CyberSeal Prüfliste

Kap.	Pt.	Kontrolle	Prio 1 - 3	Selbstdeklaration Interview Konsole	Eigene Infrastruktur	Infrastruktur beim Endkunden
5.1		**Aufgabeteilung Kunde/IT-Dienstleister**		I		
	1	Es besteht eine schriftliche Abmachung über eine Aufgabenteilung mit allen Kunden (z.B eine SLA, Wartungsvertrag, Servicedescription)	1	I		
5.2		**Verwaltung des Zugriffs auf Kundeninfrastruktur**		I		
	1	Personalmutationen beim IT-Dienstleister können einfach umgesetzt werden. Ein ehemaliger Mitarbeiter kann sich nicht mehr beim Kunden anmelden.	1	I	x	
	2	Der Kunde kann nicht auf Ressourcen beim IT-Dienstleister oder anderen Kunden zugreifen.	1	I	x	x
	3	Bei jedem Kunden werden andere Passwörter verwendet.	1	I		x
	4	Der Zugriff auf die Kundeninfrastruktur ist nur mit verwalteten Geräten möglich. Jumphosts und virtuelle Rechner gelten als verwaltet.	1	I		x
	5	Alle Kunden sind sich bewusst über den Umfang der Berechtigungen des IT-Dienstleisters	1	I		x
	6	Für den Zugriff auf die Kundeninfrastruktur ist eine Mehrfaktor-Authentisierung notwendig.	2	I		x
	7	Für einen technischen Account muss eine starke Authentisierung angewendet werden.	3	I	x	x
5.3		**Dokumentation**		I		
	1	Für jeden Kunden besteht eine Übersichtsdokumentation mit mindestens Hostname, IP-Adresse und Zweck der verwalteten Komponente.	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)	2	I	x	x
5.4		**Credentials und Berechtigungen**		S		
	1	Jede Mutation der Accounts (inkl. der Passwörter) oder der Berechtigungen ist nachvollziehbar	1	S	x	x
	2	In einem Notfall sind die Passwörter zugänglich	1	S	x	x
	3	Es existiert ein definierter und sicherer Prozess für die Mutation der Accounts, des Passwortes und der Berechtigungen.	2	S	x	x
	4	Es existiert einen definierten und sicheren Prozess für temporäre Berechtigungen	2	S	x	x
	5	Die Passwörter des Kunden sind sicher verwahrt (Passwortsafe oder ähnliches).	2	S		x
5.5		**Netzwerkdesign**		S		
	1	Das Netzwerk ist segmentiert: z.B. Office Netzwerk, Netzwerk in der Produktion (nicht patchbare Komponenten), WLAN, Gäste-WLAN	1	S	x	x
	2	Die Übergänge zwischen den Zonen haben minimale Connectivity (z.B. mittels Firewalls)	2	S	x	x
	3	IPV6 wird nur eingesetzt, falls die entsprechenden Kompetenzen vorhanden sind (Achtung: Microsoft arbeitet mit IPV6)	3	S	x	x
5.6		**Firewalls**		I		
	1	Die Regeln müssen lesbar sein (Sinnvolle, mit Dokumentation übereinstimmende Bezeichnungen). Dokumentationen im Ruleset sind erwünscht	1	I	x	x
	2	Das Ruleset ist möglichst eng definiert. Z.B. sind Any-Any-Regeln nicht erlaubt, Ausgehender Verkehr ist eingeschränkt. Ausnahmen sind zu begründen.	2	I	x	x
	3	Das Ruleset muss regelmässig und nachvollziehbar überprüft werden. Ein Vieraugenprinzip wird empfohlen.	2	I	x	x
5.7		**WLAN**		I		
	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 hat jeder Mitarbeiter seinen eigenen Account. In anderen Zonen sind generische Account erlaubt.	2	I	x	x
	4	Es werden keine veralteten oder unsichere Schutzmechanismen verwendet.	2	I	x	x
	5	Generische Account im WLAN müssem bewilligt werden	2	I	x	x
5.8		**AD Design**		S		
	1	Der Kunde besitzt einen Notfall-Administrator-Account.	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 geschützen	2	S	x	x
	4	Die IT-Dienstleister haben einen eigenen Admistrator-Account auf allen Kundensystemen	2	S	x	x
5.9		**Hardening der IT-Komponenten**		I		
	1	Der IT-Partner hat einen definierten und sicheren Prozess für die Härtung der Systeme (Clients, Server, Netzwerk-Komponenten)	1	I	x	x
5.10	**KR**	**Mail-System**		K		
	1	Der IT-Dienstleister stellt sicher, dass die Mail-Infrastrukturen vor Malware und Spam geschützt ist	1	K	x	x
	2	Der IT-Dienstleister unterstützt nur Mail-Infrastrukturen, die die Absenderauthentizität prüft (SPF. DKIM usw.)	1	K	x	x
5.11	**KR**	**Patch-Management**		K		
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Einspielen von Patches	1	K	x	x
	2	Das Patches erfolgt in einer sinnvollen Kadenz (z.B. OS-Patches für Clients müssen einen **1 Monat** nach der Verfügbarkeit installiert sein)	1	K	x	x
	3	Der IT-Dienstleister stellt sicher, dass alle relevanten Systeme und Applikationen gepatched werden, neben Microsoft OS auch andere Applikationen (z.B. ERP und	2	K	x	x
	4	Bei grösseren, bekannten Schwachstellen muss sofort reagiert werden können.	2	K	x	x
	5	In der Officezone werden nur Systeme (Betriebssysteme) eingesetzt, die noch System Patches erhalten	2	K	x	x
5.12		**Mobile Devices**		I		
