Action1

NIS2 Patch Management Guide: Actionable Steps for IT Pros

INTRODUCTION

With the **NIS2 Directive** in effect, organizations across the EU must implement stricter cybersecurity measures to safeguard critical infrastructure and digital services. Among the key requirements is effective patch management - a cornerstone of vulnerability mitigation and system resilience.

This guide is designed for IT pros seeking practical steps to ensure compliance with NIS2 patch management requirements. It provides actionable insights and checklists to simplify the process and reduce cybersecurity risks. By following the outlined steps, you can enhance your organization's defenses while meeting regulatory obligations.

PATCH MANAGEMENT REQUIREMENTS UNDER NIS2

1. Maintain an Asset Inventory

- Document all hardware, software, and network assets.
- Regularly update the inventory to identify systems requiring patches.

2. Perform Regular Vulnerability Assessments

- Continuously scan your environment for vulnerabilities.
- Use automated tools to detect outdated software or unpatched systems.

3. Establish a Risk-Based Patch Prioritization Framework

- Evaluate vulnerabilities based on CVSS scores, exploit availability, and business impact.
- Prioritize patching for critical systems exposed to the Internet or with high business value.

4. Develop a Patch Deployment Process

- Define a patching schedule (e.g., monthly or bi-weekly updates).
- Include emergency protocols for critical vulnerabilities.

5. Test Patches Before Deployment

- Use a staging environment to test patches for compatibility and stability.
- Document test results to avoid disruptions during deployment.

6. Implement Automated Patch Management

- Leverage tools to automate patch identification, distribution, and installation.
- Minimize manual effort to reduce errors and delays.

7. Monitor and Report Patch Status

- Track deployment progress and identify unpatched systems.
- Generate compliance reports for internal reviews and audits.

8. Address Supply Chain Vulnerabilities

- Assess third-party software for vulnerabilities and apply necessary patches.
- Verify that vendors provide timely updates for their products.

9. Document and Communicate Patch Management Policies

- Create a written policy outlining roles, responsibilities, and processes.
- Train staff to ensure consistent understanding and application.

10. Include Patch Management in Incident Response Plans

- Establish protocols for responding to unpatched vulnerability exploits.
- Monitor emerging threats and patch critical systems immediately.

11. Ensure Secure Configuration Management

- Regularly review configurations to identify and fix misconfigurations.
- Integrate patching into your configuration management practices.

12. Audit and Review Patch Management Processes

- Periodically audit activities to identify inefficiencies and gaps.
- Update processes to align with evolving threats and NIS2 standards.

QUICK CHECKLIST FOR IT PROS

Use this checklist to track your organization's patch management progress: To make it actionable, IT pros can use this checklist to track compliance:

- Updated asset inventory maintained.
- Regular vulnerability scans conducted.
- Risk-based prioritization framework implemented.
- Patch deployment process established.
- Patches tested before rollout.
- Automated patch management tools deployed.
- Patch status reports monitored and maintained.
- Third-party software supply chain risks addressed.
- Written policies documented and staff trained.
- Patch management integrated into incident response plans.
- Secure configurations maintained and reviewed.
- Regular audits conducted for continuous improvement.

CONCLUSION

NIS2 raises the bar for cybersecurity compliance, making effective patch management a non-negotiable priority for IT teams. By adopting the strategies and practices outlined in this guide, your organization

can reduce its attack surface, enhance operational resilience, and demonstrate compliance with regulatory standards.

Remember, patch management isn't just a requirement—it's a critical safeguard for your organization's infrastructure and reputation. **Start taking action today to ensure a secure and compliant future.**

Need More Help?

For additional resources or tools to streamline your patch management efforts, visit Action1's website.

Action1

Action1 reinvents patching with an infinitely scalable, highly secure, cloud-native platform configurable in 5 minutes — **it just works** and is always free for the first 100 endpoints, with no functional limits. Featuring unified OS and third-party patching with peer-to-peer patch distribution and real-time vulnerability assessment with no VPN needed, it enables autonomous endpoint management that preempts ransomware and security risks, all while eliminating costly routine labor. Trusted by thousands of enterprises managing millions of endpoints globally, Action1 is certified for SOC 2 and ISO 27001.

The company is founder-led by industry veterans **Alex Vovk** and **Mike Walters**, who founded Netwrix, which has grown into a multi-billion-dollar industry-leading cybersecurity company.