ANSWERS ETC. //Technical Bulletin

Securing Your Web Server In 10 Steps

Step 1 - Keep the server software up to date: Regularly update the web server using Windows updates. Windows updates are released on the second Tuesday of the month and should be installed as soon as possible to help protect your web server.

Step 2 - Use strong and unique passwords: Set strong, complex passwords for all user accounts, including the administrator account. Avoid using easily guessable passwords. Consider using a password manager to generate and store long, complex passwords securely.

Step 3 - Limit access to the server: Limit who has access to your server and cut off access once those who need access no longer need it.

Step 4 - Configure a web application firewall (WAF): A WAF, if available, helps protect your web server from common web application attacks, such as cross-site scripting (XSS) and SQL injection. Configure the WAF to filter and block malicious traffic.

Step 5 - Stay on top of Antivirus definitions: Ensure that your server's antivirus is running and updated.

Step 6 - Limit server exposure: Minimize the attack surface by disabling unnecessary services such as RDP and file and printer sharing. Only enable your specific application's features, protocols, and ports. In the case of an IIS server for Tier 3, it's recommended to only run IIS with the ports needed (443) and not run other software, such as security camera software or allow the server to be used as a workstation for regular use.

Step 7 - Regularly backup data: Implement a regular backup strategy to ensure you can recover your web server in case of data loss or compromise. Store backups securely offsite and ensure backups can't be deleted from within the local server to help protect against ransomware.

Step 8 - Monitor server logs: Enable logging for your web server and regularly review log files for suspicious activity. Implement a centralized log management system for efficient monitoring and analysis. You will get more usage from this by implementing it across all your servers, not just your web servers.

Step 9 - Implement intrusion detection and prevention systems (IDS/IPS): IDS/IPS solutions can help detect and prevent malicious activity by monitoring network traffic and comparing it against known attack patterns. Configure these systems to provide alerts or block suspicious activity.

Step 10 - Conduct security audits and penetration testing: Regularly assess your web server's security through audits and penetration testing. Identify vulnerabilities and address them promptly. Consider involving third-party security experts for more comprehensive assessments.

About Us

Our friendly staff is here to assist you with all your technical needs. We have team members who are specialists in technical support, database administration, network administration, and more.

Contact info

Address:

8713 Airport Freeway, Suite 200
North Richland Hills, TX, 76180

E-mail/Web:

techsupport@answersetc.com
www.answersetc.com

Phone:

800-275-1418
817-595-8899

Scan the QR code
to visit us online