UP KRITIS

# Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen

Version 4.0

Freigabe durch das Plenum des UP KRITIS am 07.11.2023

Erstellt von der Autorengruppe des Themenarbeitskreises „Lieferanten/Hersteller“
in Zusammenarbeit mit dem Themenarbeitskreis „Cloudbasierte Dienste“ des
UP KRITIS

www.upkritis.de

Download dieses Dokuments unter
www.bsi.bund.de/dok/upk-anforderungen-lieferanten

# Änderungshistorie

| Datum | Version | Bearbeitung | Status |
|---|---|---|---|
| Juni 2017 | 1.0 | Vom UP-KRITIS-Plenum freigegebene Version | veröffentlicht |
| November 2019 | 2.0 | Vom UP-KRITIS-Plenum freigegebene Version | veröffentlicht |
| November 2021 | 3.0 | Vom UP-KRITIS-Plenum freigegebene Version | veröffentlicht |
| November 2023 | 4.0 | Vom UP-KRITIS-Plenum freigegebene Version | veröffentlicht |

*Tabelle 1: Änderungshistorie*

Bundesamt für Sicherheit in der Informationstechnik
Referat WG 13 – Geschäftsstelle UP KRITIS
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5098
E-Mail: upkritis@bsi.bund.de
Internet: www.upkritis.de/

# Inhalt

# 1 Einleitung

Der Zweck dieser Best-Practice-Empfehlungen ist es, die wichtigsten Sicherheitsanforderungen an die Lieferanten von Produkten/Dienstleistungen für Kritische Infrastrukturen zu identifizieren und in einer Form zur Verwendung in Vereinbarungen mit dem Lieferanten zu dokumentieren. Unter Lieferanten werden in diesem Dokument auch Dienstleister und Hersteller im Sinne einer Werkleistung und Werklieferung verstanden und im Weiteren als Auftragnehmer bezeichnet. Mit einem Auftragnehmer in diesem Sinne besteht immer ein Vertragsverhältnis. Gleichzeitig wurde in diesem Dokument die Perspektive auf Clouddienstleistungen in den Begriff Auftragnehmer mit eingeschlossen.

Bezüglich der Definition von Cloud wird auf das Dokument „Empfehlungen zur Nutzung von Cloud-Dienstleistungen in kritischen Infrastrukturen“ [2] des UP KRITIS verwiesen.

Der Betreiber der Kritischen Infrastruktur wird in diesem Dokument auch als Auftraggeber bezeichnet, wenn es primär um vertragliche Beziehungen oder Themen geht.

Hierbei ist zu verdeutlichen, dass dieses Dokument eine Empfehlung (Best Practice) darstellt, so dass es dem Betreiber der Kritischen Infrastruktur freisteht, Anforderungen sowohl auszuschließen oder abzuändern als auch darüberhinausgehende Anforderungen zu definieren, wenn der Schutzbedarf besonders hoch ist oder die Standardmaßnahmen die Risiken nicht vollständig abdecken. Bei dem Betreiber einer Kritischen Infrastruktur handelt es sich in diesem Dokument immer um den Auftraggeber.

Da Kritische Infrastrukturen unterschiedliche Sicherheitsanforderungen abhängig von der Branche, dem Schutzbedarf und dem Auswirkungspotential auf die Bevölkerung und das Land haben können, wird jedoch allen Betreibern Kritischer Infrastrukturen empfohlen, eine Schutzbedarfsanalyse gemäß branchenspezifischen Vorgaben durchzuführen. Auf Basis dieser Analyse wird die Anwendbarkeit der nachfolgenden Anforderungen festgelegt. Sollten bestimmte Sicherheitsanforderungen aus dem Anwendungsbereich ausgeschlossen werden, wird empfohlen, die Begründung hierfür durch den Auftraggeber zu dokumentieren.

Zusätzlich wird empfohlen, die Anwendbarkeit der Sicherheitsanforderungen je nach Dienstleistungsart des Auftragnehmers (z. B. Softwareentwicklung, IT-Betrieb) zu bestimmen. Soll sich die Dienstleistung z. B. auf Softwareentwicklung beschränken, gilt zusätzlich das Kapitel 8. Wenn der Auftragnehmer zusätzlich für den kompletten IT-Betrieb oder Teile der IT-Betriebsleistungen zuständig ist, gelten auch bestimmte Anforderungen aus Kapitel 10. Die Festlegung der Anforderungen erfolgt durch den Betreiber der Kritischen Infrastrukturen und muss dokumentiert und vertraglich vereinbart sein.

# 2 Anwendungsbereich in verschiedenen Betriebsformen

Die nachfolgend aufgeführten Betriebsformen können in beliebigen Mischformen auftreten.

## 2.1 Eigenbetrieb von IT-Produkten

Unter Eigenbetrieb ist der vom Auftraggeber verantwortete und mit eigenem Personal durchgeführte IT-Betrieb gemeint[1].

Es wird empfohlen, Anforderungen aus den folgenden Bereichen an jede Lösung und an jeden Auftragnehmer für Kritische Infrastrukturen zu stellen. Dabei ist darauf zu achten, dass der Scope der Anforderungen sich immer auf Assets/Systeme der kDL bezieht:

a. Vulnerability-Management (Kapitel 4)

b. Patch-Management (Kapitel 5)

c. Systemhärtung (Kapitel 6)

d. Fernzugang für Drittanbieter (Kapitel 7)

e. Mandanten-/Useradministration

f. Anforderungen an die Softwareentwicklungsprozesse (Kapitel 8)

g. Einsatz der kryptographischen Lösungen (Kapitel 9)

h. Dokumentation (Kapitel 11)

i. Benachrichtigung über sicherheitsrelevante Vorfälle (Kapitel 12)

j. Nicht-technische Sicherheit (Kapitel 13)

## 2.2 Betrieb mit Unterstützung Dritter (Auftragnehmer)

Unter Unterstützung durch Dritte ist die Erbringung des IT-Betriebs in Teilen (z. B. PaaS, IaaS) oder in Gänze (z. B. SaaS) durch Dritte (z. B. Outsourcing) gemeint.

