Defense in Depth Checklist Controls

50 Easy-to-Implement Controls to Strengthen Your Security

SBS institute

SBS CyberSecurity

www.sbscyber.com

Written by: SBS CyberSecurity Network Security Team

Your Goal: Make Pivoting More Difficult

SBS CyberSecurity's Network Security department performs hundreds of penetration tests and social engineering assessments each year. SBS has had the pleasure of working with organizations of all sizes across a wide range of industries. Most organizations, especially ones that have not been rigorously tested, may have a secure network perimeter, but their people and internal security posture are often very lax. Typically, once we have even a small foothold into that type of organization, it is a fairly effortless process to pivot across the network until some level of administrative access is obtained (usually Domain Administrator credentials). The good news is that there are many easy-to-implement controls that make this type of activity more difficult.

This checklist is not comprehensive, and some controls may not be applicable for all environments. However, any of these controls that you implement will provide you with a greater level of security and make our Penetration Testers and actual attacker's lives more difficult.

Included in this checklist is information on:

- External Network Perimter
- Social Engineering
- Email/Spam Filtering
- Internal Network Security
- Wireless Security

External Network Perimter

☐ Reduce your attack surface as much as possible. If a service does not need to be Internet-accessible, restrict it to your internal network or a trusted set of external IP addresses.

☐ Perform GEO-IP blocking. Is there any legitimate reason to allow countries who are known to proliferate cyber-attacks, to even have the ability to see and interact with your network?

☐ Ensure sufficient logging and alerting is set up for your firewall, IDS/IPS, and any internet-accessible services. Not only should you ensure that you save the logs for historical purposes, but you should also be reviewing them for anomalous activities or signs of cyber-attacks

✓ For a primer on the logs that need to be enabled in the event your network incurs an incident or a breach, check out SBS' 50+ Incident Response Checklist Items here: https://sbscyber.com/resources/article-50-incident-response-preparedness-checklist-items

☐ Require multi-factor authentication (MFA) on any externally accessible services that require user authentication. MFA will prevent password reuse from phishing attacks and brute force password attacks or password spraying attacks.

☐ Ensure that any externally accessible service is communicating over encrypted channels using strong encryption.

Social Engineering

☐ Train your users to understand that a telephone number can easily be spoofed and should not be used as a means of authentication.

✓ A great (free) website for caller ID spoofing can be found here: https://www.spooftel.com/freecall/

☐ Inform your users on email security and how to spot common phishing techniques.

☐ Work orders and badges are easy to fabricate. Train your users to be wary of anyone entering the organization. Have your users validate with management before allowing anyone access to any sensitive areas of your organization or access to your network.

☐ Social engineering scams can be tricky, create an environment where your users feel comfortable in disclosing if they fell for a phishing email or other social engineering attack.

Email/Spam Filtering

☐ Deploy sender policy framework (SPF) and Domain Keys Identified Mail (DKIM) to help validate your emails and prevent others from spoofing your domain.

✓ Here's a blog post from regarding the differences between SPF, DKIM, DMARC, and how to enable those protocols around your email: https://blogs.technet.microsoft.com/fasttracktips/2016/07/16/spf-dkim-dmarc-and-exchange-online/

☐ If you have SPF and DKIM set up, DMARC (Domain-based Message Authentication, Reporting, and Conformance) can provide additional protection against email address spoofing and phishing. DMARC is used to identify emails with forged (spoofed) sender addresses that appear to originate from legitimate sources.

✓ Check out this article on how to validate email with DMARC in Office 365:
https://technet.microsoft.com/en-us/library/mt734386(v=exchg.150).aspx

☐ Set up stringent restrictions on what file types are allowed through your spam filter.

✓ Symantec has a good checklist of file extensions and types that are common email attack vectors: https://support.symantec.com/en_US/article.INFO3768.html

☐ Ensure that you can quickly block a sender address if malicious content or phishing emails are identified.

☐ Implement a disclaimer banner around any external email messages to provide users clues to help identify phishing emails. Disclaimers may help users identify phishing emails appearing to be coming from an internal user, but in reality, the email has been by an external address.

✓ Example of a warning banner may be something like: "WARNING: This email originated from outside our organization. Do not click links or open attachments unless you expected the email or have verified its authenticity."

✓ Learn how to set up organization-wide message disclaimers, signatures, footers, or headers in Office 365: https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/disclaimers-signatures-footers-or-headers

☐ Ensure that your spam filtering blocks emails from outside your organization that uses your legitimate email domain as the sender address.

☐ Consider blocking incoming emails from sender domains that are common in appearance to your legitimate email domain name.

☐ Ensure sufficient logging is set up for your email server and spam filter. This would be useful in the event of a digital forensic investigation (See SBS' 50+ Incident Response Checklist).

Internal Network Security

- ☐ Do not let your users have local administrator rights.

- ☐ If local administrator accounts are a necessity, utilize the Microsoft Local Administrator Password Solution (LAPS).

    - ✓ Check out this article on LAPS: https://technet.microsoft.com/en-us/mt227395.aspx

- ☐ Ensure that your users are assigned only the permissions that they need to perform their job. There are very few tasks that require domain administrative or higher privileges. Consider implementing Just Enough Administration (JEA) for more granular user access controls.

- ☐ Ensure that no one is using an administrative account as their daily use account. Browsing the internet and checking emails logged in as a domain administrator is a disaster waiting to happen.

- ☐ Log and review or have automated alerts set up for failed logins or account lockouts. This will help you identify password attacks or malware infections.

- ☐ Utilize antivirus / antimalware software on all workstations and servers. Use a product that it is centrally managed and capable of providing alerts and saving logs for historical purposes.

