Cybersecurity Maturity is Powerful: A Strategic Start

There are few professionals that will deter an organization from taking proactive steps to enhance their cybersecurity maturities. In this article I would like to present my three favorite ways to enhance security: asset management, permit-by-exception, and active and archived log auditing. With asset management we will discuss acquisitions, live device management, and on reasonable sun-setting process. For the purposes of this publication we will limit permit-by-exception to network devices and application whitelisting. As we wrap-up our discussion with active log auditing we will discuss SIEMs and SOARs, log retention types and periods, as well as archived log auditing. Let's begin our discussion of asset management.

Assets come and assets go (sometimes without permission) and on occasion there are even unauthorized assets so it is imperative you know what you own, where it is, and when it should be sunset or refreshed. An asset can be any hardware, software, or firmware that is integrated into the enterprise environment. The first stage of any asset is acquisition. Once an asset has been acquired it should be inventoried. BYOD devices are employee or stakeholder owned assets but should still follow an inventorying process which is usually synonymous with the enterprise authorization process. For non-BYOD devices enterprises should create three disparate types of inventories: Physical assets, digital assets, and licenses. Physical assets should be tagged with detailed identification information indexed in the asset management database. The indexed information should consist of, at a minimum, MAC address if applicable, serial number, manufacturer, model, date acquired, date of sunset, and location (or employee) to which it has been issued. The digital asset inventory should include vendor, software version, date of acquisition, date of sunset, and issuing information. Licensing inventories should include acquisition dates, renewal dates, total licenses purchased, number of licenses used, where the licenses are in use, and personnel whom are authorized to use the licenses if applicable. With these three databases created and updated to reflect changes in issuance or acquisitions finding rogue devices and software should be significantly easier to identify. Any asset that is identified on the network that does not correspond to a device in the corresponding database should trigger an alert to a security professional whom can identify the reason. Identification an be performed using a scanner that drops the output to a file with an automated script that compares the scan results to the databases or a security device that checks network traffic against the inventory databases. This technique can also alert on devices that are passed their sunset dates (date of planned decommission). Sunset dates should hard dates that have corresponding strategic plans and budgetary line items. Hardware assets that are sunset should follow secure sanitization or destruction processes and if outsourced should be supported by strongly worded and ensured SLAs. Sunset software and licenses should be enforced by restricting use of those products by removing them from the permit-by-exception host and network security rules.

Permit by exception rules can seem like a never ending road that lasts into an asset's sunset period; however, if network based and host based rules are used in a unified way the rules can be created in a way that is less burdensome. At the network level, it is ideal to use internal PKI certificate based network access control technologies to control which physical devices are permitted to attach to the network. Certificates can be issued to BYOD devices as part of the authorization process. For devices that do not support NAC technologies a separate plane or vlan can be created with specific rules that restrict the exact port/service combination that is required while rejecting all other ports and services. For network control of software assets it is prudent to implement software proxies with TLS stripping capabilities enabled for any connection that has a very low likelihood of containing personal pii. For network connections the age-old adage of configuring firewalls to only permit connections based on port/service combinations that directly map to a business process still holds true. P2P traffic is still a highly suspect candidate for examination to determine presence of zombie ware. DNS should have spf, dkim, and dmarc configured with enforcement actions. Host based solutions can be used to round out the software and firmware permit only those applications, operating systems, and drivers that have successfully passed a security review and acceptance process. If any software does happen to be present in the environment after a security acceptance has been revoked it should be easily spotted in log auditing processes.

As logs are created they should actively be monitored for indicators of active threats and attacks for a predetermined time, then the logs should be retained for a in an archive for a defined period, during the archival stage the logs should periodically be scanned for indicators of previous compromise. The key to active log monitoring is to determine which logs are the most relevant and insightful without collecting all logs from every source because all logs are not created equal. While there are a substantial number of resources that detail which logs are best to review for each piece of technology it is essential to understand there should be an enterprise review to determine if any enterprise specific need require additional logging. Essential active logs should always be sent to a secondary on-network device and, if applicable, replicated to a remote off-network location. These logs should be automatically audited using security devices such as SOARs and SIEMs. These tools can be used to identify threats and attacks that correspond to an externally created rule or signature, anomalous activity, as well as internally developed indicators. When a threat or attack is identified these devices (most of them) can take automated remediation action if configured accordingly. Active log auditing is a powerful near-real time and recent history tool but are not designed for review of long-term archived logs. The typical deviation between what constitutes recent history logging and archived logs is typically ninety days. After logs have been within the auditing database for ninety days they are typically transitioned to the archival database for compression, encryption, and long-term storage. Long-term storage is often defined as twelve months from the date of the origination of the original log creation date. This can be subject to regulatory requirements that require longer retention periods. My personal preference is a fifteen month retention period which is twelve months after the archival date but archival log retention periods must be defined by organizational policy. After logs have been archived there will be periodic need to retrieve the archives with the goal of scanning them for indicators of past compromise. For the purpose of this article indicators of past compromise are defined as newly publicized indicators of compromise that detail the TTPs of threat actors that have been

caught in the wild. When archived logs are are scanned for past indicators of compromise the goals is due diligence in determining if the organization was compromised through a security gap that was not previously identified and remediated. After the archived logs are scanned for past indicators of compromise they are returned to the archival database or securely deleted depending on the methods used to scan them. If they are returned, it is essential that the archived logs be hashed prior to being accessed, prior to scanning, after scanning, and after being returned to the archive. Active log auditing and archived log auditing are essential steps in maturing every security program and one of my personal favorite three security maturity steps.

Security maturity is a slow but powerful vehicle on a road worth traveling. My favorite three sites on the maturity road map that help drive success are asset management, permit-by-exception, and active and archived log auditing. Asset management will help ensure only authorized components are integrated into the enterprise network while permitting easier identification of rogue devices. Permit-by-exception severely reduces the ability of malware and shadow-IT from infesting the network with unauthorized risks and vulnerabilities. Active and archived log auditing permits organizations to identify any ongoing or past threats or indicators of compromise to ensure any security gaps that are being leveraged or that have been leveraged are identified and remediated.

Thank you for reading

-Andrew Kosakowski

www.Anthko.com