Es wird empfohlen, über die im Abschnitt 2.1 aufgeführten Anforderungen hinaus weiterführende Anforderungen aus den folgenden Bereichen an die Auftragnehmer, die zusätzlich zu Softwarelösungen auch weitere Dienstleistungen erbringen (z. B. IT-Betrieb, Remote-Support, Cloud-Dienstleister), zu stellen (Kapitel 10). Dabei ist darauf zu achten, dass der Scope der Anforderungen sich immer auf Assets/Systeme der kDL bezieht:

a. Informationssicherheitsprozesse/ISMS

b. Zugriffsschutz und Berechtigungsvergabe

c. Asset-Management

d. Personalsicherheit (HR-Security)

e. Physische Sicherheit und Zutrittsschutz

f. Operationelle IS-Anforderungen (Netzwerksicherheit, Virenschutz, Logging & Monitoring, Backup & Restore etc.)

g. Sicherheit in der Softwareentwicklung und Change-Prozesse

[1] Selbstverständlich gibt es auch Grenzfälle in Bezug auf Unterstützungsleistung durch Dritte.

h. Security-Incident-Management / Incident Handling

i. Sicherheit in ausgelagerten Prozessen

**Beachte: Im Cloudbetrieb** ist man in der Regel **primär** auf die **Dokumentenlage** angewiesen die der Dienstleister (Auftragnehmer) bereitstellt, um die Arbeitsabläufe/Prozesse des Dienstleisters zu verstehen, zu definieren, zu steuern und zu kontrollieren. **Dieser veränderte Risikovektor ist zu beachten.** Weitere Details sind im Kapitel 3 beschrieben.

Cloud Services können im Bereich der kritischen Infrastruktur eingesetzt werden, sofern sie den eigenen spezifischen Anforderungen und den Anforderungen an den Stand der Technik nach BSIG gerecht werden.

Wenn der Dienstleister die Themen Informations- und IT-Sicherheit, sowie Datenschutz nicht bereits in seinem Standard-Portfolio ausreichend nach dem Stand der Technik auf dem Niveau für die IT der kDL des jeweiligen Unternehmens unterstützt und nachweist, wird dringend empfohlen, diesen Service nicht einzusetzen.

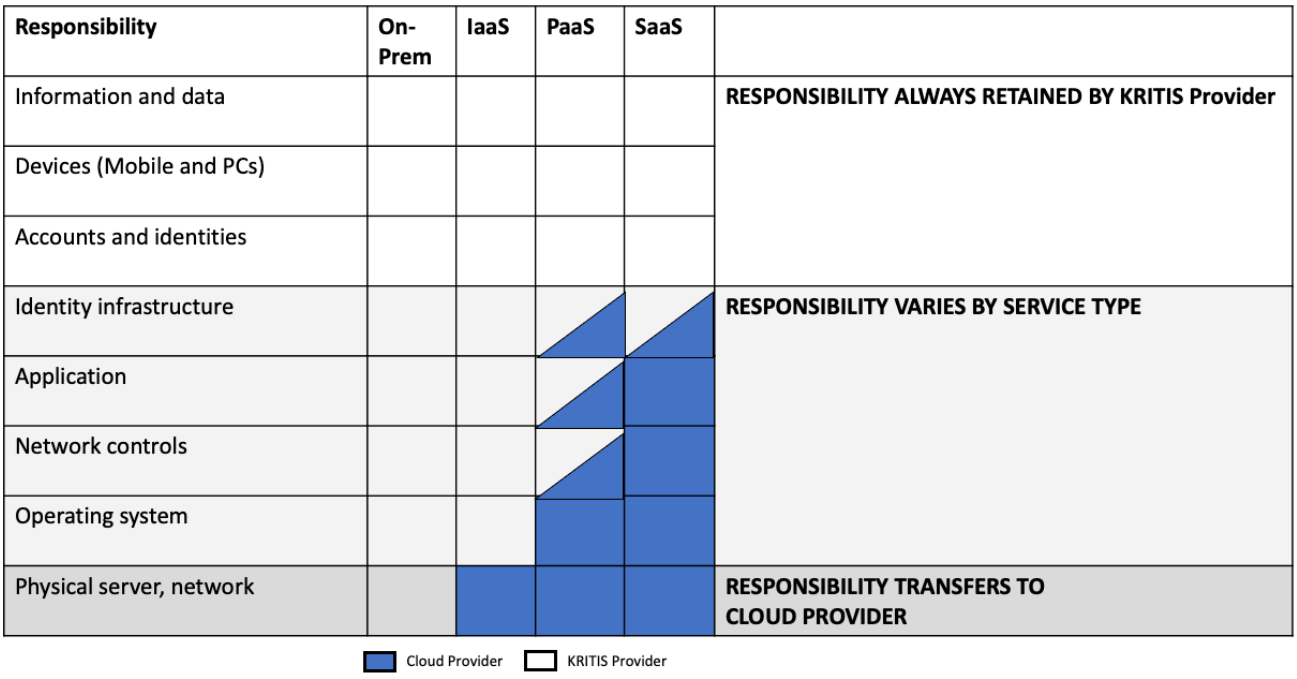


*Abbildung 1: Beispielhafte Darstellung für die Aufteilung von Verantwortlichkeiten*

# 3 Rollen und Verantwortlichkeiten

## 3.1 Allgemeine Verantwortung des Auftraggebers

Jede Vertragsbeziehung wird in der Regel einem abgestimmten Phasenmodell folgen.

Als Beispiel hier ein 5-Phasenmodell:

1. Planung inkl. Risikobewertung
2. Auftragsvergabe
3. Integration/Inbetriebnahme
4. Produktive Nutzung
5. Außerbetriebnahme.

Der Auftraggeber hat sicherzustellen, dass er/sie alle im Kapitel 2 beschriebenen und für den Auftrag als relevant bestimmten Anforderungen in jeder Phase deutlich anfordert und, ggf. gemeinsam mit dem Auftragnehmer, prüft und dokumentiert.

Als ideales Format zu einem möglichst sicheren gemeinsamen Verständnis zwischen Auftraggeber und Auftragnehmer haben sich sogenannte Service Level Agreements (SLA) herausgestellt – siehe auch Grundlagen zu ITIL. Eine Ausführung mit dem Fokus auf KRITIS-Dienstleistungen sind Security Level Agreements (SecLA), beispielhaft unter [1] zu finden.

Bei einer Cloudnutzung drehen sich in der Regel die Positionen der Vertragsgestaltung um. Hier gibt der Clouddienstleister die Standardregeln vor, an denen sich der Auftraggeber ausrichten muss. Anpassungen sind i. d. R. wegen der geforderten standardisierten Cloud-Funktionalitäten kaum möglich. Im Regelfall sind die vom Cloudanbieter gesetzten Standards zu nutzen, Individuallösungen sind kaum umsetzbar. Unter diesem Aspekt sind insbesondere die Risiken zum Betrieb der KRITIS-IT zu prüfen und zu bewerten, ob ein angemessener KRITIS-IT-Betrieb noch möglich wäre. Besonders deutlich wird das im Changemanagement – der Clouddienstleister müsste eigentlich vor jeder Änderung, die er in den Clouddiensten vornimmt, in einem Changeprozess von allen Nutzern, also hier den Auftraggebern, ein „OK“ einholen.

