CyberSeal Audithandbuch

Version 1.3, 14. April 2022

Inhaltsverzeichnis

[1 Zweck des Dokuments 3](#_Toc93313953)

[2 Das Gütesiegel CyberSeal 3](#_Toc93313954)

[3 Grundlagen 4](#_Toc93313955)

[3.1 Begriffe 4](#_Toc93313956)

[3.2 Scope des Gütesiegels 4](#_Toc93313957)

[3.3 Abgrenzung zu anderen Zertifizierungen/Frameworks 4](#_Toc93313958)

[4 Organisatorische Aspekte des Audits 5](#_Toc93313959)

[4.1 CyberSeal Standard 5](#_Toc93313960)

[4.2 Erfüllungsgrad der Audit-Anforderungen 6](#_Toc93313961)

[4.3 Selbstdeklaration 6](#_Toc93313962)

[4.4 Priorisierung der Audit-Anforderungen 6](#_Toc93313963)

[4.5 Unterscheidung in der Art der Prüfung 6](#_Toc93313964)

[4.6 Abweichungen 7](#_Toc93313965)

[4.7 Ablauf für den Erhalt des Gütesiegels 7](#_Toc93313966)

[4.8 Kosten für die Audits 8](#_Toc93313967)

[4.9 Anforderungen an den Auditor 8](#_Toc93313968)

[4.10 Durchführung des Audits 8](#_Toc93313969)

[4.11 Trägerschaft für das Gütesiegel 9](#_Toc93313970)

[4.12 Vorgehen bei unterschiedlichen Meinungen 9](#_Toc93313971)

[4.13 Sicherheitshandbuch für die Praxis 9](#_Toc93313972)

[5 Audit Anforderungen 9](#_Toc93313973)

[5.1 Aufgabenteilung Kunde/IT-Dienstleister 9](#_Toc93313974)

[5.2 Verwaltung des Zugriffes auf Kundeninfrastruktur 10](#_Toc93313975)

[5.3 Dokumentation 10](#_Toc93313976)

[5.4 Credentials und Berechtigungen der Mitarbeiter des KMU 10](#_Toc93313977)

[5.5 Netzwerkdesign 11](#_Toc93313978)

[5.6 Firewalls 11](#_Toc93313979)

[5.7 WLAN 11](#_Toc93313980)

[5.8 AD Design 12](#_Toc93313981)

[5.9 Hardening der IT-Komponenten 12](#_Toc93313982)

[5.10 Mail-System 12](#_Toc93313983)

[5.11 Patch Management 12](#_Toc93313984)

[5.12 Mobile Devices 13](#_Toc93313985)

[5.13 Home-Office 13](#_Toc93313986)

[5.14 Malware Protection 13](#_Toc93313987)

[5.15 Backup 14](#_Toc93313988)

[5.16 Change-Management/Incident Management 14](#_Toc93313989)

[5.17 Protokollierung 14](#_Toc93313990)

[5.18 Monitoring 14](#_Toc93313991)

[5.19 Entsorgung von Datenträgern 14](#_Toc93313992)

[5.20 Services von Drittanbietern 14](#_Toc93313993)

[5.21 Schwachstellen beim Kunden 15](#_Toc93313994)

[5.22 Ausbildung der Mitarbeiter 15](#_Toc93313995)

[5.23 Notfallkonzept 15](#_Toc93313996)

[5.24 Ablaufende Termine 15](#_Toc93313997)

[5.25 Physische Sicherheit 15](#_Toc93313998)

[5.26 Risiko Management 16](#_Toc93313999)

# Zweck des Dokuments

In diesem Handbuch wird die Anwendung der CyberSeal Prüfliste detailliert beschrieben. Beim Bestehen des Audits zeichnet die Allianz Digitale Sicherheit Schweiz ADSS den IT-Dienstleister mit dem CyberSeal Gütesiegel aus. Dieses Gütesiegel bestätigt, dass der IT-Dienstleister das Audit ohne Hauptabweichung bestanden hat.

**Das Gütesiegel ist 3 Jahre gültig unter der Bedingung, dass die Aufrechterhaltungsaudits in den nachfolgenden Jahren zwei und drei bestanden worden.**

Es ist geplant, das Handbuch jährlich zu überarbeiten.

# Das Gütesiegel CyberSeal

Das Gütesiegel CyberSeal basiert auf der Tatsache, dass die überwiegende Mehrheit der KMU eng mit einem primären IT-Dienstleister zusammenarbeitet, da ein KMU in der Regel nicht in der Lage ist, die Aspekte eines sicheren Aufbaus und Betriebes der heute üblichen und notwendigen Informationstechnologie (IT) sicherzustellen. Damit ist die erreichte Sicherheit eines KMU zu einem grossen Teil vom primären IT-Dienstleister abhängig. Mit dem Gütesiegel wird definiert, welche Sicherheitsaspekte der IT-Dienstleister für sich und seine Kunden implementieren muss. Das KMU kann sich darauf verlassen, dass ein mit dem CyberSeal Gütesiegel ausgezeichneter IT-Dienstleister wichtige Aspekte der Cybersicherheit ausreichend berücksichtigt.

Beim CyberSeal Audit wird der Fragenkatalog der CyberSeal Prüfliste beantwortet. Die Fragen sind nach Relevanz kategorisiert. Die Kategorisierung wurde so gewählt, dass das Gütesiegel auch für kleinere IT-Dienstleister erreichbar ist.

Es werden in erster Linie Sicherheitsaspekte berücksichtigt, die für KMU zentral sind und im KMU-Umfeld von potenziellen Angreifern häufig ausgenutzt werden. Für die Entwicklung des Standards sind die Meldungen der Versicherungen und von staatlichen Organisationen wie NCSC (Melani) über die tatsächlich aufgetretenen Schäden im letzten Jahr sehr wichtig. Das Ziel ist, die bekanntesten und häufig ausgenutzten Schwachstellen bei KMU zu beheben.