	1	Die Datenträger 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 mobiles Devices. Die Anforderungen werden durch Policies durchgesetzt.	2	I	x	x
5.13		**Home Office**		I		
	1	Der Zugriff vom Home Office ist nur über verwaltete Systeme möglich (Zugriff von BYOD-Geräten nur über virtuelle Desktops)	1	I	x	x
	2	Der Zugriff vom Home Office ist nur nach einer Zweifaktorauthentisierung möglich. Managed Geräte gelten als einen Faktor, falls Zugriff nur mit managed Geräten	1	I	x	x
	3	Weitere Dienste sind bei Home Office nur nach einer Sicherheitsprüfung erlaubt (Printer ist problematisch, Laufwerkmapping ist bei verwalteten Geräten erlaubt)	2	I	x	x
5.14	**KR**	**Malware-Protection**		K		
	1	Alle sinnvollen IT-Systeme sind mit einem Malwareschutz versehen. Whitelisting Systeme (Applocker) sind erlaubt	1	K	x	x
	2	Es wird ein zweistufiges Konzept (Firewall und Client) implementiert	2	K	x	x
	3	Systeme ohne Malwareschutz (z.B. Produktionssysteme) sind netzwerkmässig abzuschotten	2	K	x	x
5.15	**KR**	**Backup**		K		
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess den Backup der notwendigen Systeme (Server, Netzwerk-Komponenten, Clients bei Bedarf)	1	K	x	x
	2	Der Backup wird regelmässig getestet. Es sind auch Tests mit dem Ersatz des **gesamten Systems** notwendig.	1	K	x	x
	3	Eine ausreichende Sicherungskopie ist örtlich getrennt aufzubewahren.	1	K	x	x
	4	Ein Schreib-Zugriff auf die Backupdaten ist nach dem Backup nicht mehr möglich. Ein Offline Backup wird empfohlen (Band, Wechseldatenträger)	2	K	x	x
5.16		**Change Management / Incident Management**		S		
	1	alle Änderungen an Systemen sind nachvollziehbar protokolliert.	2	S	x	x
	2	alle Incidents können nachvollzogen werden	2	S	x	x
5.17		**Protokollierung**		S		
	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
	3	Die Protokolle werden mindestens für 6 Monate aufbewahrt.	2	S		x
5.18		**Monitoring**		S		
	1	Der IT-Dienstleister monitored die Kundensysteme	2	S		x
5.19		**Entsorgung von Datenträgern**		S		
	1	Der IT-Dienstleister hat einen definierten und sicheren Prozess für das Entsorgen von Datenträgern.	1	S	x	x
5.20		**Services von Drittanbietern**		I		
	1	Der IT-Dienstleister kennt die betreute Produkte von Drittanbietern und kann ein vergleichbares Niveau der Sicherheit wie bei lokalen Services anbieten.	3	I		x
5.21		**Schwachstellen beim Kunden**		S		
	1	Der IT-Dienstleister informiert die Kunden über mögliche Schwachstellen in der Infrastruktur oder bei Services	2	S		x
5.22	**KR**	**Ausbildung der Mitarbeiter**		K		
	1	Der IT-Dienstleister bietet seinen Kunden eine Schulung an (Schwerpunkt Social Engineering) oder vermittelt diese.	2	K		x
	2	Der IT-Dienstleister organisiert für eigene Mitarbeiter regelmässige Ausbildungen zum Thema IT-Sicherheit (Schwerpunkt Social Engineering)	1	K	x	
5.23	**KR**	**Notfallkonzept**		K		
	1	Der IT-Dienstleister hat ein Notfallkonzept. Er bietet seinen Kunden an, ihn bei der Erstellung des Notfallkonzeptes zu unterstützen.	1	K	x	x
	2	Das Notfallkonzept regelt insbesondere den Einbezug von externen Stellen (Polizei, NCSC, Versicherungen, unterstützende Firmen usw.)	2	K	x	x
	3	Das Notfallkonzept ist aktuell und wird angemessen getestet	2	K	x	x
	4	Der Umgang mit verschlüsselten Daten ist im Notfallkonzept geregelt	2	K	x	x
5.24		**Ablaufende Termine**		S		
	1	Die Ablaufdaten von Informatik-Komponenten (z.B. Zertifikate, Lizenzen usw.) werden geführt. Es wird automatisch eine Meldung rechtzeitig vor Ablauf generiert	2	S	x	x
	2	Der Kunde wird auf veraltete Hardware aufmerksam gemacht	2	S	x	x
5.25		**Physische Sicherheit**		I		
	1	Der Zutritt zu den Räumlichkeiten der IT-Dienstleister ist kontrolliert und sinnvoll eingeschränkt	1	I	x	
	2	Der Zutritt zum Datacenter des IT-Dienstleisters ist durch die Geschäftsleitung zu authorisieren und ist zu protokollieren	2	I		
	3	Die IT-Geräte des Dienstleisters ist gegen äussere Einflüsse geschützt (z.B. USV, Kühlung, redundanter Internet Anschluss)	2	I	x	
5.26		**IT-Risikomanagement**		I		
	1	Es wird ein IT-Risikomanagement durchgeführt und es ist sichergestellt, dass mindestens 1 jährlich die GL die akzeptierten Risiken übernimmt	2	I	x	
	2	Es wurde ein Prozess etabliert, um die IT-Risiken zu mindern	2	I	X	
	3	Es wurde ein sinnvoller Transfer von IT-Risiken auf eine Versicherungsgesellschaft geprüft	2	I	x	
	4	Der IT-Dienstleister unterstützt den Kunden bei Bedarf in den Fragen des IT-Risiko-Managements	3	I		x