com

Citation: Verma N (2020) Cybersecurity and Computer Protection (countermeasures). Am J Comput Sci Eng Surv Vol. 8 No. 3: 13.

Received: November 04, 2020; **Accepted:** November 18, 2020; **Published:** November 24, 2020

Description

Computer security, cybersecurity or information technology security (IT security) is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data and also from the disruption or misdirection of the services they supply.

Due to increased reliance on computer systems, Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and therefore the various devices that constitute the "Internet of things" this field is becoming more important. Cybersecurity is additionally one of the main challenges in the contemporary world owing to its complexity, both in terms of politics and technology.

Vulnerabilities and attacks

- Backdoor
- Denial-of-service attack
- Direct-access attacks
- Eavesdropping
- Multi-vector
- polymorphic attacks
- Phishing
- Privilege escalation
- Social engineering
- Spoofing
- Tampering

Information security culture

Employee behavior can have an enormous impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within a corporation. Information security culture is that the "totality of patterns of behavior in a corporation that contributes to the protection of data of all types".

Andersson and Reimers (2014) found that employees often don't see themselves as part of their organization's information security effort and sometimes take actions that impede organizational changes. Research shows information security culture must be improved continuously. In "Information Security Culture from Analysis to Change", authors commented, "It's a never-ending process, a cycle of evaluation and alter or maintenance."

Five steps should be taken to manage the information security culture: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.

- Pre-Evaluation: To analyse the current security policy and to identify the awareness of information security within employees.
- Strategic Planning: Clustering people is helpful to achieve it and to come up with a better awareness program, clear targets need to be set.
- Operative Planning: Based on internal communication, management-buy-in, and security awareness and a training program a good security culture can be established.
- Implementation: To implement the information security culture, four stages should be used. They are:

Commitment of the management

Communication with organizational members

Courses for all organizational members

Commitment of the employees

- Post-Evaluation: to assess the success of the planning and implementation, and to identify unresolved areas of concern.

Systems at risk

- Financial systems
- Utilities and industrial equipment
- Aviation
- Consumer devices
- Large corporations
- Automobiles
- Government
- Internet of things and physical vulnerabilities
- Medical systems
- Energy sector

Computer protection (countermeasures)

In computer security a countermeasure is an action, device, procedure or technique that reduces a threat, vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Some common countermeasures are listed in the following sections:

- Security by design
- Security architecture
- Security measures
- Vulnerability management
- Reducing vulnerabilities
- Hardware protection mechanisms
- Secure operating systems
- Secure coding
- Capabilities and access control lists
- End user security training
- Digital hygiene
- Response to breaches

Types of security and privacy

- Access control
- Anti-key loggers
- Anti-malware
- Anti-spyware
- Anti-subversion software
- Anti-tamper software
- Anti-theft
- Antivirus software
- Cryptographic software
- Computer-aided dispatch (CAD)
- Firewall
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Log management software
- Parental control
- Records management
- Sandbox
- Security information management
- SIEM
- Software and operating system updating