NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

ISACA
Cyber-Sicherheits-Check

Maßnahmenziele und Referenzen im Kontext der VdS 10000

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Verantwortlichkeiten

Funktion	**Name**
Autoren	Christian H. Gresser, Arik Seils
Qualitätskontrolle	Maria Dierks
Review und Feedback	

Änderungsverzeichnis

Version	**Datum**	**Autor**	**Änderungen**
0.1	04.05.2021	Arik Seils	Entwurf
1.0	04.06.2021	Christian H. Gresser	Finalisierung

Hinweis
Aus Gründen der Verständlichkeit und Überschaubarkeit des Satzaufbaus wird in diesem Dokument bei Nennung von Personen ausschließlich die männliche Sprachform verwendet, obwohl jeweils die männliche und weibliche Form gemeint ist.

Maßnahmenziele		Basismaßnahmen	Referenzen
A	**Absicherung von Netzübergängen** Die Absicherung von Netzübergängen ist einer der entscheidenden Faktoren für eine wirksame Abwehr von Angriffen aus dem Internet. Auf Grundlage der Netzstrukturaufnahme müssen Abwehrmaßnahmen für alle internen und externen Netzübergänge sowie die entsprechenden Prozesse (wie z. B. ein Change Management) geplant und umgesetzt werden.	- Alle Netzübergänge sind identifiziert und dokumentiert. - Das Netz ist in Segmente aufgeteilt und die Anzahl der Netzübergänge wird minimal gehalten. - Alle Netzübergänge sind durch geeignete Sicherheitsgateways abgesichert und werden regelmäßig überprüft. - Auf Client- und Server-systemen findet eine technische Schnittstellenkontrolle statt, die eine zulässige Nutzung kontrolliert und eine unzulässige Nutzung verhindert. - Zugänge mobiler IT-Geräte sind angemessen abgesichert und auf das erforderliche Mindestmaß beschränkt. - Zugänge für Remote-Administration und -Überwachung sind angemessen abgesichert. - Es werden nur zeitgemäße Verschlüsselungs- und Authentisierungsverfahren eingesetzt.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.2.4, OPS.1.2.5, OPS.2.1, OPS.2.2, OPS.3.1, SYS.3.2.1, SYS.3.2.2, SYS.3.2.3, SYS.3.2.4, SYS.4.3, SYS.4.4, NET.1.1, NET.1.2, NET.2.1, NET.2.2, NET.3.1, NET.3.2, NET.3.3, IND.1.A16 **COBIT 2019:** DSS05.02, DSS05.03, DSS06.06 **ISO/IEC 27001:2013:** A.6.2.1, A.6.2.2, A.9.1.2, A.13.1.1, A.13.1.2, A.13.1.3 **PCI DSS 3.2.1:** 1.1.1, 1.1.2, 1.1.4, 1.1.6, 1.1.7, 1.2.1, 1.2.3, 1.3.1, 1.3.3, 1.4, 2.2.2, 2.2.4, 2.3 **VdS 10000:** 6.4, 9.3, 10.1, 10.2.1, 10.2.2, 10.3.1, 10.3.2, 10.3.4, 10.3.7, 10.5.4, 11.1, 11.2, 11.3, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 13.1, 13.3, 18.2

Kommentar zur VdS 10000 - Maßnahmenziele A:

6.4 Weitere Regelungen

Es müssen themenspezifische IS-Richtlinien für Mobile IT-Systeme, Mobile Datenträger, IT-Outsourcing, Datensicherung, Störungen, Ausfälle und Sicherheitsvorfälle erstellt werden. Dies betrifft auch Netzübergänge.

9.3 IT-Ressourcen

Kritische IT-Ressourcen (IT-Systeme, mobile Datenträger und Verbindungen) sind zu bestimmen und diese zu dokumentieren. Die VdS 10000 definiert IT-Systeme als kritisch, die kritische Informationen verarbeiten, speichern oder übertragen oder für den Betrieb von kritischen IT-Ressourcen dringend benötigt werden. Die Übertragung kritischer Informationen kann auf Netzübergänge zutreffen, häufig sind Netzübergänge wie die Internetanbindung selbst bereits kritisch.

10.1 Inventarisierung

Die VdS 10000 fordert die Inventarisierung aller IT-Systeme einer Organisation, dazu zählen auch Komponenten der Netzübergänge.

10.2.1 Inbetriebnahme und Änderung

Die VdS 10000 fordert ein Verfahren für die Inbetriebnahme von und Änderungen an IT-Systemen zu etablieren. Das schließt auch die Komponenten der Netzübergänge ein.

10.2.2 Ausmusterung und Wiederverwendung

Die VdS 10000 fordert ein Verfahren für das Ausmustern und Wiederverwenden von IT-Systemen. Das schließt auch die Komponenten der Netzübergänge ein.

10.3.1 Software

System- und Anwendungssoftware muss aus vertrauenswürdigen Quellen bezogen werden. Des Weiteren sollte ausschließlich Software verwendet werden die Sicherheitsupdates des Herstellers enthält und nur Software installiert werden, die zur Erfüllung der Aufgabe benötigt wird. Auch sollten sämtliche Zugriffsrechte und Privilegien der Software auf ein Mindestmaß reduziert werden. Dies trifft auch auf die Komponenten der Netzübergänge zu.

10.3.2 Beschränkung des Netzwerkverkehrs

Netzwerkverkehr muss auf das für die Funktionsfähigkeit nötige Minimum beschränkt werden, wenn über das Netzwerk ausnutzbare Schwachstellen bestehen, die nicht behoben werden können oder es sich um besonders exponierte IT-Systeme handelt. Dies muss für alle Netzübergänge überprüft und umgesetzt werden.

10.3.4 Externe Schnittstellen und Laufwerke

Externe Schnittstellen und Laufwerke, die nicht für die Aufgabenerfüllung benötigt werden, sollten auszubaut, stillgelegt, deaktiviert oder anderweitig für Nutzer unzugänglich gemacht werden. Diese Schnittstellen stellen Netzübergänge dar.