Die Konzentration auf die häufigsten Schäden bedingt aber, dass nicht alle von IT-Sicherheitsfachleuten bezeichnenden «notwendigen Massnahmen» überprüft werden. Der Fokus richtet sich hauptsächlich auf KMU und ihre typischen IT-Dienstleister in der Schweiz. Das obige Vorgehen entspricht nicht in allen Belangen den Vorgaben von rechtlicher Seite und den üblichen Annahmen der IT-Security-Fachleute. Es entspricht aber den in der Schweiz üblichen Sachverhalten im KMU-Umfeld.

Das Gütesiegel CyberSeal hat einen hohen Anspruch an Aktualität. Neueste Entwicklungen bei den An-greifern und Schadensarten werden jährlich im angepassten Standard eingearbeitet. Dieser aktuelle Standard erlaubt konkretere Fragen in der CyberSeal Prüfliste. Konkretere Fragen minimieren die Abhängigkeit vom jeweiligen Auditor.

Das Gütesiegel CyberSeal unterscheidet sich in mehreren Punkten von gängigen Information-Security-Labels, Gütesiegeln und Zertifizierungen (wie beispielsweise ISO/IEC 27001):

* Das Gütesiegel berücksichtigt die Einbettung der IT in die schweizerischen KMU. Es sind insbesondere die KMU und ihre IT-Dienstleister angesprochen. Hier ist es üblich, dass die KMU ihrem IT-Dienstleister in allen Aspekten der IT-Sicherheit vertrauen.
* Das Gütesiegel stellt sicher, dass der IT-Dienstleister die relevantesten Sicherheitsmassnahmen für übliche KMU trifft. Das Schwergewicht liegt auf der Cybersicherheit.
* Das Gütesiegel ist massiv einfacher zu erreichen als eine ISO/IEC 27001 Zertifizierung.
* Das Gütesiegel erlaubt KMU einen guten IT-Dienstleister zu finden.
* Das Gütesiegel widerspiegelt die aktuelle Gefährdungslage.

# Grundlagen

## Begriffe

**IT-Dienstleister**: Der IT-Dienstleister ist eine Firma, die IT-Dienstleistungen verschiedenen KMU zur Verfügung stellt. Der IT-Dienstleister ist damit auch die zentrale Vertrauensstelle bezüglich der IT-Sicherheit der KMU. Es gibt ca. 5'000 Firmen in der Schweiz, die als IT-Dienstleister gelten.

**KMU**: Ein KMU ist eine kleinere oder mittlere Firma. Für das Gütesiegel wird davon ausgegangen, dass eine KMU eher klein ist und sich in den Belangen der IT-Sicherheit auf die Empfehlungen eines IT-Dienstleisters stützt.

**Drittanbieter**: Weitere Dienstleister, welche durch den IT-Dienstleister oder die KMU beauftragt werden, Dienstleistungen oder Services zu erbringen. Der IT-Dienstleister ist für die sichere Integration dieses Drittanbieters verantwortlich. Die Drittanbieter können sehr unterschiedlich sein: Applikationsanbieter (z. B. Abacus), Dropbox, Office 365 und andere Cloudanbieter.

**Auditor**: Ein von der Trägerorganisation Allianz Digitale Sicherheit Schweiz ADSS bestimmter Auditor, der das Gütesiegel vergeben kann. ADSS kann die Ernennung von Auditoren auch an weitere Firmen im Auditbereich (z. B. SGS, BDO usw.) delegieren.

**Privilegierter Account**: Ein Account, mit dem man erhöhte Berechtigungen hat.

**Mehrfaktorauthentifizierung**: Es werden üblicherweise zwei unterschiedliche Faktoren für die Authentifizierung verwendet. Dies umfasst in diesem Dokument sowohl gängige Verfahren mittels eines Tokens (SMS, Authenticator usw.) und auch weitere Verfahren wie beispielsweise eingeschränkte IP-Adressbereiche und zertifikatsgeschützte Geräte. Mehrfach notwendige Authentifizierungen (z. B. Systemlogin und nachher ein Applikationslogin gelten nicht als Mehrfaktorauthentifizierungen).

**Starke Authentifizierung**: Passwortbasierte Authentifizierungsverfahren, welche mit herkömmlichen Mitteln nur mit sehr grossem Aufwand zu überlisten sind. Die Passwörter dürfen durch natürliche Personen nicht einfach merkbar sein.

**Dokumentation**: Eine Dokumentation ist jegliche Form von Informationen, welche auffindbar, nachvollziehbar, periodisch überprüft und einem Änderungsverfahren unterworfen sind. Eine Dokumentation kann insbesondere auch im Programm-Code oder einer Konfiguration vorhanden sein.

**Mobile Geräte**: Geräte, welche nicht an einen geografischen Standort gebunden sind und/oder eine mobile Stromversorgung (integrierter Energiespeicher) besitzen. Typische mobile Geräte sind Notebooks und Smartphones.

## Scope des Gütesiegels

Das Gütesiegel wird IT-Dienstleistern vergeben, welche die IT eines KMU aufbauen und betreiben. Bei grösseren IT-Dienstleistern wird allenfalls nur ein Teilbereich der Firma mit einem Gütesiegel versehen. Der Scope muss durch IT-Dienstleister definiert werden. Der Scope wird auf dem Gütesiegel vermerkt. Ein Auditor überprüft nur den definierten Scope einer Firma.

## Abgrenzung zu anderen Zertifizierungen/Frameworks

Es gibt andere Zertifizierungen, die in der Schweiz durchaus üblich und sinnvoll sind. Hinweis: Beim CyberSeal wird bewusst von einem Gütesiegel gesprochen und nicht von einer Zertifizierung. Damit soll ausgedrückt werden, dass die Ansprüche bei CyberSeal kleiner sind als beispielsweise bei einer Zertifizierung nach ISO/IEC 27001.

