Weakness of Internet Security

Posted on March 28, 2018

Internet users should identify weaknesses of Internet security in their information system security and outline areas where they are most prone to be hacked. Weaknesses of internet security can be classified as internal factors that affect the security of the internet. Mostly weakness of internet security originates from the violations of the security information system by employees. For the past twenty years, information system theft by employees has been evidenced in many companies and institutions others have been able to transfer faulty information protocols. This has been achieved since most employees are trusted and able to access most of the firm credentials logins whom whoever turns to be opposite. Furthermore, inadequate capital to fund internet security systems has become a significant weakness of internet security. For example, most corporations are unable to purchase privacy and security tools that offer maximum protection security while connected to the internet. Despite this, they usually opt to buy relatively cheap and mostly free security tools, i.e., antivirus software such as Kaspersky Internet Antivirus, which is expensive. Besides, with inadequate capital, corporations are unable to hire skilled technicians to monitor and ensure maximum security of the internet and properly fix any attack discovered. (National Institute of Standards and Technology [NIST], 2024)

Internet security opportunities

In accordance with ITWorld.com, opportunities can be described as few hanging fruits that cannot be afforded to take any advantage. Software developers have been releasing new internet security systems and tools on the market. For example, software developers have developed cloud computing. Through cloud computing, corporations and businesses can store data that can be accessed when it is required. This helps the business from the burden of having a server to store their data; hence information is stored and backed up in secure storage outside the company. Nevertheless, the saved capital can be used in facilitating other internet security measures.

Internet security threats

Threats can be described as external attacks on the company or business. Most are hackers' attacks and other malicious programs such as a virus, worms, and scams, among others. Therefore, this implies that companies, institutions, governments, and businesses that are highly targeted by hackers should always be prepared by having a well-established security system to counter these cyber-attacks from the access of vital confidential information. (NIST, 2024)

Evaluation of the current ethical and legal concerns surrounding Internet Security

Most of the ethical issues surrounding internet security involve privacy. For example, is it right to read private, confidential emails from other connected network users because you can access them? Is it worthy for any employer to obtain private information of an employee, such as private emails, as a way of ensuring no confidential information of the organization is disclosed as a means of security in the organization? Besides, is it ok for an employer to access private employee emails and read them as a way of monitoring that all rules and regulations of the organization are adhered to? Also, if the employers go through their employee emails is it necessary to disclose their employee information or not? These remain ethical issues between the employee and employers and the actions they will take either before or after an act.

Furthermore, is it secure for any online user connected to the internet to provide keyloggers on computers as a means of accessing and obtaining whatever the user types? Also, is it worth examining websites that your other network users have visited and monitoring their internet usage?

On another hand of legal concerns, an organization may have legal rules and regulations that allow employers to monitor and access private employee emails and also examining the visited websites by the employee. This will be a means of ensuring no organization information is leaked outside or disclosed.

Improvements in internet security over the last two years

Over the previous two years, there has been increasing in internet security; for example, the International Business Machines Corporation (IBM) has reported that they have improved internet security forces to the extent that hackers and cybercriminals have been forced to change their hacking tactics. Also, the report carried out in 2011 by IBM X force shows that there has been a 50% decline in the spread of email spam as compared to the previous years, 2010 and 2009. This has been enhanced through the development of sophisticated, high-quality software.

Suggestion for improvement of internet security based on the current internet security issues.

Governments, institutions, and companies should be able to create robust information security systems that should follow all procedures as outlined in the System Development Life Cycle without omitting or ignoring any steps. (Souppaya et al., 2022) The internet security system should be

ensured to be sufficiently comprehensive. Besides, verified data must be encrypted, for example, by sending information that is confidential through the internet, like credit card details, passwords, and usernames. Individuals prone to internet attack threats should ensure all computers' software and operating systems are up to date. This is because most of the updates released are primarily developed for handling security issues. (NIST, 2024)

Future prediction of Internet security

There have been many questions concerning the future predictions of internet security. For example, what may happen with increasing technology against increasing cybercrime activities? Hackers are growing at a rapid speed with high skills in accessing, manipulating, and corrupting data. Besides, technology is developing at a high rate hence increasing the number of users of the internet. This implies the number of DDOS attacks will increase in future days. Other predictions are organizations will be at high risk to attacks by hackers, and political campaign propaganda will spread through the technique of try and test. Also, there will be a high rate of ransomware models in businesses and organizations, together with the increase in scams. Furthermore, cybercriminals will use machine learning and artificial intelligence (AI) to carry out their hacking activities.

Conclusion

For successful internet security of any system, i.e., government, education, business, home, or networking, layers should be protected by developing a security layer for each layer. These security layers include operational security, physical security, network security, personal security, and communications security. Measures taken to develop the security system must ensure all critical areas are covered, for example, authenticity, integrity, utility, confidentiality, availability, and possession. Furthermore, all elements and components of data and information systems must be adequately protected from any attack. (NIST, 2020, 2024)

References

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure Software Development Framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities* (NIST Special Publication 800-218). National Institute of Standards and Technology.

https://doi.org/10.6028/NIST.SP.800-218