10.3.7 Authentifizierung

Der Zugang zu allen nicht öffentlichen Bereichen der IT-Systeme muss durch ein geeignetes Anmeldeverfahren, welches eine Authentisierung vorsieht, abgesichert werden. Eine Mehr-Faktor-Authentifizierung sollte eingesetzt werden. Das gilt insbesondere für Remote-Zugänge.

10.5.4 Externe Schnittstellen und Laufwerke

Die VdS 10000 fordert zusätzliche Maßnahmen für kritische Systeme. Insbesondere müssen externe Schnittstellen und Laufwerke, die nicht für die Aufgabenerfüllung benötigt werden, ausgebaut, stillgelegt, deaktiviert oder unzugänglich gemacht werden. Sicherheitsgateways sind häufig kritische Systeme.

11.1 Netzwerkplan

Die Netzwerke der Organisation müssen die physikalische und logische Netzwerkstruktur mit allen Netzwerkkopplungen und Netzübergängen dokumentieren.

11.2 Aktive Netzkomponenten

Aktive Netzkomponenten müssen wie IT-Systeme behandelt werden. Es gelten alle Anforderungen aus Kapitel 10.

11.3 Netzübergänge

Der Netzwerkverkehr muss auf das für die Funktionsfähigkeit notwendige Minimum beschränkt werden. Der Inhalt erlaubter Verbindungen muss auf Schadsoftware und Angriffe untersucht werden und erkannte Schadsoftware und Angriffe müssen blockiert werden.

11.4.1 Netzwerkanschlüsse

Dauerhaft nicht genutzte Netzwerkanschlüsse müssen vor unberechtigter Nutzung gesichert werden.

11.4.2 Segmentierung

Die Notwendigkeit einer Segmentierung der Netzwerke der Organisation muss geprüft und die Entscheidung dokumentiert werden. Die Umsetzung der Segmentierung muss eine möglichst umfassende Beschränkung der Verbindungen sowie die Möglichkeit der Protokollierung von blockierten Verbindungen beinhalten.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

11.4.3 Fernzugang

Der Zugang zu internen Netzen über weniger oder nicht vertrauenswürdige Netze muss abgesichert werden. Der Zugang muss auf die notwendigen Zugriffe beschränkt werden. Die Nutzer sollten mit einer Mehr-Faktor-Authentisierung authentifiziert werden.

11.4.4 Netzwerkkopplung

Die Kopplung von internen Netzen über externe Netze muss abgesichert werden. Dabei müssen sichere Maßnahmen zur Verschlüsselung sowie zur Sicherstellung der Integrität und Authentizität eingesetzt werden.

13.1 Server, aktive Netzwerkkomponenten und Netzwerkverteilstellen

Aktive Netzwerkkomponenten und Netzwerkverteilstellen müssen vor Beschädigungen und unberechtigtem Zugriff geschützt werden. Dabei sollten folgende Bedrohungen bewertet und behandelt werden: 1. Ungeeignete Umgebungsbedingungen, 2. Negative Umwelteinflüsse, 3. Unzuverlässige Stromversorgung, 4. Beschädigung und Verlust.

13.3 Zusätzliche Maßnahmen für kritische IT-Systeme

Für kritische IT-Systeme müssen im Zuge der Risikoanalyse und -behandlung die folgenden Bedrohungen behandelt werden: 1 ungeeignete Umgebungsbedingungen, 2. Negative Umwelteinflüsse, 3. Unzuverlässige Stromversorgung, 4. Beschädigung und Verlust, 5. Unautorisierter Zugriff, 6. Ausspähen vertraulicher Informationen.

18.2 Erkennen

Es sollten Maßnahmen implementiert werden, die es ermöglichen Sicherheitsvorfälle zu erkennen: 1. Intrusion Detection Systeme (IDS), 2. Integritätsprüfungen auf Prüfsummenbasis, 3. Sensor-Systeme (Honeypots), 4. Überwachen der Zugriffe auf besonders sensible Dateien, 5. Erfassen und Auswerten von Logmeldungen.

Maßnahmenziele		Basismaßnahmen	Referenzen
B	**Abwehr von Schadprogrammen** Im Sinne einer gestaffelten Verteidigung gegen Angriffe durch Schadprogramme (Viren, Würmer und trojanische Pferde) muss die Abwehr über eine große Zahl von IT-Systemen einschließlich der Sicherheitsgateways verteilt werden. Der eigentliche Client als Arbeitsplatzsystem ist dabei die letzte Verteidigungslinie.	- Schutzsoftware gegen Schadprogramme kommt durchgängig zum Einsatz und wird fortlaufend aktuell gehalten. - Verteilt über die verschiedenen IT-Systeme kommen mehrere Lösungen möglichst unterschiedlicher Anbieter und Technologien zum Einsatz (gestaffelte Verteidigung). - IT-Systeme ohne angemessenen Schutz vor Schadprogrammen, sind in speziellen Netzsegmenten isoliert.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.2, OPS.1.1.3, OPS.1.1.4, SYS.1, SYS.2, SYS.3, IND.1.A12 **COBIT 2019:** DSS05.01 **ISO/IEC 27001:2013:** A.12.2.1 **PCI DSS 3.2.1:** 5.1, 5.2 **VdS 10000:** 10.3.2, 10.3.5, 11.3, 11.4.2, 18.2, 18.3

Kommentar zur VdS 10000 - Maßnahmenziele B:

10.3.2 Beschränkung des Netzwerkverkehrs

Netzwerkverkehr muss auf das für die Funktionsfähigkeit nötige Minimum beschränkt werden, wenn über das Netzwerk ausnutzbare Schwachstellen bestehen, die nicht behoben werden können oder es sich um besonders exponierte IT-Systeme handelt, weil beispielsweise kein Virenschutzprogramm installiert werden kann.

