SiKoSH
SICHERHEIT FÜR KOMMUNEN
IN SCHLESWIG-HOLSTEIN

Hilfsmittel: Richtlinie Virenschutz

Version:	1.0
Datum:	10.07.2018
Kontakt:	KomFIT e.V. Kiel sikosh@komfit.de https://www.sikosh.de

Inhalt

1 Zielsetzung

Schadsoftware bedroht den Geschäftsbetrieb durch Verlust oder Einschränkung der Vertraulichkeit, Verfügbarkeit und Integrität der von den Behörden innerhalb Schleswig-Holsteins genutzten DV-Verfahren und DV-Infrastrukturen.

Durch den Einsatz eines Virenschutzmanagements und der nötigen Schutzsoftware werden diese Risiken reduziert und ein angemessenes Sicherheitsniveau erreicht.

Diese Richtlinie definiert Anforderungen und Regelungen an Virenschutzlösungen und Virenschutzmanagementprozesse.

2 Geltungsbereich

Diese Regelungen gelten für [Name der Behörde].

Sie gelten für alle physischen und virtuellen IT-Systeme, die betrieben werden. Ausgenommen sind Systeme, für die ein Virenschutz technisch nicht möglich ist. Dazu gehören z.B. diverse Netzwerkkomponenten (Switches, Router und dergl.).

3 Zuständigkeiten

Für den IT-Betrieb verantwortliche Person (IT-Leiter/in): [Name]

Für die Überwachung der Funktionalität / Aktualität verantwortliche Person (Virenschutzadministrator/in): [Name]

Informationssicherheitsbeauftragte/r: [Name]

4 Betrieb des Virenschutzes

4.1 Planung und Konzeption

Alle Endgeräte und Server, unabhängig vom eingesetzten Betriebssystem, sind mit einem Virenschutzprogramm auszustatten. Dabei sind die Virenschutzprogramme und – Signaturen, sowie eingesetzte Zusatzmodule stets aktuell zu halten.

4.2 Prüfung

Die eingesetzten Produkte des Virenschutzes sind regelmäßig, mindestens jährlich, anhand festgelegter Kriterien auf Ihre Wirksamkeit hin zu überprüfen und ggf. zu ersetzen oder durch Zusatzmaßnahmen zu ergänzen. Dabei sind die Prüfkriterien unter Berücksichtigung des Fortschritts der Technik ebenfalls regelmäßig, mindestens jährlich, fortzuschreiben.

Die Prüfkriterien für den behördlichen Virenschutz sind schriftlich festzulegen und orientieren sich an:

- der Reaktionszeit,
- den Erkennungsraten in unabhängigen Vergleichen,
- der Update-Häufigkeit,
- dem Funktionsumfang und
- der Handhabbarkeit.

4.3 Beschaffung

Das eingesetzte Softwareprodukt sollte mindestens folgenden Funktionsumfang bieten:

- zentrale Managementkonsole und dazugehöriges Berichtswesen
- On-Access und On-Demand Scanning, zeitgesteuerte Suche (Vollscan)
- Dateien per Signaturen scannen und heuristische Suche (Verhaltenserkennung z. B. zum Schutz vor Ransomware)
- komprimierte Dateien sowie Mailanhänge untersuchen
- Schutz vor jeglichen Formen von Schadsoftware (Viren, Trojaner, Rootkits, Spam, Hoaxes, Ransomware etc.)
- Automatische Aktualisierung der Pattern mehrmals täglich

Wünschenswert ist folgende zusätzliche Funktionalität:

- Verhinderung der Ausführung nicht freigegebener Programme (z. B. Schadcode über Internet oder über USB-Sticks)
- Devicemanagement (nur freigegebene Geräte können mit den Endgeräten kommunizieren)
- Mobile Device Management (MDM)[1]

4.4 Betrieb

Der Virenschutz ist auf allen Endgeräten und Servern ständig aktiv und prüft alle Zugriffe und Datentransfers zur Laufzeit.

Zusätzlich werden Möglichkeiten geboten, das Durchsuchen und Bereinigen eines definierten Endgerätes oder Servers manuell anzustoßen.

Für Endgeräte und Server, die durch die zentrale Virenschutzinfrastruktur dauernd physisch nicht erreichbar sind oder inkompatibel zu der eingesetzten Virenschutzlösung sind, ist der Betreiber für die Aktualisierung der Virenschutzprogramme und der Signaturen und den Nachweis darüber verantwortlich. In jedem Fall gelten die Regelungen dieses Virenschutzkonzepts.

Externe Auftragnehmer sind vertraglich zu verpflichten, einen aktuellen und ausreichenden Virenschutz auf Ihren Endgeräten und Servern herzustellen, bevor Sie für die Auftragsabwicklung eigene Endgeräte und Server mit Schleswig-Holsteins Netzinfrastruktur verbinden.

