Topic 5 Discussion 2

Your company has recently identified a vulnerability outlined in the OWASP Top Ten. Refer to the website provided in the topic Resources. Choose one vulnerability and provide a brief summary of the issue. What mitigation steps could be utilized to offset the vulnerability from a server and network standpoint?

Hello Class,

Broken Access Control is one of the most critical vulnerabilities listed in the OWASP Top Ten. This vulnerability occurs when an application does not properly restrict user access to resources or functions, allowing unauthorized users to perform actions they should not be able to(OWASP, 2024). For instance, a user might gain access to another user's account or sensitive data simply by manipulating the URL or API requests. This can lead to significant data breaches and unauthorized actions within the application.

Mitigation Steps

To effectively mitigate the risks associated with Broken Access Control from both a server and network standpoint, organizations can implement the following strategies:

Implement Role-Based Access Control (RBAC) - Ensure that users are granted access based on their roles within the organization. This limits access to sensitive functions and data only to those who need it(Authgear, 2023).

Enforce Strong Authentication Mechanisms - Utilize multi-factor authentication (MFA) to add an additional layer of security, making it more difficult for unauthorized users to gain access.

Regularly Review Access Permissions - Conduct periodic audits of user permissions to ensure that access levels are appropriate and that no unnecessary privileges are granted.

Use Secure Coding Practices - Developers should follow secure coding guidelines to prevent access control vulnerabilities. This includes validating user input and ensuring that access checks are performed on the server side.

Implement Logging and Monitoring - Set up logging for access attempts and monitor these logs for unusual activity(Cloudflare, 2024). This can help detect and respond to potential breaches quickly.

Network Segmentation - Use network segmentation to isolate sensitive data and applications. This limits the potential impact of a breach by restricting access to critical systems(PortSwigger, 2023).

References:

Authgear. (2023, August 31). *What is Broken Access Control Vulnerability And How to Prevent it - Authgear*. Www.authgear.com. https://www.authgear.com/post/what-is-broken-access-control-vulnerability-and-how-to-prevent-it

CloudFlare. (2024). What is OWASP? What Are The OWASP Top 10? | Cloudflare. *Cloudflare*. https://www.cloudflare.com/learning/security/threats/owasp-top-10/

OWASP. (2024, September). *OWASP Top Ten*. Owasp.org; OWASP. https://owasp.org/www-project-top-ten/

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