10.3.5 Schadsoftware

Die VdS 10000 fordert, dass alle IT-Systeme über einen Schutz vor Schadsoftware verfügen müssen. Weiterhin müssen alle IT-Systeme täglich vollständig auf die Anwesenheit von Schadsoftware untersucht werden. Darüber hinaus sollten alle IT-Systeme über einen Echtzeitschutz verfügen, der alle Dateien bei Zugriff auf Schadsoftware prüft.

11.3 Netzübergänge

Der Inhalt erlaubter Verbindungen zu weniger oder nicht vertrauenswürdigen Netzwerken muss auf Schadsoftware und Angriffe überprüft werden und erkannte Schadsoftware und Angriffe müssen blockiert werden.

11.4.2 Segmentierung

Die Notwendigkeit einer Segmentierung der Netzwerke der Organisation muss geprüft und die Entscheidung dokumentiert werden. Die Umsetzung der Segmentierung muss eine möglichst umfassende Beschränkung der Verbindungen sowie die Möglichkeit der Protokollierung von blockierten Verbindungen beinhalten.

18.2 Erkennen

Es sollten Maßnahmen implementiert werden, die es ermöglichen Sicherheitsvorfälle zu erkennen: 1. Intrusion Detection Systeme (IDS), 2. Integritätsprüfungen auf Prüfsummenbasis, 3. Sensor-Systeme (Honeypots), 4. Überwachen der Zugriffe auf besonders sensible Dateien, 5. Erfassen und Auswerten von Logmeldungen.

18.3 Reaktion

Die VdS 10000 fordert, dass ein Verfahren implementiert werden muss, welches eine Reaktion bei Auftreten eines Sicherheitsvorfalls, z.B. erkannte Schadsoftware, sicherstellt.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Maßnahmenziele		Basismaßnahmen	Referenzen
C	**Inventarisierung der IT-Systeme** Zur Planung und anschließenden Umsetzung von Abwehrmaßnahmen auf den eingesetzten IT-Systemen ist eine vollständige Inventarisierung der eingesetzten IT-Systeme notwendig. Mithilfe dieses Inventarverzeichnisses ist insbesondere zu klären, welche verschiedenen Systemtypen in der Organisation im Einsatz sind.	- Bestand an Hard- und Software ist vollständig inventarisiert und wird fortlaufend aktualisiert. - Versionen und Patchstände von Betriebssystemen und Anwendungen werden regelmäßig aufgenommen. - Es existieren automatisierte Verfahren zur Erkennung nicht autorisierter IT-Systeme und Anwendungen.	**BSI IT-Grundschutz-Kompendium 2/2020:** ORP.1, SYS.1.5.A10, IND.1.A4, IND.1.A5, CON.4, CON.5, OPS.1.1.6, ORP.1.A7, ORP.1.A8 **COBIT 2019:** APO01.07, BAI03.04, BAI09.01, BAI09.03, BAI09.05 **ISO/IEC 27001:2013:** A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.4 **PCI DSS 3.2.1:** 2.4, 9.7, 11.1, 12.3.3, 12.3.4 **VdS 10000:** 9.3, 10.1, 10.2.1, 10.2.2

Kommentar zur VdS 10000- Maßnahmenziele C:

9.3 IT-Ressourcen

Die Organisation muss ihre kritischen Ressourcen (insbesondere die kritischen IT-Systeme, mobilen Datenträger, Verbindungen sowie die kritische Individualsoftware) bestimmen und dokumentieren.

10.1 Inventarisierung

Es muss eine Inventarisierung vorhanden sein, in der alle IT-Systeme der Organisation verzeichnet sind. Ebenfalls muss die Inventarisierung durch geeignete Verfahren vollständig und aktuell gehalten werden.

10.2.1 Inbetriebnahme und Änderung

Die VdS 10000 fordert in 10.2.1 Abs. 3, dass ein Verfahren für die Inbetriebnahme und Änderung der IT-Systeme implementiert werden muss, welches sicherstellt, dass die Inventarisierung und der Netzwerkplan aktualisiert werden.

10.2.2 Ausmusterung und Wiederverwendung

Die VdS 10000 fordert in 10.2.2 Abs. 3, dass ein Verfahren für das Ausmustern und Wiederverwenden der IT-Systeme implementiert werden muss, welches sicherstellt, dass die Inventarisierung der IT-Systeme und der Netzplan aktualisiert werden.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Maßnahmenziele		Basismaßnahmen	Referenzen
D	**Vermeidung von ausnutzbaren Sicherheitslücken** Um das Risiko erfolgreicher Cyber-Angriffe zu minimieren, müssen ausnutzbare Sicherheitslücken konsequent vermieden werden. Vorhandene Sicherheitsmechanismen von Betriebssystemen sollten daher genutzt werden. Verfügbare Sicherheitsaktualisierungen von genutzter Software müssen zeitnah getestet und anschließend installiert werden. Ein wirksamer Change-Management-Prozess sollte etabliert werden.	- Ein effizienter Prozess zum Schwachstellen- und Patchmanagement ist etabliert. - Im Rahmen der Softwareplanung wird die Nutzung stärkerer Abwehrmechanismen in aktuellerer Software gefördert. - Bekannte Sicherheitslücken werden kurzfristig durch Workarounds und bereitgestellte Sicher-heitsaktualisierungen geschlossen. - Betriebssysteme, Serverdienste und Anwendungen werden vor Inbetriebnahme gehärtet. - Ein Prozess zur sicheren Softwareentwicklung ist etabliert. - Bei der Beschaffung neuer Hard- und Software werden Sicherheitsanforderungen berücksichtigt.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1, OPS.1.1.2, OPS.1.1.3, OPS.1.1.4, OPS.1.1.6, SYS.1, SYS.2, SYS.3, APP.1, APP.2 APP.3, APP.4, APP.5, IND.1.A17, NET.3.2.A11 **COBIT 2019:** APO12.01, BAI02.01, BAI10.02, BAI10.03, BAI10.05, DSS05.03, DSS05.07 **ISO/IEC 27001:2013:** A.9.4.4, A.12.1.2, A.12.5.1, A.12.6.1, A.14.1.1, A.14.2.2, A.14.2.3, A.14.2.4 **PCI DSS 3.2.1:** 2.2, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7 **VdS 10000:** 10.2.1, 10.3.1, 10.5

Kommentar zur VdS 10000- Maßnahmenziele D:

10.2.1 Inbetriebnahme und Änderung

Es muss ein Verfahren implementiert werden, das sicherstellt, dass der Basisschutz bei der Inbetriebnahme und Änderung von IT-Systemen umgesetzt wird. Zum Basisschutz gehört auch die Härtung der Systeme.

