Dokumentenstatus

Dokumententitel	Leitlinie Schutz vor Malware
Referenz ISO 27001	A.12.2
Dateiname	Leitlinie Schutz vor Malware.docx
Version	1.0
Letzter Ausdruck	

Änderungsvermerke

Version	Datum	Beschreibung	Autoren
1.0	19.02.2015	Initiale Version	Genter / Tholen

Freigabevermerke

Version	Datum	Beschreibung	Freigabe
1.0	01.11.2018	Abstimmung in der IT-SIKO 2018	IT-Sicherheitskonferenz
1.0	30.11.2018	Freigabe durch den ITSB	Joachim Bareiß

1. Geltungsbereich

Diese Leitlinie gilt für den gesamten Geltungsbereich des Informationssicherheits-Managementsystems (ISMS) des SWR.

2. Rollen und Verantwortlichkeiten

Die Rollen und Verantwortlichkeiten dieser Leitlinie sind im ISMS des SWR definiert.

3. Zielsetzung

Die IT-Systeme und IT-Datenbestände sind vor Malware zu schützen.

4. Maßnahmen

Es sind Erkennungs-, Präventions- und Wiederherstellungsmaßnahmen nach dem Stand der Technik zum Schutz vor Malware in Verbindung mit einer angemessenen Sensibilisierung der Benutzer zu implementieren.

Dieses Dokument gehört zum ISMS des SWR. Weitergehende Veröffentlichungen, Nachdruck, Vervielfältigungen oder Speicherung — gleich in welcher Form, ganz oder teilweise — sind nur mit Zustimmung des SWR zulässig.

4.1 Erkennung

Es sind Maßnahmen zu ergreifen, die eine Erkennung von Malware ermöglichen. Diese sind mit Hilfe von ständiger Informationsbeschaffung kontinuierlich zu optimieren. Dies beinhaltet z.B. die aktuelle Pflege von Positiv- und Negativlisten sowie von Schutzregeln, um eine Malware als solche zu erkennen.

4.2 Prävention

Sämtliche Datenquellen (physisch und netzwerkgebunden, also z.B. Speichermedien, E-Mail, Internetdienste) sind vor ihrer Verwendung auf Malware zu überprüfen.

4.3 Wiederherstellung

Vor der Einleitung von Wiederherstellungsmaßnahmen sind im Rahmen der Untersuchung des Vorfalls nach eigenem Ermessen in angemessenem Umfang Beispieldateien, Quelltexte und Datenspuren zu sichern, um die aktuellen Erkennungsmaßnahmen zu verbessern.

Im Rahmen der Wiederherstellungsmaßnahmen hat der Schutz vernetzter IT-Systeme Vorrang vor der Wiederherstellung der Betriebskontinuität eines einzelnen Systems.

4.4 Sensibilisierung

Die Wirksamkeit der Maßnahmen zum Schutz vor Malware ist organisatorisch zu unterstützen. Dies betrifft insbesondere die Nutzersensibilisierung, die Eigenverantwortung sowie Schulungen. Auffälligkeiten und Malware-Verdachtsfälle sind umgehend dem IT-Betrieb zu melden.

Baden-Baden, den 12.01.2018

Joachim Bareiß
IT-Sicherheitsbeauftragter

Dieses Dokument gehört zum ISMS des SWR. Weitergehende Veröffentlichungen, Nachdruck, Vervielfältigungen oder Speicherung — gleich in welcher Form, ganz oder teilweise — sind nur mit Zustimmung des SWR zulässig.