Topic 3 Discussion 2

Examining the functionality of user and administrative privileges in an operating system or network. What effects can administrative access have on a vulnerability? Provide an example.

Hello Class,

Administrative access in an operating system or network plays a crucial role in determining the security posture of an organization. When users are granted administrative privileges, they gain the ability to perform actions that can significantly impact the system's security, stability, and usability. This elevated access can lead to various vulnerabilities, primarily because it allows users to bypass security controls, install unauthorized software, or alter system configurations. For instance, if a non-administrative user somehow gains access to an administrative panel, they could potentially delete user accounts or modify critical system settings, leading to a **vertical privilege escalation**. This type of vulnerability can expose sensitive data, disrupt services, and create entry points for malicious actors.

One notable example of the risks associated with administrative access is the **2017 Equifax data breach**, where attackers exploited a vulnerability in a web application framework. The breach was exacerbated by the fact that administrative access was not properly controlled, allowing attackers to access sensitive personal information of approximately **147 million** individuals. This incident highlights how improper management of administrative privileges can lead to severe security breaches and data loss.

In summary, while administrative access is essential for system management, it must be carefully controlled and monitored to mitigate the risks of vulnerabilities that can arise from its misuse. Organizations should implement strict policies regarding administrative privileges, ensuring that only authorized personnel have access and that their actions are logged and audited regularly.

References:

PortSwigger. (2023). *Access control vulnerabilities and privilege escalation | web security academy*. Portswigger.net. https://portswigger.net/web-security/access-control

SBS Cybersecurity. (2021, April 27). *The Danger of Local Administrative Privileges*. Sbscyber.com. https://sbscyber.com/blog/the-danger-of-local-administrative-privileges

Security, C. C. for C. (2020, July 29). *Managing and controlling administrative privileges (ITSAP.10.094)*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/managing-and-controlling-administrative-privileges-itsap10094