System Administrator Roles & Responsibilities

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

February 6, 2025

Assignment, Cyber Roles & Responsibilities:

Using NIST 800-12 , start at page 13 "Roles and Responsibilities". Choose one role within the Cybersecurity team to discuss. Address questions such as who they are, why are they part of the team, etc.

Chosen Cybersecurity Role: System Administrator

The System Administrator (SA) is responsible for setting up and maintaining a network or specific components of a network on a day-to-day basis. A SA can be a specific individual, a hierarchical group of individuals, or even whole department or separate organization. They may work 'behind-the-scenes' on special projects, or they may work on the 'frontlines' in a call center or in-person handling network and local workstation issues.

Who they are? What are some required credentials/experience?

They generally manage the configuration of servers, patches, system access control, monitoring, and applications using tools and technologies (Nieles, Dempsey, & Yan Pilli, 2017). The role of the SA requires a broad knowledge-based approach—a 'Jack-of-All-Trades' mentality—when handling organizational needs and troubleshooting issues. For example, most organizations use Python as their primary computer programming language for its readability and ease of use. Organizations will also commonly use Windows/Linux-based operating systems because of their flexibility, simplicity, and affordability. However, specialization will help meet requirements within unique areas of an organization. For example, many startups or small businesses use Apple products and the Mac operating system because of its streamlined and inclusive ecosystem and diverse content creation applications in web development and marketing. Lastly, they will usually need a combination of one or more of the following credentials to successfully address the needs of the organization, its employees, and its customers or end-users: Credentials include professional certifications, degrees from established institutions, and work-related experience and completed projects (Guides, 2024).

How do they ‘fit’ in an organization? What are some of their roles and responsibilities?

The first role and responsibility of SAs is to supervise and serve as an escalation point to provide technical support for the organization. SAs may aid end-users—including company customers and clients—with hardware, software, and networking-related issues. SAs may create, maintain, modify, and decommission user accounts, assisting HR with the onboarding and

offboarding process of employees. One of the most prevalent and time-consuming tasks is resetting user passwords.

Second, SAs design, test, and implement process and systems automation capabilities to improve overall operational effectiveness and performance—including cloud computing like software as a service (SaaS) (Statistics, 2024). They will perform routine security backups and recovery tasks before upgrading current systems or implementing new software applications and patches to the production line. Routine security backups and recovery tasks are crucial for availability, fault tolerance, and redundancy when various forces like DDoS attacks and natural disasters cause outages.

Third, SAs implement technical security controls. They implement regular firmware and software updates to protect the company against vulnerabilities and possible threats—both internal and external. They perform authorized, controlled, routine penetration tests to simulate real-life cyber-attacks. They will use various tools to scan for possible vulnerabilities that may harm the network and fall short of meeting compliance requirements. SAs will regularly check system logs, CPU usage, memory usage, and network performance to ensure optimal functioning. Software and hardware tools to help with security hardening include Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).

Fourth, SAs maintain internal documentation through Wikis. They maintain comprehensive documentation of system configurations, procedures, and changes. Reviewing documentation before system changes and updating documentation after system changes is imperative during change control or management requests. Lastly, most companies will use a global or universal 'golden' security standard, like the ISO (International Organization for

Standardization) or NIST (National Institute of Standards and Technology), as a baseline and reference for their security protocols and procedures.

Conclusion

The SA is a fluid role that can on many forms and different responsibilities depending on the size and the needs of the organization. A SA is responsible for installing, configuring, and maintaining various technical equipment, including server, software and virtual components (Statistics, 2024). SAs will troubleshoot hardware and software issues, running diagnostics, documenting problems, prioritizing resolutions, and risk assessment of current policies and procedures. SAs are the de facto technical support representatives to troubleshoot most network issues for internal company employees and external end-users like customers.

References

Guides, C. E. (2024, November 15). *Career Profiles*. Retrieved from Cybersecurity Education Guides: https://www.cybersecurityeducationguides.org/career-profiles/

Nieles, M., Dempsey, K., & Yan Pilli, V. (2017). An Introduction to Information Security. *Computer Security, NIST Special Publication 800-12 Revision 1*, 101.

Staff, C. (2024, October 24). *What Does a System Administrator Do? Your Career Guide*. Retrieved from Coursera: https://www.coursera.org/articles/what-is-a-system-administrator-a-career-guide

Statistics, U. B. (2024, August 24). *Network and Computer Systems Administrators*. (Office of Occupational Statistics and Employment Projections) Retrieved from Statistics, U.S. Bureau of Labor: https://www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm