Vulnerability Management

6 Things to Know About Vulnerability Management

There’s more IT in the wild than ever: Wi-Fi enabled coffee makers, smart home technology, building automation, and an increasingly remote workforce. All these endpoints now provide attackers more gateways than ever, meaning more places to hide and more connections to exploit. We spoke to Jacob White, Ingram Micro Technology Consultant II, to learn more about how vulnerability management can help mitigate the risks of more endpoints on the network.

IT sprawl is real, and a major security issue

With organizations adding more and more to their IT stack and overall network, the risk for attack increases. The more endpoints there are, the more vulnerable your systems are to attack! Attackers leverage these vulnerabilities to run malware and install backdoors, allowing access to corporate networks. As networks get bigger and more complicated, threat actors have more places to hide malware; it’s kind of like the game “Whack-a-Mole” where you’re trying to keep track of potential weaknesses and patch them! When managed manually, patching can be difficult to stay ahead of, leaving gaping holes for attackers to exploit.

Vulnerability management helps organizations with this problem

Vulnerability management tools help organizations mitigate IT sprawl by giving internal IT and security teams visibility into how they are exposed, identifying issues that need to be resolved, and prioritizing their efforts based on level of risk.

What is vulnerability management?

In a nutshell, vulnerability management is looking at your organization the same way a threat actor would and mitigating the risks before they’re exposed. These tools look at what vulnerabilities and risks exist and then prioritize those remediation efforts.

I’m already managing my network on a spreadsheet. Do I still need vulnerability management support?

When you’re using a spreadsheet to manage your endpoints, you look at everything on a level playing field with the same level of urgency; not to mention, that manual process is time-consuming and opens organizations up to risk from human error. Vulnerability management tools give users an automated, sorted list of what to focus on by priority. This increases visibility into the endpoints connected to a network and offers protection for each.
Vulnerability management tools can help your IT team be more efficient

With today’s shortage of security and IT professionals, it’s more important than ever to empower and enable a company’s existing IT staff with tools to help them manage security with as much automation as possible. Especially in SMBs that may not have a security-specific staff, IT technicians are wearing many hats and potentially leaving security to chance. Vulnerability management tools help manage time and increase level of automation. The tools do all the heavy lifting!

How do I get started with vulnerability management?

First, look at your organization’s current process. Then, answer questions around staffing: will you have dedicated people to focus on security every day or is someone wearing many hats? Finally, you will then pick an “as a service,” or in-house tool depending on the amount of automation that your organization requires.

Ingram Micro’s Cybersecurity Delta Force is here to help you determine what vulnerability management tools are the best fit for the staffing levels and environment in question. Leverage our team to help work through available options that meet your needs and maximize security posture. Contact us at cybersecurity@ingrammicro.com to learn more!