eclypsium

Assessing Enterprise Firmware Risk Checklist

1 Do You Have Visibility Into Your Firmware Vulnerabilities and Assets?

- ☐ Gain greater visibility into your potential attack surface by adding firmware attributes to the data collected as part of your asset management program.
- ☐ Integrate managing firmware with existing hardware and operating system lifecycle programs.
- ☐ In addition to system firmware, ensure you have visibility into firmware vulnerabilities in device components.
- ☐ Add regular automated vulnerability scanning for firmware vulnerabilities and misconfigurations.
- ☐ Incorporate firmware vulnerability metrics into your existing vulnerability management program reports.
- ☐ Conduct an assessment of the discoverability of vulnerabilities in external facing assets using tools such as Shodan and Nmap to understand what adversaries may uncover as part of initial reconnaissance activities.
- ☐ Consider tools to streamline the firmware update process.

2 Can Your Organization Detect Firmware Tampering?

- ☐ Review existing capabilities to detect firmware attacks and asset tampering, paying particular attention to travel and other high-risk environments. Assess the likelihood of attack and the impact if such attacks go undetected.
- ☐ Consider incorporating firmware attacks into planned 2020 red and purple team engagements.
- ☐ Add security tools to automatically monitor the integrity of system and component firmware and alert to any compromises.
- ☐ Include a combination of whitelisting, threat signatures, and behavioral analysis to detect both known and unknown firmware implants.

3 Do You Have Visibility Into and Control Over Risks in Your Technology Supply Chain?

- ☐ Add scanning processes to evaluate newly acquired hardware for firmware integrity and the presence of vulnerabilities, particularly for assets that serve critical functions or roles in the organization.
- ☐ Establish processes to scan acquired hardware infrastructure during any M&A process.
- ☐ Evaluate prospective technology and service providers in terms of firmware security as part of the overall supplier evaluation and due diligence process.
- ☐ Regularly monitor firmware behavior to identify malicious or anomalous firmware behaviors.
- ☐ Ensure your procurement and vendor engagement programs include assigning responsibility to appropriate parties for the assurance of 3rd party components involved in the delivery or products and services. When delegating responsibility to groups outside your organization, ask for details describing how they manage this risk that you inherit.
- ☐ Establish appropriate runbook sections for how your organization will deal with potential issues that extend to your vendors/partners via supply network chain related firmware issues.

4 Are Your SOC and IR Teams Equipped to Deal With Firmware Threats?

- ☐ Include firmware scanning as a standard component of incident response of devices that are potentially compromised.
- ☐ Use firmware scanning to verify the integrity of all firmware before returning a device to service.
- ☐ Arm threat hunters with tools that monitor for unusual firmware behavior to further analyze suspicious devices.
- ☐ Identify any gaps in how firmware-related alerts are handled both in existing security tools as well as the SIEM.
- ☐ Add firmware processes to standard IR triage and response runbooks.
- ☐ Evaluate and update the IR Knowledge Base to include firmware-related information.

5 Are You Prepared For Firmware-Related Business Risks?

- ☐ Define and document the role of firmware and firmware security in the organization's security policies, practices, and procedures.
- ☐ Review regulatory requirements in terms of hardware and firmware to fully understand the organization's obligations.
- ☐ Consider implementing risk management and security controls aimed at the firmware layer of the enterprise.
- ☐ Add appropriate language to contracts of vendors who may be considered 3rd party suppliers to your customers and partners.

This checklist is excerpted from Eclypsium's report: **Assessing Firmware Security Risk**. Get the full report **here**.