|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Schutz vor Schadprogrammen"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300011 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc79384722)

[Dokumentenhistorie 3](#_Toc79384723)

[Inhaltsverzeichnis 4](#_Toc79384724)

[Allgemeine Festlegungen 5](#_Toc79384725)

[Ziel / Zweck 5](#_Toc79384726)

[Geltungsbereich 5](#_Toc79384727)

[Zuständigkeiten 5](#_Toc79384728)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79384729)

[Aufbau des Dokuments 6](#_Toc79384730)

[Sicherheitsrichtlinie „Schutz vor Schadprogrammen" 7](#_Toc79384731)

[Basismaßnahmen 7](#_Toc79384732)

[Erstellung eines Konzepts für den Schutz vor Schadprogrammen (OPS.1.1.4.A1) 7](#_Toc79384733)

[Nutzung systemspezifischer Schutzmechanismen (OPS.1.1.4.A2) 7](#_Toc79384734)

[Auswahl eines Virenschutzprogrammes für Endgeräte (OPS.1.1.4.A3) 7](#_Toc79384735)

[Auswahl eines Virenschutzprogrammes für Gateways und IT-Systeme zum Datenaustausch (OPS.1.1.4.A4) 7](#_Toc79384736)

[Betrieb und Konfiguration von Virenschutzprogrammen (OPS.1.1.4.A5) 7](#_Toc79384737)

[Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen (OPS.1.1.4.A6) 8](#_Toc79384738)

[Sensibilisierung und Verpflichtung der Benutzer (OPS.1.1.4.A7) 8](#_Toc79384739)

[Standardmaßnahmen 9](#_Toc79384740)

[Nutzung von Cloud-Diensten zur Detektionsverbesserung (OPS.1.1.4.A8) 9](#_Toc79384741)

[Meldung von Infektionen mit Schadprogrammen (OPS.1.1.4.A9) 9](#_Toc79384742)

[Maßnahmen zur Minimierung des Infektionsrisikos (OPS.1.1.4.bd.A1) 9](#_Toc79384743)

[Anforderungen an das Reporting (OPS.1.1.4.bd.A2) 10](#_Toc79384744)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc79384745)

[Nutzung spezieller Analyseumgebungen (OPS.1.1.4.A10 - CA) 10](#_Toc79384746)

[Einsatz mehrerer Scan-Engines (OPS.1.1.4.A11 - C) 10](#_Toc79384747)

[Einsatz von Datenträgerschleusen (OPS.1.1.4.A12 - CA) 11](#_Toc79384748)

[Umgang mit nicht vertrauenswürdigen Dateien (OPS.1.1.4.A13 - C) 11](#_Toc79384749)

[Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (OPS.1.1.4.A14 - CIA) 11](#_Toc79384750)

[Externe Beratung zum Schutz vor Schadprogrammen (OPS.1.1.4.A15 - C) 11](#_Toc79384751)

# Allgemeine Festlegungen

## Ziel / Zweck

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung des Benutzers schädliche Funktionen auf einem IT-System ausführen. Diese Schadfunktionen können ein breites Feld abdecken, das von Spionage über Erpressung (sogenannte Ransomware) bis hin zur Sabotage und Zerstörung von Informationen oder gar Geräten reicht.

Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen ausgeführt werden. Dazu gehören neben klassischen IT-Systemen wie Clients und Servern auch mobile Geräte wie Smartphones. Netzkomponenten, wie Router und sogar IoT-Geräte, wie vernetzte Kameras, sind heutzutage ebenfalls vielfach durch Schadprogramme gefährdet.

Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Smartphones werden in der Regel über die Installation von schädlichen Apps infiziert, auch Drive-by-Downloads sind möglich. Darüber hinaus sind offene Netzschnittstellen, fehlerhafte Konfigurationen und Softwareschwachstellen häufige Einfallstore auf allen IT-Systemen.

