Patch Management & Updates: The PureIoT Security Guideline

Introduction

Patch management is the process of identifying, acquiring, testing, and installing patches (code changes) to fix security vulnerabilities and bugs in software and firmware. A rigorous patch management process is the single most effective defense against cyberattacks.

1. The Patch Management Lifecycle

Effective patch management follows a structured, four-stage lifecycle:

Stage	Description	Key Action
1. Discovery & Assessment	Identify all assets (servers, OS, applications) and determine which patches are relevant to your environment.	Maintain a comprehensive asset inventory. Subscribe to vendor security alerts.
2. Testing & Validation	Apply the patch to a small group of non-production servers (a **sandbox** or staging environment) to ensure it does not break critical applications.	Create a staging environment that mirrors production. Document test results.
3. Deployment	Roll out the patch to production servers, starting with non-critical systems and moving to mission-critical systems.	Use automated deployment tools (e.g., SCCM, Ansible, WSUS).
4. Verification & Reporting	Confirm the patch was successfully installed and that the system is functioning normally. Report on compliance.	Check system logs and run post-patch health checks.

2. Prioritization and Cadence

Not all patches are created equal. Prioritization is key to managing risk.

- **Critical Patches:** Patches that fix publicly known vulnerabilities (Zero-Day or actively exploited) must be deployed within **48 hours**.
- **Security Patches:** Patches that fix high-severity vulnerabilities should be deployed within **7 days**.
- **Non-Security Patches:** General bug fixes and feature updates can be deployed on a regular monthly or quarterly cadence.

3. Best Practices for Server Patching

- **Centralized Tooling:** Use a centralized patch management system (e.g., Microsoft WSUS, Red Hat Satellite, or a third-party RMM tool) to ensure consistency and track compliance.
- **Pre-Patch Snapshot:** Before applying any patch to a production server, take a **full system snapshot or backup**. This allows for immediate rollback if the patch causes an issue.
- **Firmware and BIOS:** Do not neglect firmware and BIOS updates for hardware components (RAID controllers, network cards). These often contain critical security fixes.
- **Out-of-Band Management:** Ensure you have a method for managing servers (e.g., iDRAC, iLO, IPMI) that is separate from the main network, in case a patch breaks network connectivity.

Patch Management Checklist

Item	Status	Notes
Asset Inventory is Current	[ ]	
Staging Environment Used for Testing	[ ]	
Critical Patches Deployed within 48 Hours	[ ]	
Pre-Patch Snapshots Taken	[ ]	
Firmware/BIOS Updates Included	[ ]	

Conclusion

A disciplined patch management strategy is non-negotiable for server security. PureIoT provides fully managed patch management services, ensuring your entire infrastructure is secure and compliant.