### ISO/IEC 27001

Dies ist ein internationaler Standard. In der Schweiz ist die SAS (Schweizerische Akkreditierungs-Stelle), eine Abteilung des Bundes, für die Umsetzung des Standards beauftragt. In der Schweiz bestimmt SAS, welche Firmen Audits durchführen dürfen. Die aktuellen Firmen sind auf der Webseite «[Suche akkreditierte Stellen SAS (admin.ch)](https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas.html)» aufgeführt. Es ist für eine von einem Land zugelassene Firma üblich, auch im Ausland zu zertifizieren.

Der Fokus liegt eher bei grösseren Firmen. Dies ist auch preislich bedingt, da eine Zertifizierung recht aufwändig sein kann.

Der Standard ist generisch aufgebaut. Dies erlaubt den Standard recht konstant zu halten. Aktuell wird nach der Version vom Jahr 2013 auditiert. Ein neuer Standard ist aktuell in Ausarbeitung.

Neuere Entwicklungen (z. B. Datenschutz, Cloud-Computing) werden in Zusatzstandards definiert. Eine Zertifizierung nach diesen Zusatzstandards ist nicht möglich. Sie zeigen aber auf, wie der eigentliche Standard interpretiert werden soll.

### BSI IT-Grundschutz

Der BSI IT-Grundschutz wird vom deutschen BSI ausgearbeitet und gepflegt. Der IT-Grundschutz basiert auf über 100 IT-Grundschutz-Bausteinen (z. B. APP 1.2 = Webbrowser, NET.3.2 = Firewall). Die einzelnen Bausteine sind sehr praxisorientiert und beschreiben beispielsweise eine sichere Konfiguration einer Komponente. Es ist aber sehr herausfordernd, die Bausteine einigermassen aktuell zu halten.

In der Schweiz spielt der BSI-IT-Grundschutz vor allem in der Verwaltung (öffentliche Hand) eine grosse Rolle. Auch viele grössere Firmen berücksichtigen den Standard mindestens teilweise.

Interessant ist, dass es zudem seit einiger Zeit den BSI-Standard gibt. Dieser ist aber weitgehend kompatibel zu den ISO-Normen.

### IKT Minimalstandard

Der IKT Minimalstandard ist eine schweizerische Norm zur Verbesserung der IKT-Resilienz. IKT steht für Informations- und Kommunikations-Technologie.

Der Standard wurde vom Bundesamt für wirtschaftliche Landesversorgung BWL herausgegeben und richtet sich insbesondere an die Betreiber von kritischen Infrastrukturen.

Der IKT Minimalstandard basiert im Wesentlichen auf dem NIST-Framework.

### Weitere Standards

Es gibt viele weitere Standards wie Cobit, NIST-Framework, die in der Schweiz eine untergeordnete Rolle spielen.

# Organisatorische Aspekte des Audits

## CyberSeal Standard

Der Standard besteht aus dem CyberSeal Handbuch, der CyberSeal Prüfliste und dem Bericht des Audits.

Das Audithandbuch des CyberSeal Standards wird auf der Webseite digitalsecurityswitzerland.ch veröffentlicht. Ebenso ist auf der Webseite eine Kurzfassung der Prüfliste zu finden.

Allianz Digitale Sicherheit Schweiz ADSS bestimmt den Zeitpunkt, zu dem die definitive Prüfliste an den IT-Dienstleister abgegeben wird. Dabei muss berücksichtigt werden, dass die Prüfliste für die Schulung und den Workshop mit dem IT-Dienstleister benötigt wird.

Den Auditbericht erhalten die IT-Dienstleister in schriftlicher Form nach dem CyberSeal Audit.

Die kritischen Punkte von NCSC und von den Versicherungsgesellschaften müssen zwingend zu einem Konsolenaudit führen.

## Erfüllungsgrad der Audit-Anforderungen

Das Gütesiegel CyberSeal kann vergeben werden, auch wenn nicht alle Kunden des IT-Dienstleisters alle Aspekte der IT-Sicherheit erfüllen. Dies kann der Fall sein, wenn beispielsweise die Aufarbeitung von Altlasten beim KMU kostspielig oder zeitintensiv sind oder das Beheben von Sicherheitsaspekten vom KMU nicht erwünscht ist. Der IT-Dienstleister sollte diese Kunden mindestens einmal jährlich auf unvollständige Sicherheitsaspekte aufmerksam machen, wobei die Behebung mehrere Jahre in Anspruch nehmen kann.

Der Erfüllungsgrad des CyberSeal ist in diesem Falle nicht 100%. Der minimal notwendige Erfüllungsgrad zum Erreichen des CyberSeal Gütesiegel wird vom Auditor bestimmt. Entscheidend ist, dass sich der Erfüllungsgrad jedes Jahr erkennbar verbessert.

## Selbstdeklaration

Mindestens 10 Tage vor dem Audit muss der IT-Dienstleister dem Auditor eine Selbstdeklaration der voll-ständigen der CyberSeal Prüfliste zur Verfügung stellen.

## Priorisierung der Audit-Anforderungen

Die Audit-Anforderungen sind wie folgt priorisiert:

* Priorität 1: Dies sind Mindestanforderungen, die zwingend implementiert sein müssen. Eine teil-weise Implementierung führt zu einer Nebenabweichung, die zwingend bis zum nächsten Audit behandelt werden muss. Die Behandlung muss eine wesentliche Verbesserung der Erfüllung der Anforderungen mit sich bringen (siehe Kapitel 4.2 «Erfüllungsgrad der Audit-Anforderungen»).
* Priorität 2: Diese Anforderungen sollten von guten IT-Dienstleistern erfüllt werden (Best Practice). Eine Nichterfüllung führt zu keiner Nebenabweichung. Der Auditor kann jedoch einen Hinweis formulieren.
* Priorität 3: Diese Anforderung gilt unter IT-Sicherheitsfachleuten als sinnvoll. Im KMU-Umfeld wird diese Anforderung aktuell als nicht zwingend notwendig betrachtet und es finden nur selten grössere Bedrohungen statt.