In dieser Sicherheitsrichtlinie wird der Begriff „Virenschutzprogramm“ verwendet. „Viren“ stehen dabei als Synonym für alle Arten von Schadprogrammen. Gemeint ist mit „Virenschutzprogramm“ demnach ein Programm zum Schutz vor jeglicher Art von Schadprogrammen. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines OPS.1.1.4 "Schutz vor Schadprogrammen" beachtet.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument „Sicherheitsrichtlinie Schutz vor Schadprogrammen“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Schutz vor Schadprogrammen"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Erstellung eines Konzepts für den Schutz vor Schadprogrammen (OPS.1.1.4.A1)

Es ist ein Konzept für den Schutz vor Schadprogrammen (Malware) zu erstellen, welches aufzeigt wie IT-Systeme und Anwendungen durch eine verwaltete mehrstufige Multilayer Anti-Threat-Infrastruktur geschützt werden sollen. Außerdem muss in dem Konzept festgehalten werden, wie auf welchem Layer mit welchen Technologienwerden der Schutz zu erfolgen hat. Ist kein verlässlicher Schutz möglich, so sollten die identifizierten IT-Systeme nicht betrieben werden. Das Konzept sollte nachvollziehbar dokumentiert und aktuell gehalten werden.

### Nutzung systemspezifischer Schutzmechanismen (OPS.1.1.4.A2)

Zum Schutz vor Schadprogrammen ist eine verwaltete mehrstufige Multilayer Anti-Threat-Infrastruktur aufzubauen. In diese sind alle Systeme mit einem entsprechenden Schutzbedarf integriert und aktiviert.

In Fällen, in denen das zentrale System nicht genutzt werden kann, müssen Schutzmechanismen genutzt werden, die das Betriebssystem bzw. die installierten Anwendungen bieten. Die Auswahl und das Vorgehen sind für jedes System zu dokumentieren.

### Auswahl eines Virenschutzprogrammes für Endgeräte (OPS.1.1.4.A3)

Bei der Auswahl des Virenschutzprogramm sind die zu unterstützenden Betriebssysteme sowie die Service- und Supportleistungen des Herstellers sowie die Kompatibilitäten zu der Lösung der mehrstufigen Multilayer Anti-Threat-Infrastruktur zu berücksichtigen.

Es dürfen nur Produkte für den Enterprise-Bereich mit auf die <Institution> zugeschnittene Service- und Supportleistungen eingesetzt werden. Produkte für reine Heimanwender oder Produkte ohne Herstellersupport dürfen nicht eingesetzt werden. Es dürfen nur Cloud-Funktionen solcher Produkte verwendet werden, bei denen keine gravierenden und nachweisbaren Datenschutzaspekte dagegensprechen.

### Auswahl eines Virenschutzprogrammes für Gateways und IT-Systeme zum Datenaustausch (OPS.1.1.4.A4)

Alle Gateways und IT-Systeme, die dem Datenaustausch dienen, sind ebenfalls in die zentral verwaltete mehrstufige Multilayer Anti-Threat-Infrastruktur zu integrieren und zu aktivieren.

### Betrieb und Konfiguration von Virenschutzprogrammen (OPS.1.1.4.A5)

Das Virenschutzprogramm ist entsprechend seiner Einsatzumgebung auf dem Zielsystem installiert, konfiguriert und aktiviert. Die maximale Erkennungsleistung steht dabei im Vordergrund.

In begründeten Fällen, in denen die Leistung im Vordergrund steht oder der Datenschutz beeinträchtigt wird, können Funktionen abgeschaltet werden. Sofern Funktionen zur Verbesserung der Performance aktiviert werden, ist dieses Vorgehen zu dokumentieren.

Die fehlerfreie und sichere Konfiguration aller Virenschutzprogramme ist die wesentliche Voraussetzung für einen wirksamen Schutz der bedrohten Systeme. Es gelten folgende allgemeinen Mindestvorgaben:

* Aktivierter Hintergrundprozess „Scan bei Zugriff“ für lesenden und schreibenden Zugriff
* Überprüfung aller Dateien
* Überprüfung von Archiven (Verschachtelungstiefe der Archive mindestens 5 maximal 20 Ebenen)
* Automatisierte, stündliche Prüfung auf aktuelle Signaturen und Konfigurationsrichtlinien
* Automatisierte Richtliniendurchsetzung im Intervall von 5 Minuten
* Verweigerung des Zugriffs auf infizierte Dateien
* Bei fehlgeschlagener Bereinigung durch den Benutzer wird die Datei in einen Quarantäne-Bereich verschoben
* Protokollierung und Meldung jeder Warnung, Fehlfunktion oder Infektion an zentrale Management-Server