Der Virenschutzadministrator hält Notfall-Medien, bzw. Notfallprozesse und Lösungen vor, um eine lokale Bereinigung bei Virenbefall vornehmen zu können. Der ISB wird über Virenvorfälle unterrichtet.

Für einen Notfall, der durch einen großflächigen Virenbefall ausgelöst wurde, gelten die entsprechenden Regelungen des Notfall-Handbuchs.

4.4.1 Eingebundene Systeme

Für Endgeräte und Server, die netzseitig erreichbar sind, gilt Folgendes:

Die Virenschutzsoftware ist so zu konfigurieren,

- dass eine Verbindung zum zentralen Administrationswerkzeug automatisiert erfolgt.
- dass der On-Access Modus zur Laufzeit eingeschaltet ist.
- dass diese Konfiguration – auch vom lokalen Administrator - nicht verändert werden kann.

[1] S. auch die SiKoSH-Richtlinie Mobile Endgeräte

Die Signaturdatei ist unter Berücksichtigung folgender Vorgaben automatisiert zu aktualisieren:

- Die Aktualisierung der Signaturdatei soll schnellstmöglich automatisiert im Rahmen eines Standardchanges erfolgen.

Ein Vollscan aller Endgeräte und Server mit Systemrechten (On-Demand Scan) hat regelmäßig, mindestens [einmal pro Woche, Monat, Quartal] automatisiert zu erfolgen.

Sämtliche Scan-Funktionen der Virenschutz-Software sind möglichst schonend für die Systemressourcen zu konfigurieren. Systembelastungen durch Scan-Funktionen begründen keinen Ausschluss von einem Scan.

4.4.2 Nicht eingebundene Systeme

Für Endgeräte und Server, die nicht in einem zentral administrierten Virenschutz eingebunden und netzseitig nicht erreichbar sind (z. B. Testrechner), gilt Folgendes:

Der Betreiber hat deren Aktualisierung und die Aktualisierung der Signaturdatei schriftlich nachzuweisen. Der Nachweis ist fortzuschreiben und auf Aufforderung dem ISB vorzulegen. Bei automatischer Aktualisierung der Signaturdatei ist monatlich eine Stichprobe auf Aktualität durchzuführen. Diese Stichprobe ist ebenfalls schriftlich zu dokumentieren.

4.4.3 Überwachung

Der Virenschutzadmin führt regelmäßig [täglich/wöchentlich] eine Überprüfung des Virenschutzstatus (Aktualität der Pattern, Aktualität der versorgten Endgeräte) durch. Das Ergebnis ist zu protokollieren und dem ISB bei Bedarf vorzulegen.

4.4.4 Konfiguration

Die Konfiguration ist durch den Virenschutzadmin zu dokumentieren. Eine Ausfertigung der Dokumentation nimmt der ISB zum Sicherheitskonzept.

4.4.5 Port-Blockierungen

Um der Verbreitung von Schadcode vorzubeugen, ist der ISB berechtigt, einige Ports, entsprechend der jeweils aktuellen Gefährdungslage durch den Virenscanner blockieren zu lassen. Das sind z.B. die IRC-Ports (6666-6669) eingehend sowie der SMTP-Port 25.

Prozesse, die diese Ports nutzen und als sicher eingestuft werden, können innerhalb der Behörde durch den ISB von der Blockierung ausgenommen werden. Das gilt sowohl für Endgeräte als auch für Server.

Port-Blockierungen sind durch den ISB zu dokumentieren.

4.4.6 Domainblacklist

In Absprache zwischen ISB und Firewalladministrator sollte eine Domainblacklist auf der Firewall hinterlegt werden, die den Zugriff auf bekannt gefährliche Internetadressen blockiert. Dies kann wahlweise manuell, oder mit Hilfe frei downloadbarer Blacklists erfolgen. Beispiele für freie Anbieter von Blacklists finden sich u.a. hier[2].

4.5 Berichtswesen

Alle gemeldeten und verarbeiteten Schadcodeereignisse sind zu dokumentieren.

⇨	In der Anlage sind Vorschläge für eine Klassifikation von Schadcodeereignissen beschrieben. Dabei sind die Schwellwerte, wie etwa die Anzahl der betroffenen Systeme auf die Größe der IT-Umgebung des Anwenders anzupassen. Das Ziel der Klassifikation ist es weniger kritische Bedrohungsereignisse, welche z.B. vom Antivirenprodukt automatisch bereinigt werden, von Schadcodeereignissen mit einer gewissen Schadwirkung (z.B. das Verschlüsseln einiger IT-Systeme durch Kryptotrojaner) zu unterscheiden und damit einen transparenten Managementbericht zu erzeugen. Der SiKoSH Anwender sollte also die in der Anlage geschilderten Klassifikationen entsprechend auf die eigenen Bedürfnisse anpassen.

Die Berichte werden mindestens vierteljährlich erstellt und dem ISB zur Verfügung gestellt.

