Greenbone

IT Security Checklist: Six Actions for Measurably Better Security

This checklist outlines concrete steps to systematically reduce vulnerabilities and effectively protect your IT infrastructure.

Background: 99.9% of successfully exploited vulnerabilities have been known for over a year. By implementing the six measures in this checklist, you systematically close the most common entry points for attackers.

200.000+	100.000+	Täglich
Vulnerability Tests	Installations Worldwide	Feed Updates

☐ Enable Multi-Factor Authentication (MFA)

Passwords alone do not provide sufficient protection. A second layer of authentication prevents 99.9% of account hijacking attacks, even if the password has been compromised.

- Protection against password-based account takeover
- Meets compliance requirements
- Reduces unauthorized account access
- Easy implementation

Concrete Implementation:
Based on frameworks such as NIST CSF 2.0, first identify online accounts and assess the risk of account hijacking. Apply multi factor authentication to accounts that access financial systems, customer data, administrative functions, or other sensitive information, and verify MFA enforcement regularly. Start with administrative accounts and the IT team, then extend MFA to all employees. Authentication apps such as Microsoft Authenticator or Google Authenticator are practical choices, while hardware tokens can be used for highly critical access. A documented backup process for lost or faulty devices should be defined and communicated during onboarding.

Regularly Review Access Rights

Overly broad permissions are a serious threat: employees often have access to systems, data, or settings they don't require for their work. The principle of Least Privilege dictates that every user is only granted the minimum necessary permissions..

- Minimise insider threats
- Prevent lateral movement
- Ensure compliance (GDPR, NIS2)
- Improve audit trail

Concrete Implementation:
Review all permissions quarterly. Use Identity & Access Management (IAM) systems that can automate and document the process. Upon role changes or employee departure, permissions must be adjusted immediately. For particularly critical tasks, Just-in-Time Access is recommended: privileges are granted only temporarily and upon request. Document all changes traceably.

Test and Validate Backup Strategy

A backup is worthless if the data cannot be recovered in an emergency. Regular testing shows whether your backup strategy is functional. This is especially important after ransomware attacks when backup integrity and quick recovery becomes critical.

- Increase ransomware resilience
- Ensure business continuity
- Prevent data loss

Concrete Implementation:
Follow the 3-2-1 rule: Three copies of your data on two different media, one of which is offsite. Test restoration periodically with realistic scenarios, not just individual files, but complete system states. Air-gapped or immutable backups also provide extra protection against ransomware attempting to encrypt backups. Document recovery processes in detail and keep your team trained.

Automate Patch Management

Missing security updates are the most common cause of successful attacks. Many vulnerabilities exploited in cyber attacks have been known and documented for months. Automated patch management consistently closes these gaps.

- Prevent known exploits
- Reduce time expenditure
- Meet compliance requirements
- Minimise zero-day response time

Concrete Implementation:
Rely on central patch management tools like WSUS, SCCM, or Ansible. Prioritise security updates according to their CVSS score. Vulnerabilities with a CVSS score above 7.0 should be installed promptly. Test critical patches in a staging environment beforehand to detect compatibility issues. Define fixed maintenance windows for production systems. The combination with regular vulnerability scans shows you where gaps still exist.

Implement OPENVAS SCAN

RECOMMENDED

OPENVAS SCAN identifies vulnerabilities in your IT infrastructure before attackers can exploit them. The appliance performs automated scans, evaluates risks by criticality, and provides concrete remediation recommendations.

- Over 200,000 vulnerability tests, updated daily
- Authenticated & unauthenticated scans
- Master-Sensor architecture for distributed locations
- European vendor, fully GDPR-compliant and ISO certified
- Air-gapped technology for maximum security
- Ready-to-use hardware and virtual appliances

European Vendor

Headquartered in Osnabrück (Germany), all data remains within the EU. Full GDPR compliance by design, not by adaptation.

Certified Security

ISO 27001, ISO 9001, TISAX, and ISO 14001 certified. Highest quality and security standards guaranteed.

Ready-to-use Appliances

The world's only provider of ready-to-use hardware appliances for Vulnerability Management. Instantly operational without complex installation.

Scalable

From flexible entry-level solutions to adaptable options for a wide range of use cases. Our portfolio grows with your requirements.

Why deploy OPENVAS SCAN?

Comprehensive Coverage: The OPENVAS ENTERPRISE FEED contains over 200,000 vulnerability tests and new tests are added daily. The feed covers a broad range of common IT and OT environments, including servers, workstations, network devices, IoT, and selected industrial components. Greenbone maintains a fast response process for emerging vulnerabilities, with high priority issues typically addressed shortly after public disclosure.

Practical Examples: Companies with 500+ endpoints use OPENVAS SCAN for regular compliance scans (GDPR, NIS2, ISO 27001). Multi-location scenarios are covered via Master-Sensor architectures. Critical infrastructures benefit from authenticated scans that also check applications without network services.

Automated Compliance: Automated scans, detailed reports, and full documentation support compliance with regulatory requirements. The audit trail function documents all scanner activities in a legally compliant manner.

First Steps with OPENVAS SCAN:

1. **Select Appliance Model:** Use a hardware appliance for high-performance or a virtual appliance for flexible deployment
2. **Define Network Segments:** Namespace separation divides management and scan traffic
3. **Configure First Scans:** The Task Wizard guides you through the scan setup
4. **Set up Authenticated Scans:** Remote access via SSH or SMB enable deep system checks
5. **Enable Automation:** Define schedules for regular scans and automated reporting

Develop an Incident Response Plan

When a security incident occurs, preparation determines the duration of the disruption, and the extent of the damages. A documented Incident Response Plan defines responsibilities, communication channels, and action steps for various scenarios.

- Drastically reduce response time
- Minimise damage
- Activates forensic follow-up
- Meet legal requirements

Concrete Implementation:

- Form an Incident Response Team with defined roles: Incident Manager, IT Manager, Communications, Legal Department.
- Create playbooks for typical scenarios such as ransomware, data leaks, or DDoS attacks.
- Set up communication channels that still function even if the IT infrastructure is compromised.
- Conduct quarterly tabletop exercises where the team simulates realistic scenarios.
- Document the lessons learned after every real incident.

OPENVAS SCAN in Action

Professional Vulnerability Management deployed as a hardware or virtual appliance, from initial vulnerability detection through continuous monitoring. Contact us for personalised consultation and technical details.

Interested in OPENVAS SCAN?

Web: www.greenbone.net

E-Mail: info@greenbone.net

Free Trial: OPENVAS BASIC, 14-day trial version available