Dokumentenstatus

Dokumententitel	Leitlinie IT-Sicherheit Lieferanten
Referenz	ISO 27001 - A.15.1.2 / IT-Grundschutz
Dateiname	Leitlinie IT-Sicherheit Lieferanten.docx
Version	1.2a
Letzter Ausdruck	
Quelle	UPKRITIS Best Practice Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in kritischen Infrastrukturen, www.upkritis.de – Stand: Juni 2017

Änderungsvermerke

Version	Datum	Beschreibung	Autoren
1.0		Initiale Version	W. Strobel / M. Genter
1.1	02.11.2018	Aktualisierung bzgl. Datenschutz	Prof. Dr. Herb
1.2a	24.05.2019	Überarbeitung	W. Strobel / M. Genter

Freigabevermerke

Version	Datum	Beschreibung	Freigabe
1.1	01.11.2018	Abstimmung in der IT-SIKO 2018	IT-Sicherheitskonferenz
1.1	30.11.2018	Freigabe durch IT-Sicherheitsbeauftragten	Joachim Bareiß
1.2a	01.07.2019	Abstimmung Mitglieder IT-Sicherheitskonferenz	IT-Sicherheitskonferenz

Anforderungen zur IT-Sicherheit an Lieferanten des SWR

Ziel dieses Dokumentes ist die Berücksichtigung der IT-Sicherheit des SWR als Betreiber einer kritischen Infrastruktur. Es soll Lieferanten von IT-Produkten, IT-Systemen, Software oder IT-Dienstleistungen einen Überblick über die beim Südwestrundfunk geltenden Anforderungen zur IT-Sicherheit geben.

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.

1. Inhaltsverzeichnis

2. Anwendungsbereich 3
3. Rollen und Verantwortlichkeiten 3
3.1 Allgemeine Verantwortlichkeit des Auftragnehmers 3
4. Schwachstellen-Management 3
4.1 Methodik und Umfang 4
5. Softwareaktualisierung 4
5.1 Umfang 4
5.2 Patch-Level während einer Systemabnahme 4
5.3 Patch-Management nach einer Systemabnahme 4
5.3.1 Produkt-Lebenszyklus 4
5.3.2 Ende des Produktlebenszyklus 4
5.3.3 Lieferanten von reinen Anwendungen oder Funktionalitäten 5
6. Systemhärtung 5
6.1 Minimale Installationsprinzipien 5
6.2 Netzwerkdienste (Netzwerkzugänge) 5
6.3 Standardpasswörter 5
6.4 Backdoors 6
6.5 Kontrolle und Audit der in diesem Kapitel genannten Konditionen 6
7. Fernzugang für Drittanbieter 6
7.1 Allgemeine Verantwortung 6
7.2 Benutzerverwaltung 6
8. Einsatz von Verschlüsselungs-Technologien 7
9. Sicherheitsanforderungen für einen IT-Betrieb 7
10. Benachrichtigung über sicherheits- und datenschutzrelevante Vorfälle 7

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.

2. Anwendungsbereich

Für Auftragnehmer des SWR gelten die folgenden grundsätzlichen Anforderungen:

- Schwachstellen-Management (Kapitel 4)
- Softwareaktualisierung (Kapitel 5)
- Systemhärtung (Kapitel 6)
- Fernzugang für Drittanbieter (Kapitel 7)
- Einsatz von Verschlüsselungs-Technologien (Kapitel 8)
- Sicherheitsanforderungen für einen IT-Betrieb (Kapitel 9)
- Benachrichtigung über sicherheitsrelevante Vorfälle (Kapitel 10)

3. Rollen und Verantwortlichkeiten

3.1 Allgemeine Verantwortlichkeit des Auftragnehmers

Generell ist es die Verantwortung eines Auftragnehmers, die durch den Südwestrundfunk geltenden Anforderungen zur Gewährleistung der IT-Sicherheit einzuhalten.

Der Auftragnehmer ist dafür verantwortlich, dass Subunternehmer, die Teile der Dienstleistung des Auftragnehmers erbringen oder wesentliche Bedeutung für die Erbringung der Dienstleistung haben, diese Anforderungen auch einhalten.

