CyberSeal Audithandbuch

Version 2.0, 1. Mai 2024

Inhaltsverzeichnis

1 Zweck des Dokuments

In diesem Handbuch wird die Anwendung der CyberSeal Prüfliste detailliert beschrieben. Zudem wird der Audit-Prozess, die Kosten, die Rahmenbedingungen und weitere Details der Vergabe des CyberSeal Gütesiegels beschrieben. Das Handbuch wird jährlich überarbeitet.

2 Das Gütesiegel CyberSeal

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 wurden.

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 BACS (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.

Das Gütesiegel CyberSeal hat einen hohen Anspruch an Aktualität. Neueste Entwicklungen bei den Angreifern und Schadensarten werden jährlich im angepassten Standard eingearbeitet.

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.
- 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 den KMU einen guten IT-Dienstleister zu finden.
- Das Gütesiegel spiegelt die aktuelle Gefährdungslage wider.

3 Grundlagen

3.1 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 ein 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. BDO usw.) delegieren.

Privilegierter Account: Ein Account, welcher über erhöhte System-, Konfigurations- und/oder Schreibberechtigungen verfügt.

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 Passwörter: Das BACS beschreibt auf der Webseite Schützen Sie Ihre Konten / Passwörter (admin.ch) die Voraussetzungen dafür, dass Passwörter als recht sichere Authentisierung betrachtet werden können.

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.

3.2 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 den IT-Dienstleister definiert werden. Sollte der Scope nicht die ganze Firma mit allen ihren Dienstleistungen betreffen, wird der geprüfte Scope auf dem Siegel vermerkt.

3.3 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.

3.3.1 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 akkreditierten Firmen sind auf der Webseite «Suche akkreditierte Stellen SAS (admin.ch)» 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 2022 auditiert.

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.

3.3.2 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.

3.3.3 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.

3.3.4 Weitere Standards

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

4 Organisatorische Aspekte des Audits

4.1 CyberSeal Standard

Der Standard besteht aus dem CyberSeal Handbuch, der CyberSeal Prüfliste und dem Auditbericht.

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.

Der Auditbericht steht den IT-Dienstleistern nach dem CyberSeal Audit online in ihrem Kundenportal auf

digitalsecurityswitzerland.ch zur Verfügung.

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

4.2 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.

4.3 Deklaration durch den IT-Dienstleister

Mindestens 10 Tage vor dem Audit muss der IT-Dienstleister dem Auditor eine Deklaration der vollständigen CyberSeal Prüfliste zur Verfügung stellen. Bei der «Unterscheidung in der Art der Prüfung» (Siehe Kapitel 4.5) werden nur bei Unklarheiten auf Fragen, die mit Selbstdeklaration (S) in der Prüfliste deklariert sind, eingegangen. Es ist wichtig, dass vor dem Audit alle Fragen (auch Fragen, die in der Prüfliste mit I (Interview) oder K (Konsolenaudit) bezeichnet sind, nach bestem Wissen beantwortet werden.

4.4 Priorisierung der Audit-Anforderungen

Die Audit-Anforderungen sind wie folgt priorisiert:

- Priorität 1: Dies sind Mindestanforderungen, die zwingend implementiert sein müssen. Eine teilweise 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.

4.5 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 führen. 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 wichtige Fragen der Cybersicherheit. 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.

4.6 Ausschluss einzelner Kapitel

Falls einzelne Kapitel in der Prüfliste für einen Dienstleister keinen Sinn machen (z.B. der Dienstleister betreibt keine eigene E-Mail-Infrastruktur und bietet dies auch nicht seinen Kunden an), kann der Auditor diese Kapitel von der Prüfung ausnehmen. Der Auditor bezeichnet dieses Kapitel im Feld «Resultat» mit «Nicht Verfügbar» (NV).

