CyberSeal - Prüfliste

Kap.	Pt.	Kontrolle	Prio	Audit-methode: S=Selbst-deklaration I=Interview K=Konsole	Infra-struktur Dienst-leister	Infra-struktur Kunde
5.1		**Aufgabeteilung Kunde/IT-Dienstleister**				
	1	Es besteht eine schriftliche Abmachung über eine Aufgabenteilung mit allen Kunden (z.B. ein SLA, Wartungsvertrag, Servicedescription).	1	I	x	x
	2	Es gibt eine für Cybersicherheit verantwortliche Person/Rolle.	1	I	x	
	3	Der IT-Dienstleister erstattet dem Kunden gegenüber ein regelmässiges Security-Reporting.	2	I	x	
5.2		**Verwaltung des Zugriffs auf Kundeninfrastruktur**				
	1	Personalmutationen beim IT-Dienstleister können einfach umgesetzt werden. Ein ehemaliger Mitarbeiter kann nicht mehr auf die Kundeninfrastruktur/-daten zugreifen.	1	I	x	
	2	Der Kunde kann nicht auf Ressourcen beim IT-Dienstleister oder anderen Kunden zugreifen.	1	I	x	x
	3	Der Zugriff auf die Kundeninfrastruktur ist nur mit verwalteten Geräten möglich. Jumphosts und virtuelle Rechner gelten als verwaltet.	1	I		x
	4	Alle Kunden sind sich bewusst über den Umfang der Berechtigungen des IT-Dienstleisters.	1	I		x
	5	Für den Zugriff auf die Kundeninfrastruktur ist eine Mehrfaktor-Authentisierung notwendig.	1	I		x
	6	Zugriffe auf die Kundeninfrastruktur werden protokolliert.	2	I	x	
5.3		**Credentials und Berechtigungen**				
	1	Jede Mutation der Accounts (inkl. der Passwörter) oder der Berechtigungen ist nachvollziehbar.	1	S	x	x
	2	Die Passwörter des Kunden sind stark, einmalig und sicher verwahrt (Passwortsafe oder ähnliches).	1	S	x	
	3	In einem Notfall sind die Passwörter zugänglich.	1	S	x	x
	4	Privilegierte Accounts müssen besonders stark abgesichert sein.	1	S	x	x
	5	Es existiert ein definierter und sicherer Prozess für die Mutation der Accounts, des Passwortes und der Berechtigungen.	2	S	x	x
	6	Es existiert ein definierter und sicherer Prozess für temporäre Berechtigungen.	2	S	x	x
5.4		**Dokumentation**				
	1	Für jeden Kunden besteht eine Übersichtsdokumentation mit mindestens Hostname, IP-Adresse und Zweck der verwalteten Komponenten (Inventar).	1	I		x
	2	Die Dokumentation kann dem Kunden auf Antrag abgegeben werden (allgemein verbreitetes elektronisches Format wie PDF oder Papier).	1	I		x
	3	Die Dokumentation ist aktuell (nicht älter als 1 Monat nach der letzten Änderung).	2	I	x	x
5.5		**Netzwerkdesign**				
	1	Das Netzwerk ist segmentiert: z.B. Office Netzwerk, Core-Komponenten (Storage, Virtualisierungsplattform, Netzwerkkomponenten), Netzwerk in der Produktion, WLAN, Gäste-WLAN.	1	S	x	x
	2	Nicht patchbare Systeme/Applikationen müssen in einem separierten Netzwerk betrieben werden.	1	S	x	x
	3	Die Übergänge zwischen den Zonen haben minimale Connectivity (z.B. mittels Firewalls).	2	S	x	x
5.6		**Firewalls**				
	1	Die Regeln müssen lesbar sein (sinnvolle, mit Dokumentation übereinstimmende Bezeichnungen). Dokumentationen im Ruleset sind erwünscht.	1	I	x	x
	2	Das Ruleset muss regelmässig und nachvollziehbar überprüft werden. Ein Vieraugenprinzip wird empfohlen.	1	I	x	x
	3	Das Ruleset ist möglichst eng definiert. Z.B. sind Any-Any-Regeln nicht erlaubt, auch ausgehender Verkehr ist eingeschränkt. Ausnahmen sind zu begründen.	2	I	x	x
5.7		**WLAN**				
	1	Für jeden Kunden müssen separate, nicht ableitbare Passwörter verwendet werden.	1	I	x	x
	2	Es muss ein separates WLAN für private Geräte von Mitarbeitern und für Gäste eingerichtet werden.	1	I	x	x
	3	In der Officezone wird mit Zertifikaten authentifiziert.	2	I	x	x
	4	Es werden ausschliesslich aktuelle und sichere Schutzmechanismen verwendet.	2	I	x	x
5.8		**Identity Management (Active Directory, Azure, ...)**				
	1	Der Kunde besitzt einen Notfall-Administrator-Account, ausser er verzichtet explizit darauf.	1	S		x
