Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.4 Schutz vor Schadprogrammen

1. Beschreibung

1.1. Einleitung

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung der Benutzenden 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, Industriesteuerungsanlagen 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 diesem Baustein 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.

1.2. Zielsetzung

Dieser Baustein beschreibt Anforderungen, die zu erfüllen und umzusetzen sind, um eine Institution effektiv gegen Schadprogramme zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* ist einmal auf den Informationsverbund anzuwenden.

In diesem Baustein werden die allgemeinen Anforderungen für den Schutz gegen Schadprogramme beschrieben. Spezifische Anforderungen, um bestimmte IT-Systeme der Institution vor

Schadprogrammen zu schützen, finden sich bei Bedarf in den jeweiligen Bausteinen der Schicht SYS *IT-Systeme*. Führt ein identifiziertes Schadprogramm zu einem Sicherheitsvorfall, sollten die Anforderungen des Bausteins DER.2.1 *Behandlung von Sicherheitsvorfällen* berücksichtigt werden. Die Anforderungen des Bausteins DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* helfen dabei, identifizierte Schadprogramme zu entfernen und einen bereinigten Zustand wiederherzustellen.

Die im Rahmen dieses Bausteins eingesetzten Virenschutzprogramme sollten grundsätzlich auch im Patch- und Änderungsmanagement (OPS.1.1.3 *Patch- und Änderungsmanagement*) berücksichtigt werden. Weiterhin sollte das Thema Schutz vor Schadprogrammen im Rahmen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und CON.3 *Datensicherungskonzept* mit berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* von besonderer Bedeutung.

2.1. Softwareschwachstellen und Drive-by-Downloads

Sind IT-Systeme nicht ausreichend vor Schadprogrammen geschützt, können Softwareschwachstellen bei Angriffen ausgenutzt werden, um Schadcode auszuführen. Dies kann unter anderem passieren, wenn Patches nicht zeitnah eingespielt und Schutzmechanismen von Anwendungsprogrammen, wie Browsern, nicht richtig konfiguriert sind. Bei den sogenannten Drive-by-Downloads reicht es beispielsweise aus, eine mit Schadcode behaftete Website zu besuchen. Eine Schwachstelle im Browser oder in einem installierten Plug-in, wie Java oder Adobe Flash, kann dann ausgenutzt werden, um das IT-System zu infizieren und Angreifenden umfangreiche Kontrolle sowie einen Zugang zum Netz einer Institution zu verschaffen. Besonders gefährdet sind hier IT-Systeme, die nicht regelmäßig aktualisiert werden, z. B. viele Smartphones.

2.2. Erpressung durch Ransomware

Eine weitverbreitete Art von Schadprogrammen ist die sogenannte Ransomware. Diese verschlüsselt die Daten des infizierten IT-Systems sowie häufig auch weitere Daten, die etwa über Netzfreigaben erreichbar sind. In der Regel verwenden die Angreifenden dabei Verschlüsselungsmethoden, die ohne Kenntnis des Schlüssels nicht umkehrbar sind, und erpressen damit ihre Opfer um hohe Geldsummen. Besteht kein wirksamer Schutz gegen Schadprogramme und sind keine ergänzenden Vorkehrungen, wie Datensicherungen, getroffen, kann die Verfügbarkeit von Informationen erheblich eingeschränkt werden, Daten können verloren gehen, sowie massive finanzielle und Image-Schäden können eintreten.

2.3. Gezielte Angriffe und Social Engineering

Institutionen werden häufig mit maßgeschneiderten Schadprogrammen angegriffen. Dabei werden z. B. Führungskräfte über Methoden des Social Engineerings dazu verleitet, schädliche E-Mail-Anhänge zu öffnen. Maßgeschneiderte Schadprogramme können zudem häufig nicht unmittelbar von Virenschutzprogrammen erkannt werden. Auch die Personalabteilung einer Institution kann beispielsweise ein Angriffsziel sein, indem etwa mit Schadsoftware infizierte Bewerbungsunterlagen auf elektronischem Wege zugesendet werden. Konnten die Angreifenden auf diese Weise ein IT-System infizieren, so können sie sich innerhalb der Institution ausbreiten und beispielsweise Informationen einsehen, manipulieren oder zerstören.

2.4. Botnetze

Über Schadprogramme können IT-Systeme einer Institution Teil von sogenannten Botnetzen werden. Angreifende, die in einem solchen Botnetz häufig tausende von Systemen kontrollieren, können diese beispielsweise einsetzen, um Spam zu versenden oder verteilte Denial-of-Service (DDoS)-Angriffe auf Dritte zu starten. Auch wenn die eigene Institution möglicherweise nicht unmittelbar geschädigt wird, kann sich dies trotzdem negativ bezüglich der Verfügbarkeit und Integrität der eigenen Dienste und IT-Systeme auswirken und sogar rechtliche Probleme nach sich ziehen. Wenn z. B. der E-Mail-Server einer Institution auf eine Blockliste gelangt, ist möglicherweise kein Versand und Empfang von E-Mails mehr möglich.