4.7 Abweichungen

Der Auditor verwendet die Spalte «Resultat» um die Erfüllung / Nicht Erfüllung der einzelnen Fragen zu beurteilen. Hierzu verwendet er ausschliesslich folgende Abkürzungen:

- **OK:** Die Anforderung wird genügend erfüllt

Abweichungen
Bei den Abweichungen wird unterschieden zwischen:

- **HA (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.

Wenn eine oder mehrere Hauptabweichung vorliegt, hat der Kunde 3 Monate Zeit, um diese zu beheben. Nach Ablauf dieser Frist beurteilt der Auditor die Behebung der Hauptabweichung.

- **NA (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.

- **HW (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.

4.8 Ablauf für den Erhalt des Gütesiegels

Der zeitliche Ablauf sieht wie folgt aus:

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

4.8.1 Vorbereitung

Die Allianz Digitale Sicherheit Schweiz ADSS bietet Orientierungsworkshops an. An diesen kostenlosen Workshops wird u.a. die Prüfliste erklärt. Es wird empfohlen, diesen Workshop zu besuchen. 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.

4.8.2 Deklaration

Der IT-Dienstleister lädt die Prüfliste herunter. Er füllt alle Punkte aus. Die ausgefüllte Deklaration ist

Bestandteil der Anmeldung. Die Deklaration muss mindestens 10 Tage vor dem Audit eingereicht werden.

4.8.3 Audit

Beim 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 Deklaration und die Einarbeitung der Bemerkungen in die Prüfliste werden vom Auditor rund 4 Stunden aufgewendet. Das Gütesiegel wird erteilt, wenn keine Hauptabweichungen vorhanden sind. Über allfällige Hauptabweichungen muss am Schlusse des Audits diskutiert werden. Der Kunde muss wissen, dass er das Zertifikat nicht erhält.

4.8.4 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.

4.9 Kosten für die Audits

Die Kosten für das Audit entsprechen den aktuellen Preisen, welche auf www.digitalsecurityswitzerland.ch hinterlegt sind.

4.10 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 Auditoren Schulung erwünscht. ADSS erstellt auch ein

Dokument, das die Ausbildung der Auditoren regelt und Kosten der Ausbildung definiert.

4.11 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.

4.12 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.

4.13 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.

4.14 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.

5 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. Die verbindliche

Formulierung jedes Prüfpunktes kann der Prüfliste entnommen werden.

5.1 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 muss.
- Die Verantwortungen des IT-Dienstleisters sowie jene des KMU beschreiben

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-Beschreibung können ausreichend sein.

5.2 Verwaltung des Zugriffes auf Kundeninfrastruktur

Der IT-Dienstleister muss aufzeigen, wie er Zugriffe auf die Kundeninfrastruktur regelt und verwaltet.

Dabei müssen die folgenden Zwecke erreicht werden:

- Es muss sichergestellt werden, dass der Kunde den IT-Dienstleister jederzeit wechseln kann.
- Es wird eine hohe Sicherheit beim Zugriff auf die Kundeninfrastruktur implementiert (Mehrfach-Authentisierung). Mitarbeiter, die einen IT-Dienstleister verlassen, haben in keinem Falle mehr Zugriff auf die Kundeninfrastruktur.
- Der Kunde muss sich bewusst sein, auf welche Informationen der IT-Dienstleister zugreifen kann.

5.3 Credentials und Berechtigungen

Als Credentials werden normalweise der Benutzername und das Passwort verstanden. Es muss sichergestellt werden, dass die folgenden Punkte erfüllt sind:

- Es muss ein Prozess implementiert sein, welcher jede Veränderung von Credentials (auch Zurückstellen von Passwörtern) und Berechtigungen nachvollziehbar sind. Der Prozess muss auch temporäre Berechtigungen umfassen.
- Der Kunde kann im Notfall auf alle seine Credentials und Berechtigungen zugreifen.
- Die Passwörter des Kunden sind sicher verwahrt (z.B. Passwortsafe).