Es ist notwendig, vorhandene Zertifikate des Clouddienstleisters bei der Bewertung des Sicherheitsniveaus mit einzubeziehen. Beispielsweise werden beim Standard C5 (Cloud Computing Compliance Criteria Catalogue) des BSI alle in Kapitel 2 aufgelisteten Anforderungen an den Clouddienstleister mit betrachtet. Gleichermaßen ist es auch sinnvoll, anhand vorhandener Standards (wie beispielsweise dem Baustein OPS 2.2 im IT-Grundschutz-Kompendium) das Sicherheitsniveau bei der Cloudnutzung seitens des Auftraggebers zu bewerten. Mitunter ist dies dahingehend vorteilhaft, da diese Zertifizierungen bei der Erbringung der Nachweise gemäß § 8a BSI-Gesetz verwendet werden können (sofern das Zertifikat zum Zeitpunkt der Einreichung beim BSI nicht älter als ein Jahr ist).

## 3.2 Allgemeine Verantwortlichkeit des Auftragnehmers

Generell ist es die Verantwortung eines Auftragnehmers, die durch den Auftraggeber festgelegten Anforderungen einzuhalten. Darüber hinaus muss ein Auftragnehmer von Produkten/Dienstleistungen für Kritische Infrastrukturen die in der Industrie anerkannten Standards der Informationssicherheit und/oder andere regulatorische Standards und Vorgaben für Dienstleistungen/Produkte kontinuierlich beachten[2].

[2] Ein probater Ansatz wird vom TeleTrust e. V. regelmäßig aktualisiert zur Verfügung gestellt – siehe www.teletrust.de/publikationen/broschueren/stand-der-technik

Zusätzlich muss ein Eskalationsprozess vereinbart werden, um Verstöße gegen Vereinbarungen und Sicherheitsfragen zu behandeln. Die Kontaktinformationen sollen Teil der Vertrags-/Projektdokumentation zwischen dem Auftraggeber und dem Auftragnehmer sein.

Es können Situationen auftreten, die die Anpassung von verwendeten und oder vereinbarten Sicherheitsstandards fordern (beachte den All-Gefahren-Ansatz[3]). Mit dem Auftragnehmer sollte geklärt und dokumentiert werden, wie dieser konstruktiv auf diese Veränderungen reagiert, sich an den neuen Standards und Anforderungen orientiert und proaktiv Trends in der Sicherheit verfolgt, umsetzt und nutzt (Changemanagement).

Bei Clouddiensten ist eine individuelle Anpassung von Sicherheitsmaßnahmen aufgrund der Standardisierung der Cloudservices für einzelne Kunden in der Regel nur schwer möglich. Umso wichtiger ist es, dass die für den Clouddienst implementierten Sicherheitsmaßnahmen auf einem so hohen Stand der Technik laufen und regelmäßig und im Bedarfsfall angepasst werden, dass sie die Anforderungen aus der Perspektive KRITIS-IT erfüllen. Ein geeigneter Clouddiensteanbieter muss angemessene Sicherheitsmaßnahmen zur Verfügung stellen können.

Sollte eine Situation entsprechend der Best-Practice- Empfehlung eintreten, die die Bereitstellung von internen Ressourcen durch den Auftragnehmer erfordert, ist es die Aufgabe des Auftragnehmers, diese zur Verfügung zu stellen.

Der Auftragnehmer muss Sicherheitsanforderungen mit seinen Dienstleistern/Subunternehmern, die Teile der Dienstleistung erbringen oder wesentliche Bedeutung für die Erbringung der Dienstleistung haben, schriftlich vereinbaren. Die Sicherheitsanforderungen an die Subunternehmer müssen mindestens in dem vereinbarten Umfang weitergereicht bzw. definiert werden, damit der Auftragnehmer sicherstellen kann, dass seine Verpflichtungen gegenüber dem Auftraggeber vollständig erfüllt werden. Der Auftragnehmer ist gegenüber dem Auftraggeber für die Überwachung seiner Subunternehmer zuständig sowie für die Einhaltung der weitergereichten Anforderungen. Kontrollrechte sind durch den Auftraggeber zu vereinbaren. Der Auftragnehmer hat dem Auftraggeber die Ketten der verbundenen Subunternehmen und deren Funktionalität selbstständig proaktiv mitzuteilen.

Bei Cloud-Dienstleistungen ist eine direkte Zuordnung von Infrastruktur und Service oft nicht möglich. In solchen Fällen kann ein Nachweis oder eine Kontrolle nur über die Dokumentation und Zertifizierungen erfolgen.

[3] Siehe Kapitel 14

# 4 Vulnerability-Management

Auftragnehmer müssen ihre Produkte einer kontinuierlichen Prüfung auf Schwachstellen unterziehen, bspw. in Form eines sogenannten Vulnerability-Managements, um in der Lage zu sein, auf neue Schwachstellen so schnell wie möglich zu reagieren. Das Vulnerability-Management basiert auf der Transparenz der Funktionalität, der technischen Architektur und von Unterkomponenten einschließlich der Betriebssysteme, Datenbanken, Server (z. B. Web, Telnet, SSH), Middleware und Bibliotheken. Ziel ist es, neue Schwachstellen in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen zu beurteilen.

Der Auftragnehmer muss sich verpflichten, Fehler in seinen Produkten, die Auswirkungen auf den Betrieb Kritischer Infrastrukturen haben können, dem Betreiber aktiv mitzuteilen. Das kann auch über öffentlich erreichbare Plattformen (z. B. CERT-Bund, CVE u. a.) erfolgen.

Genauso muss der Auftraggeber dem Auftragnehmer Erkenntnisse über relevante Schwachstellen und Schwächen in den eingesetzten Produkten mitteilen.

## 4.1 Methodik und Umfang

Jede Schwachstelle/Sicherheitslücke sollte vom Auftragnehmer an den Auftraggeber gemeldet und bzgl. möglicher funktionaler und sicherheitsrelevante Auswirkungen bewertet werden. Eine mögliche Bewertung der Kritikalität kann z. B. auf Basis der Schutzbedarfsanalyse durch den Auftraggeber festgelegt werden. Der Umfang des Vulnerability-Managements umfasst jede potenzielle Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität und Vertraulichkeit der Vermögenswerte (materielle oder immaterielle) oder auf eine beim Auftraggeber operierende Dienstleistung des Auftragnehmers mit Bezug auf die kDL nehmen kann.

## 4.2 Vulnerability-Assessment

Der Auftragnehmer ist verpflichtet, kontinuierlich Quellen für Sicherheitsempfehlungen zu sichten und diese in Bezug auf die an den Auftraggeber gelieferten oder bereitgestellten Assets zu bewerten. Sollte eine Komponente von der Schwachstelle/Sicherheitslücke betroffenen sein, wird von dem Auftragnehmer erwartet, die Einstufung der Kritikalität und die „zeitliche“ Bewertung durchzuführen (siehe Hinweise in Kapitel 12).