2.5. Infektion von Produktionssystemen und IoT-Geräten

Neben klassischen IT-Systemen werden vermehrt auch Geräte durch Schadprogramme angegriffen, die auf den ersten Blick nicht wie offensichtliche Ziele aussehen. Bei einem Angriff könnte beispielsweise eine über das Internet erreichbare Überwachungskamera infiziert werden, um in der Institution zu spionieren. Aber auch eine vernetzte Glühbirne oder eine Kaffeemaschine mit App-Steuerung kann als Eintrittspunkt in das Netz der Institution oder als Teil eines Botnetzes dienen, wenn diese Geräte nicht ausreichend vor Schadprogrammen geschützt werden. Vernetzte Produktionssysteme oder Industriesteuerungen können ebenfalls durch Schadprogramme manipuliert oder sogar zerstört werden, was Ausfälle und viele weitere Gefährdungen für die Institution und ihre Mitarbeitenden, z. B. durch Brände, nach sich ziehen kann.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.*1.1.4 Schutz vor Schadprogrammen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

Es MUSS ein Konzept erstellt werden, das beschreibt, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Hierbei MÜSSEN auch IoT-Geräte und Produktionssysteme berücksichtigt werden. Außerdem MUSS festgehalten werden, wie 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.

OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen (B)

Es MUSS geprüft werden, welche Schutzmechanismen die verwendeten IT-Systeme sowie die darauf genutzten Betriebssysteme und Anwendungen bieten. Diese Mechanismen MÜSSEN genutzt werden, sofern es keinen mindestens gleichwertigen Ersatz gibt oder gute Gründe dagegen sprechen. Werden sie nicht genutzt, MUSS dies begründet und dokumentiert werden.

OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes (B)

Abhängig vom verwendeten Betriebssystem, anderen vorhandenen Schutzmechanismen sowie der Verfügbarkeit geeigneter Virenschutzprogramme MUSS für den konkreten Einsatzzweck ein entsprechendes Schutzprogramm ausgewählt und installiert werden. Für Gateways und IT-Systeme, die dem Datenaustausch dienen, MUSS ein geeignetes Virenschutzprogramm ausgewählt und installiert werden.

Es DÜRFEN NUR Produkte für den Enterprise-Bereich mit auf die Institution zugeschnittenen Service- und Supportleistungen eingesetzt werden. Produkte für die reine Heimanwendung oder Produkte ohne Support DÜRFEN NICHT im professionellen Wirkbetrieb eingesetzt werden.

Cloud-Dienste zur Verbesserung der Detektionsleistung der Virenschutzprogramme SOLLTEN genutzt werden. Falls Cloud-Funktionen solcher Produkte verwendet werden, MUSS sichergestellt werden, dass dies nicht im Widerspruch zum Daten- oder Geheimschutz steht. Neben Echtzeit- und On-Demand-Scans MUSS eine eingesetzte Lösung die Möglichkeit bieten, auch komprimierte Daten nach Schadprogrammen zu durchsuchen.

OPS.1.1.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

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

Das Virenschutzprogramm MUSS für seine Einsatzumgebung geeignet konfiguriert werden. Die Erkennungsleistung SOLLTE dabei im Vordergrund stehen, sofern nicht Datenschutz- oder Leistungsgründe im jeweiligen Einzelfall dagegen sprechen. Wenn sicherheitsrelevante Funktionen des Virenschutzprogramms nicht genutzt werden, SOLLTE dies begründet und dokumentiert werden. Bei Schutzprogrammen, die speziell für die Desktop-Virtualisierung optimiert sind, SOLLTE nachvollziehbar dokumentiert sein, ob auf bestimmte Detektionsverfahren zugunsten der Leistung verzichtet wird. Es MUSS sichergestellt werden, dass die Benutzenden keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können.

OPS.1.1.4.A6 Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme (B)

Auf den damit ausgestatteten IT-Systemen MÜSSEN die Virenschutzprogramme nach Empfehlung der herstellenden Institution regelmäßig und zeitnah aktualisiert werden.

OPS.1.1.4.A7 Sensibilisierung und Verpflichtung der Benutzenden (B) [Benutzende]

Benutzende MÜSSEN regelmäßig über die Bedrohung durch Schadprogramme aufgeklärt werden. Sie MÜSSEN die grundlegenden Verhaltensregeln einhalten, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien, E-Mails, Webseiten usw. aus nicht vertrauenswürdigen Quellen SOLLTEN NICHT geöffnet werden. Sie MÜSSEN entsprechenden Kontaktpersonen für den Fall eines Verdacht auf eine Infektion mit einem Schadprogramm bekannt sein. Sie MÜSSEN sich an die ihnen benannten Kontaktpersonen wenden, wenn der Verdacht auf eine Infektion mit einem Schadprogramm besteht.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.4.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen (S) [Benutzende]

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

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.4.A10 Nutzung spezieller Analyseumgebungen (H)

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.

OPS.1.1.4.A11 Einsatz mehrerer Scan-Engines (H)

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.

OPS.1.1.4.A12 Einsatz von Datenträgerschleusen (H)

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

OPS.1.1.4.A13 Umgang mit nicht vertrauenswürdigen Dateien (H)

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 oder ausgedruckt werden, wenn sich hierdurch das Risiko einer Infektion durch Schadsoftware verringert.

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

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.

OPS.1.1.4.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.12.2 „protection from malware“, Vorgaben für den Schutz vor Schadprogrammen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“, insbesondere Area TS1 Security Solutions, Vorgaben für den Schutz vor Schadprogrammen.