5.4 Dokumentation

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

- Alle Systeme sind auf einer Übersicht verzeichnet.
- Die Dokumentation der Systeme kann an den Kunden abgegeben werden. Es werden keine speziellen Systeme benötigt, um die Dokumentation zu lesen.
- Der IT-Dienstleister aktualisiert die Dokumentation regelmässig.

5.5 Netzwerkdesign

Das Netzwerkdesign berücksichtigt die unterschiedlichen Zonen;

- Office-Zone
- Fabrikation-Zone, teilweise können nicht patchbare Devices in dieser Zone sein.
- Öffentliche Zone für Gäste und private Geräte von Mitarbeitern.

Dabei ist zu beachten, dass die Übergänge zwischen den Zonen nur den minimal nötigen Verkehr zulassen. Es sind auf jeden Fall Router oder ähnliche Geräte einzusetzen, die entsprechende Regeln unterstützen.

5.6 Firewalls

Folgende Rahmenbedingungen müssen erfüllt sein:

- Die einzelnen Verbindungen der Firewall erlauben nur den notwendigen Verkehr. Auch der ausgehende Verkehr in das Internet ist einzuschränken.
- Die Firewall-Regeln müssen für einen externen Spezialisten lesbar sein.
- Das Ruleset muss regelmässig überprüft werden. Eine erfolgte Überprüfung muss nachvollziehbar sein.

5.7 WLAN

Das WLAN beim IT-Dienstleister und bei dem KMU orientiert sich grundsätzlich am Konzept im Kapitel 5.5. 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 ausschliesslich aktuelle und sichere Schutzmechanismen eingesetzt.

5.8 Identity Management (Active Directory, Azure, etc.)

Es ist sichergestellt, dass folgendes implementiert ist:

- Der Kunde kann das AD selbst administrieren oder kann einen anderen Dienstleister damit beauftragen. Dies kann sichergestellt werden, indem der Kunde einen Notfall-Administrator-Account besitzt.
- Accounts mit erweiterten Berechtigungen werden nicht für die tägliche Anwendungsarbeit genutzt.
- Öffentlich zugreifbare Portale und Cloudinfrastrukturen, auf welche mittels AD-Credentials zugegriffen werden kann, sind sicher implementiert.
- Es werden ausschliesslich personalisierte Administratoren-Accounts verwendet.

5.9 Hardening der IT-Komponenten

Alle Kundensysteme und Devices, die vom IT-Dienstleister konfiguriert werden, sind gehärtet. Typischerweise existiert eine Checkliste, mit den notwendigen Einstellungen.

5.10 Mail-System

Gemäss den Angaben vom BACS und den Versicherungen steht am Anfang eines Cyberangriffes eine Kontaktnahme mit einer E-Mail. Daher fällt diesem Punkt eine besondere Bedeutung zu.

Wird die E-Mail-Infrastruktur lokal betrieben, gelten nachfolgende Mindestanforderungen:

- Die E-Mail-Infrastruktur muss sicher aufgebaut und betrieben werden. Ein Anti-Malware-Schutz ist notwendig sowie die Prüfung der Absender-Authentizität, dies kann mit der Installation von SPF oder DKIM erreicht werden. Zugriff mit Mobile-Devices wird kontrolliert und entsprechend eingeschränkt.

Vielfach wird die E-Mail-Infrastruktur der Kunden in der Cloud betrieben. Bei den meisten Anbietern kann damit eine sehr hohe Sicherheit garantiert werden.

5.11 Patch Management

Nicht ausreichendes und schnelles Patchen wird vom BACS und den Versicherungen als Ursache für viele Angriffe im Cyberumfeld angesehen. Zudem können, je nach vorhandenen Schwachstellen, diese für eine Ausweitung der Berechtigungen verwendet werden. Daher fällt diesem Punkt eine besondere Bedeutung zu.

