Journal of Information Technology & Software Engineering

OPEN ACCESS Freely available online

Perspective

A Comprehensive Internet Measurement Technique Caused by Cyber Attacks

Christelle Noradin*

Department of Computer Science and Engineering, University of Warwick, Coventry, United Kingdom

DESCRIPTION

Over the years, the term cyber security has been so widely used that it has become almost synonymous with terms such as IT security and information security. A cyber security analyst protects the network of computers from cyber-attacks and unauthorized access. Cyber security can be divided into two parts such as cyber and security. Cyber refers to technology, including systems, networks, programs, and data. Security is about protecting systems, networks, applications, and information. It is also sometimes called electronic information security or information technology security. This is done by anticipating and defending against cyber threats and attempting to respond to security breaches when they occur. The main key role is to protect the company's valuable data. The day-to-day work of a cyber-security analyst varies from company to company. In today's digital world, cyber security has become an integral part of an organization's strategy for sustainability, security, and growth. As businesses grow, the demand for cybersecurity talent will also increase. Cybersecurity is a growing industry that requires skilled professionals. Some organizations acquire world-class technology to build their cyber defenses. Cyber security is the protection of computers, servers, mobile, devices, electronic systems, networks, and data from malicious attacks which is also known as IT security or electronic information security. Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.

This practice is used by individuals and businesses to protect against unauthorized access to data centers and other computerized systems. A strong cyber security strategy can provide a good security posture against malicious attacks aimed at accessing, modifying, deleting, destroying, or extorting an organization's or users' systems and sensitive data. Cyber security also helps prevent attacks aimed at disabling or disrupting the operation of systems and devices. The cyber security field can be categorized into several different areas. Coordination within an organization is critical to the success of a cyber-security program. The term applies in many different contexts, from business to mobile computing, and can be divided into several general categories.

Network security

It is the means by which computer networks are protected against intruders, whether they are targeted attackers or opportunistic malware. This includes hardware and software implementations to protect computer networks from unauthorized access, intrusion, attack, interference, and misuse. This security helps organizations protect their assets from external and internal threats.

Information security

It protects the integrity and confidentiality of data, both at rest and in transit.

Application security

It focuses on keeping software and devices threat-free. A compromised application may allow access to the data it was designed to protect. Successful security starts at the design stage, long before any program or device is deployed. This protection can be achieved by constantly updating the apps to protect against attacks. Successful security begins with the design phase, writing source code, verification, and threat modeling before any program or device is deployed. Address processes, monitoring, alerting and planning for how the organization will respond in the event of loss of operations or data due to malicious activity. The policy mandates that lost operations be resumed after a disaster at the same operational capacity as before the disaster.

Disaster recovery and business continuity

It defines how an organization responds to cyber security incidents and other events that cause loss of operations or data. A disaster recovery policy determines how an organization can restore its operations and information to the same operational capabilities as before the event. Business continuity is the plan that an organization resorts to when trying to operate without specific resources.

Correspondence to: Christelle Noradin, Department of Computer Science and Engineering, University of Warwick, Coventry, United Kingdom, E-mail: christellenordin@edu.uk

Received: 02-Jan-2023, Manuscript No. JITSE-23-21860; **Editor assigned:** 05-Jan-2023, PreQC No. JITSE-23-21860 (PQ); **Reviewed:** 19-Jan-2023, QC No. JITSE-23-21860; **Revised:** 26-Jan-2023, Manuscript No. JITSE-23-21860 (R); **Published:** 02-Feb-2023, DOI: 10.35248/2165-7866.23.13.312

Citation: Noradin C (2023) A Comprehensive Internet Measurement Technique Caused by Cyber Attacks. J Inform Tech Softw Eng. 13:312.

End-users

This training addresses the most unpredictable factors in cyber security. Viruses can inadvertently infiltrate secure systems if security best practices are not followed. Teaching users to remove suspicious e-mail attachments avoid plugging in unidentified USB drives, and a variety of other important lessons is essential to an organization's security. Address processes, monitoring, alerting and planning for how the organization will respond in the event of loss of operations or data due to malicious activity. The policy mandates that lost operations be resumed after a disaster at the same operational capacity as before the disaster.

Maintaining cyber security in an ever-evolving threat landscape is a challenge for all organizations. The most common attacks include botnets, drive-by download attacks, exploit kits, malvertising, vishing, credential stuffing attacks, cross-site scripting attacks, SQL injection attacks, Business Email Compromise (BEC), and zero-day exploits. Today, we live in a digital age where every aspect of our lives depends on networks, computers, other electronic devices, and software applications. All critical infrastructures such as banking systems, healthcare, financial institutions, governments, and manufacturing use internet-connected devices at the core of their operations. Some of the information, such as intellectual property, financial information, and personally identifiable information, is sensitive and may be vulnerable to unauthorized access or disclosure. This information allows intruders and threat actors to enter for financial gain, extortion, political or social motives, or simple vandalism.