Es ist selbstverständlich akzeptiert, dass die Informationen über die umliegende Infrastruktur oder andere einflussnehmende Umstände nicht vollständig sein können und dass das bestmögliche Ergebnis auf Basis des Wissens in dem Branchenumfeld des Auftragnehmers beruht.

Zu Informationspflichten siehe Kapitel 12.

## 4.3 Behebung von Schwachstellen am Beispiel Kritikalität/Reaktionszeit

Die folgende Tabelle zeigt beispielhaft die Kritikalität der Sicherheitslücken und die erwartete Zeit zur Implementierung einer Lösung bzw. eines Workarounds. Andere Bewertungskriterien können durch den Betreiber der Kritischen Infrastruktur festgelegt werden:

Finale Lösungszeit = Zeit benötigt für den Patch/die Wartungsfreigabe/die korrekte Installation der Lösung; Zeitraum, in dem auf den Service aus öffentlichen/externen Netzwerken zugegriffen werden kann.

Zeit bis zum Workaround = Zeit für eine vorläufige Lösung oder einen Workaround für den Fall, dass ein finaler Patch nicht innerhalb eines bestimmten Zeitrahmens verfügbar ist. Vom Auftragnehmer wird erwartet, dass eine Lösung mit einem Best-Effort-Ansatz und nach bestem Wissen erarbeitet wird. „Zurzeit ist kein Workaround verfügbar" ist eine gültige Aussage im Kontext dieses Absatzes. Die Zeitzählung beginnt mit der Benachrichtigung über die Schwachstelle an den Dienstleister (intern oder extern).

Neutralisierung = Kompensation der Auswirkungen durch einen Workaround oder einer finalen Lösung

| Priorität | Kritikalitätsstufe | CVSS | Zeit bis Neutralisierung |
|---|---|---|---|
| 1 | Critical | 9.0 - 10.0 | 3 Stunden |
| 2 | High | 7.0 - 8.9 | 3 Tage |
| 3 | Average | 4.0 - 6.9 | 1 Monat |
| 4 | Low | 0.1 - 3.9 | 3 Monate |

*Tabelle 2 – Beispiele für zeitliche Anforderungen zur Behebung von kritischen Schwachstellen*

Es ist möglich und empfohlen, öffentlich publizierte CVSS-Einstufungen unter Berücksichtigung der „eigenen" Sicherheitsmaßnahmen und Umgebung zu prüfen und im konkreten Einzelfall ggf. zu einer anderen CVSS-Einstufung zu kommen.

## 4.4 Kommunikation

Jegliche Kommunikationswege sollten mit dem Auftragnehmer bzgl. Art und Form vereinbart werden. Kryptographische Techniken nach dem Stand der Technik sollten zur Geheimhaltung und Integrität für die Übermittlung von Mitteilungen und Dokumenten im Rahmen des Vulnerability Managements verwendet werden.

# 5 Patch-Management

Dieser Abschnitt unterteilt sich in drei Punkte. Der erste Teil legt den Anwendungsbereich des Patchings fest, der zweite Teil definiert die Erwartungen des Patch-Levels während der Systemabnahme durch den Auftraggeber. Der dritte Teil beschreibt die Anforderungen an das kontinuierliche Patch-Management nach der Systemabnahme.

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

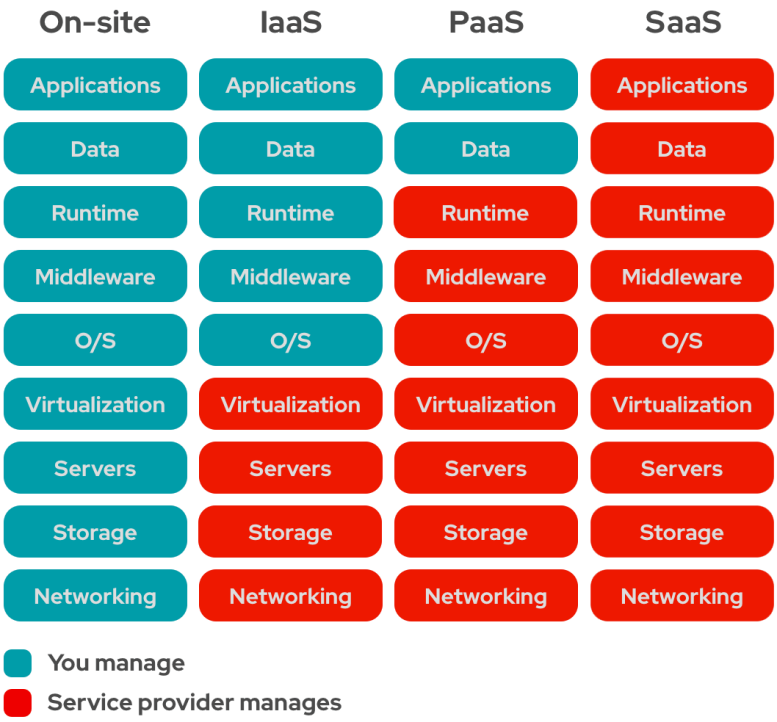


*Abbildung 2 – Beispiel für eine mögliche Verteilung der Verantwortung für das Patchmanagement, Bildquelle: verschiedene öffentliche Publikationen – gefunden auf redhat.com*

## 5.1 Umfang des Patchings

Der Umfang des Patchings muss zwischen Auftragnehmer und Auftraggeber vereinbart sein. Dazu gehören in der Regel:

- Betriebssystem
- Alle Softwarepakete und Services, die Teil des Betriebssystems sind
- Alle Tools und Applikationen, die der Hersteller zu Betriebs- und Wartungszwecken installiert hat
- Zielapplikation (Servicelogik)
- Alle Middleware-Application-Layer, Datenbanken, Access-, Monitoring- oder Applikationsserver, die für den Service genutzt werden

## 5.2 Patch-Level während der Systemabnahme

Der Auftragnehmer hat sicherzustellen, dass alle Systeme vor der Abnahme nachweislich gepatcht und aktualisiert werden. Der Patch-Level sollte am Tag der Systemabnahmeerklärung immer aktuell sein. Der Auftragnehmer muss alle öffentlich verfügbaren und durch den Auftraggeber freigegebenen Patches als Teil der Lieferung installieren.

Je nach Lösung müssen ggf. auch sehr kurze Aktualisierungszeiträume von Patches zur Abnahme beachtet werden.

Beim Einsatz von Cloudlösungen kann man in der Regel vom Anbieter keinen expliziten Patchlevel abverlangen. In diesen Fällen muss ein nachweislich zertifizierter Prozess vom Anbieter als Ersatz dienen.