Es sind mindestens die folgenden Anforderungen umzusetzen:

- Das Patch Management ist in einem Prozess definiert, der zwingend eingehalten werden muss. Der Prozess enthält auch das Patch Management von nicht Microsoft-Produkten. Die Patch-Zyklen werden sinnvoll gewählt.
- Ausnahmen vom Patch Management (z. B. Java für eine Applikation darf nicht gepatched werden) müssen schriftlich festgehalten werden.
- Bei grösseren, schwerwiegenden Schwachstellen (z.B. Exchange-Schwachstelle) muss ein Notfallprozess zwingend gestartet werden.

5.12 Mobile Devices

Aktuell sind die Mobilen Devices nicht die Ursache von grösseren Cybersicherheitsvorfällen in KMU. Trotzdem muss eine minimale Sicherheit gewährleitet werden.

- Datenträger auf mobilen Geräten müssen nach Möglichkeit verschlüsselt werden.
- Der Zugriff auf Firmendaten ist nur nach einer ausreichenden Authentisierung möglich.

Viele Einstellungen können mit Policies technisch erzwungen werden. Der Einsatz von Policies kann für KMU sinnvoll und effizient sein.

5.13 Remote Work / Home-Office

Viele IT-Dienstleister können die Anforderungen der Kunden erfüllen, auch wenn die Mitarbeiter des IT-Dienstleister zuhause arbeiten. Zudem ermöglicht Home-Office auch eine Gewährleistung der versprochenen Leistungen im Falle von Pandemien.

Daher sind sichere Home-Office-Umgebungen von grosser Bedeutung:

- Der IT-Dienstleister erarbeitet ein Konzept für ein sinnvolles und sicheres Arbeiten für Remote Work und implementiert dieses.
- Das Konzept stellt sicher, dass keine direkte Netzwerkverbindung zwischen Kunden-Systemen und dem Home-Office aufgebaut werden können.
- Es ist eine Form der mehrfachen Authentisierung zu implementieren.
- Das Konzept beschreibt auch die erlaubten Zusatzfunktionen (z.B. Printing, Laufwerkmapping usw.)

5.14 Malware Protection

Mit einer guten Malware Protection (Virenschutz) können viele Infektionen verhindert werden. Das BACS und die Versicherungen legen einen grossen Wert auf einen guten Malwareschutz. Tests zeigten in der Vergangenheit, dass grosse Unterschiede bei den vielen am Markt verfügbaren Produkten bestehen. Damit wird die Auswahl des konkret eingesetzten Produktes sehr wichtig.

Die meisten Server und Clients werden in der Regel recht gut geschützt. Viele Angriffe erfolgen über ein E-Mail-System. Daher ist ein zweistufiges Konzept (Firewall und Client) bei E-Mail-Systemen zwingend notwendig.

Üblich, auch im KMU-Umfeld, ist ein besonderer Schutz des Internetzuganges.

Nach wie vor ist es üblich, dass auf einigen Systemen kein Malwareschutz installiert werden darf. Der Grund dafür muss dokumentiert werden. Zudem sind solche Systeme netzwerkmässig zu isolieren.

5.15 Backup / Restore

Das BACS und die Versicherungen definieren ein gutes Backup als essenziell für das Überleben einer Firma im Falle eines Cyberangriffes. Bei einem Cyberangriff wird oft auch versucht, das Backup unbrauchbar zu machen.

Daher fällt einem guten Backup eine sehr wichtige Funktion zu. Neben einer guten Dokumentation des Backups muss die Funktionsweise häufig getestet werden. Dabei sind nicht nur einzelne Files zu restoren, sondern auch gesamte Systeme müssen komplett restored und auf Funktionalität geprüft werden. Aktuelle Virtualisierungsumgebungen und Backup-Tools unterstützen einen solchen regelmässigen Test.

Auch grosse Firmen legen Wert darauf, dass das Backup nachträglich nicht mehr verändert werden kann. Das Band als Backupmedium erlebt deshalb aktuell ein «Come Back». Alternativ werden in viele Projekten auch Wechseldatenträger eingesetzt. Diese sind weniger sicher als ein Band, aber oft günstiger.

Eine Kopie des Backups muss örtlich getrennt aufbewahrt werden.