## Unterscheidung in der Art der Prüfung

Die Kapitel der Audit-Anforderungen werden unterschiedlich überprüft:

* **Selbstdeklaration**: Die Kapitel werden am Audit in der Regel nicht diskutiert. Es sind vor allem Kapitel, deren Nichterfüllung im KMU-Umfeld meistens nicht zu grösseren Schäden führt. Es ist dem IT-Dienstleister überlassen, die in der Prüfliste aufgeführten Details zu implementieren. Der Auditor kann jedoch einzelne Fragen dieser Kapitel diskutieren und klären, falls die Antworten des IT-Dienstleisters von ihm nicht verstanden werden.
* **Interview**: Diese Kapitel sind auch für KMU recht wichtige Fragen der Cybersecurity. Die ausgefüllte Selbstdeklaration wird am Audit mittels Interviews überprüft.
* **Konsolenaudit**: Dies sind Kapitel, die als sehr kritisch für Schäden im KMU-Umfeld beurteilt werden. Der Auditor führt beim Konsolenaudit eine konkrete Überprüfung der Implementierung durch.

## Abweichungen

Bei den Abweichungen wird unterschieden zwischen:

**Hauptabweichungen**: Diese verhindern die Vergabe des Gütesiegels. Ein Punkt des Standards wurde nicht erfüllt. Hauptabweichungen werden immer vom Auditor formuliert. Bei einem Kapitel, das mit «Selbstdeklaration» bezeichnet ist, gibt es keine Hauptabweichungen.

Bei einer Hauptabweichung hat der Kunde 3 Monate Zeit, um die Hauptabweichung zu beheben. In dieser Zeit beurteilt der Auditor die Behebung der Hauptabweichung.

**Nebenabweichungen**: Diese verhindern die Vergabe des Gütesiegels nicht. Ein Punkt des Standards wurde nur teilweise umgesetzt. Die Nebenabweichung muss bis zur nächsten Aufrechterhaltung behandelt werden und wird beim nächsten Audit detailliert geprüft. Eine nicht 100 %ige Erfüllung der Nebenabweichung kann im nächsten Audit wieder als Nebenabweichung deklariert werden. Es muss aber eine erkennbare Verbesserung stattgefunden haben.

**Hinweise**: Hinweise sind Feststellungen des Auditors, die zu einer Verbesserung führen können. Sie sind zu prüfen. Der IT-Dienstleister entscheidet, ob und wie die Hinweise umgesetzt werden.

## Ablauf für den Erhalt des Gütesiegels

Der zeitliche Ablauf sieht wie folgt aus:

* Selbstdeklaration des IT-Dienstleisters.
* Audit zum Erhalt des Gütesiegel, alle 3 Jahre erneutes Audit nach jeweils aktuellem Standard.
* Aufrechterhaltungsaudit, jährlich zwischen den Audits.

### Selbstdeklaration

Der IT-Dienstleister lädt die Prüfliste herunter. Er füllt alle Punkte des Selbstdeklarationsblattes aus. Dies bedingt, dass die Prüfliste von einem typischen IT-Dienstleister verstanden werden muss. Daher bietet Allianz Digitale Sicherheit Schweiz ADSS Orientierungsworkshops an, an denen die Prüfliste erklärt wird. Wenn der IT-Dienstleister keine Probleme für den Erhalt des Gütesiegels sieht (d. h. bei allen Punkten sind mindestens alle Anforderungen von Priorität 1 ausreichend erfüllt), kann er sich für das Audit anmelden. Die ausgefüllte Selbstdeklaration ist Bestandteil der Anmeldung. Das Anmeldeblatt enthält die wesentlichen Angaben der Firma (Anzahl Mitarbeiter, Tätigkeitsfeld der Firma, definierter Scope, eingesetzte Tools usw.). Die Selbstdeklaration muss mindestens 10 Tage vor dem Audit eingereicht werden.

### Audit

Am Audit überprüft der Auditor die Audit-Anforderungen mit der Kategorie «Interview» auf die Korrektheit. Die Anforderungen mit der Kategorie «Konsolenaudit» müssen zwingend physisch geprüft werden, d. h. der IT-Dienstleister muss die konkrete Implementation aufzeigen. Es ist dem Auditor überlassen, wie eine bestimmte Frage der Prüfliste überprüft wird. Es kann beispielsweise die Dokumentation und das Setup der entsprechenden Tools angeschaut werden. Das Vorort-Audit dauert 4 Stunden. Dabei müssen für das «Interview» mindestens 1 Stunde und für das Konsolenaudit 2 bis 3 Stunden aufgewendet werden. Für die Vorprüfung der Selbstdeklaration und die Einarbeitung der Bemerkungen in die Prüfliste vom Auditor rund 4 Stunden aufgewendet. Das Gütesiegel wird erteilt, wenn keine Hauptabweichungen vorhanden sind.

### Aufrechterhaltungsaudit

Jedes Jahr, wenn kein Audit stattfindet, muss ein Aufrechterhaltungsaudit stattfinden. Das Aufrechterhaltungsaudit wird vom IT-Dienstleister selbstständig durchgeführt. Der IT-Dienstleister beschreibt alle durchgeführten Arbeiten, die Nebenabweichungen und Hinweise betreffen. Diese Beschreibung des IT-Dienstleisters wird von einem Auditor geprüft und im Rahmen einer Remotesessions mit dem IT-Dienstleister diskutiert. Die Remotesession dauert ca. 1 Stunde und kann ein Telefongespräch oder eine Videokonferenz sein.

## Kosten für die Audits

Die Kosten für das Audit betragen Fr. 3'000.--. Für ein Aufrechterhaltungsaudit werden Fr. 500.-- in Rechnung gestellt. Die Kosten beinhalten die Arbeit des Auditors und die administrativen Arbeiten von Allianz Digitale Sicherheit Schweiz ADSS.

## Anforderungen an den Auditor

Der Auditor muss ein ausgewiesener Fachexperte in Information Security sein. Er muss die aktuelle Entwicklung kennen und eine korrekte Umsetzung erklären können. Er muss in der Lage sein, auch ungewöhnliche Umsetzungen technisch zu beurteilen. Die Weiterbildungen des Fachexperten müssen ausgewiesen sein.