## 5.3 Patch-Management nach der Systemabnahme

### 5.3.1 Patch-Management-Lifecycle

Der Auftragnehmer verpflichtet sich, mindestens zweimal pro Jahr oder bei Bedarf umgehend Updates und Patches bereitzustellen, um die Anforderung aus dem Stand der Technik einzuhalten. Für die Bereitstellung durch den Auftragnehmer gelten die über Abschnitt 4.3 vereinbarten Zeitrahmen.

Der Auftragnehmer soll für die im Patchzyklus adressierten Schwachstellen einen Bericht erstellen und dem Auftraggeber zur Verfügung stellen. Dieser kann detaillierte oder aggregierte Daten unter Berücksichtigung der Kritikalitätsstufe und den betroffenen Bereich (Verfügbarkeit, Integrität oder Vertraulichkeit) enthalten.

### 5.3.2 Ende des Lifecycles

Sollte es zu der Situation kommen, in der der Drittanbieter eines Betriebssystems oder einer anderen Komponente (Software, Datenbanken, Anwendungen, etc.) das Ende des Lifecycles verkündet, wird vom Auftragnehmer erwartet, dass er angemessene Alternativlösungen anbietet und oder gemeinsam mit dem Auftraggeber nach Lösungsansätzen sucht und diese anbietet. Anderenfalls müssen offene Sicherheitslücken durch Maßnahmen vor Ort kompensiert werden.

Grundsätzlich hat der Auftragnehmer dafür Sorge zu tragen, dass er rechtzeitig vor dem Ende von Lifecyles den Auftraggeber darüber informiert.

### 5.3.3 Lieferanten von Anwendungen oder Funktionalitäten

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

# 6 Systemhärtung

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

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

## 6.1 Minimale Installationsprinzipien

Es wird von dem Auftragnehmer erwartet, folgende Komponenten des Betriebssystems oder anderer Software zu installieren:

a. Jede Softwarekomponente, die für die Anwendung oder nach der Logik des Dienstes benötigt wird

b. Jede aus der Integration mit anderen Services resultierende andere Anwendung oder Softwarekomponente

c. Jede aus Betriebs- und Wartungsanforderungen resultierende Softwarekomponente

Jede andere Software darf nicht installiert werden, außer der Auftragnehmer und der Auftraggeber 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 Konfigurationsstandards

Der Auftragnehmer stellt sicher, dass die vom Auftraggeber vorgegebenen allgemeinen Konfigurationsstandard(s) und Sicherheitsvorschriften eingehalten werden.

## 6.4 Passwörter

Der Auftragnehmer stellt sicher, dass jedes Passwort, insbesondere auch die voreingestellten Initialpasswörter, in allen möglichen Fällen geändert werden können.

## 6.5 Backdoors

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

## 6.6 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 Auftraggebers und/oder dessen zugehörigen Unternehmen wird unter den nachfolgend beschriebenen Bedingungen gestattet. Prozess und Funktion dieses Zugriffs werden allein vom Auftraggeber definiert.

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

## 7.1 Allgemeine Erwartungen

Der Auftragnehmer muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit und Integrität der Assets und Services des Auftraggebers gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer während eines Fernzugriffes Kenntnis erlangt hat. Er ist für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf Systemen des Auftraggebers verantwortlich.

Beispielliste:

- Zugänge zur KRITIS-IT sollten nie direkt, sondern immer über Sprungserver oder vergleichbare Funktionalität in die geschützten Zonen hinein und auf KRITIS-IT erfolgen.
- Für Fernzugänge sollte mindestens eine 2-Faktor-Authentifizierung eingesetzt werden.
- Fernzugänge sollten nur zeitbeschränkt geöffnet werden bzw. automatisch geschlossen werden.
- Fernzugänge sollten immer „von innen“, also durch bewusstes Handeln des Auftraggebers, geöffnet werden.

## 7.2 User-Account-Management

Es wird allgemein erwartet, dass jeder Nutzer ein persönliches Nutzerkonto bereitgestellt bekommt. Der Auftraggeber akzeptiert Ausnahmen, sollten Umstände auftreten (Unternehmen mit mehreren Supportcentern und einer großen Anzahl an Personal), die dies erschweren.

Solche Ausnahmen müssen vorab dokumentiert und in einem SLA (Service Level Agreement) festgehalten werden. In diesem Fall wird der Auftragnehmer die komplette Rückverfolgbarkeit der Nutzung eines Accounts (wer, wann) festhalten (im besten Fall revisionssicher) und diese dem Auftraggeber mindestens einmal jährlich und zusätzlich auf Verlangen aushändigen.

Sollte die Situation auftreten, dass der Auftragnehmer ein Nutzerkonto nicht mehr benötigt, muss der Auftraggeber darüber unverzüglich informiert werden, so dass das entsprechende Konto gesperrt werden kann. Der Auftraggeber kann durch eine Betriebsfunktion oder eine alternative Service-Management-Funktion repräsentiert werden. Derartige Kontakte sind im SLA zu definieren.

Es wird vom Auftragnehmer erwartet, Nutzerkonten mit Fernzugangsfunktion alle 6 Monate zu überprüfen und den Auftraggeber über notwendige Änderungen zu informieren. Diesbezüglich sind Authentisierungsverfahren sind mit dem Auftraggeber zu vereinbaren.

Der AN sollte einen Nachweis erbringen, wie das Zugangsdaten- und Schlüsselmanagement im Verantwortungsbereich des AN für die betrachtete Lösung aufgebaut ist. Das „need-to-know-Prinzip“ wird als selbstverständlich vorausgesetzt.

Bei den physischen Einrichtungen sind die Regelungen von Abschnitt 10.5 zu berücksichtigen.

# 8 Anforderungen an die Softwareentwicklungsprozesse

Die Berücksichtigung der Sicherheit in Entwicklungsprozessen (Security by Design) ist in vielen Fällen ein effizienterer Weg, um ein sicheres Softwareprodukt herzustellen, als das nachträgliche Patching und Ausrollen in der Produktion.

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

Die Softwareentwicklungsprozesse des Auftragnehmers müssen so ausgelegt sein, dass der Sicherheit der entwickelten Software angemessene Beachtung in allen Entwicklungsphasen geschenkt wird und die Prozesse sich an den allgemein anerkannten Industriestandards orientieren.