	2	Accounts mit erweiterten Berechtigungen werden nicht für die täglichen Anwendungsarbeiten verwendet.	2	S	x	x
	3	Öffentlich zugreifbare Portale (z.B. Azure), welche mit dem eigenen AD synchronisiert sind, werden mit Mehrfaktorauthentifizierung geschützt.	2	S	x	x
	4	Der IT-Dienstleister hat einen eigenen Administrator-Account auf allen Kundensystemen.	2	S	x	x
	5	Die Identitäten und Berechtigungen müssen regelmässig überprüft werden (zumindest jährlich).	2	S	x	
5.9		**Hardening der IT-Komponenten**				
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für die Härtung der Systeme (Clients, Server, Netzwerk-Komponenten).	1	I	x	x
5.10		**Mail-System**				
	1	Der IT-Dienstleister stellt sicher, dass die E-Mail-Infrastrukturen vor Malware und Spam geschützt ist.	1	K	x	x
	2	Der IT-Dienstleister unterstützt nur E-Mail-Infrastrukturen, die die Absenderauthentizität prüfen (SPF. DKIM usw.).	1	K	x	x
	3	Zugriff mit Mobile Devices auf E-Mail-Systeme wird nur mit einer angepassten, technisch einschränkenden Company Policy der Firma zugelassen.	1	K	*x*	*x*
5.11		**Patch-Management**				
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Einspielen von Patches.	1	K	x	x
	2	Das Patching erfolgt in einer sinnvollen Kadenz.	1	K	x	x
	3	Der IT-Dienstleister stellt sicher, dass alle relevanten Systeme und Applikationen gepatched werden, neben Betriebssystemen auch Applikationen/Apps, Systeme in der Produktion, Firewall und Netzwerkgeräte. Begründete Ausnahmen sind schriftlich festgehalten.	2	K	x	x
	4	Bei grösseren, bekannten Schwachstellen muss sofort reagiert werden können.	2	K	x	x
	5	Das Patchsystem für Clients ist automatisiert und zentralisiert.	2	K	x	x
5.12		**Mobile Devices (Laptops, Tablets, Smartphones)**				
	1	Die Datenträger resp. Container auf mobilen Systemen sind verschlüsselt.	1	I	x	x
	2	Der Zugriff auf Firmendaten ist nur nach einer ausreichenden Authentisierung möglich.	1	I	x	x
	3	Es existieren Anforderungen an die mobilen Geräte. Die Anforderungen werden durch Policies durchgesetzt.	2	I	x	x
	4	Ein Device- oder Application-Management wird eingesetzt.	3	S	x	x

CyberSeal - Prüfliste

Kap.	Pt.	Kontrolle	Prio	Audit-methode: S=Selbst-deklaration I=Interview K=Konsole	Infra-struktur Dienst-leister	Infra-struktur Kunde
5.13		**Remote Work / Home Office**				
	1	Remote Work Zugriff ist nur über verwaltete Systeme möglich (z.B. Zugriff von BYOD-Geräten nur über virtuelle Desktops).	1	I	x	x
	2	Remote Work Zugriff ist nur nach einer Mehrfaktor-Authentisierung möglich.	1	I	x	x
	3	Eine Remote Work Richtlinie ist mit Mitarbeitenden vereinbart.	2	I	x	
5.14		**Malware-Protection**				
	1	Alle Systeme sind mit einem Malwareschutz versehen, sofern sie dies technisch zulassen.	1	K	x	x
	2	Es wird ein zweistufiges Konzept (Firewall und Client) implementiert.	1	K	x	x
	3	Systeme ohne Malwareschutz (z.B. Produktionssysteme) sind netzwerkmässig abzuschotten.	2	I	x	x
	4	Eine Endpoint Detection and Responce Lösung ist im Einsatz.	3	S	x	x
5.15		**Backup / Restore**				
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Backup/Restore der notwendigen Systeme und Services (zb.: Server, Netzwerk-Komponenten, Cloud Services).	1	K	x	x
	2	Das Backup wird regelmässig getestet. Es sind regelmässige Restore-Tests von gesamten Systemen (Server) inkl. Daten notwendig.	1	K	x	x
	3	Eine ausreichende Sicherungskopie besteht aus mehreren Generationen, ist örtlich getrennt und unveränderbar aufzubewahren.	1	K	x	x
	4	Der Zugriff auf die Backup-Infrastruktur erfolgt nicht über das reguläre Identity Management.	2	I	x	x
5.16		**Change Management / Incident Management**				
