Richtlinie für den Schutz vor Schadprogrammen und zur Nutzung von Schutzmechanismen

Inhaltsverzeichnis

Dokument

Dieses Dokument ist GÜLTIG. Es ist für alle Administrator:innen von Clients und Servern an der UR verbindlich.

- Freigabe am: 07.08.2025
- Freigabe durch: Leitung ITMZ

Für die UR besteht für die Anbindung an das Landesverwaltungsnetz des Landes MV die verpflichtende Vorgabe zur Umsetzung von Maßnahmen im Bereich „OPS.1.1.4 – Schutz vor Schadprogrammen“. Der Schutz vor Schadprogrammen ist eine wesentliche Voraussetzung für die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme sowie für die Sicherheit von Forschung, Lehre und Verwaltung. Die technischen und organisatorischen Maßnahmen werden in diesem Dokument festgelegt.

Schutz vor Schadprogrammen inkl. systemspezifischer Schutzmaßnahmen

IT-Systeme sind vor Schadprogrammen zu schützen. Eine Verwendung einer „Anti-Malware“-

Lösung KANN dafür ein Bestandteil sein, jedoch laufen diese Programme mit Systemverwalterrechten und stellen damit zusätzliche Sicherheitsrisiken dar.

Bestandteile des Schutzes vor Schadprogrammen für Clients und Server können z.B. sein:

- Nutzungszeit: Betrieb des IT-Systems nur während der Nutzung
- Anti-Malware-Lösung: Betrieb einer Anti-Malware-Lösung inkl. möglichst tagesaktueller Aktualisierung der Malwaresignaturen. Cloud-basierte Lösungen sind nur dann zulässig, wenn die Datenschutzfragen geklärt sind (Auftragsverarbeitung, VVT, ..).
- Aktuell halten: zeitnahes Einspielen von Sicherheitspatches
- Nur notwendige Dienste: Deaktivieren von nicht benötigten Diensten und Dienstbestandteilen
- Physischer Zugangsschutz
- Nutzung von bereits vorhandenen Schutzmechanismen der IT-Systeme
- Arbeiten nur mit Nutzerrechten (Adminrechte nur bei Bedarf nutzen)
- Firewall: Einschränkung des Netzwerkverkehrs an zentraler Firewall und auf dem Gerät
- DNS: restriktiver DNS mit Blocken von Schadsoftware
- Monitoring: Frühzeitiges Erkennen von Schadsoftware durch Monitoring des Systems
- Einschränkung der administrativen Zugänge
- Dienste immer mit den geringstmöglichen Rechten ausführen
- Nutzung von E-Mail nur in Webmailern, Verzicht auf installierte Mailclients und Verzicht auf Downloads
- physische Schnittstellen deaktivieren oder mit Zugangsschutz versehen (z.B. USB-Geräte per Port-Security nur per Whitelist erlauben)
- Arbeiten im Internet (z.B. im Web browsen und E-Mails lesen) erfolgen nicht mit Adminrechten, sondern nur mit Nutzerrechten

Dokumentation von Entscheidungen

Für alle Klassen von IT-Systemen MÜSSEN die zuständigen Administrator:innen jeweils einen geeigneten Schutz vor Schadsoftware auswählen und die Entscheidung dokumentieren. Eingebaute Schutzmechanismen der verwendeten IT-Systeme und Anwendungen sind zu nutzen, sofern keine wirksameren Mittel und Methoden zur Verfügung stehen. Der angemessene Schutz für ein IT-System kann aus verschiedenen ineinandergreifenden Schutzmaßnahmen bestehen.

Vorgaben für spezifische Systeme - Clients

Der Schutz SOLLTE an verschiedenen Stellen ansetzen, u.a.:

- Härten: Die Systeme sollten gehärtet sein (z.B. Deaktivieren von nicht benötigten Diensten).
- Firewall: Die Netzwerkverbindungen sollten eingeschränkt sein (z.B. DNS Block von Werbung und Malware, Netztrennung von ungepatchten Systemen).

- Virenschutz: Abhängig vom verwendeten Betriebssystem sowie der Verfügbarkeit geeigneter Virenschutzprogramme sollte ein entsprechendes Schutzprogramm in geeigneter Konfiguration eingesetzt werden.
- Anti-Malware-Lösung: Ein Programm zum Malwareschutz kann eingesetzt werden.
- Ausführschutz: Das Ausführen von Schadprogrammen sollte auf den Systemen nicht möglich sein, z.B. per Whitelisting der erlaubten Anwendungen.

VERPFLICHTEND für alle Clients gilt:

- Die Systeme MÜSSEN aktuell gehalten werden, es dürfen nur vom Hersteller mit Sicherheitspatches versorgte Systeme im Uninetz betrieben werden. Diese Patches MÜSSEN regelmäßig eingespielt werden.
- Vertrauenswürdige Herkunft: Software MUSS aus vertrauenswürdigen Quellen installiert werden (z.B. offizieller App-Shop des Betriebssystems).

Windows-Clients

Es MUSS ein Malwareschutz genutzt werden. Dieser MUSS regelmäßig aktualisiert werden. Die Verwendung von Microsoft Defender KANN dafür als ausreichend festgelegt werden.

Linux-Clients

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

MacOS-Clients

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

Mobile Geräte

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

Anwendungsserver der UR (Remote Desktop Server)

Es MUSS das Ausführen von Malware verhindert werden, dies SOLLTE durch Whitelisting der erlaubten Programme erfolgen.

Vorgaben für spezifische Systeme - Server, Netzwerk- und IoT-Geräte

Der Schutz muss an verschiedenen Stellen ansetzen, eine generelle Vorgabe ist bis auf wenige verpflichtende Regeln jedoch nicht sinnvoll möglich.

VERPFLICHTEND für alle Server gilt:

- Die Systeme MÜSSEN aktuell gehalten werden, es dürfen nur vom Hersteller mit Sicherheitspatches versorgte Systeme im Uninetz betrieben werden. Diese Patches MÜSSEN regelmäßig eingespielt werden.
- Sofern Dateien von Nutzer:innen verarbeitet werden SOLLTEN diese Dateien von einem Schutzprogramm gescannt und ggf. gelöscht/in Quarantäne verschoben werden.

Windows-Server

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

Linux-Server

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

Appliances

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

IoT Geräte

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

IT-Infrastruktur inkl. Netzwerkgeräte

Eine Anti-Malware-Lösung ist verzichtbar, wenn angemessene andere Schutzmaßnahmen erfolgen.

Sensibilisierung und Verpflichtung der Benutzenden

Alle Benutzenden werden über Maßnahmen zum Schutz vor Schadprogrammen informiert. Sie sind aufgefordert, sich an die ihnen benannten Kontaktpersonen zu wenden, wenn der Verdacht auf eine Infektion mit einem Schadprogramm besteht. Informationen stehen auf den Seiten des IT- und Medienzentrums unter dem Punkt IT-Sicherheit zur Verfügung.