ISAUnited

International Security Architects

Security Architect Introduction

Security Architect Introduction

Introduction

A security architect plays a crucial role in society since he/she is responsible for designing and putting security systems in place. Due to the improvements in business technology, there is a great demand for architects globally. For the preservation of their sensitive data and information, most enterprises are attempting to adopt digital networking systems. Additionally, this article helps students or engineers have a better grasp of the duties and responsibilities of the IT professions and career options presented.

Security Architect

An individual who develops, constructs, tests, and deploys security technologies inside an organization's IT network is known as a security architect. A security architect must be well-versed in the intricate security network systems. The most recent security procedures, technologies, and standards are also kept up to date by security architects. Additionally, the individual is quite knowledgeable with security product best practices.

Duties and Responsibilities of Security Architect

An architect oversees creating the security networks of an organization that would prevent hacker entry into the organization's security systems. After the security networks are created, the security architect checks the network for any flaws and does an audit of the entire security system to ensure that it is operating effectively. For the aim of testing the security system, businesses typically employ an outside hacker and ask him to hack the system if he can, to inform the architect of whether the system is secure adequately or not (Costa, 2019).

To safeguard a system, a security architect must have a thorough awareness of both the users of the system and the weak spots inside it. The architect offers suggestions for various software and hardware after doing a complete inspection. These suggestions are made for upgrading and improving the security systems. Along with that, he establishes the user policies and regulations and keeps an eye on whether they are followed throughout the company. Additionally, these safeguards guard against outsiders and unapproved hackers accessing the organization's IT infrastructure (Matern, 2019).

Security architects' roles are less strategic and tactical than other positions. DevOps, integration, and automation performance metrics make up the bulk of their metrics. It is less important to rate the outcomes of security architecture based on technical actions like vulnerabilities discovered, incursions avoided, and violation avoidance. The organization's security and risk management are at a high level, according to security architects, but there are still hazards that are not yet known to them. The notion that one can defend oneself against recognized threats is shared by all security architects. Even Nevertheless, more than half acknowledge the difficulties in defending against unknown vulnerabilities (Jang-Jaccard & Nepal, 2014).

To maintain the security of the computer systems utilized by a company is the mission of a security architect. Being able to anticipate the actions and tactics that hackers would likely take to gain unauthorized access to a system requires a security architect to think like an attacker. An extra effort should be made by a security architect to ensure that they are current with both offensive and defensive developments. Most IT professionals think that experienced hackers make effective security architects because they are skilled at identifying the tactics used by attackers (rboucher, n.d.).

Protecting the perimeter of information centers is the primary goal of a security architect. Due to multi-cloud installations, the corporate perimeter has disappeared. A software-defined wide-area network and the internet of things are also examples. It is difficult to maintain constant awareness and unambiguous policy control over the enlarged assault area due to the network perimeter becoming marginalized. Because of this, an organization's risk profile, expenses, and inefficiencies have increased. To mitigate the dangers of a larger attack surface, several businesses have turned to protective complexity. Complex security has improved because of the increase in compliance requirements. For creating a customized compliance report for various receivers, network and security teams oversee keeping an audit trail. Boards of directors, CEOs, and others include regulatory agencies.

Education and Training Requirements

A bachelor's degree is generally preferred for positions as a security architect, while many employees hold master's degrees in the field. A security architect can increase their general knowledge and abilities by earning more cybersecurity certifications or by having an information technology (IT) background and experience.

Programming languages, database administration, statistical analysis, and storage systems and management are all essential skills for security architects.

Computer and network systems are related to additional hard skills for security architects. Specific technology and technical expertise differ depending on what a business performs.

Security software, cryptography, and protocol knowledge are all essential for security architects. In addition to knowing how to analyze security threats, test systems and networks, and look into and react to security incidents, security architects must also be able to design, implement, and manage security inside an organization.

Security auditing and compliance, identity and access management, and data protection are further areas of competence in security architecture (Sartore, 2022).

- Security engineers are familiar with data security techniques such as encryption, pseudonymization, and shuffling. They are aware of when to employ these techniques in order to prevent data loss, compromise, and corruption.
- To find security holes in current systems and networks, penetration testing entails mimicking a cyberattack. Different ethical hacking techniques, such as covert pen testing, internal pen tests, and open-box pen tests, may be necessary for security architects to practice.
- When conducting a security audit, a company's information system security is thoroughly evaluated in accordance with a predetermined set of standards. After security measures are put in place, security architects will continue to monitor compliance with this standard and assist in its development.

- The protection of both human and nonhuman identities is a component of identity security. Identity security may be monitored, evaluated, and improved throughout a computer network or system thanks to the expertise of security architects.

Opportunities of Employment

Designing and constructing security networks, a security architect must keep abreast of the most recent and current security advances. The security architects should be at ease collaborating with various members of the staff and serving as a mentor to staff members who are having problems using the security systems. Due to the advancement in technology currently, there are several possibilities accessible for security architects. Today, most businesses rely on automated computer network systems to carry out a variety of internal functions and store a variety of data. Consequently, corporations must employ security architects to create security networks on their behalf to keep that private information secure and only utilized by authorized individuals (Harrington, 2016).

Nearly every business need security architect, however the following list of examples illustrates some of the potential for professionals in this field:

1. Government agencies require security architects to protect their private data from hackers.
2. Government organizations (military intelligence agencies) require a high degree of security network to prevent the theft of information from other nations.
3. Numerous government agencies, like passport and ID card offices, require a high level of security since they handle sensitive personal data about citizens.

4. The creation of security networks for other private businesses like banks and insurance organizations may also be necessary.

REFERENCES

Costa, C., 2019. Data Science. OAE – Organizational Architect and Engineer Journal

Matern, S., 2019. e-Platform Architecture for Organisational Collaboration and IT Education. Information & Security: An International Journal, 43(2), pp.161-172.

Harrington, T. and Srai, J., 2016. Designing a 'concept of operations' architecture for next-generation multi-organisational service networks. AI & SOCIETY This study source was downloaded by 100000851108717 from CourseHero.com on 09-21-2022 11:03:15 GMT -05:00 Powered by TCPDF (www.tcpdf.org).

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. Sciencedirect. https://doi.org/10.1016/j.jcss.2014.02.005

rboucher. (n.d.). Azure Policy Regulatory Compliance controls for Azure Monitor - Azure Monitor. Learn.microsoft.com. Retrieved September 22, 2022, from https://learn.microsoft.com/en-us/azure/azure-monitor/security-controls-policy

Sartore, M. (2022a, March 2). What Is A Security Architect? | Skills And Career Paths. Www.cyberdegrees.org. https://www.cyberdegrees.org/jobs/security-architect/#:~:text=Security%20architect%20jobs%20require%20a