10.3.1 Software

System- und Anwendungssoftware muss aus vertrauenswürdigen Quellen bezogen werden. Des Weiteren müssen vom Hersteller zur Verfügung gestellte Sicherheitsupdates für die System- und Anwendungssoftware getestet und bei Eignung freigegeben und nach ihrer Freigabe umgehend installiert werden.

10.5 Zusätzliche Maßnahmen für kritische IT-Systeme

Für kritische Systeme müssen zusätzliche Maßnahmen umgesetzt werden. Insbesondere müssen kritische Systeme besonders gehärtet und abgesichert werden (Abschnitt 10.5.3 und 10.5.4).

Maßnahmenziele		Basismaßnahmen	Referenzen
E	**Sichere Interaktion mit dem Internet** Alle Vorgänge, bei denen Daten und Dienste aus dem Internet abgefragt und verarbeitet werden, sind mit geeigneten Maßnahmen abzusichern. Die jeweilige Stärke der eingesetzten Schutzmechanismen muss dem Schutzbedarf der auf dem jeweiligen IT-System verarbeiteten Daten sowie den einem Angreifer zur Verfügung stehenden möglichen Weiterleitungs-mechanismen gerecht werden.	- Der Browser inklusive aller Erweiterungen (Flash, Java, ActiveX usw.) verfügt über starke Sicherheitseigenschaften und ist bei einem hohen Cyber-Sicherheits-Risiko besonders abgeschottet (z. B. Sandbox). - Eingehender E-Mail- Verkehr wird zentral auf Bedrohungen, wie Schadprogramme und Phishing-Angriffe, untersucht. - Für die Darstellung von Dokumenten aus externen Quellen werden sichere Darstellungsoptionen verwendet. - Unerwünschte aktive Inhalte werden zentral gefiltert. - Apps und andere Internetanwendungen sind durch geeignete Schutzmechanismen abgesichert. - Es existieren verbindliche Vorgaben zur sicheren Nutzung von Cloud- Services und anderen Diensten im Internet.	**BSI IT-Grundschutz-Kompendium 2/2020:** CON.7.A8, CON.7.A14, OPS.1.2.4.A7, NET.1.2.A13, ORP.4.A22, ORP.4.A23 **COBIT 2019:** BAI10.02, BAI10.03, BAI10.05, DSS05.01 **ISO/IEC 27001:2013:** A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4 **PCI DSS 3.2.1:** 1.1, 1.4, 4.1, 6.6, A1 **VdS 10000:** 7.2, 11.3

Kommentar zur VdS 10000- Maßnahmenziele E:

7.2 Aufnahme der Tätigkeit

Die VdS 10000 fordert, dass ein Verfahren implementiert wird, welches im Zuge der Aufnahme der Tätigkeit eines Mitarbeiters sicherstellt, dass Mitarbeiter in die IS-Leitlinie und in sämtliche für sie relevante Regelungen zur Informationssicherheit eingewiesen und geschult werden.

11.3 Netzübergänge

Der Inhalt erlaubter Verbindungen zu weniger oder nicht vertrauenswürdigen Netzwerken muss auf Schadsoftware und Angriffe überprüft werden und erkannte Schadsoftware und Angriffe müssen blockiert werden.

Maßnahmenziele		Basismaßnahmen	Referenzen
F	**Logdatenerfassung und Auswertung** Oftmals bleiben Sicherheitsvorfälle unerkannt, weil kurzfristig kein sichtbarer oder offensichtlicher Schaden eintritt. Mithilfe eines gut getarnten und hinreichend vorsichtigen Vorgehens ist es Angreifern aber u. U. möglich, über längere Zeiträume die Kontrolle über Zielsysteme zu übernehmen, ohne dass diese Angriffe unmittelbar aufgrund singulärer Ereignisse detektiert werden. Daher ist es notwendig, ebenfalls Verfahren zur Aufdeckung von nicht offensichtlichen Sicherheitsvorfällen und langfristig angelegten Angriffen zu entwickeln.	- Relevante Logdaten werden zusätzlich zur Umsetzung einschlägiger gesetzlicher, regulatorischer und organisatorischer Anforderungen auch mit dem Ziel der Angriffsdetektion erfasst und regelmäßig ausgewertet. - Die Nutzung privilegierter Konten und administrativer Zugriffe wird fortlaufend überwacht. - Logdaten sind angemessen vor Manipulation und Zerstörung geschützt, z. B. durch Auslagerung auf zentrale Log- Management-Server.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.5, DER.1.A6, DER.1.A7, DER.1.A8, DER.1.A9, DER.1.A10, DER.1.A11, DER.1.A12, DER.1.A13, DER.1.A14, DER.1.A15, DER.1.A16, DER.1.A17, DER.1.A18, IND.1.A10, IND.1.A15 **COBIT 2019:** APO11.04, DSS05.04, DSS05.07 **ISO/IEC 27001:2013:** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4 **PCI DSS 3.2.1:** 10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.4, 10.2.5, 10.2.6, 10.2.7, 10.3, 10.4, 10.5, 10.6 **VdS 10000:** 10.3.3, 10.5.8, 16.5.2, 16.6.2, 18.2

Kommentar zur VdS 10000- Maßnahmenziele F:

10.3.3 Protokollierung

Jedes IT-System muss erfolgreiche und erfolglose Anmeldeversuche, Fehler und Informationssicherheitsereignisse protokollieren. Weiter fordert sie, dass Protokolldateien zentral gespeichert werden sollten. Protokolldateien müssen sechs Monate lang aufbewahrt werden, sofern keine gesetzlichen Lösch- oder Aufbewahrungsfristen entgegenstehen.