5.16 Change-Management/Incident Management

Der Schwerpunkt dieses Themas liegt bei der Nachvollziehbarkeit. Das kann auch im Falle eines Cyberangriffes von Bedeutung sein. Der IT-Dienstleister stellt sicher, dass alle Änderungen am System nachvollzogen werden können. Auch alle Vorfälle (Incidents) können nachvollzogen werden.

Bei den IT-Dienstleistern der KMU wird teilweise dieses Management vernachlässigt. Dabei wird aber nicht berücksichtigt, dass viel Zeit eingespart werden kann, wenn ein Vorfall (Incident) oder eine Änderung leicht gefunden werden kann. Zudem unterstützen die Systeme ein primitives Change-Management von sich aus. Man muss aber diese Systeme konsequent benutzen.

5.17 Protokollierung

Jedes System unterstützt eine recht gute Protokollierung. Man muss aber unter Umständen diese Protokollierung einschalten beziehungsweise konfigurieren. Dies kann man mit einer Checkliste (siehe auch Kapitel 5.9) definieren. Es ist ein wichtiger Punkt einer SLA. Darin sollte die Aufbewahrungsdauer und die zu protokollierenden Werte definiert werden.

5.18 Monitoring

Ein gutes Monitoring kann sehr effizient für einen IT-Dienstleister sein. Das Monitoring-System kann das Change-Management unterstützen bzw. implementieren. Zudem kann ein Monitoring viele Angriffe erkennen.

Ein proaktives Monitoring kann weiter Cyberangriffe erkennen und bei der Schadensermittlung unterstützen.

Der Umfang des Monitorings sollte im Rahmen von SLAs mit den Kunden definiert werden. Die Feststellungen sind regelmässig dem Kunden zu rapportieren.

5.19 Entsorgung von Datenträgern & Datenlöschung

Auf jedem Datenträger sind sensitive Informationen gespeichert. Der IT-Dienstleister muss gewährleisten, dass diese Daten nicht in fremde Hände gelangen. Normalerweise wird der Datenträger physisch zerstört. Der Kunde wird vom IT-Dienstleister auf die Pflicht der regelmässigen Löschung von Daten auf seinen Systemen aufmerksam gemacht.

5.20 Services von Drittanbietern

Jeder IT-Dienstleister muss heute Produkte von Drittanbietern bei Kunden installieren. So kann der Kunde beispielsweise bestimmen, dass er mit Office 365 arbeitet oder gewisse Cloud-Dienste beansprucht. Der IT-Dienstleister kennt diese Produkte und kann ein vergleichbares Niveau der Sicherheit konfigurieren wie bei lokalen Services.

5.21 Umgang mit Bedrohungen und Schwachstellen bei Kunden

Viele Kunden setzen veraltete und unsichere Hardware oder Software ein. Der IT-Dienstleister macht den Kunden darauf aufmerksam. Dies geschieht am besten in einem regelmässigen Gespräch. Eine kurze Gesprächsnotiz mit den wesentlichen Entscheidungen wird sehr empfohlen.

5.22 Ausbildung der Mitarbeiter

Dieser Punkt wird von BACS und den Versicherungen als sehr kritisch bezeichnet. Ein grosser Teil der Cyberangriffe startet mit einer kompromittieren E-Mail. Jeder Mitarbeitende muss zwingend in der Lage sein, Fake-Emails zu erkennen und sich richtig zu verhalten. Daher müssen die Kunden und die IT-

Dienstleister regelmässig geschult werden. Diese Schulung beinhaltet auch das korrekte Verhalten des Mitarbeiters beim Empfang von solchen Fake-Emails.

5.23 Notfallkonzept

BACS und die Versicherungen erachten die Erstellung eines Notfallkonzeptes als sehr wichtig.

Ein Notfallkonzept stellt sicher, dass in einem ausserordentlichen Event an alles gedacht wird und dass notwendige Vorbereitungen ohne Hektik erarbeitet und getestet werden können. Das Notfallkonzept muss die wichtigsten Events abdecken. Ein grosses Risiko ist aktuell die Cyberkriminalität (Ransomware,

Datenverschlüsselung, Datendiebstahl und Androhung der Veröffentlichung), welche zwingend abgedeckt werden muss.