Wichtig sind die Kundenorientierung und die Freundlichkeit des Auditors.

* Die Ausbildung der Auditoren findet in den Räumlichkeiten der Allianz Digitale Sicherheit Schweiz ADSS in Zug statt. Die Ausbildung soll die folgenden Ziele sicherstellen:
* Die Auditoren kennen die wichtigen Dokumente des CyberSeal Standards detailliert. Dies sind das CyberSeal Audit Handbuch, die CyberSeal Prüfliste und die Vorlage des CyberSeal Auditberichtes.
* Die Auditoren kennen die wichtigsten Abläufe der Administration.
* Die Auditoren kennen die eingesetzten Tools (Webseite), die Voraussetzung an den verwendeten Computer (Notebook) und Möglichkeiten des sicheren Datentransfers.
* Die Auditoren auditieren möglichst einheitlich.

Die eigentliche Ausbildung der Auditoren wird durch eine jährliche Weiterbildung ergänzt. Während dieser Weiterbildung werden Änderungen im Standard besprochen und es findet ein Erfahrungsaustausch zwischen den Auditoren statt. Dieser Anlass kann auch Einfluss auf den Standard haben.

Allianz Digitale Sicherheit Schweiz ADSS ist für die Ernennung der Auditoren zuständig. Die Bedingungen legt ADSS fest. In der Regel ist der Besuch der Auditorenschulung zwingend. ADSS erstellt auch ein Dokument, das die Ausbildung der Auditoren regelt und Kosten der Ausbildung definiert.

## Durchführung des Audits

Das Audit wird nach Möglichkeit physisch vor Ort durchgeführt. Damit steigt die Wahrscheinlichkeit, dass kritische Punkte entdeckt werden. In Sonderfällen (Reisezeiten, Pandemie usw.) können Audits auch remote durchgeführt werden. Der Auditor entscheidet in Rücksprache mit Allianz Digitale Sicherheit Schweiz ADSS, ob ein Audit remote durchgeführt werden kann.

## Trägerschaft für das Gütesiegel

Die Trägerschaft für das Gütesiegel ist Allianz Digitale Sicherheit Schweiz ADSS. ADSS betreibt eine Niederlassung (aktuell in Zug) mit einer entsprechenden Administration. Die Administration hat u. a. die folgenden Aufgaben:

* Verantwortlich für die Weiterentwicklung des Standards. ADSS kann die Weiterentwicklung an eine Arbeitsgruppe delegieren. Aktuell existiert eine Arbeitsgruppe mit dem Namen «Audit Committee», die für die Entwicklung des Standards zuständig ist.
* Verantwortlich für die Webseite mit den entsprechenden Funktionen für eine automatisierte Anmeldung von IT-Dienstleistern.
* Gewährleisten eines sicheren Datentransfers zwischen ADSS, Auditoren und den Kunden.
* Sicherstellen, dass die Audits durchgeführt werden (inkl. Aufrechterhaltung und neues CyberSeal Audit nach drei Jahren) und eine ausreichende Kommunikation zwischen den IT-Dienstleistern und den Auditoren stattfindet.
* Führen der Liste mit den aktuellen Auditoren.
* Koordination und Ansprechpartner bei Reklamation und unterschiedlichen Meinungen zwischen Auditoren, Kunden und ADSS.
* Ausstellen des Gütesiegels.
* Marketing und Finanzen.

## Vorgehen bei unterschiedlichen Meinungen

Falls ein IT-Dienstleister das Auditresultat anzweifelt, wird der Fall durch einen zweiten Auditor beurteilt und abschliessend entschieden. Die Koordination der Zweitmeinung wird von der Administration übernommen.

Die Frist für die Reklamation beträgt 30 Tage nach Erhalt des Auditberichtes.

## Sicherheitshandbuch für die Praxis

Es existiert das «Sicherheitshandbuch für die Praxis» der Firma isec ag. Das Sicherheitshandbuch entstand unabhängig vom Standard, beschreibt aber mögliche Implementationen zur Erreichung des Standards. Das Handbuch kann als Werkzeugkiste verstanden werden. Die Details können auf der folgenden Webseite entnommen werden: https://sihb.ch.

# Audit Anforderungen

Das CyberSeal Audit wird vom Auditor anhand der CyberSeal Prüfliste durchgeführt.

Die einzelnen Fragen der CyberSeal Prüfliste sind wie in Kapitel 4.4. beschrieben Prioritäten zugeordnet. Zudem ist in der CyberSeal Prüfliste gemäss Kapitel 4.5 definiert, welche Abschnitte in Selbstdeklaration, per Interview oder Konsolenaudit durchgeführt werden. Die Verwendung der CyberSeal Prüfliste stellt eine einheitliche Durchführung der CyberSeal Audits sicher und definiert den aktuellen CyberSeal Standard.

Nachfolgend werden die wichtigsten Inhalte der CyberSeal Audit Prüfliste skizziert.

## Aufgabenteilung Kunde/IT-Dienstleister

Die Aufgabenteilung zwischen dem IT-Dienstleister und der KMU muss schriftlich und ausreichend detailliert beschrieben sein. Die Dokumentation muss

* die Aufgaben des IT-Dienstleisters beschreiben,
* die Aufgaben definieren, die der Kunde selbst erledigen will.

Es soll insbesondere auch klar sein, wer für welche Aspekte der Sicherheit verantwortlich ist.

Es muss nicht zwingend für jeden Kunden ein eigenes Dokument erstellt werden. Wartungsverträge oder Service-Descriptions können ausreichend sein.