- ☐ Require your users to have long, complex passwords. While eight characters may still be considered the bare minimum, fourteen-character passwords are tremendously more difficult to crack. The use of passphrases should be encouraged.

    - ✓ Alternatively, consider utilizing an enterprise password management solution. There is some added risk in centralizing passwords, whether internally or in the cloud (do your research on the solution's security controls; they're typically excellent), the benefits far outweigh the risks. Password managers give your organization the ability to enforce extremely long and complex passwords that are unique to EVERY account, the applications typically work across multiple platforms and devices, and the best part is that no one has to remember ANY of their passwords (except the one to log into the password manager).

    - ✓ CSO Online has a nice review of the Top 6 password managers (but be sure to investigate enterprise options for rolling out to your organization): https://www.csoonline.com/article/3198507/security/the-6-best-password-managers.html

- ☐ Use system deployment and hardening standards that disable any unnecessary services, protocols, and change all default credentials. Protocols such as LLMNR and NBT-NS are enabled by default and are easily abused.

- ☐ Use login restriction times appropriate to your organization and users.

    - ✓ Example: Users cannot log into the corporate network (or specific application) from 11:00 PM to 6:00 AM.

Internal Network Security, continued

☐ Segregate your network infrastructure based on risk. High-risk targets such as HR and sales should not have access to your organization's crown jewels.

☐ Enable SMB signing to prevent SMB relaying attacks.

✓ Check out this helpful article on SMB Signing: http://techgenix.com/windows-smb-signing/

☐ Ensure that operating systems and third-party products are patched timely and consistently.

☐ Disable PowerShell if it is not needed in your environment. If it is a necessity, ensure that you are running the latest version with extended PowerShell logging enabled.

☐ Restrict access to USB devices.

☐ Perform periodic user reviews of all user accounts.

☐ Perform periodic internal network scanning to identify any changes in the network.

☐ Enable account lockout features to lock accounts after a set number of failed login attempts.

☐ Do not share passwords among multiple accounts.

☐ Do not use Group Policy Preferences (GPP) to assign local user passwords.

☐ Perform periodic internal vulnerability assessments or penetration testing.

☐ Do not store credentials or sensitive information in clear text on the network.

☐ Ensure that content filtering and appropriate egress filtering is enabled. Review the logs for signs of malicious behavior.

☐ If possible, utilize application whitelisting.

☐ Utilize full disk encryption on workstations and laptops.

✓ How to deploy BitLocker FDE encryption via Group Policy (Windows 10): https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-basic-deployment

☐ Enable local system firewalls on workstations and servers even while connected to your internal network. Rarely do endpoints need to communicate with each other.

☐ Perform centralized logging and alerting of security events on end-point devices. Use a SIEM if possible.

☐ Consider blocking office macros via Group Policy Objects (GPOs).

☐ Enable file and directory logging for sensitive directories and files. This information can be invaluable in determining what information was accessed after a breach.

Wireless Security

☐ Hiding the name (SSID) of your wireless network does not provide any protection. It is easily discoverable by attackers.

☐ WPA/WPA2 personal authentication handshakes can easily be captured and potentially cracked to retrieve the network key. If WPA/WPA2 personal authentication is used, a strong (20+) character network key should be used.

☐ WPA/WPA2 Enterprise encryption should not rely solely on a username and password for authentication. It is trivial to setup a rogue access point and trick end users into providing their credentials. Certificates or some other form of multifactor authentication should be deployed.

☐ On guest networks, ensure that client isolation is turned on to prevent wireless clients from interacting with one another.

☐ For the best security, segregate the wireless network from any other internal or corporate network(s)

Defense in Depth Bottom Line

If you truly want to mitigate risk for your company and its confidential information, think like an attacker. Over 90% of all data breaches are the result of an internal employee clicking on a link or downloading an attachment from a phishing email. Assume the bad guys are going to get in. If they do, will you be able to tell? How would you know?

If you assume that someone is able to compromise your network, you will begin to pay more attention to the security of your internal network (where the bulk of these controls lie). If an attacker can get into your network, the average time-to-detection sits at right around 200 days. That’s a long time for anyone to work their way around your network, escalate their privileges, find your confidential information, and ship it out the back door.

Don’t be the low-hanging fruit. Think like a hacker. Mature the security of your internal and external networks, even if that involves implementing one of these controls. That’s one step closer to keeping the bad guys at bay.

ADDITIONAL FREE RESOURCES

available at www.sbscyber.com.

MONTHLY HACKER HOUR

Join our interactive webinar series focused on discussing cybersecurity issues and trends.

PRODUCT DEMOS

Discover the power of our offerings with live demos scheduled each week highlighting individual products or services.

SECURITY AWARENESS TRAINING

Share our cybersecurity training tools with both your employees and your customers.

CYBER-RISK™

Go beyond the spreadsheet with an automated FFIEC cybersecurity assessment.

TRAC™ ACTION TRACKING

Remain diligent with your remediation tracking and follow up by creating security plans associated with your risk assessment.

JOIN OUR MAILING LIST

Stay current with the latest trends in cybersecurity, information technology, and upcoming educational events from SBS CyberSecurity. Join our email list and be in the know!

ABOUT US

YOUR CYBERSECURITY PARTNER

SBS CyberSecurity, LLC (SBS) is a premier cybersecurity consulting and audit firm. Since 2004, SBS has been dedicated to assisting organizations with the implementation of valuable risk management programs and to mitigating cybersecurity risks. The company has provided cybersecurity solutions to organizations across the United States and abroad. SBS delivers unique, turnkey solutions tailored to each client's needs, including risk management solutions, auditing, and education. SBS CyberSecurity empowers customers to make more informed security decisions and trust the safety of their data.

FOR MORE INFORMATION PLEASE VISIT WWW.SBSCYBER.COM OR CALL 605-923-8722.