Ein Notfall kann sowohl beim IT-Dienstleister als auch bei den Kunden eines IT-Dienstleisters auftreten. Daher ist es sinnvoll, mindestens im IT-Umfeld ein kompatibles Notfallkonzept zu erarbeiten. Es wird notwendig sein, dass im Notfallkonzept eines Endkunden der IT-Dienstleister mit einbezogen wird.

Im IT-Umfeld hat das Notfallkonzept zu definieren, wer und wie die Kommunikation nach aussen sicherstellt. Zudem wird definiert, welche Stellen zur Behebung des Notfalles informiert werden müssen Polizei, BACS, Versicherungen, unterstützende Firmen, usw.). Die entsprechenden Kontaktadressen sind Bestandteil des Notfallkonzeptes.

Im IT-Umfeld ist der Umgang mit verschlüsselten Daten zu regeln. Es ist sicherzustellen, dass ein Recovery der Daten beispielsweise auch beim Ausfall eines AD möglich ist. Regelmässige Tests des Notfallkonzepts sind wichtig. Sie schulen die Schlüsselpersonen und decken Schwachstellen auf.

5.24 Ablaufende Termine

Es gibt immer mehr Informatik-Komponenten, die nach einem Ablaufdatum die Funktion einstellen (Lizenzen, Zertifikate, Wartungsablauf von Komponenten usw.). Alle Komponenten, die ein Ablaufdatum haben, müssen vom IT-Dienstleister überwacht werden.

Ein weiteres Risiko stellt veraltete Hardware dar. Wenn keine Security-Patches mehr erhältlich sind, müssen die Komponenten ersetzt werden.

5.25 Physische Sicherheit

Die physische Sicherheit muss durch den IT-Dienstleister gewährleistet werden. Der Zutritt zu den Räumlichkeiten des IT-Dienstleisters muss geregelt sein. Insbesondere ist der Zutritt zu allfälligen Datacentern des IT-Dienstleisters auf ein Minimum zu beschränken.

Die Geräte des IT-Dienstleister sind gegen äussere Einflüsse sinnvoll zu schützen (USV, Kühlung, redundanter Internet-Anschluss, usw.)

5.26 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 vorgängigen Kapitel im Kapitel 5 sind Risikominderungsmassnahmen.
- Risiko-Transfer: Einzelne Risiken können versichert werden. Die Art der Versicherung (Berufshaftpflicht, Cyber-Schäden, Finanzschäden usw.), die Versicherungssumme und die zusätzlichen Leistungen (z.B. Unterstützung bei einem Cyberangriff) müssen sorgfältig gewählt werden.
- Risiko-Akzeptanz: Jede Firma muss einzelne Risiken (oder Rest-Risiken) tragen. Das Tragen von Risiken muss zwingend von der Unternehmensleitung des IT-Dienstleisters akzeptiert werden und kann nicht delegiert werden.

Ein IT-Dienstleister sollte seine Kunden bei der Erstellung eines eigenen Risikomanagements unterstützen. Ein IT-Dienstleister kann ihnen in vielen Fällen weiterhelfen und ihre Fragen beantworten.

Auditoren-Komitee der Allianz Digitale Sicherheit Schweiz

6 Anhang

Abkürzungsverzeichnis

ADSS	Allianz Digitale Sicherheit Schweiz ADSS
BACS	Bundesamt für Cybersicherheit
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
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

Abkürzungen Prüfliste

HA	Hauptabweichung
NA	Nebenabweichung
NV	Nicht verfügbar / nicht prüfbar
HW	Hinweis
KD	Kunden Infrastruktur
EG	Eigene Infrastruktur / Infrastruktur des IT- Dienstleisters
S	Selbstdeklaration
I	Interview
K	Konsolen Audit