10.5.8 Überwachung

Die VdS 10000 fordert, dass überwacht werden muss, ob sich kritische IT-Systeme im Regelbetrieb befinden. Dabei muss sichergestellt werden, dass der Ausfall eines kritischen IT-Systems erkannt und entsprechende Gegenmaßnahmen eingeleitet werden. Darüber hinaus sollten die Ressourcen kritischer IT-Systeme überwacht werden, um Engpässe zu erkennen, bevor sie akut werden.

16.5.2 Server

Die VdS 10000 fordert, dass Server so gesichert sein müssen, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist. Explizit wird gefordert, dass sich auch Logdaten wiederherstellen lassen.

16.6.2 Verfahren

Die VdS 10000 fordert, dass kritische IT-Systeme vollständig gesichert werden müssen. Diese Sicherung muss auch die Logdaten beinhalten.

18.2 Erkennen

Es sollten Maßnahmen implementiert werden, die es ermöglichen Sicherheitsvorfälle zu erkennen: 1. Intrusion Detection Systeme (IDS), 2. Integritätsprüfungen auf Prüfsummenbasis, 3. Sensor-Systeme (Honeypots), 4. Überwachen der Zugriffe auf besonders sensible Dateien, 5. Erfassen und Auswerten von Logmeldungen.

Maßnahmenziele		Basismaßnahmen	Referenzen
G	**Sicherstellung eines aktuellen Informationsstandes** Die Fähigkeit zur Planung wirksamer Cyber-Sicherheits-Maßnahmen wird im Wesentlichen durch die Qualität und den Umfang des eigenen Informationsstands bestimmt. Daher muss die Versorgung mit aktuellen und fachlich verlässlichen Informationen zur Cyber-Sicherheit sichergestellt werden.	- Aktuelle Informationen zur Cyber-Sicherheit werden fortlaufend aus verlässlichen Quellen bezogen und ausgewertet. - Cyber-Sicherheits- Maßnahmen werden regelmäßig auf der Basis vorhandener Informationen hinsichtlich ihrer Wirksamkeit überprüft und angepasst.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1 IND.1.A1, ORP.4.A4 **COBIT 2019:** APO12.01, APO13.02, DSS04.02, DSS05.01 **ISO/IEC 27001:2013:** A.6.1.1, A.6.1.2, A.6.1.4, A.16.1.3 **PCI DSS 3.2.1:** 6.1, 6.2 **VdS 10000:** 4.3, 6.1, 8, 8.1

Kommentar zur VdS 10000- Maßnahmenziele G:

4.3. Informationssicherheitsbeauftragter (ISB)

Die VdS 10000 fordert, dass der Informationssicherheitsbeauftragte folgende Verantwortlichkeiten wahrnimmt: Steuern, Koordinieren und Prüfen der technischen und organisatorischen Maßnahmen, kontinuierliches Verbessern der Informationssicherheit, insbesondere Anpassen der Informationssicherheit an neue Bedrohungen, Änderungen im technischen und organisatorischen Umfeld und an neue gesetzliche, betriebliche und vertragliche Anforderungen.

6.1 Allgemeine Anforderungen

Jede IS-Richtlinie muss jährlich auf Aktualität geprüft und ggf. angepasst werden. Bei der Erstellung und Anpassung sollten alle Anforderungen ermittelt und umgesetzt werden.

8 Wissen

Die VdS 10000 weist in 8 auf die Notwendigkeit hin, dass die Organisation über aktuelles Wissen in Bezug auf Informationssicherheit verfügt.

8.1 Aktualität des Wissens

Es muss ein Verfahren implementiert werden, das sicherstellt, dass regelmäßig aus verlässlichen Quellen Informationen über die aktuellen technischen und rechtlichen Entwicklungen im Bereich der Informationssicherheit, insbesondere über neue Gefährdungen und mögliche Gegenmaßnahmen, bezogen werden.

Maßnahmenziele		Basismaßnahmen	Referenzen
H	**Bewältigung von Sicherheitsvorfällen/Notfällen** Geeignete Prozesse und Verfahren zur Bewältigung von Sicherheitsvorfällen sind zu etablieren und zu üben, um eine schnelle und angemessene Bewältigung von Sicherheitsvorfällen und damit die Aufrecht-erhaltung des Geschäftsbetriebs sicherzustellen.	- Es existieren etablierte Prozesse und Verfahren zur schnellen und angemessenen Bewältigung von Sicherheitsvorfällen. - Die Bewältigung von Sicherheitsvorfällen wird regelmäßig geübt. - Abgeschlossene Sicherheits-vorfälle werden hinsichtlich der Ursachen und möglicher Konsequenzen ausgewertet. - Sicherheitsvorfälle werden zur Strafverfolgung und Lagebild-erstellung an die zuständigen Behörden gemeldet.	**BSI IT-Grundschutz-Kompendium 2/2020:** IND.1.A13, IND.2.7.A5, NET.2.1.A8, NET.2.2.A4, NET.3.2.A12, ORP.1.A10, OPS.1.1.2.A2, OPS.2.1.A14, DER.2.1.A1, DER.2.1.A2, DER.2.1.A3, DER.2.1.A4, DER.2.1.A5, DER.2.1.A6, DER.2.1.A7, DER.2.1.A8, DER.2.1.A9, DER.2.1.A10, DER.2.1.A11, DER.2.1.A13, DER.2.1.A14 **COBIT 2019:** APO12.06, DSS02.02, DSS02.04, DSS04.03 **ISO/IEC 27001:2013:** A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.17.1.1, A.17.1.2, A17.1.3, A.17.2.1 **PCI DSS 3.2.1:** 11.1.2, 12.5.3, 12.10, A1.4 **VdS 10000:** 6.4, 8.2, 18, 18.1, 18.3

