THE ASD ESSENTIAL EIGHT – PROACTIVE MEASURES TO BOLSTER YOUR CYBERSECURITY POSITION

By: Dick Bussiere

There is a recent trend towards focusing more energy on proactive security measures that can help to reduce your cyber exposure. Applying proactive measures can stop many attacks cold since the attack vector has been completely removed. Fixing issues after a breach is far more costly than proactively preventing the breach in the first place. To help organizations proactively reduce their cyber exposure, the Australian Signals Directorate (ASD) has published a cybersecurity baseline known as the “The Strategies to Mitigate Cyber Security Incidents,” a prioritized list of initiatives to enhance computer security. The Essential Eight are the most fundamental elements of this list, having the most impact for the required investment. The Essential Eight engenders good security habits, and helps all organisations better protect themselves from myriad attack vectors. The guidelines presented here are best used as a baseline, and then adapted to the specific needs of the organization.

Tenable’s cyber exposure measurement technologies can help you to follow the Essential Eight Guidelines. Some of the guidelines lean towards technical implementation, while others are oriented toward organizational practice. We recommend that you read and understand the information provided by ASD before you dive into how Tenable™ can help with implementation.

We now outline the specific components of the ASD Essential Eight that can be implemented using Tenable’s technology.

1. **Application Whitelisting** — Whitelisting applications allows only trusted applications to run on your network, thus preventing malware and untrusted software from causing harm to systems in your environment. Tenable helps by providing a list of applications detected on systems in your environment. Applications outside the scope of your whitelist can then be easily identified and disabled.

2. **Patch Applications** — Patching known security vulnerabilities in a timely manner is one of the most simple and effective activities an organization can take to ensure the security of their network and environment. In addition to operating systems, fully patched applications are essential to providing a foundation on which other security controls can be overlaid. Tenable helps administrators prioritize the patching of applications by providing dashboards that readily identify the systems at the greatest risk.
3. Disable Untrusted Microsoft Office Macros — Automating routine tasks with Microsoft Office macros is convenient; however, macros can contain malware or malicious commands and often result in unauthorized access to sensitive information or the manipulation of critical data. The use of macros should be restricted to signed and trusted macros. Macros should also be routinely audited to determine if the macro is still needed.

4. User Application Hardening — In environments where web browsing is allowed, common attack vectors include malicious webpages, advertisements and emails with infected attachments. Hardening user applications, such as web browsers, can help reduce the risk associated with these vectors. The ASD recommends that administrators block web browser access to Adobe Flash and untrusted Oracle Java applications, disable unneeded features and plugins and implement a web advertisement blocking solution. Tenable’s solutions provide a summary of web browsers detected on the network along with a summary of risky components such as Flash and Java. Additionally, vulnerable versions of such components will be identified for remediation.

5. Restrict administrative privileges — Due to staff turnover, overlooked default accounts, or ease-of-use, there may be administrator accounts that provide far too much privilege which can be used to make significant changes or to bypass critical security settings. Administrator privileges should be restricted to only those users that need privileges, and administrator accounts should only be used for managing systems, installing legitimate software and applying security patches. Administrator accounts, rights and privileges should be regularly audited, and controls should be put in place to address organizational changes, like staff transfers. Tenable’s solutions can assist with identifying accounts that match different group membership settings, such as Windows Domain administrators or LDAP group administrators.

6. Patch operating systems — Operating system vendors are continually issuing patches to remedy security vulnerabilities. Applying patches in a timely manner is critical to ensuring the security of a system and the security of data that reside on the system. Tenable.sc provides metrics, including a risk reduction percentage and number of affected hosts, to help administrators prioritize patches of operating systems.

7. Multi-factor authentication — Strong access controls, like multi-factor authentication, can prevent an attacker from compromising a system or resource even if the attacker possesses a user password. With multi-factor authentication, a user must present multiple, separate pieces of evidence in order to verify his identity. Evidence typically includes something you know, like a password or PIN; something you have, like a physical token or smart card; or something you are, like biometric data.

8. Daily backup of important data — The daily backup of important data has never been more critical as attackers develop increasingly sophisticated ransomware tools like Petya and WannaCry. Daily backups of important data and the secure storage of that data offline ensure that your organisation can recover data in the event of a cybersecurity incident.

THE ESSENTIAL EIGHT PHILOSOPHY

The Essential Eight is not a checklist to be followed, but instead a security philosophy that should be implemented and maintained to create a more secure IT environment. Following each of these steps is a good starting point to creating a stronger and more secure environment for your organization. Tenable.sc assists administrators in not only practicing good vulnerability management described in the Essential Eight, but also helps organisations manage, measure and reduce their modern attack surface.

ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 27,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world’s first continuous view and log correlation engine. Tenable.sc assists administrators to understand and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 25 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.