Application and Software Inventory: The Good, the Bad, the Process!

By Allison Davis, Senior Manager and Katie Kane, Manager

Hardware inventories — most organizations have them and understand why they are important. What's often forgotten or overlooked, however, is the hardware inventory's pesky little brother: the application and software inventory.

If you already have an inventory of all the software and applications in use at your organization, you're ahead of the game. (But keep reading to make sure you're using and maintaining it effectively.) If you don't, you may be wondering why you need one.

Asking these questions will help highlight the importance of an application and software inventory:

- Do we know what applications people are accessing within our organization?
- Do we know if the applications are installed locally or if they are hosted by a third party?
- How do we determine which applications we need to patch?
- Do we know which software or applications are reaching end-of-life?
- Is any rogue or unnecessary software installed?
- Are we sure that each application employees access is properly secured with password, account lockout, and multi-factor authentication parameters?
- Can we identify what data each application and software stores and accesses?

As this shows, you cannot maintain and manage what you do not know you have. If your organization is like most, you're using more and more software and applications. It's imperative to have a handle on the solutions your employees access.

This article provides three steps to help you create and manage an effective application and software inventory system to maintain a secure environment.

Step 1: Determine What Is in Use

What systems are employees logging into on a daily basis? This should include not only software and applications installed locally on workstations and servers but also any web-based applications employees can access.

Determining what is being used and what exists in your environment is one of the most difficult steps in the inventory process. To do this:

- **Poll the departments within your organization**. Ask them what they are using, what they use it for, and who should have access to it.
- **Review web activity reports or employees' browsing histories.** This will help you determine which sites your employees are actually accessing. Compare this information to your poll results. You may be surprised at how many more systems you find!
- **Determine the applications installed on servers and workstations.** There are automated tools that can report on all software installed on systems at a point in time. If you don't have one of these solutions you can manually review devices to see what is installed.

If your organization is like most, you're using more and more software and applications. It's imperative to have a handle on the solutions your employees access.

Step 2: Document, Document, Document

Everything you uncover above should be documented within your inventory system. This can be as simple as an Excel spreadsheet or database. This inventory should include details that would be helpful to your organization, such as the application or system name, vendor information, license period, system administrator or owner, type of data stored, website address, application controls configured, etc. These details are critical for ongoing management.

If any concerning software, applications, or exceptions are noted during the evaluation process, be sure to document them. Exceptions could include software you didn't know staff members were using or an application that is outdated or obsolete but still used for a specific reason, such as a vendor requirement. Any exceptions should be approved by the appropriate level of management.

Step 3: Ongoing Management

Now that we've addressed the big but vital task of creating your application and software inventory, it's time to talk about processes and controls to help with ongoing management. This is generally much easier than creating the inventory, especially if you have automated tools. If your management processes are more manual, it may be a little more complicated.

Follow these steps:

- **Restrict administrative access rights on local systems.** By limiting local administrative access, you reduce the risk that end users could install applications on their workstations or laptops.
- **Configure web filter blacklisting or whitelisting, or both**. A web filter blacklist restricts access to certain sites, while a whitelist details the sites that can be accessed. Whitelisting is typically much more restrictive and a great control, but it can be more difficult to implement and manage. By restricting access to websites, you reduce the likelihood that employees can access or install extraneous or unapproved software. This forces end users to reach out to the IT department if they need access to a site or application.
- **Review web filter activity reports.** As noted before, this can alert you to sites employees are accessing to ensure you are aware of all the applications they may be using.
- **Review for extraneous or obsolete software and applications.** If you have an automated tool, generate a report of all installations on your servers, workstations, and laptops. Otherwise, manually inspect systems for extraneous items. Note that without an automated inventorying tool, this task becomes much more cumbersome and is often less efficient and effective. The timeliness of identification often decreases, which could result in increased exposure to vulnerabilities associated with unmanaged, outdated, or obsolete software.

  When taking this step, ensure that:
  - No extraneous software is installed. This could include software that was not approved or approved software that is no longer needed.
  - Applications are running current versions and no obsolete software exists. Proactive monitoring can also help you identify software that is nearing end-of-life.
- **Revisit exceptions**. Exceptions should be reapproved at least annually. For example, if you approved outdated or obsolete software due to a vendor requirement, contact the vendor to see if it has updated its system to be compatible with a more secure and current solution.

Now that we have covered the basic process of software inventory creation and management, you are ready to conquer this task at your own organization. By identifying and properly managing the software and applications in use, you can implement layered controls and processes to help better secure your environment.

Everything you uncover should be documented within your inventory system. These details are critical for ongoing management.

About the Authors

Allison Davis, Senior Manager
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

Katie Kane, Manager
CapinTech
kkane@capincrouse.com
o 505.50.CAPIN ext. 2007

Katie has 15 years of banking technology experience and nearly four years of information security auditing experience. Katie also has an extensive knowledge of Automated Clearing House (ACH) rules and regulations and is the ACH specialist on staff. She stays current on changing threats and government regulations to better assist clients in protection against cybersecurity threats.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.