Kommentar zur VdS 10000- Maßnahmenziele H:

6.4 Weitere Regelungen

Die VdS 10000 fordert in 6.4 Abs. 6, dass ggf. weitere themenspezifische IS-Richtlinien erarbeitet werden. Ausdrücklich genannt wird eine Richtlinie zur Behandlung von Störungen und Ausfällen sowie eine Richtlinie zu Sicherheitsvorfällen.

8.2 Schulung und Sensibilisierung

Es muss ein Verfahren für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden, das den Umgang mit vorhandenen Sicherheitsmaßnahmen sowie das Verhalten bei Störungen, Ausfällen und Sicherheitsvorfällen schult.

18 Sicherheitsvorfälle

Eine angemessene Reaktion auf Sicherheitsvorfälle ermöglicht, Schäden schnell einzudämmen und beheben zu können. Deshalb ist es notwendig, angemessen auf Sicherheitsvorfälle vorbereitet zu sein.

18.1 IS-Richtlinie

Es müssen Regelungen für den Umgang mit Sicherheitsvorfällen getroffen werden. Das umfasst: 1. Die Definition des Begriffs Sicherheitsvorfall, 2. Jeder Mitarbeiter meldet mögliche Sicherheitsvorfälle an den ISB, 3. Der ISB untersucht, ggf. in Zusammenarbeit mit den jeweiligen Prozessverantwortlichen, dem IT-Verantwortlichen und den Administratoren, Sicherheitsvorfälle vordringlich, 4. Es wird definiert, in welchen Fällen das Topmanagement über Sicherheitsvorfälle informiert wird, 5. Es wird definiert, wie die Organisation intern und nach außen über akute und bewältigte Sicherheitsvorfälle kommuniziert.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

18.3 Reaktion

Es muss ein Verfahren implementiert werden, dass beim Auftreten eines Sicherheitsvorfalls eine angemessene Reaktion zeitnah sicherstellt.

Maßnahmenziele		Basismaßnahmen	Referenzen
I	**Sichere Authentisierung** Zur sicheren Authentisierung von Benutzern sollten komplexe Passwörter und/oder Multifaktor-Authentisierungsverfahren genutzt werden. Authentisierungsdaten für Bereiche unterschiedlichen Schutzbedarfs sollten voneinander getrennt werden.	- Der Zugang zu kritischen Ressourcen wird durch den Einsatz von Multifaktor-Authentisierungsverfahren abgesichert. - Authentisierungsdaten für Bereiche unterschiedlichen Schutzbedarfs sind voneinander getrennt, z. B. Konten von Administratoren und anderen Nutzern. - Es werden nur sichere Authentisierungsprotokolle eingesetzt. - Authentisierungsdaten wie z. B. Passwort-Hashes oder private Schlüssel werden angemessen geschützt.	**BSI IT-Grundschutz-Kompendium 2/2020:** ORP.4.A9, ORP.4.A10, ORP.4.A12, ORP.4.A13, ORP.4.A21 **COBIT 2019:** DSS05.04, DSS06.03 **ISO/IEC 27001:2013:** A.9.1.1, A.9.1.2, A.9.2.4, A9.3.1, A.9.4.2, A.9.4.3, A.9.4.4 **PCI DSS 3.2.1:** 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.8 **VdS 10000:** 8.2, 10.3.7, 10.3.8, 15.1, 15.2

Kommentar zur VdS 10000- Maßnahmenziele I:

8.2 Schulung und Sensibilisierung

Die VdS 10000 fordert, dass ein Verfahren für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden muss, welches den Umgang mit den vorhandenen Sicherheitsmaßnahmen schult.

10.3.7 Authentifizierung

Der Zugang zu allen nichtöffentlichen Bereichen der IT-Systeme muss durch geeignete Anmeldeverfahren abgesichert werden. Zugänge müssen strukturiert verwaltet werden. Mehr-Faktor-Authentifizierung sollte eingesetzt werden.

10.3.8 Zugänge und Zugriffe

Die VdS 10000 fordert, dass mit Hilfe von getrennten Zugängen und geeigneter Zugriffsrechte sichergestellt werden muss, dass Nutzer keine administrativen Arbeiten durchführen können.

15.1 Verwaltung

Ein Verfahren für das Anlegen und Verwalten von Zugängen und Zugriffsrechten muss implementiert werden. Zugänge und Zugriffsrechte dürfen nur genehmigt werden, wenn sie für die Aufgabenerfüllung des jeweiligen Nutzers oder für die betrieblichen Abläufe der Organisation notwendig sind

15.2 Zusätzliche Maßnahmen für kritische IT-Systeme und Informationen

Die VdS 10000 fordert für kritische IT-Systeme und Informationen, dass alle Zugänge zu kritischen IT-Systemen sowie sämtliche Zugriffsrechte auf kritische Informationen jährlich erfasst und daraufhin geprüft werden müssen, ob sie korrekt angelegt wurden und noch benötigt werden.

