BLACK BELT SECURE
Defend Today, Thrive Tomorrow.

Post-Ransomware Hardening Checklist

Technical Guide for Long-Term Recovery and Prevention of Repeat Attacks

January 2026

Overview for Technical Teams
Several months post-ransomware incident, the immediate crisis has passed, but the window for re-victimization remains open. Recent 2025–2026 attack trends show threat actors frequently re-target prior victims by exploiting persistent footholds: legacy servers, stale privileged credentials, unpatched systems, and shadow IT.

This checklist focuses on the post-recovery phase—systematic cleanup, attack surface reduction, and implementation of automated controls to prevent repeat exploitation. It is tailored for security, infrastructure, and identity teams rebuilding for resilience.

Phase 1: Comprehensive Assessment & Root-Cause Validation

- Review forensic/IR report: Confirm initial access vector, lateral movement paths, and persistence mechanisms.
- Validate full eradication of known indicators of compromise (IOCs) from the incident.
- Perform fresh network discovery to baseline current environment state.

Phase 2: Identity & Credential Hygiene

- Complete enterprise-wide password rotation if not already done; enforce phishing-resistant MFA everywhere.
- Rotate all non-human credentials: service accounts, application passwords, SSH keys, certificates.

- Audit and minimize privileged group membership (Domain/Enterprise Admins, local Administrators).
- Implement or refine tiered administration model (Tier 0/1/2).
- Deploy Azure AD/Entra ID Conditional Access policies with risk-based controls.

Phase 3: Asset Inventory & Legacy Risk Remediation

- Conduct active and passive discovery to map all on-prem, cloud, and hybrid assets.
- Identify and prioritize end-of-support systems: Exchange 2016/2019 (EOL October 2025), Server 2012/R2, etc.
- Check external exposure via for forgotten services (RDP, OWA, VPN endpoints, legacy web apps).
- Safely decommission unsupported assets, e.g., legacy servers:
    - Confirm no remaining dependencies (mailboxes, public folders, hybrid connectors, SMTP relays).
    - Uninstall roles via Setup.exe; remove AD objects if no future on-prem Exchange planned.
- Detect and remove or isolate shadow IT and unmanaged devices.

Phase 4: System Hardening & Secure Rebuild Validation

- Verify all systems are patched to current levels and aligned with CIS benchmarks/Microsoft Security Baselines.
- Confirm restores were performed from clean, immutable backups; establish ongoing integrity testing.
- Re-image any systems rebuilt from potentially compromised images during initial recovery.

Phase 5: Defensive Architecture & Continuous Controls

- Ensure full EDR/XDR deployment and tuning across endpoints, servers, and cloud workloads.
- Implement network micro-segmentation and Zero Trust principles (application allow-listing, JIT access).

- Automate continuous asset discovery, configuration drift detection, and vulnerability prioritization.
- Secure backup infrastructure with immutability, air-gapping, and multi-factor deletion protection.
- Schedule regular red-team exercises and tabletop simulations targeting common persistence techniques.

Additional Items

We've compiled a list of some of the most common additional items we have learned over the years while doing ransomware mitigation.

- **Unsecured Credentials:** Sitting in file shares, SharePoint, Wikis, Ticketing Systems, and DMS platforms. The #1 most common finding we've observed over the years that have allowed attackers to gain access to and stay in systems.
- **Misconfigured AD CS (Active Directory Certificate Services):** Such as certificates that allow Everyone to impersonate Domain Admins. Far and away the most common are EC1, ES4, and ESC5. Anyone of these could result in full domain compromise.
- **Local Admin Password Reuse:** Across Workstations and Servers. The unfortunate reality is this is a very easy win for attackers. If you're not using LAPS, you should be.
- **Kerberoastable Domain Admin Accounts:** That shouldn't be service accounts to begin with. We've seen the built-in Administrator accounts being used as a service account far too many times.
- **Weak or Default Passwords:** On administrative portals, network devices, and yes even on legacy systems such as IBM iSeries. Especially problematic for IoT that comes out of China.
- **Hosts without EDR:** making it virtually impossible to identify threat actor activity. We guarantee you that attackers are looking for these types of hosts. Don't give them easy wins.
- **Insecure Permissions in Active Directory:** like Everyone with Full Control over the root of the domain.
- **Domain Users in Local Admin Groups**, granting unintended privilege escalation paths. It's incredibly difficult to secure and harden your environment when users have privileges they shouldn't. Suzie doesn't need admin creds despite all the cute cat screensavers she says she needs.

About Our Team

For the past 14 years, we have partnered with technical teams on hundreds of ransomware recoveries—focusing on forensic analysis, environmental cleanup, and automated long-term hardening.

Our JUTSU program delivers agentless, continuous discovery of legacy and shadow assets, automated configuration validation, and secure decommissioning workflows. It integrates seamlessly with existing SIEM/EDR environments to provide prioritized, actionable remediation—allowing teams to maintain a dramatically reduced attack surface with minimal manual overhead.

Post-incident clients frequently adopt JUTSU because it eliminates the persistent reconnaissance and foothold gaps that enable repeat attacks.

For more details:

Peter Vavrosky
blackbeltsecure.com (Contact: 469-557-2007 | pvavrosky@blackbeltsecure.com).

BLACK BELT SECURE
Defend Today, Thrive Tomorrow.