Insbesondere sollen folgende Punkte berücksichtigt werden:

- Vorhandene Standards der sicheren Softwarearchitektur
- Die Entwickler müssen sich an vorhandene Standards zur sicheren Programmierung halten (generische Anforderung siehe z. B. ISO 27001:2022 – 8.25-8.28 und ISO 25010), um Schwachstellen vorzubeugen. Diese Standards müssen dokumentiert werden und den Entwicklern z. B. in Schulungen bekannt gemacht werden.
- Secure-Code-Reviews als Teil der Qualitätssicherung und Testing. Zum Beispiel müssen die eigenentwickelten Webapplikationen, die für den Betrieb in nicht geschützten Netzen vorgesehen sind, ein Code-Review nach einem Industriestandard wie OWASP oder gleichwertig durchlaufen.
- Benutzung der Open-Source-Komponenten, angemessene Konfiguration, Dokumentation und Wartung dieser Komponenten
- Die Testverfahren beim Auftragnehmer sollen die implementierten Sicherheitsmechanismen und -funktionen (Verschlüsselung, Zugriffskontrollen, Authentisierung und andere) explizit beinhalten. Der Auftragnehmer stellt zu jeder Lieferung und zu jedem Update dem Auftraggeber die notwendige Menge von funktionalen Testfällen und -skripten zur Verfügung, die zum sicheren Funktionsnachweis benötigt werden.
- Sicherheitsüberprüfungen entsprechend den vorgesehenen Betriebsumgebungen, z. B. unabhängige Penetrationstests für die Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sein sollen.
- Ergebnisse der Secure-Code-Reviews bzw. Penetrationstests sollen dem Auftraggeber (zumindest für die finale Version des Produktes) zur Verfügung gestellt werden.
- Regelmäßige Prüfung auf veraltete Protokolle und Bibliotheken
- Regelmäßige Prüfung neuer Bibliotheken und deren weiterführende, ggf. über den Auftrag hinausgehende, Funktionalitäten, da diese auch Rückwirkungen auf die beauftragten Funktionen haben können.

# 9 Einsatz der kryptographischen Lösungen

Um sicherzustellen, dass keine veralteten und als unsicher bekannten Kryptographielösungen in den Produkten verwendet werden, soll der Auftragnehmer eine schriftliche Richtlinie etablieren und mit dem Auftraggeber abstimmen, die die zulässigen Kryptographiealgorithmen definiert. Diese Richtlinie sollte sich an einen Industriestandard oder anerkannte Richtlinien halten (z. B. BSI TR-02102) und regelmäßig überprüft werden.

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

Wenn eine Kryptographielösung in der Industrie als nicht mehr sicher bekannt wird, muss die Richtlinie angepasst werden. Wenn eine solche Kryptographielösung in dem bereits beim Auftraggeber eingesetzten Produkt verwendet wird, muss der Auftragnehmer sie im Rahmen vom Vulnerability-Management-Prozess (siehe Kapitel 4) als Schwachstelle 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. Der Einsatz der kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf (z. B. Steuerungsdaten der Kritischen Infrastruktur oder vertrauliche Daten) über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

# 10 Sicherheitsanforderungen für den IT-Betrieb

Wenn der Auftragnehmer zusätzlich für den kompletten IT-Betrieb oder Teile der IT-Betriebsleistungen zuständig ist, gelten auch bestimmte Anforderungen aus der nachfolgenden Liste. Die Festlegung der Anforderungen erfolgt durch den Auftraggeber und muss dokumentiert sein.

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

## 10.1 Informationssicherheitsprozesse / ISMS

Der Auftragnehmer muss Informationssicherheitsmanagementprozesse (ISMS) nach einem anerkannten Sicherheitsstandard aufsetzen. Diese Prozesse sowie entsprechende Rollen und Verantwortlichkeiten müssen als Teil seiner Informationssicherheitsrichtlinien dokumentiert sein. Die Richtlinien müssen seiner Belegschaft bekannt sein und regelmäßig auf Aktualität und Richtigkeit überprüft werden.

## 10.2 Zugriffsschutz und Berechtigungsvergabe

Prozesse und Kontrollen zum Zugriffsschutz und zur Berechtigungsvergabe müssen implementiert werden:

- Dokumentierte Freigabeprozesse für Berechtigungen auf Systemen und Informationen
- Prozesse zur zeitnahen Löschung von Zugriffsrechten bei Austritt oder Abteilungswechsel
- Definierte und angemessene Passwortkomplexität und -gültigkeit
- Bildschirmsperre nach Inaktivität

## 10.3 Asset-Management

Zusätzlich zu den im Abschnitt „Nicht-technische Sicherheit – Asset Management“ definierten Anforderungen, müssen Standards zur sicheren Löschung der Daten / Zerstörung von Datenträgern definiert werden, um zu vermeiden, dass die gelöschten Daten von Dritten unautorisiert wiederhergestellt werden. Die „Vertraulichkeit“ der Informationen ist bei den Löschverfahren zu berücksichtigen.

## 10.4 Personalsicherheit (HR-Security)

Zusätzlich zu den im Abschnitt „Nicht-technische Sicherheit – Human-Resources-Security“ definierten Anforderungen, müssen beim IT-Betrieb durch den Auftragnehmer folgende Punkte beachtet werden:

- Security-Awareness-Trainings für die Mitarbeiter müssen periodisch durchgeführt werden.
- Die Inhalte der Schulungen müssen entsprechend den aktuellen Erkenntnissen regelmäßig aktualisiert werden.

## 10.5 Physische Sicherheit und Zutrittsschutz

Der Auftragnehmer muss angemessene Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz treffen. Insbesondere sollen folgende Maßnahmen implementiert sein:

- Schutz gegen Feuer und Wasser,
- Schutz vor bzw. Vermeidung von extremen Temperaturen (Klimaanlage),
- Notstromversorgung

Zutritt zu Bereichen mit Informationen oder Systemen mit Schutzbedarf müssen auf den autorisierten Personenkreis beschränkt werden. Dazu gehören auch die Zutrittsschutzmaßnahmen für Rechenzentren inklusive Überwachung der kritischen Bereiche, Zutrittsprotokoll und Sicherung gegen Einbruch u. a.

## 10.6 Netzwerksicherheit und operationelle Sicherheit:

- Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen müssen (z. B. durch Firewalls) voneinander getrennt werden. Netzwerkperimeter müssen einen Firewallschutz haben. Firewallregeln müssen einen dokumentierten Freigabeprozess durchlaufen.
- Authentisierungsmerkmale (Passwörter, PINs) dürfen nur verschlüsselt über das Netzwerk übermittelt werden.
- Aus dem Internet erreichbare administrative Zugänge oder Netzwerkports für den technischen Zugriff müssen abgeschaltet oder angemessen abgesichert werden (z. B. durch 2-Faktor-Authentisierung).
- Netzwerkverbindungen, Systemzugriffe und administrative Tätigkeiten werden zur Nachvollziehbarkeit von Angriffen oder Fehlbedienungen protokolliert. Die Aufbewahrung der Protokolle richtet sich nach den geltenden gesetzlichen, geschäftlichen und Anforderungen des Auftraggebers.
- Malwareschutz (für Server, Workstations sowie andere IT-Komponenten mit Zugriff auf die Informationen oder Systeme mit Schutzbedarf) muss implementiert und aktuell sein.
- Datensicherungs- und Wiederherstellungsprozesse sind etabliert. Datenwiederherstellungstests werden regelmäßig durchgeführt.
- Sicherer physischer Transport von Speichermedien (Verschlüsselung, physische Absicherung).
- Software-Change-Prozesse für Produktivumgebungen sind etabliert und werden befolgt.
- Prozesse zu regelmäßigen Schwachstellenscans und Behebung von Schwachstellen sind etabliert und werden befolgt.
- Wenn drahtlose Netzwerke benutzt werden, müssen sie kryptographisch abgesichert sein (siehe auch Kapitel 9). Es muss sichergestellt werden, dass die Systeme sich nicht mit unautorisierten Access-Points verbinden können bzw. dass keine unautorisierten Netzwerke aufgebaut werden.