Es gelten die folgenden abweichenden Vorgaben für die Systeme zum Zwecke eines Dateiaustausches:

* Kein aktivierter Hintergrundprozess „Scan im Zugriff“
* Bei fehlgeschlagener Bereinigung muss anstelle der Quarantäne gelöscht werden

Mobile Datenträger wie beispielsweise Wechseldatenträger mit USB- oder Firewire-Anschlüssen und CD-, DVD- und Blu-Ray-Medien umgehen die Virenprüfung der schützenden Perimeter-Systeme. Von diesen Medien geht daher ein erhöhtes Risiko für Infektionen der internen Systeme aus. Der Zugriff auf diese Medien ist durch den Zugriffs-Scanner der Virenschutzprogramme abzusichern.

### Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme und Signaturen (OPS.1.1.4.A6)

Die Virenschutzprogramme und deren Signaturen werden nach Herstellervorgeben aktualisiert. Vor der Produktivsetzung erfolgen Tests.

Nach dem Update des Virenschutzprogramms werden die Konfigurationseinstellungen mit den dokumentierten Vorgaben abgeglichen.

Alle Änderung an dem Virenschutzprogramm sind dokumentiert.

### Sensibilisierung und Verpflichtung der Benutzer (OPS.1.1.4.A7)

Die Mitarbeitenden sind regelmäßig über die Bedrohung durch Schadprogramme zu schulen. Sie müssen die grundlegenden Verhaltensregeln einhalten, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien aus nicht vertrauenswürdigen Quellen sollten nicht geöffnet werden.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Nutzung von Cloud-Diensten zur Detektionsverbesserung (OPS.1.1.4.A8)

Sofern keine Datenschutzaspekte dagegensprechen, ist die Nutzung von Clouddiensten zur Verbesserung der Detektionsleistung zu prüfen und dokumentiert einzusetzen.

### Meldung von Infektionen mit Schadprogrammen (OPS.1.1.4.A9)

Das eingesetzte Virenschutzprogramm sollten eine Infektion mit einem Schadprogramm automatisch blockieren und melden. Die automatische Meldung muss an einer zentralen Stelle angenommen werden. Dabei sollten die zuständigen Mitarbeitenden je nach Sachlage über das weitere Vorgehen entscheiden.

Unabhängig von der automatischen Meldung sollte sich jedoch auch der Mitarbeitende an die ihm benannten Ansprechpartner wenden, wenn der Verdacht auf eine Infektion mit einem Schadprogramm besteht. Das Vorgehen bei Meldungen und Alarmen der Virenschutzprogramme sollte geplant, dokumentiert und getestet werden. Es sollte insbesondere geregelt sein, was im Falle einer bestätigten Infektion geschehen soll.

Prozesse regeln, wie mit dem betroffenen System umzugehen ist.

### Maßnahmen zur Minimierung des Infektionsrisikos (OPS.1.1.4.bd.A1)

Um die Gefahr einer Infizierung von Arbeitsplatzrechners der <Institution> oder eine Kompromittierung von Infrastrukturkomponenten zu reduzieren, sollen alle Mail-Anhänge, welche nicht den freigegebenen Dateiformaten entsprechen in die Quarantäne gestellt und nach 16 Tagen gelöscht werden.

Unter Berücksichtigung, welche Dateiformate bei der Kommunikation eines Mitarbeitenden mit seinen Partnern ausgetauscht werden, sind wie folgt erlaubt:

* \*.xlsx,
* \*.docx,
* \*.pdf,
* \*.txt,
* \*.ppt, \*.pptx,
* \*.png,
* \*.gif,
* \*.jpg und
* Passwortgeschützte und nicht geschützte Zip und 7-Zip-Archive.

### Anforderungen an das Reporting (OPS.1.1.4.bd.A2)

Sämtliche Virenschutzprogramme müssen ihren aktuellen Status und Warnungen an zentrale Virenschutzmanagementsysteme melden. An die protokollierten Informationen werden folgende Mindestanforderungen gestellt.

