Journal Of Harmonized Research (JOHR)

Journal of Harmonized Research in Engineering 10(2), 2022,05-06

ISSN: 2347-7393

Commentary

PROTECTING WAYS TO PRIVATIZE PERSONAL DATA FROM UNAUTHORIZED PERSON

Marie Sophia[*]

Department of Cyber Security, Appalachian State University, Boone, United States

Received: 02-Jun-2022, Manuscript No. JHRE-22-66633; **Editor assigned:** 07-Jun-2022, PreQC No. JHRE-22-66633(PQ); **Reviewed:** 28-Jun-2022, QC No JHRE-22-66633; **Revised:** 05-Jul-2022, Manuscript No. JHRE-22-66633(R); **Published:** 15-Jul-2022, DOI:10.30876/2347-7393.22.10.199

DESCRIPTION

The methods that business employ performs to protect information are referred to information security (or InfoSec). This includes policy settings that prevent unauthorised individuals from gaining access to corporate or personal data. InfoSec is a speed expanding and changing field that encompasses everything from network and infrastructure security to test and auditing. Information security safeguards have sensitive data against illegal access, modification, or recording, as well as any disturbance. The purpose is to protect vital data such as customer information, financial information, and intellectual properties. Repercussions of security Incidents include theft of private information, data tampering, and data erasure. Attacks can work operations and harm a company's reputation as well as incur a monetary cost. Organizations must budget for security and make sure they are prepared to identify, respond to, and prevent threats including phishing, malware, viruses, malicious insiders, and ransomware.

Information security principles

The main important concepts of information security are Confidentiality, integrity, and availability. One or more of these principles should be implemented in every aspect of the information security programme. Collective name of information security is CIA Traid.

For Correspondence:

sophiamarie@asu.edu

Downloaded from: https://www.johronline.com/harmonized-research-engineering.html

Confidentiality: Confidentiality safeguards are in place to avoid unauthorised information dissemination. The confidentiality principle's goal is to keep personal information private and only make it public and available to those who possess it or require it to execute their organisational functions.

Integrity: Protection against unwanted data modifications (additions, deletions, alterations, and so on) is included in consistency. The integrity principle assures that data is accurate and dependable, and that it is not tampered in any way, whether mistakenly or maliciously.

Availability: Availability is the capacity of a system to create software systems and data completely available to user when they require (or at a specified time). The goal of availability is to design technological infrastructure, applications, and data available when they are needed for a business process or by a company's customers.

Information security and cyber security

In terms of breadth and aim, information security differs from cybersecurity. Although the two terms are frequently used interchangeably, cybersecurity is a subclass of information security. Physical security, endpoint security, data encryption, and network security are only few of the topics covered by information security. It's also linked to information assurance, which safeguards data against hazards like natural catastrophes and server outages.

Cyber security is primarily concerned with technological threats, methods and technologies that are used to avoid or mitigate them. Another similar area is data security, which focuses on preventing an organization's data from being exposed to unauthorised parties by accident or maliciously.

Information security threats

There are thousands of identified threat vectors and hundreds of categories of information security threats. Some of the major dangers that security teams at modern businesses are concerned about. Security measures are frequently compromised as a result of the speed and technical development. In other circumstances, systems are built without security in mind and remain operational as legacy systems within an enterprise. Organizations must identify and reduce the hazard by protecting or patching these vulnerable systems, decommissioning them, or isolating them.

Social media attacks

Many people use social media accounts in which they accidentally expose a great deal of personal information. Attackers can use social media to launch assaults directly, such as disseminating malware through social media messaging, or indirectly such as analysing user and organisational vulnerabilities and designing an attack using information gathered from these sites.

Social engineering

Social engineering is the practise of sending emails and messages to people in order to persuade them to take actions that may jeopardise their security or reveal personal information. Curiosity, haste, and fear are psychological triggers used by attackers to manipulate users. People are more likely to comply with a social engineering message if the source looks to be trustworthy, such as by clicking a link that installs malware on their device or by providing personal information, passwords, or financial information. Organizations can minimize the risk of social engineering by educating users about the threats, risks and training them to recognise and avoid suspicious messages. Furthermore, technical methods can be utilised to prevent users from performing risky acts such as clicking on unknown links or downloading unexpected attachments, or to halt social engineering at its source.

Malware on endpoints

Malware, which can be communicated through variety of methods and can result in endpoint compromise as well as privilege escalation to other corporate systems, is a primary danger on all of these endpoints. Traditional antivirus software is insufficient to block all modern forms of malware, so newer techniques to endpoint security, such as Endpoint Detection and Response, are being developed (EDR).