## 10.7 Security-Incident-Management

Prozesse zur Reaktion auf Sicherheitsvorfälle, sowie die dazugehörigen Rollen und Verantwortlichkeiten müssen nach dem Allgefahrenansatz aufgesetzt werden. Es sind neben den reinen IT-Security Szenarien auch non-IT Szenarien zu betrachten (siehe Kapitel 13). Schulungen und Übungen zu diesem Komplex sind obligatorisch.

Grundlage für ein wirksames Security-Incident-Management ist wegen der möglichen weiterführenden Auswirkungen ein ausgeprägtes IT-Notfallmanagement. Beide Ansätze sollten auf das unternehmerische BCM aufsetzen und mit diesem abgestimmt sein.

Zur Meldung der Sicherheitsvorfälle siehe Kapitel 12.

## 10.8 Sicherheit in Auslagerungsprozessen

Wenn der Auftragnehmer Teile der Betriebsleistung oder anderer Dienstleistungen für den Auftraggeber an weitere Dienstleister auslagert, müssen Sicherheitsanforderungen in den Vereinbarungen mit den Dienstleistern berücksichtigt werden.

Die Sicherheitsanforderungen mit den Dienstleistern müssen so definiert werden, dass die Sicherheitsstandards für die Daten des Auftraggebers und Leistungen für den Auftraggeber in jedem Fall eingehalten werden können und dass der Auftragnehmer in der Lage ist, eigene Verpflichtungen zur Sicherheit gegenüber dem Auftraggeber vollumfassend zu erfüllen. Eine transparente Darstellung der durchgehenden Lieferkette einschließlich Subunternehmer ist gegenüber dem Auftraggeber nachzuweisen. Der Auftragnehmer muss den Auftraggeber im Vorfeld von Entscheidungen über die Auslagerung von Betriebs- oder Dienstleistungen informieren. Die Einhaltung muss überwacht und je nach Kritikalität auch durch Lieferantenaudits nachweisbar sein.

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

# 11 Dokumentation

Es wird vom Auftragnehmer erwartet, dass dieser jegliche Dokumentation zur Verfügung stellt, die die Nutzung der angebotenen Lösung erleichtert.

Die in Kapitel 3 beschriebenen Hinweise für den Umgang mit Cloudlösungen sind zu beachten.

Der gebräuchliche Umfang einer derartigen Dokumentation, wenn auch nicht auf diese beschränkt, inkludiert die folgenden Punkte:

- Liste der Hardware
- Liste der Software (inklusive Betriebssystem und Patch-Level)
- Überblick über die Systemarchitektur (kann Teil der Designdokumentation sein)
- Kommunikationsmatrix
- Überblick über die Datenflüsse (Datenflussschemata)
- Existierende Benutzerkonten und Rollen sowie deren Berechtigungen
- Beschreibung von proprietären (nicht in der Industrie standardisierten) Sicherheitsmechanismen (Erwartung, die Prinzipien und Implementierung einer solchen Lösung zu verstehen)
- Weitere Dokumentationen, spezifiziert als Teil des Liefergegenstandes oder Auftrages, die die Sicherheit der Lösung gewährleiten

Sollten Änderungen an der gelieferten Lösung durchgeführt werden, wird vom Auftragnehmer erwartet, diese in die Dokumentation einzupflegen.

# 12 Informationspflicht über sicherheitsrelevante Vorfälle

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle, die potentiell einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Informations-/Vermögenswerte beim Auftraggeber haben könnten, unverzüglich dem Auftraggeber zu melden. Dies könnten z. B. auch Industriespionage oder eine Sicherheitslücke im Source-Code sein.

Es sind mit dem Aufragnehmer Kriterien für Schwachstellen zu vereinbaren (siehe auch Abschnitt 4.2), nach denen der Auftraggeber vom Auftragnehmer oder Hersteller informiert werden muss und die beschreiben, wie dieses erfolgen sollte.

Zusätzlich muss der Auftragnehmer die Abweichungen von den vereinbarten Sicherheitsanforderungen melden.

Der Auftragnehmer wird in solchen Fällen neben selbstverständlichen Zwischeninformationen einen finalen Abschlussbericht bereitstellen.

# 13 Nicht-technische Sicherheit

## 13.1 Organisation der Informationssicherheit

Der Auftragnehmer hat dem Antrag des Auftraggebers nachzukommen, Informationen seiner Sicherheitsorganisation offenzulegen, auf dessen Basis der Auftraggeber eine Auftragnehmerbewertung durchführen kann. Diese Einschätzung ist ein interner Prozess, der den Auftraggeber dabei unterstützt, die Metriken und Reife der Sicherheitsorganisation des Auftragnehmers zu beurteilen.

Der Auftragnehmer soll, falls vorhanden, ein ISO 27001-Zertifikat oder Äquivalente (Historie und Umfang) bereitstellen, sowie weitere Dokumente wie Berichte und Vorschriften etc. in diesem Kontext.

## 13.2 Asset-Management

Der Auftragnehmer hat alle Assets in seinem Informationssystem zu identifizieren und zu dokumentieren, die einen Bezug zum Informationssystem des Auftraggebers zwecks Wartung oder Betriebszugang haben können. Die Verantwortung für die Aufrechterhaltung der entsprechenden Sicherheitskontrollen dieser Assets muss zugewiesen werden. Diese Dokumentation ist möglicherweise Teil des Audits (Abschnitt 13.4), demnach werden alle Unterlagen vom Auftragnehmer nachweislich gepflegt.

Zum Schutz der Assets kann der Auftragnehmer die Anwendung spezifischer Sicherheitsmaßnahmen delegieren, jedoch bleibt der Auftragnehmer für den angemessenen Schutz der Assets, die in Bezug zu dem Informationssystem des Auftraggebers stehen, verantwortlich.

Die beim Auftragnehmer gespeicherten Daten müssen in dessen Eigentum verbleiben (besonders Kundeninformationen), da er für die Daten haftet, z. B. im Falle von Datenverlust.