Allgemeine Statusinformationen:

* Eindeutige Identifikation des Systems (IP-Adresse und Hostname)
* Eindeutige Identifikation der Viren-Signatur
* Datum und Uhrzeit der Installation der aktuell verwendeten Signatur
* Status und zurückliegende Aktivitäten des Virenscanners
* Start- und Stopp-Zeitpunkte des Virenscannerdienstes
* Sämtliche Fehlermeldungen (bspw. Gescheiterte Aktualisierungen der Signaturen, unvorhergesehene Beendigung des Virenscannerdienstes etc.)

Zusätzliche Informationen im Falle einer Infektion:

* Name des Virus
* Datum und Uhrzeit des Virenfundes
* Eindeutige Pfadangabe der infizierten Daten
* Ausgeführte Aktionen nach Identifikation des Virus
* Ergebnis der ausgeführten Aktionen

Bei Eintritt eines Sicherheitsvorfalls durch eine Vireninfektion sollte der <Informationssicherheitsbeauftragter> und der <Helpdesk> umgehend per E-Mail bzw. telefonischer Meldung in Kenntnis gesetzt werden.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Nutzung spezieller Analyseumgebungen (OPS.1.1.4.A10 - CA)

Automatisierte Analysen in einer speziellen Testumgebung (basierend auf Sandboxen bzw. separaten virtuellen oder physischen Systemen) sollten für eine Bewertung von verdächtigen Dateien ergänzend herangezogen werden.

### Einsatz mehrerer Scan-Engines (OPS.1.1.4.A11 - C)

Zur Verbesserung der Erkennungsleistung sollten für besonders schutzwürdige IT-Systeme, wie Gateways und IT-Systeme zum Datenaustausch, Virenschutzprogramme mit mehreren alternativen Scan-Engines eingesetzt werden.

### Einsatz von Datenträgerschleusen (OPS.1.1.4.A12 - CA)

Bevor insbesondere Datenträger von Dritten mit den IT-Systemen der <Institution> verbunden werden, sollten diese durch eine Datenträgerschleuse geprüft werden.

### Umgang mit nicht vertrauenswürdigen Dateien (OPS.1.1.4.A13 - C)

Ist es notwendig, nicht vertrauenswürdige Dateien zu öffnen, sollte dies nur auf einem isolierten IT-System geschehen. Die betroffenen Dateien sollten dort z. B. in ein ungefährliches Format umgewandelt werden, wenn sich hierdurch das Risiko einer Infektion durch Schadsoftware verringert.

### Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (OPS.1.1.4.A14 - CIA)

Der Einsatz sowie der Mehrwert von Produkten und Services, die im Vergleich zu herkömmlichen Virenschutzprogrammen einen erweiterten Schutzumfang bieten, sollte geprüft werden. Solche Sicherheitsprodukte gegen gezielte Angriffe sollten z. B. bei der Ausführung von Dateien in speziellen Analyseumgebungen, bei der Härtung von Clients oder bei der Kapselung von Prozessen eingesetzt werden. Vor einer Kaufentscheidung für ein Sicherheitsprodukt sollten Schutzwirkung und Kompatibilität zur eigenen IT-Umgebung getestet werden.

### Externe Beratung zum Schutz vor Schadprogrammen (OPS.1.1.4.A15 - C)

Bei der Erstellung eines Konzepts zum Schutz vor Schadprogrammen sollte externe Unterstützung in Anspruch genommen werden, wenn das eigene Know-how oder die Marktkenntnis nicht ausreichen. Um insbesondere Leistungsproblemen innerhalb der IT-Systeme und Netze sowie in PaaS und IaaS Infrastrukturen vorzubeugen und den Schutz vor Schadprogrammen sinnvoll in ein Gesamtkonzept einzufügen, sollte in komplexen IT-Infrastrukturen die Implementierung von Schutzprodukten nur durch erfahrene Administratoren oder Dienstleister vorgenommen werden.

Nach der Inbetriebnahme einer Anti-Threat-Infrastruktur sollte die Konfiguration einem externen Expertenreview unterzogen werden und alle Audit-Ergebnisse der Risikoanalyse übergeben werden.