	1	Alle Änderungen an kritischen Systemen des Dienstleisters erfolgen nach definierten Prozessen und sind nachvollziehbar protokolliert.	1	S	x	
	2	Alle Änderungen an Kunden-Systemen sind nachvollziehbar protokolliert.	2	S		x
	3	Alle security relevanten Incidents werden nach einem definierten Prozess behandelt und können nachvollzogen werden.	2	S	x	x
5.17		**Protokollierung**				
	1	Der IT-Dienstleister stellt sicher, dass alle System-Protokolle gemäss Vereinbarung aufbewahrt werden (SLA empfohlen).	1	S		x
	2	Mindestens jeder Zugriff des IT-Dienstleisters auf Kundensysteme und Hardwarefehler müssen protokolliert werden.	1	S		x
5.18		**Monitoring**				
	1	Der IT-Dienstleister betreibt ein Systemmonitoring der Systeme und leitet bei Bedarf geeignete Massnahmen ein.	2	S	x	x
	2	Die Sicherheitssysteme werden überwacht. Alarme werden behandelt.	3	S	x	x
5.19		**Entsorgung von Datenträgern / Löschung von Daten**				
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Entsorgen von Datenträgern.	1	S	x	x
	2	Es ist ein Prozess für die Datenlöschung vorhanden	2	S	x	
5.20		**Services von Drittanbietern**				
	1	Der IT-Dienstleister kennt die betreuten Produkte von Drittanbietern und kann ein vergleichbares Niveau der Sicherheit wie bei lokalen Services anbieten.	2	S		x
	2	Der IT-Dienstleiter sorgt dafür, dass seine Kunden regelmässig ein Reporting über die erbrachten Leistungen und die Verfügbarkeiten von Drittanbietern erhalten.	3	S	x	
5.21		**Umgang mit Bedrohungen und Schwachstellen bei Kunden**				
	1	Der IT-Dienstleister informiert die Kunden über mögliche Bedrohungen und Schwachstellen in der betreuten Infrastruktur oder bei Services.	2	S		x
	2	Ein Schwachstellen Management wird betrieben.	3	S	x	x
5.22		**Ausbildung der Mitarbeiter**				
	1	Eine Benutzer- und Administrationsrichtlinie (z.B. Acceptable Use Policy) ist definiert und wird angewendet.	1	K	x	
	2	Der IT-Dienstleister organisiert für eigene Mitarbeitende regelmässige Ausbildungen zum Thema Informationssicherheit.	1	K	x	
	3	Der IT-Dienstleister bietet seinen Kunden Awareness-Dienste an oder vermittelt ihm einen Drittanbieter.	2	S		x
5.23		**Notfallkonzept**				
	1	Ein aktuelles Notfallkonzept ist vorhanden und im Notfall verfügbar. Es berücksichtigt u.a. Daten-Verschlüsselungen und -Offenlegung, sowie Erpressung.	1	K	x	x
	2	Das Notfallkonzept wird angemessen und regelmässig getestet.	2	S	x	x
	3	Das Notfallkonzept regelt auch den Einbezug von externen Stellen (Polizei, BACS, Versicherungen, unterstützende Firmen usw.).	2	S	x	x
	4	Der IT-Dienstleiter bietet seinen Kunden Unterstützung an bei der Erstellung eines zeitgemässen Notfallkonzepts.	2	S	x	x
5.24		**Ablaufende Termine**				
	1	Die Ablaufdaten von Informatik-Komponenten (z.B. Zertifikate, Lizenzen usw.) werden geführt. Es wird rechtzeitig eine Meldung vor Ablauf generiert.	2	S	x	x
	2	Der Kunde wird auf veraltete Hard- und Software inklusive den damit verbundenen Risiken aufmerksam gemacht.	2	S	x	x
5.25		**Physische Sicherheit**				
	1	Der Zutritt zu den Räumlichkeiten des IT-Dienstleisters ist kontrolliert und sinnvoll eingeschränkt.	1	I	x	
	2	Der Zutritt zum Datacenter des IT-Dienstleisters ist zu autorisieren und zu protokollieren.	1	I		
	3	Die IT-Geräte des Dienstleisters sind gegen äussere Einflüsse geschützt (z.B. USV, Kühlung, redundanter Internet Anschluss).	2	I	x	
5.26		**IT-Risikomanagement**				
	1	Es wird jährlich ein Risikomanagement / Risikoanalyse durchgeführt. Der VR unterzeichnet den Risk Report zu Händen der GL und akzeptiert damit die verbleibenden Risiken.	2	I	x	
	2	Es wurde ein Prozess etabliert, um nicht akzeptable Risiken zu behandeln.	2	I	x	
	3	Der IT-Dienstleister unterstützt den Kunden bei Bedarf in den Fragen des Risiko-Managements.	3	S		x