## Verwaltung des Zugriffes auf Kundeninfrastruktur

Der IT-Dienstleister muss aufzeigen, wie er Zugriffe auf die Kundeninfrastruktur regelt und verwaltet. Da-bei müssen folgende Anforderungen erfüllt werden:

* Zugangsmutation beim IT-Dienstleister muss zeitnah abgebildet werden können. Insbesondere muss bei Freistellung von Mitarbeitern des IT-Dienstleisters eine Sperrung aller Zugänge zeitnah möglich sein.
* Es ist sicherzustellen, dass der Kunde keinen Zugriff auf die Ressourcen des IT-Dienstleisters oder anderer Kunden hat.
* Es dürfen nicht die gleichen Passwörter für unterschiedliche Kunden verwendet werden.
* Der Zugriff hat über eine angemessen gesicherte Infrastruktur zu erfolgen. Insbesondere hat der Zugriff mit verwalteten Geräten des IT-Dienstleisters zu erfolgen. Mit privaten Geräten ist der direkte Zugriff auf Kundeninfrastrukturen nicht gestattet.
* Für den Zugriff auf eine Kundeninfrastruktur muss eine Zweifaktor-Authentisierung verwendet werden.
* Für die Authentisierung für technische Accounts wie Service-Accounts (kein Zugriff durch natürliche Personen) muss eine starke Authentisierung eingesetzt werden.
* Der Zugang vom IT-Dienstleister auf die Systeme des KMU muss dokumentiert sein und vom KMU bewilligt sein. Die Bewilligung muss die entsprechenden Berechtigungen des IT-Dienstleisters klar ausweisen.

## Dokumentation

Der IT-Dienstleister muss eine aktuelle Dokumentation der Infrastruktur der KMU besitzen. Diese Dokumentation umfasst mindestens:

* Alle Systeme sind auf einer Übersicht verzeichnet. Im mindesten sind Hostname, IP-Adresse und Zweck dokumentiert.
* Die Dokumentation der Systeme kann an den Kunden abgegeben werden. Es werden keine speziellen Systeme benötigt, um die Dokumentation zu lesen.
* Der IT-Dienstleister verpflichtet sich die Dokumentation für die von ihm verwalteten Systeme zeitnah (nach-)zuführen.

## Credentials und Berechtigungen der Mitarbeiter des KMU

Falls der IT-Dienstleister die Credentials und die Berechtigungen für die KMU verwaltet, gelten die folgenden Anforderungen:

Als «Mutation» gelten beispielsweise, aber nicht abschliessend, folgende Vorgänge:

* Erstellen, Ändern, Löschen sowie das Aktivieren oder Deaktivieren von Accounts.
* Zurücksetzen von Kennwörtern oder anderen Secrets.
* Ändern von Berechtigungen jeglicher Art (z. B. Fileserverzugriffe, Mailbox-Access).

Folgende Massnahmen sind umzusetzen:

* Jede Änderung der Credentials und der Berechtigungen ist nachvollziehbar.
* Der IT-Dienstleister definiert einen Prozess, welcher nachvollziehbar das Vorgehen bei Mutationen aufzeigt.
* Es existiert ein definierter und sicherer Prozess für temporäre Berechtigungen.
* Die Passwörter des Kunden sind sicher verwahrt (Passwortsafe oder Ähnliches).
* Es wird sichergestellt, dass ein Zugriff auf die Passwörter auch im Notfall möglich ist.

## Netzwerkdesign

Der IT-Dienstleister berät den Kunden hinsichtlich Netzwerkarchitektur und setzt diese um.

Alle Netzwerkknotenpunkte (namentlich Firewalls, Router, WLAN-Controller und andere Routing-Devices) sind zu definieren und zu dokumentieren.

Die folgenden Netzwerksegmente sind in der Architektur zu berücksichtigen (falls vorhanden) und zu trennen:

* Büroautomation.
* Stark schutzbedürftige Netzwerksegmente (Produktionsanlagen, Infrastruktursysteme usw.). Dies betrifft insbesondere Systeme, welche sich nicht nach Stand der Technik schützen lassen (fehlende Updates, Anforderungen von Wartungsverträgen, Zertifizierungen etc.).
* Nicht vertrauenswürdige Netzwerksegmente, z. B. Gäste-WLANs etc.

Im Weiteren gelten die folgenden Anforderungen:

* Die erlaubten Netzwerkverbindungen zwischen den Netzwerk-Segmenten sind minimal. Insbesondere ist ein volles Routing nicht erlaubt.
* Falls das Protokoll IPv6 eingesetzt wird, muss dies bewusst geschehen. Das IPv6 Netzwerk ist korrekt zu konfigurieren und der IT-Dienstleister muss die dafür notwendigen Kompetenzen aufgebaut haben.

## Firewalls

Folgende Rahmenbedingungen müssen erfüllt sein:

* Die Firewall-Regeln müssen lesbar sein. Die Dokumentation/Begründung einer Regel kann direkt im Kommentarfeld des Rulesets erfolgen.
* Das Firewall-Ruleset ist möglichst eng konfiguriert. Es dürfen beispielsweise keine Any-Any-Regeln verwendet werden und der ausgehende Verkehr muss auf die notwendigen Verbindungen eingeschränkt sein.
* Das Ruleset muss regelmässig überprüft werden. Dabei wird das Vier-Augen-Prinzip empfohlen. Eine erfolgte Überprüfung muss nachvollziehbar sein.

## WLAN

Das WLAN beim IT-Dienstleister und bei der KMU orientiert sich grundsätzlich am Konzept im Kapitel 5.5, d. h. die Anforderungen des Netzwerkdesigns müssen erfüllt sein. Zusätzlich sind die folgenden Anforderungen definiert:

* Für jeden Kunden müssen separate, nicht ableitbare Passwörter verwendet werden.
* Es muss ein separates WLAN für private Geräte von Mitarbeitern und für Gäste eingerichtet werden.
* Die Authentisierung mittels gemeinsam genutzten Credentials darf ausschliesslich für öffentliche Netzwerkzonen eingesetzt werden. Der Zugriff auf alle anderen Zonen (gem. Kapitel 5.5) hat ausschliesslich mit persönlichen Credentials zu erfolgen.
* Es werden keine veralteten und unsicheren Schutzmechanismen eingesetzt.
* Generische Accounts im WLAN müssen bewilligt werden.