Maßnahmenziele		Basismaßnahmen	Referenzen
J	**Gewährleistung der Verfügbarkeit notwendiger Ressourcen** Zur wirksamen Abwehr von Bedrohungen der Cyber-Sicherheit sollten ausreichend eigene finanzielle und personelle Ressourcen bereitgestellt und bei Bedarf auf qualifizierte externe Dienstleister zurückgegriffen werden.	- Finanzielle und personelle Ressourcen zur Abwehr von Bedrohungen der Cyber-Sicherheit stehen ausreichend zur Verfügung. - Bei Bedarf werden qualifizierte und zuverlässige externe Dienstleister eingebunden. - Datensicherungen und Wiederherstellungstests müssen regelmäßig durchgeführt werden.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1.A1, ISMS.1.A2, ISMS.1.A3, ISMS.1.A4, ISMS.1.A5, ISMS.1.A6, ISMS.1.A8, ISMS.1.A15, OPS.1.1.2.A9, OPS.1.1.2.A10 **COBIT 2019:** APO07.01, APO10.02, APO14.01, APO14.10, DSS4.07 **ISO/IEC 27001:2013:** A.6.1.1, A.2.1.2, A.7.2.1 **PCI DSS 3.2.1:** 6.4.5.4, 12.10.1 **VdS 10000:** 4.1.1, 4.1.3, 4.2, 16, 16.2, 16.3

Kommentar zur VdS 10000- Maßnahmenziele J:

4.1.1 Zuweisung und Dokumentation

Die VdS 10000 fordert, dass für jede Verantwortlichkeit dokumentiert wird, welche Ressourcen für die Wahrnehmung der Verantwortlichkeit zur Verfügung stehen.

4.1.3 Zeitliche Ressourcen

Um die zugewiesenen Verantwortlichkeiten wahrzunehmen, müssen die entsprechenden Mitarbeiter im erforderlichen Umfang von anderen Tätigkeiten freigestellt werden.

4.2 Topmanagement

Die VdS 10000 fordert, dass sich das Topmanagement zur Bereitstellung der notwendigen technischen, finanziellen und personellen Ressourcen für die Informationssicherheit verpflichtet.

16 Datensicherung und Archivierung

Datensicherung sollte auf Basis eines anerkannten Standards durchgeführt werden.

16.2 Archivierung

Die Organisation muss prüfen, welche Daten archiviert werden müssen.

16.3 Verfahren

Für die Datensicherung, -wiederherstellung und -archivierung müssen Verfahren implementiert werden. Es muss sichergestellt werden, dass Daten vor Änderungen, Beschädigung, Verlust und unberechtigter Einsichtnahme geschützt werden. Die Datensicherung und -wiederherstellung muss jährlich oder bei einer Änderung des Verfahrens getestet werden.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Maßnahmenziele		Basismaßnahmen	Referenzen
K	**Sensibilisierung und Schulung von Mitarbeitern** Auch das eigene Personal muss in den Mittelpunkt einer Cyber-Sicherheitsstrategie gerückt werden. Sämtliche technischen Vorkehrungen können durch menschliche Fehler oder bewusste Fehlhandlungen unwirksam werden.	- Anwender und IT-Personal werden zielgruppenorientiert regelmäßig für die Gefahren eines Cyber-Angriffs sensibilisiert und hinsichtlich des korrekten Verhaltens geschult. - IT-Personal und Management sind mit ihren Rollen und Verantwortlichkeiten vertraut. - Es ist eine klare Rollentrennung vorhanden. Eine Konzentration zu vieler Zuständigkeiten in einer Rolle wird vermieden.	**BSI IT-Grundschutz-Kompendium 2/2020:** ISMS.1.A8, ISMS.1.A9, ISMS.1.A14, ORP.1.A1, ORP.1.A2, ORP.1.A6, OPS.1.1.2.A10 **COBIT 2019:** APO07.02, APO07.03, APO13.02, DSS05.01, DSS05.04, DSS06.03 **ISO/IEC 27001:2013:** A.6.1.1, A.7.2.2, A8.1.2 **PCI DSS 3.2.1:** 6.4.2, 7.1, 7.2, 12.6 **VdS 10000:** 4.1, 4.1.1, 4.1.2, 8.2

Kommentar zur VdS 10000- Maßnahmenziele K:

4.1 Verantwortlichkeiten

Die VdS 10000 fordert, dass Verantwortlichkeiten eindeutig und widerspruchsfrei zugewiesen werden müssen.

4.1.1 Zuweisung und Dokumentation

Für jede Verantwortlichkeit muss dokumentiert werden, welche Ziele erreicht werden sollen, welche Berechtigungen an die Verantwortlichkeit gebunden sind, um diese wahrnehmen zu können und welche

4.1.2 Funktionstrennung

Bei der Verteilung der Verantwortlichkeiten muss das Prinzip der Funktionstrennung umgesetzt werden. Widersprüchliche Verantwortlichkeiten nicht von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

8.2 Schulung und Sensibilisierung von Mitarbeitern

Es muss ein Verfahren für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden, das sicherstellt, dass Maßnahmen regelmäßig und bei Bedarf sowie zielgruppenorientiert durchgeführt werden.

Maßnahmenziele		Basismaßnahmen	Referenzen
L	**Sichere Nutzung sozialer Netze** Die Sensibilisierung von Mitarbeitern muss insbesondere das Verhalten in sozialen Netzen in Form verbindlicher Vorgaben (Social Media Guidelines) und Aufklärungsmaßnahmen umfassen.	- Es existieren verbindliche Vorgaben (Social Media Guidelines) hinsichtlich des sicheren und seriösen Auftritts der Organisation sowie der beruflichen Profile der Beschäftigten in sozialen Netzwerken. - Mitarbeiter werden regelmäßig hinsichtlich der Risiken und des korrekten Verhaltens in sozialen Netzwerken sensibilisiert. - Direkte Schnittstellen zwischen sozialen Netzwerken und der organisationseigenen Infrastruktur, sofern vorhanden, sind angemessen abgesichert.	**BSI IT-Grundschutz-Kompendium 2/2020:** APP.1.4.A2, CON.9.A1, CON.9.A2, CON.9.A3, CON.9.A4 **COBIT 2019:** APO07.03 **ISO/IEC 27001:2013:** A.7.2.2, A.8.1.3, A.8.2.3, A.13.2.1, A.13.2.2, A.13.2.3 **PCI DSS 3.2.1:** n. a. **VdS 10000:** 6.3, 8.2

Kommentar zur VdS 10000- Maßnahmenziele L:

6.3 Regelungen für Nutzer

Die VdS 10000 fordert, dass für den Umgang mit der IT, Regelungen getroffen werden müssen, die in ihrer Gesamtheit für alle Nutzer (inkl. aller Führungsebenen) sowie für die gesamte IT verbindlich sind. Diese Regelungen sollten auch den Umgang mit den sozialen Netzen behandeln.

