Andree Salvo

Southern New Hampshire University

CYB 400 – 5-1 Project One Submission: Security Assessment Recommendations

Instructor: Robert Chubbuck

Security Recommendations

The vulnerabilities categorized for my scheduled maintenance can be resolved within a week, as they focus on patching, service configuration, and turning off insecure features. The Microsoft SQL Server end-of-life detection can be mitigated by upgrading to a supported version of SQL Server. If an immediate upgrade isn't possible, it's essential to update the servers with the latest patches. In essence, access should be limited using firewalls and permissions to help minimize exposure and risks. When it comes to the Microsoft SQL Server elevation of privilege vulnerability, it's essential to apply the vendor's patches and follow the principle of least privilege so that users have only the access they need to do their jobs.

The MS15-034 HTTP.sys remote code execution vulnerability poses a major threat, as it lets attackers execute arbitrary code on a computer system. It is crucial to resolve this issue because we can immediately apply Microsoft’s official patch. Disabling kernel caching in HTTP.sys can serve as a vital safeguard until the update is fully deployed. There is a concern that multiple SQL Server vulnerabilities (3065718) require urgent attention. Once we implement Microsoft’s security updates and monitor database logs for unauthorized access, these vulnerabilities can be effectively mitigated. Furthermore, the DEC/RPC and MSRPC services enumeration reporting issue requires decisive action. Restricting RPC traffic at the firewall, turning off unnecessary services, and enforcing authentication are essential steps to prevent unauthorized enumeration. Promptly addressing these vulnerabilities will not only fortify

BrainMeld's security posture but also ensure minimal disruption to its operations. Taking these actions is not just advisable but also essential for safeguarding the integrity and security of the system.

Policy Updates

The vulnerabilities categorized in my policy update can be resolved within a month, since they focus on strengthening internal security practices and enforcing consistent patch management. One concern from the scan was the use of default credentials for SMB services, such as "admin: guest" and "ftp: guest." These weak accounts can create an easy path for brute force attacks, and addressing this requires a policy change to eliminate or deactivate default accounts entirely. To protect access, stronger password policies should be highly enforced, requiring users to create more unique and complex passwords that meet specific criteria. Account lockout settings can also help prevent repeated login attempts. Enabling multi-factor authentication (MFA) adds another layer of protection.

A significant part of the policy update involves ensuring that patches are being applied consistently. The scan showed that the MS15-034 HTTP.sys issue and the SQL Server vulnerabilities are both still unpatched, which points to gaps in the update process. To address this issue, the company requires a more robust patch policy that can be set to vendor schedules and conducts regular audits to ensure everything's up to date. This way, BrainMeld can stop the same problems from coming back and keep its security posture solid and secure.

Other Security Issues

The vulnerabilities in this category aren't easy to fix and need to be addressed, but they can't be ignored. One issue the scan flagged was the use of weak SSL/TLS cipher suites. If these

stay in place, attackers could take advantage of any outdated encryption to break into sensitive communications. Updating the servers to use TLS 1.2 or 1.3 or higher will make sure BrainMeld's data stays safe during any transmission and give the company a much stronger layer form of protection.

Another security issue is the Microsoft ASP.NET information disclosure vulnerability. This can be dangerous because it may leak system details or error messages that attackers could use to plan more sophisticated attacks. To resolve this, Microsoft's patches should be applied, and the ASP.NET settings should be tightened to make sure errors don't give away unnecessary details. Limiting that information keeps outsiders from gathering clues about the system, which helps cut off potential attack paths before they can be exploited.

Implementation

The first vulnerabilities I would address are the MS15-034 HTTP.sys remote code execution issue and the Microsoft SQL Server vulnerabilities, as they pose the highest risk and have available patches that can be applied quickly. Fixing this right away cuts off any major attack paths and provides the biggest improvement in the shortest time. Once that's done, the focus should shift to only updating account and patch management policies to prevent recurring issues, and then to longer-term fixes, such as improving encryption and addressing information disclosure.