4. Schwachstellen-Management

Auftragnehmer müssen ihre Produkte einer kontinuierlichen Prüfung auf Schwachstellen unterziehen, um in der Lage zu sein, so schnell wie möglich zu reagieren.
Sind vom Auftragnehmer entwickelte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der Auftragnehmer verpflichtet, die Schwachstellen an den Auftrag-geber zu melden.

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 Methodik und Umfang

Jede bekannte Schwachstelle muss vom Auftragnehmer an den Auftraggeber gemeldet und bzgl. möglicher funktionaler und sicherheitsrelevanter Auswirkungen bewertet werden.

5. Softwareaktualisierung

5.1 Umfang

Vom Auftragnehmer gelieferte Software oder Systeme müssen kontinuierlich aktualisiert werden. Dazu gehören in der Regel:

- Betriebssystem
- Alle Softwarepakete und Dienste, die Teil des Betriebssystems sind
- Alle Werkzeuge und Anwendungen, die der Hersteller zu Betriebs- und Wartungszwecken installiert hat
- Zusätzliche Systemkomponenten, wie z.B. Datenbanken oder Monitoring-Lösungen

Art und Umfang des Aktualisierungsprozesses muss zwischen Auftragnehmer und Auftraggeber abgestimmt und dokumentiert werden.

5.2 Patch-Level während einer Systemabnahme

Der Auftragnehmer hat sicherzustellen, dass alle von ihm gelieferten Systeme vor der Abnahme aktualisiert werden. Der Patch-Level sollte dabei so aktuell wie möglich sein.

5.3 Patch-Management nach einer Systemabnahme

5.3.1 Produkt-Lebenszyklus

Der Auftragnehmer muss eine Aussage zur Bereitstellung von Aktualisierungen für die gesamte Produktlebensdauer seiner gelieferten Systeme treffen. Die Gesamtproduktlebensdauer ist festzulegen.

5.3.2 Ende des Produktlebenszyklus

Sollte es zu der Situation kommen, in der der Drittanbieter eines Betriebssystems oder einer anderen Komponente (Software, Datenbanken, Anwendungen, etc.) das Ende des Lebenszyklus verkündet, ist der Auftragnehmer verpflichtet, die Komponente auf die aktualisierte neuere Version zu erweitern, eine adäquate Alternative einzusetzen oder den

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.

weiteren Support von Aktualisierungen für die ältere Version vertraglich mit dem Drittanbieter sicherstellen.

5.3.3 Lieferanten von reinen Anwendungen oder Funktionalitäten

In Fällen, in denen der Auftragnehmer nur Anwendungen und/ oder andere Funktionalitäten liefert und der Südwestrundfunk für das Update-Management auf den darunterliegenden Schichten wie Betriebssystem verantwortlich ist, muss der Auftragnehmer eine kontinuierliche Funktionsfähigkeit seiner gelieferten Leistung auch bei Patches der darunterliegenden Systemplattform gewährleisten.

6. Systemhärtung

Der Auftragnehmer verpflichtet sich, die von ihm gelieferten Systeme zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren. Dies muss vor der Erklärung einer Systemabnahme durch den Auftraggeber geschehen sein.

6.1 Minimale Installationsprinzipien

Es dürfen ausschließlich Software-Komponenten installiert werden, die für den anforderungsgemäßen Betrieb des Systems erforderlich sind.

Grundsätzlich erweitert jede zusätzliche Software-Installationen die Angriffsfläche. Im Rahmen der Härtung müssen nicht benötigte Komponenten entfernt oder deaktiviert werden.

Jede andere Software darf nicht installiert werden, außer der Auftragnehmer und der Südwestrundfunk einigen sich darüber.

6.2 Netzwerkdienste (Netzwerkzugänge)

Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss deaktiviert sein. Die Nutzung jedes Zugangs muss in der Dokumentation des Auftragnehmers erläutert werden.