8.2 Schulung und Sensibilisierung von Mitarbeitern

Es muss ein Verfahren für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden, das sicherstellt, dass Maßnahmen regelmäßig und bei Bedarf sowie zielgruppenorientiert durchgeführt werden.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Maßnahmenziele		Basismaßnahmen	Referenzen
M	**Durchführung von Penetrationstests** Es sollten regelmäßige Penetrationstests von qualifizierten und erfahrenen Personen, die nicht an der Planung oder Implementierung der zu beurteilenden IT-Systeme beteiligt waren, durchgeführt werden.	- Um die technische Maßnahmenwirksamkeit zu prüfen und zu bestätigen, werden regelmäßig Penetrationstests von qualifizierten Personen durchgeführt. - Umfang und Intensität der Penetrationstests sind der Cyber-Sicherheits-Risikoeinschätzung angemessen. - Die Ergebnisse von Penetrationstests werden konsequent zur Reduzierung von Risiken genutzt.	**BSI IT-Grundschutz-Kompendium 2/2020:** OPS.1.1.6.A14 **COBIT 2019:** APO12.01, APO13.02, DSS05.02 **ISO/IEC 27001:2013:** A.14.2.8, A.18.2.1, A.18.2.3 **PCI DSS 3.2.1:** 11.3, A3.2.4 **VdS 10000:** -

Kommentar zur VdS 10000- Maßnahmenziele M:

Die VdS 10000 enthält keine Vorgaben zur Durchführung von Penetrationstests.

Maßnahmenziele		Basismaßnahmen	Referenzen
N	**Sicherer Umgang mit Cloud-Anwendungen** Es sollten regelmäßig die genutzten Cloud-Anwendungen überprüft werden und einem Freigabeprozess unterliegen. Nicht zulässige Cloud-Anwendungen sollten gesperrt, erlaubte durch geeignete Sicherheitsmaßnahmen geschützt werden.	- Es existieren verbindliche Vorgaben hinsichtlich der Speicherung, Verwendung und Verarbeitung von Daten in Cloud-Anwendungen. - Anwendbare Sicherheitsstandards und vertragliche Anforderungen werden gegenüber dem Cloud Service Provider durchgesetzt. - Cloud-Dienste werden fachgerecht provisioniert, administriert und überwacht. - Mitarbeiter werden regelmäßig hinsichtlich der Risiken und des korrekten Umgangs mit Cloud-Anwendungen sensibilisiert. - Direkte Schnittstellen zwischen Cloud- Anwendungen und der organisationseigenen Infrastruktur, sofern vorhanden, sind angemessen abgesichert.	**BSI-Standard 200-2 V1.0:** Kapitel 10.1.1, insbesondere 10.1.3 **BSI IT-Grundschutz-Kompendium 2/2020:** OPS.2.1.A1, OPS.2.1.A3, OPS.2.1.A4, OPS.2.1.A5, OPS.2.1.A6, OPS.2.1.A7, OPS.2.1.A8, OPS.2.1.A9, OPS.2.1.A10, OPS.2.1.A11, OPS.2.1.A12, OPS.2.1.A13, OPS.2.1.A15 **COBIT 2019:** APO07.03, APO09.01, APO09.02, APO09.03, DSS01.02, DSS01.03, DSS05.02, DSS06.03 **ISO/IEC 27001:2013:** A.15.1.1, A15.1.2, A15.1.3, A15.2.1, A15.2.2, A.18.2.1, A.18.2.2, A.18.2.3 **PCI DSS 3.2.1:** 2.6, 12.8, A1 **VdS 10000:** 8.2, 14, 14.1, 14.2, 14.3, 14.4

Kommentar zur VdS 10000- Maßnahmenziele N:

8.2 Schulung und Sensibilisierung von Mitarbeitern

Es muss ein Verfahren für Schulungs- und Sensibilisierungsmaßnahmen implementiert werden, das sicherstellt, dass Maßnahmen regelmäßig und bei Bedarf sowie zielgruppenorientiert durchgeführt werden.

14 IT-Outsourcing und Cloud-Computing

Die Sicherheitsinteressen der Organisation müssen berücksichtigt werden.

14.1 IS-Richtlinien

Die VdS 10000 fordert, dass in einer IS-Richtlinie die Bedingungen festgelegt werden müssen, unter denen IT-Ressourcen ausgelagert werden dürfen.

14.2 Vorbereitung

Für jedes Vorhaben, das zur Auslagerung von IT-Ressourcen führt, muss dokumentiert werden, welche Ressourcen ausgelagert werden sollen, ob die Ressourcen kritisch sind und welche betrieblichen, gesetzlichen und vertraglichen Bestimmungen erfüllt werden müssen.

14.3 Vertragsgestaltung

Wenn IT-Ressourcen ausgelagert werden sollen, muss ein Vertrag mit dem Anbieter geschlossen werden, der die Anforderungen enthält und den Anbieter zu deren Erfüllung verpflichtet.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

14.4 Zusätzliche Maßnahmen für kritische IT-Ressourcen

Die VdS 10000 fordert für kritische IT-Ressourcen, dass wenn IT-Ressourcen ausgelagert werden, die Anforderungen an ihre Vertraulichkeit, Verfügbarkeit und Integrität im Rahmen einer Risikoanalyse ermittelt und notwendige Punkte vertraglich geregelt werden.