4.6 Ausnahmeregelungen

Endgeräte und Server können nur mit begründetem schriftlichem Antrag und Genehmigung durch den ISB von der zentralen Virenerkennung ausgenommen werden. Generelle Herstellerempfehlungen sollten nicht als Begründung angesehen werden.

Als Grund für eine Ausnahmeregelung können insbesondere gelten:

- Eine nachgewiesene Einschränkung der Funktionalität einer Anwendung.
- [Weitere Beispielkriterien, je nach eingesetztem Produkt und anwendende Institution]

Liegt ein Ausnahmegrund vor, sind die nötigen Maßnahmen zu erarbeiten. Mögliche Handlungsoptionen sind dabei:

[2] https://docs.danami.com/juggernaut/user-guide/ip-block-lists

⇨ Die folgenden Behandlungsoptionen von Ausnahmen, zielen auf Produkte, welche ein Ausnahmemanagement auf Prozessebene anbieten, womit Ausnahmen auf Dateipfadebene vermieden werden, da diese grundsätzlich weniger restriktiv sind. Es wird empfohlen die folgenden Regelungen an die tatsächlichen Gegebenheiten des eingesetzten Antivirenproduktes anzupassen.

- Identifikation und Bewertung des Prozesses, der für die Probleme sorgt.
- Wird der Prozess als vertrauenswürdig eingestuft, wird er ins geringe Risiko aufgenommen.
- Sollten die Probleme damit nicht behoben werden, können sichere Dateitypen zusätzlich vom schreibenden Scan ausgenommen werden.
- Sind die Dateitypen unsicher oder nicht konkret zu benennen, werden Ordnerpfade für die Prozesse im geringen Risiko vom Scan ausgeschlossen.

Die von einer Ausnahme vom Vollscan betroffenen Systeme sind zu dokumentieren.

4.7 Prüfung und Durchsetzung

Die Überprüfung der Regelungen erfolgt im Rahmen turnusmäßiger Reviews. Sie können ferner Prüfungsgegenstand der IT-Revision oder bei Sicherheitsaudits sein.

5 Änderungsverzeichnis

Version	Datum	Kapitel, Änderung	Autor/in

6 Anlagen

6.1 Tabelle Schadcode-Ereignisklassifikation

Schadcode-Ereigniskategorie	Schadcode-Ereignisbeschreibung
0	Fehlerhafter Schadcodeverdacht (False Alert - automatisiert erzeugt oder durch Anwendermeldung)
1	Automatische Bereinigung von Schadcode – kein manueller Eingriff erforderlich.
2	Manuelle Nacharbeiten erforderlich. Dies können Kontrollmaßnahmen bis hin zur einfachen Schadcodeentfernung sein.
3	Manuelle Bereinigung von Schadcode und begleitende Forensik erforderlich. Ermittlung von Schadwirkungen und Schwachstellen.
4	Gleichartige oder korrelierende, automatisiert entfernbare Schadcodeereignisse auf mehr als [X] Systemen.
5	Gleichartige oder korrelierende Schadcodeereignisse auf mehr als [X] Systemen. Manuelle Bereinigung von Schadcode und begleitende Forensik erforderlich.
6	Großflächiger Ausbruch von Schadcode / Schadwirkungen auf mehr als [Y] Systemen.

7	Gezielter Angriff auf bestimmte Informationssicherheitswerte der Behörde

Schadcode-Ereigniskategorie	**Reaktive Gegenmaßnahmen**
0	Keine
1	Keine. Bei einem Ausbruch siehe Schadcodeereigniskategorie 4
2	Kontrollmaßnahmen durch den behördlichen Virenschutzadministrator mittels des zentralen Virenschutzmanagementtools. Nachprüfung eines betroffenen Endgeräts durch nach [X] Tagen. Server und alle Systeme mit hohem Schutzbedarf in einem der primären Informationssicherheitswerte müssen durch den Fachbereich grundsätzlich neu installiert werden.
3	Alle Gegenmaßnahmen von 2 werden umgesetzt. Zusätzlich Anfrage nach Signaturupdate beim Antivirenhersteller. Zusätzlich formale oder freie Forensik auf besonderen Bedarf nach Weisung durch den ISB. .
4	Alle Gegenmaßnahmen von 3 werden umgesetzt. Zusätzlich freie Ursachenforschung durch z.B. durch den behördlichen Virenschutzadministrator und Ausarbeitung möglicher nötiger Gegenmaßnahmen, nebst anschließender Umsetzung eventueller Gegenmaßnahmen .
5	Alle Gegenmaßnahmen von 3 und 4 werden umgesetzt. Zusätzlich wird nach entsprechendem Auftrag durch die betroffene Behörde mindestens ein

	Referenzsystem durch den behördlichen Virenschutzadministrator untersucht.
6	Alle Gegenmaßnahmen von 3, 4 und 5 werden umgesetzt. Zusätzlich werden der jeweilige Krisenprozess bzw. der jeweilige behördliche Notfallplan initiiert.
7	Alle Gegenmaßnahmen von 3, 4, 5 und 6 werden umgesetzt.