## AD Design

Es sind die folgenden Mindestanforderungen definiert:

* Der Kunde besitzt einen Notfall-Administrator-Account.
* Privilegierte Accounts (DOA, EA, SA, lokale administrative Rechte und weitere) werden nicht für die tägliche Anwendungsarbeit genutzt.
* Öffentlich zugreifbare Portale, auf welche mittels AD-Credentials zugegriffen werden kann, sind mit Mehrfaktorauthentifizierung zu schützen[[1]](#footnote-2).
* Die Nachvollziehbarkeit auf die Kundeninfrastruktur ist gewährleistet.
* Es werden ausschliesslich personalisierte Administratoren-Accounts verwendet.

## Hardening der IT-Komponenten

Es sind die folgenden Mindestanforderungen definiert:

* Der IT-Dienstleister pflegt und dokumentiert einen Prozess zur Härtung von Kundensystemen (z. B. Clients, Server, Firewalls etc.).

## Mail-System

Es sind die folgenden Mindestanforderungen definiert:

* Der Partner stellt sicher, dass er alle üblichen Schutzmechanismen zum Schutz vor Spam und Malware auf dem eigenen Mail-System und dem Mail-System aller Kunden installiert hat.
* Der IT-Dienstleister unterstützt nur Mail-Infrastrukturen, die die Absenderauthentizität prüft (SPF, DKIM usw.)

## Patch Management

Es sind die folgenden Mindestanforderungen definiert:

* Der IT-Dienstleister definiert, pflegt und dokumentiert einen Prozess zur Aktualisierung von Soft-ware auf KMU-Systemen, wie auch auf eigenen Systemen.
* Der Prozess stellt sicher, dass verfügbare Aktualisierungen zeitnahe und in nützlicher Frist eingespielt werden. So muss beispielsweise sichergestellt werden, dass die Patches für Client-OS innerhalb eines Monats installiert werden.
* Der IT-Dienstleister stellt sicher, dass alle IT-Systeme (inkl. Firewalls, Netzwerkgeräte, Adobe-Produkte und alle Applikationen) in den Prozess involviert sind. Begründete Ausnahmen (z. B. Java für eine Applikation darf nicht gepatched werden) sind schriftlich festzuhalten.
* Bei grösseren Schwachstellen muss ein Notfallprozess etabliert sein.

## Mobile Devices

Es sind die folgenden Mindestanforderungen definiert:

* Datenträger auf mobilen Geräten müssen verschlüsselt werden.
* Der Zugriff auf Firmendaten ist nur nach einer ausreichenden Authentisierung möglich.
* Es sind Anforderungen an die Mobile Devices formuliert. Diese Anforderungen werden durch entsprechende Policies durchgesetzt.

## Home-Office

Es sind die folgenden Mindestanforderungen definiert:

* Der Zugriff vom Home-Office findet ausschliesslich über gesicherte und verwaltete Systeme statt.
* Ein Aufbau einer indirekten Verbindung von einem nicht verwalteten Gerät mit einem virtuellen Desktop (z. B. Citrix, RDP oder Ähnlichem) im Sinne eines «Jumphost-Access» ist zulässig.
* Es ist eine Mehr-Faktor-Authentifizierung für den Zugriff aus dem Home-Office zu erzwingen.
* Weitere Dienste sind bei Home-Office nur nach einer Sicherheitsprüfung erlaubt (beispielsweise: Printer ist problematisch, Laufwerkmapping ist bei verwalteten Geräten erlaubt).

## Malware Protection

Der Malwareschutz ist kritisch. Alle sinnvollen Systeme sind mit einem Malware-Schutz auszustatten. Sinnvoll sind sicher die folgenden Systeme:

* Server
* Clients
* Firewalls und ev. Router
* Mail-Systeme

Es sind die folgenden Mindestanforderungen definiert:

* Alle sinnvollen IT-Systeme sind mittels Malwareschutz mit Malware-Erkennung oder gleichwertigem Mechanismus zu schützen. Der Auditor entscheidet, ob ein System als sinnvoll betrachtet wird. Vorgaben vom Softwareanbieter müssen aber berücksichtigt werden.
* Der IT-Dienstleister setzt ein Konzept mit einem mehrstufigen und technisch unabhängigen Malwareschutz um.[[2]](#footnote-3).
* Spezielle Systeme (z. B. Produktionssysteme) können vom Malwareschutz ausgenommen werden. Ein fehlender Malwareschutz ist aber zu dokumentieren und das System ist netzwerkmässig abzuschotten.

## Backup

Es sind die folgenden Mindestanforderungen definiert:

* Es existiert ein definierter, gepflegter und dokumentierter Prozess zur Sicherung der Daten. Der Prozess muss für alle IT-Systeme gültig sein (z. B. auch Firewalls).
* Der Backup wird regelmässig getestet. Der Test umfasst auch den Restore der gesamten Systeme.
* Eine Sicherungskopie ist örtlich getrennt aufzubewahren.
* Die Datensicherung muss mediengetrennt und darf nicht online zugreifbar sein (Offline-Backup).

## Change-Management/Incident Management

Der Schwerpunkt dieses Themas liegt bei der Nachvollziehbarkeit. Es sind die folgenden Mindestanforderungen definiert:

* Der IT-Dienstleister stellt sicher, dass Änderungen an Systemen nachvollziehbar protokolliert werden und er jederzeit Auskunft darüber geben kann.
* Manipulationen, ausgelöst durch Incidents, werden analog dem Vorgehen bei Änderungen gehandhabt.

## Protokollierung

Es sind die folgenden Mindestanforderungen definiert:

* Der Partner stellt sicher, dass alle Systemprotokolle gemäss einer Vereinbarung mit dem KMU gespeichert werden.
* Jeder Zugriff (insb. Zugriffe des IT-Dienstleisters) auf die Kundeninfrastruktur muss protokolliert werden.
* Protokolle werden mindestens 6 Monate aufbewahrt.

## Monitoring

Der IT-Dienstleister stellt sicher, dass er ein Monitoring gemäss der Definition im SLA betreibt.

