GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Ford, Kevin

Title: "SMB Cybersecurity Series: Asset Inventory is the Foundation of Cybersecurity"

Website: cybergrx.com

Organization: cyber GRX

Date: 08 November 2018

URL: https://www.cybergrx.com/resources/blog/smb-cybersecurity-series-asset-inventory-is-the-foundation-of-cybersecurity/

Accessed: 12 July 2019

Synopsis: In my last SMB post, I examined the importance of managing cyber and privacy risk by performing a few basic activities that greatly increase your security posture. Most security professionals refer to these activities as "cyber hygiene." Now, we're taking a deeper dive into creating your asset inventory and identifying assets for cyber protection. An asset inventory is a logical first step for any organization starting to manage their cyber and privacy risks, and serves as the foundation for most of the other activities on my cyber hygiene list.

What Should Be On Our Inventory?

SMB Series: Asset Inventory is the Foundation of Cybersecurity

Posted on November 8, 2018 in News & Blog

In my last SMB post, I examined the importance of managing cyber and privacy risk by performing a few basic activities that greatly increase your security posture. Most security professionals refer to these activities as "cyber hygiene." Now, we're taking a deeper dive into creating your asset inventory and identifying assets for cyber protection. An asset inventory is a logical first step for any organization starting to manage their cyber and privacy risks, and serves as the foundation for most of the other activities on my cyber hygiene list.

What Should Be On Our Inventory?

You should track all technology (i.e. computers, printers, network devices), software, and data in your inventory of assets. Consider developing a system of unique ID's for each item in the inventory, so you won't get confused by overlapping technologies, or by large buys of technologies such as workstations. You may also consider creating asset tags with which to label physical devices.

What Should We Track?

Once you know what you have, you should identify and track certain key pieces of information associated with the assets in your inventory. I suggest tracking at least the following data:

- Any unique information to identify the asset (i.e. machine name, serial number, and/or MAC address),
- Network address (IP address, or address ranges),
- Who owns the asset,
- The geographic location of the asset,

- The criticality of the asset to your business (e.g. low, moderate, or high),
- The business function the asset supports,
- Any applicable OS versions,
- Any applicable software version,
- The status of any applicable software licensing (i.e. when is the next renewal),
- The amount and capacity of the software being licensed (i.e. how many seats do you have left?), and
- The status of operation (planned, maintenance, deactivated, destroyed are all informative statuses).

Having this information at your fingertips will give you a wealth of information to make important security and privacy decisions.

How Do We Use The Inventory?

With this information at hand, you can start to make key decisions about your risk posture as well as ensure that all assets are covered by security considerations. Understanding your environment enables you to make better decisions about security and privacy tools. For instance, if you know you have windows workstations and also a significant amount of Mac laptops in your environment, and you are looking at deploying AI based antimalware, it may be useful to see if that antimalware offers AI capabilities for both Windows and MacOS, as many will only use signature-based capabilities for MacOS.

Your inventory should also help drive your patching program. Track and keep a close eye on versioning. Make sure the versions in your inventory are at a level with which you are comfortable. Remember older versions mean higher risk as you may be more susceptible to attacks that take advantage of known vulnerabilities, so it is important to take into account the criticality of the system when making decisions to patch. Additionally, make sure that the version of your asset is still supported. Since many manufacturers will stop issuing patches for older products, make sure your assets are still supported, and if not, consider replacing them.

How Do We Make An Inventory?

I would suggest leveraging good old fashioned leg work. Talk to your leadership, the owners of major systems in the organization, and your IT department. Many may have inventories of the systems within their purview. Additionally, if you have tools that involve client installations on devices (i.e. antimalware, host-based firewalls, configuration management tools, host-based intrusion detection and host-based intrusion prevention tools), you might check the management panel on those to create an initial baseline. There are also plenty of tools that can help you with discovery and enumeration of networked devices if you have the resources to purchase and implement them.

Once you are satisfied you have an accurate asset inventory, keep it updated! When your company purchases new equipment, make sure they are required to log it in the asset inventory. Likewise, if old equipment is removed from the environment, make sure it is accounted as deactivated or destroyed in the inventory. Make sure your versions are up to date, and make sure that if an asset moves between offices, its location is accounted for.

I will be continuing my discussion on SMB cybersecurity and privacy in later blog

posts, so keep an eye out for the ongoing series.

Other Post From The SMB Cybersecurity Series:

- 4 Tips to Improve Small and Medium Business (SMB) Security
- Making and Standardizing Unique IDs
- Why You Need Authentication

KEVIN FORD

CISO OF CYBERGRX