## 13.3 Human-Resources-Security (Personelle Sicherheit)

Jeder, der im Namen des Auftragnehmers agiert, der entfernten oder lokalen Zugriff auf das Informationssystem des Auftraggebers haben muss, muss Informationen zu seiner Identität bereitstellen. Der Auftragnehmer stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt.

Sollte der Auftragnehmer mit Subunternehmern zusammenarbeiten, um den Vertrag mit dem Auftraggeber zu erfüllen, muss der Auftragnehmer diesen ausdrücklich als Subunternehmer identifizieren und er muss sicherstellen, dass der Subunternehmer die gleichen Anforderungen erfüllt.

Auf Verlangen des Auftraggebers ist der Auftragnehmer verpflichtet, nur überprüftes Sicherheitspersonal, z. B. geprüft von nationalen Behörden, zum Umgang mit sensiblem Equipment einzusetzen, sowohl vor der der Integration in das Netzwerk des Auftraggebers als auch für die Wartung des sensiblen Equipments während der gesamten Betriebsphase. Relevante Informationen (insbesondere die Identifizierung und Bestimmung des sensiblen Equipments) müssen schriftlich vereinbart werden. Die von den lokalen gesetzlichen Bestimmungen festgelegten Ausnahmen sind zu beachten (so müssen z. B. für Auftraggeber in anderen Regionen, wie Afrika, Asien, Nordamerika sonstige Anforderungen entsprechend der örtlichen Gesetze geachtet werden).

Der Auftragnehmer beauftragt nur Personen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der aktuellen Lösung verfügen.

## 13.4 Audits

Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein anderer beauftragter Dritter im Auftrag des Auftraggebers die Organisation in Bezug auf die Informationssicherheit des Auftragnehmers auditieren darf. Dies kann einmal oder mehrmals geschehen. Die Audits werden auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden in einem Dienstleistungsvertrag oder gleichwertige Formate einvernehmlich vereinbart.

# 14 Definitionen und Abkürzungen

| | |
|---|---|
| All-Gefahren-Ansatz | Der All-Gefahren-Ansatz geht über die reine IT-Perspektive hinaus:<br>„Berücksichtigung aller (bekannten) Gefahren gleichermaßen, z. B. bei Durchführung einer Risikoanalyse, und nicht nur einzelner Bereiche wie Terrorismus oder Sabotage."<br>Quelle (06/2021): www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/KRITIS-Gefahrenlagen/kritis-gefahrenlagen_node.html |
| Assets | Wie in ISO/IEC 27005 definiert, Assets umfassen primäre (Prozesse und Informationen) und sekundäre bzw. unterstützende Vermögenswerte. |
| Auftraggeber | Im Rahmen dieses Dokumentes ist hier primär der Betreiber Kritischer Infrastrukturen gemeint. Selbstverständlich kann in diese Rolle auch jeder andere Betreiber unterhalb des Sicherheitsniveaus „Kritische Infrastruktur" einsteigen. |
| Auftragnehmer | Im Rahmen dieses Dokumentes ist der Hersteller und oder Lieferant gemeint, der als Vertragspartner des Auftraggebers auftritt. |
| BCM | Business Continuity Management |
| CVSS | Common Vulnerability Scoring System (CVSS) – Bewertungssystem für häufige Schwachstellen:<br>Internationaler Industriestandard zur Bewertung des Schweregrades von möglichen oder tatsächlichen Sicherheitslücken in IT-Systemen.<br>Siehe auch www.first.org/cvss/specification-document |
| Fernzugang | Zugang in das Netz des Auftraggebers – i. d. R. durch den Auftragnehmer |
| Kritikalität | Ein wichtiges Kriterium dafür ist die Kritikalität als relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat. |
| Penetrationstest | Ein Penetrationstest beschreibt die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks- oder Softwaresystems mit Mitteln und Methoden, die ein Angreifer anwenden würde, um unautorisiert in das System einzudringen (Penetration). Der Penetrationstest ermittelt somit die Empfindlichkeit des zu testenden Systems gegen derartige Angriffe. |
| Secure Code Review | Ein Secure Code Review ist eine spezielle Form des allgemeinen Code Reviews bei der mit Hilfe verschiedener Methoden noch bestehende Schwachstellen identifiziert werden. |
| Security by Design | Security by Design beschreibt die Integration von Sicherheitsaspekten in den vollständigen Lebenszyklus eines Produktes (Software, Hardware, Dienstleistung) bereits in der Designphase des Produktes. |
| Service Level Agreement | Ein Service Level Agreement (SLA) ist Teil eines Servicevertrages. Zwischen Auftragnehmer und -geber werden verschiedenen Eigenschaften des Service wie Umfang Qualität und Verantwortlichkeiten vereinbart. |
| Security Level Agreement | Ein Security Level Agreement (SecLA) ist eine Sonderform der SLA mit dem Fokus auf Security-Aspekten. |

| | |
|---|---|
| Schutzbedarfsanalyse | Im Rahmen der Schutzbedarfsanalyse werden sogenannte Schutzobjekte (schützenswerte Daten, Hardware, Infrastruktur etc. von Unternehmen) erkannt und mit einem realen Angriffsrisiko verknüpft. |
| Stand der Technik | Stand der Technik ist eine Technikklausel, die in verschiedenen Rechtsgebieten Verwendung findet. Man versteht darunter den bekannten technischen Entwicklungsstand und die darauf basierenden technischen Möglichkeiten zur Erreichung eines bestimmten praktischen Ziels. Der Stand der Technik (beste verfügbare Technik – BVT), steht nach der im Kalkar-Beschluss des Bundesverfassungsgerichts entwickelten Drei-Stufen-Theorie zwischen den bewährten anerkannten Regeln der Technik und dem weiter fortgeschrittenen Stand der Wissenschaft |
| Vulnerability Management | Prozess zur Erkennung und Behebung von Schwachstellen |

# 15 Literatur

[1] Beispiel für ein Security Level Agreement zum Einsatz in Kritischen Infrastrukturen
www.bsi.bund.de/dok/upk-beispiel-secla

[2] Nutzung von cloudbasierten Diensten in Kritischen Infrastrukturen - eine Hilfestellung des UP KRITIS
www.bsi.bund.de/dok/upk-hilfestellung-cloudnutzung

**Aktualisierung durch die Autorengruppe TAK Lieferanten/Hersteller in Zusammenarbeit mit dem TAK Cloudbasierte Dienste**

- Christian Behre
- Klaus Biß
- Daniel Fengler
- Sven Greven
- Uwe Jendricke
- Andreas Jünger – Sprecher
- Peter Kaminski
- Matthias Müller
- Christoph Roth
- Christian Sachgau – Leiter
- Lars Schmidt
- Philipp Töbich
- Thomas Wienand