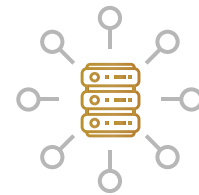


20 Strategies to Elevate Your Cybersecurity Digital Defense Posture



Twenty Cybersecurity Strategies

1. **Review User Accounts:** Regularly audit domain controllers, servers, workstations, and active directories for new employees, ex-employees, and unrecognized user accounts to detect any unauthorized access early.
2. **Perform Data Backups:** Routinely perform data backups and keep them air-gapped (isolated from the network) and password-protected. Safeguard these backups in offline storage to prevent unauthorized alterations or deletions from the primary data system.
3. **Schedule Task Reviews:** Conduct routine inspections of the Task Scheduler and any scheduled tasks set by the operating system. Manually inspect each task to verify its legitimacy and scrutinize the details for any signs of malicious activity.
4. **Review the Antivirus Log:** Actively monitor your antivirus logs to quickly spot any unexpected deactivation, which may indicate a security breach or intrusion attempt.
5. **Implement Network Segmentation:** Establish barriers within the network infrastructure to limit the spread of ransomware should a network infiltration occur.
6. **Enforce Software Installation Controls:** Require administrator credentials to install software to prevent unauthorized installations.
7. **Implement a Recovery Plan:** Develop comprehensive recovery protocols for duplicating and safeguarding sensitive data and infrastructure in a secure, segregated environment to ensure business continuity and mitigate data loss risks.
8. **Prioritize Critical Patching:** Identify and apply patches for critical vulnerabilities in operating systems, software, and firmware as soon as possible. Utilize vulnerability scanning tools and threat intelligence feeds to stay informed. Implement automated updates for non-critical systems.
9. **Implement Multifactor Authentication (MFA):** Deploy multifactor authentication across all systems to bolster security measures and protect against unauthorized access.
10. **Strengthen Password Protocols:** Regularly change network system and account passwords, avoid reusing passwords for different accounts, and implement the shortest acceptable timeframe for password changes.



66%
of organizations
reported being affected
by ransomware in 2023



Ransomware payments
averaged over
\$1.5 million
in 2023, a 29,900%
increase from 2018

20 Strategies to Elevate Your Cybersecurity Digital Defense Posture

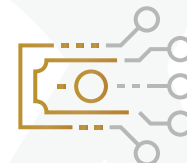


11. **Tighten Remote Access Controls:** Disable unused remote access/Remote Desktop Protocol (RDP) ports, monitor remote access/RDP logs, and audit user accounts with administrative privileges.
12. **Enforce Least Privilege Principles:** Configure access controls to adhere to the least privilege necessary to reduce the risk and impact of unauthorized access or breaches, with the goal of Zero Trust architecture.
13. **Implement Anti-Malware Measures:** Install and regularly update antivirus and anti-malware software on all hosts.
14. **Optimize Network Security:** Prioritize secure networks and, when using public Wi-Fi, consider employing a VPN. Additionally, use strong passwords and avoid engaging in sensitive activities on public networks for enhanced protection.
15. **Bolster Email Security Measures:** Add an email banner to emails received from outside your organization to alert users of potential security risks and disable hyperlinks in incoming emails to reduce the risk of phishing attacks.
16. **Educate Employees:** Regularly conduct security awareness training for employees that includes simulated phishing attacks and other critical security topics to help them recognize and respond to phishing attempts and suspicious activities.
17. **Create an Incident Response Plan:** Develop and regularly update an incident response strategy to quickly and effectively address any ransomware attacks.
18. **Complete Regular Security Audits and Penetration Testing:** Initiate periodic security audits to pinpoint and rectify vulnerabilities and conduct regular penetration testing to uncover hidden vulnerabilities and weaknesses in your digital defenses.
19. **Use Advanced Threat Protection Tools:** Implement advanced threat protection tools to detect and prevent ransomware and other malware.
20. **Conduct Legal and Compliance Reviews:** Regularly assess and ensure that you comply with legal and industry-specific security standards and regulations.

For more information about how we can help you strengthen your digital defense, [contact us here](#).



Over 37%
of ransomware attacks in 2023 originated from compromised third-party suppliers



The average cost of a ransomware attack in 2023, excluding the ransom itself, escalated to **\$5.13 million**