## Entsorgung von Datenträgern

Es sind die folgenden Mindestanforderungen definiert:

* Der IT-Dienstleister muss dem KMU ein dokumentiertes Konzept anbieten, um ihm eine sichere Entsorgung von Datenträgern zu ermöglichen.

## Services von Drittanbietern

Es sind die folgenden Mindestanforderungen definiert:

* Der IT-Dienstleister kennt die betreuten Produkte von Drittanbietern und kann ein vergleichbares Niveau der Sicherheit wie bei lokalen Services anbieten.

## Schwachstellen beim Kunden

Es sind die folgenden Mindestanforderungen definiert:

* Der IT-Dienstleister informiert die Kunden über mögliche Schwachstellen in der Infrastruktur oder bei Services.

## Ausbildung der Mitarbeiter

Der IT-Dienstleister stellt sicher, dass die eigenen Mitarbeitenden in regelmässigen Abständen Schulungen zum Thema IT-Sicherheit besuchen. Zudem muss der IT-Dienstleister auch Kunden eine

Schulung anbieten oder vermitteln. Der Schwerpunkt liegt auf dem Erkennen und dem richtigen Verhalten von Social-Engineering-Angriffen.

## Notfallkonzept

Jeder IT-Dienstleister hat ein Notfallkonzept zu erstellen. Er bietet auch seinen Kunden an, ihn bei der Erstellung eines KMU-spezifischen Notfallkonzepts zu unterstützen. Das Notfall-Konzept muss folgenden Anforderungen mindestens genügen:

* Das Notfallkonzept regelt, wann welche Stellen (Polizei, NCSC, Versicherungen, unterstützende Firmen) einbezogen werden müssen. Die Kontaktadressen sind Bestandteil des Notfallkonzeptes.
* Der Umgang mit verschlüsselten Daten (z. B. Verschlüsselung eines Excel-Sheets) muss geregelt sein. Ein Recovery-Prozess muss vorhanden sein.
* Das Notfallkonzept muss den Fall, dass ein Kunde Probleme mit Cyberkriminalität hat, abdecken.
* Das Notfallkonzept ist regelmässig auf Aktualität zu prüfen und angemessen zu testen.

## Ablaufende Termine

Es gibt immer mehr Informatik-Komponenten, die nach einem Ablaufdatum die Funktion einstellen (Lizenzen, Zertifikate, Wartungsablauf von Komponenten usw.). Um Probleme mit solchen Komponenten zu verhindern, sind die folgenden Mindestanforderungen zwingend:

* Es muss für jeden Kunden eine Verwaltung von kritischen Daten geführt werden. Es wird rechtzeitig eine Meldung generiert.
* Der Kunde wird auf veraltete Hardware (z. B. keine Patches mehr) aufmerksam gemacht.

## Physische Sicherheit

Der IT-Dienstleister muss sicherstellen, dass seine IT-Systeme ausreichend geschützt sind. Es sind die folgenden Anforderungen zu erfüllen:

* Der Zutritt zu den Räumlichkeiten des IT-Dienstleisters ist ausreichend kontrolliert.
* Der Zutritt zum Datacenter des IT-Dienstleisters ist durch die Geschäftsleitung zu autorisieren und ist zu protokollieren.
* Die IT-Geräte des Dienstleisters sind gegen äussere Einflüsse geschützt (z. B. USV, Kühlung, redundanter Internet-Anschluss).

## Risiko Management

Ein IT-Dienstleister muss ein sinnvolles Risiko Management betreiben. Die wesentlichen Risiken müssen bekannt sein. Die Risiken können mit den folgenden Massnahmen gemindert werden:

* Risiko-Vermeidung: Unter Umständen kann eine Risikobetrachtung dazu führen, dass gewisse Dienstleistungen nicht angeboten werden können.
* Risiko-Minderung: Massnahmen werden ergriffen, um ein bestimmtes Risiko zu mindern. Alle Kapitel im Abschnitt 5 sind Risikominderungsmassnahmen.
* Risiko-Transfer: Einzelne Risiken können versichert werden. Die Art der Versicherung (Berufshaft-pflicht, Cyber-Schäden usw.) und die Versicherungssumme müssen sorgfältig gewählt werden.
* Risiko-Akzeptanz: Jede Firma muss einzelne Risiken (oder Rest-Risiken) tragen. Das Tragen von Risiken muss aber vor der Leitung des IT-Dienstleisters akzeptiert werden und kann nicht delegiert werden.

Das Risiko Management muss die folgenden Anforderungen erfüllen:

* Es wird mindestens eine jährliche Risikobeurteilung durchgeführt, d. h. der IT-Dienstleister kennt die wesentlichen Risiken.
* Die grossen Risiken werden gemäss der obigen Liste gemindert.
* Der Transfer der Risiken zu einer Versicherungsgesellschaft wurde geprüft.
* Es existiert ein Prozess, der sicherstellt, dass die Restrisiken von der Leitung des IT-Dienstleisters getragen werden.

Roland Portmann, Allianz Digitale Sicherheit Schweiz

Anhang

Abkürzungsverzeichnis

ADSS Allianz Digitale Sicherheit Schweiz ADSS

AWS Amazon Web Service

BSI Bundesamt für Sicherheit in der Informationstechnik

Cobit Control Objectives for Information and Related Technology

DKIM DomainKeys Identified Mail

IEC International Electrotechnical Commission

IKT Informations- und Kommunikationstechnik

IPv6 Internet Protocol Version 6

ISO Internationale Organisation für Normung

KMU Kleinere(s) und mittlere(s) Unternehmen [Kleinere und mittlere Unternehmung(en)]

NCSC National Cyber Security Center

NIST National Institute of Standards and Technology

SLA Service Level Agreement

SPF Sender Policy Framework

1. Betrifft insbesondere Azure AD. [↑](#footnote-ref-2)
2. Z. B. Malwarefilter kaskadiert auf Mail-System, UTM-Firewall, Client/Server. [↑](#footnote-ref-3)