6.3 Standardpasswörter

Der Auftragnehmer stellt sicher, dass jedes Standardpasswort in allen möglichen Fällen geändert werden kann. Im Software-Quellcode fest verankerte Passwörter sind nicht erlaubt.

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.

6.4 Backdoors

Der Auftragnehmer muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors“ sind, die die verwendeten Sicherheitsmechanismen umgehen können.

6.5 Kontrolle und Audit der in diesem Kapitel genannten Konditionen

Der Auftragnehmer verpflichtet sich, dass er hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen, die mit dem Auftraggeber abzustimmen sind, nachweist, dass alle in diesem Kapitel genannten Anforderungen eingehalten werden.

7. Fernzugang für Drittanbieter

Fernzugänge von Drittanbietern zum Netzwerk des Südwestrundfunks und/oder dessen zugehörigen Unternehmen werden unter den nachfolgenden Bedingungen gestattet. Prozess und Funktion dieses Zugriffs werden allein vom Südwestrundfunk definiert.

7.1 Allgemeine Verantwortung

Der Auftragnehmer ist für alle Aktionen seiner Benutzerkonten mit Fernzugangsfunktion auf Systemen des Südwestrundfunks verantwortlich.

7.2 Benutzerverwaltung

Der Südwestrundfunk (SWR) stellt jedem Nutzer des Auftragnehmers ein eigenes Nutzerkonto bereit. Ausnahmefälle müssen gesondert begründet und dokumentiert (z.B. im Service Level Agreement) werden. Die individuelle Lösung eines Falles wird vom SWR bestimmt.

In diesem Fall wird der Auftragnehmer die komplette Rückverfolgbarkeit der Nutzung eines Accounts (wer, wann) festhalten (im besten Fall revisionssicher) und diese dem Auftraggeber auf Verlangen aushändigen.
Sollte die Situation auftreten, dass der Auftragnehmer ein Nutzerkonto nicht mehr benötigt, muss der Südwestrundfunk darüber unverzüglich informiert werden, so dass das entsprechende Konto gesperrt werden kann.

Der Auftragnehmer muss Nutzerkonten mit Fernzugangsfunktion kontinuierlich überprüfen, und den SWR über notwendige Änderungen informieren. Diesbezüglich sind Authentisierungsverfahren mit dem Auftraggeber zu vereinbaren.

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.

8. Einsatz von Verschlüsselungs-Technologien

Werden Verschlüsselungs-Technologien eingesetzt, dürfen keine veralteten und als unsicher bekannten Kryptographie-Verfahren in Produkten des Auftragsnehmers verwendet werden.

Wenn eine veraltetes Kryptographie-Verfahren in dem bereits beim Südwestrundfunk eingesetzten Produkt verwendet wird, muss der Auftragnehmer dieses als Schwachstelle (s. Abschnitt 4) bewerten und melden. Der Lieferant hat Vorschläge zur Umgehung der Schwachstelle zu unterbreiten.

Der Auftragnehmer muss sicherstellen, dass der Einsatz der kryptographischen Absicherung der Kommunikation und Ablage überall erfolgt, wo es notwendig ist, um die Grundsätze der sicheren Softwarearchitektur zu unterstützen.

9. Sicherheitsanforderungen für einen IT-Betrieb

Wenn der Auftragnehmer zusätzlich für den kompletten IT-Betrieb oder Teile der IT-Betriebsleistungen verantwortlich ist, muss der Auftragnehmer über einen Informationssicherheitsmanagementprozess (ISMS) verfügen, und eine branchenübliche Zertifizierung nachweisen.

10. Benachrichtigung über sicherheits- und datenschutzrelevante Vorfälle

Der Auftragnehmer ist verpflichtet, potentiell für die Produkt- bzw. Betriebssicherheit relevante Sicherheitsvorfälle in seiner Organisation unverzüglich an den definierten Ansprechpartner des Südwestrundfunks zu melden. Ebenso ist die Verletzung des Schutzes personenbezogener Daten entsprechend Art. 33 EU-Datenschutz-Grundverordnung unverzüglich zu melden.

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.