Checklisten IT-Sicherheit

Die folgende Checkliste soll helfen, sicherheitsrelevante Schwachstellen in IT-Infrastrukturen aufzuspüren. Sie erhebt keinen Anspruch auf Vollständigkeit und kann nicht jeder Situation gerecht werden.

Inhaltsverzeichnis

1 Zugriffsschutz

1.1 Passwortkonzept

Thema	Status	Bemerkung
Gibt es Regeln für die Passwortbildung bei Clients?		
Gibt es Regeln für die Passwortbildung bei der IT-Infrastruktur?		
Sind die Passwörter für die IT-Infrastruktur schriftlich an einem sichern Ort zu Handen des Auftragsgebers (z.B. Geschäftsleitung) deponiert?		
Gibt es Hilfen (z.B. Passworttresore) für Mitarbeitende, welche mehrere Passwörter für ihre Aufgaben benötigen?		
Ist das gesamte Passworthändling schriftlich in einem Konzept festgehalten?		

2 Datenspeicherung

2.1 Betrieb Speichersysteme

Thema	Status	Bemerkung
Aufbau und Örtlichkeiten		
• Befinden sich die Speichermedien an einem von Elementarschäden (Feuer, Wasser…) möglichst geschützten Ort?		
• Sind die Speichermedien in einem abgeschlossenen Raum (Schrank)?		
Gibt es ein schriftliches Konzept für die Datenspeicherung, in dem die folgenden Punkte festgehalten sind:		
• Sind die Verantwortlichen bezeichnet?		
• Wer hat Zugriff für die Verwaltung?		
• Ist die Stellvertretung sichergestellt?		
• Ort und Zugänglichkeit der Schlüssel für die Räumlichkeiten?		
• Zugänglichkeit im Passwortkonzept beschrieben?		

2.2 Arbeitsspeicher (Primärspeicher)

Thema	Status	Bemerkung
Gibt es Bereiche, auf denen die Benutzer gemeinsame Daten speichern/lesen können?		
Wird der Speicher regelmässig auf Viren gescannt?		

2.2.1 Anforderungen externe Datenspeicherung (nur falls extern)

Thema	Status	Bemerkung
Sind die Geschäftsbeziehungen in AGBs festgehalten?		
Sind die Geschäftsbeziehungen in einem Vertrag festgehalten?		
Sind folgenden Themen klar geregelt:		

• Gibt es keine Auswertung oder Weitergabe der Daten durch den Provider?		
• Sind die Mitarbeitenden des Providers zur Geheimhaltung verpflichtet?		
• Erfolgt der Datenverkehr verschlüsselt und verfügt der Anbieter über ein Zertifikat?		
• Update der Verwaltungssoftware geregelt?		

2.2.2 Anforderungen interne Datenspeicherung (nur falls intern)

Thema	**Status**	**Bemerkung**
Aufbau und Örtlichkeiten		
• Ist er örtlich getrennt vom Backup und vom Archiv?		
Speicherorganisation		
• Kommen RAID Systeme zum Einsatz?		
• Gibt es eine Notstromversorgung?		
Betrieb		
• Update der Betriebssoftware geregelt?		

2.3 Sicherung

Thema	**Status**	**Bemerkung**
Aufbau und Örtlichkeiten		
• Ist es örtlich getrennt vom Primärspeicher und vom Archiv?		
Durchführen der Sicherung		
• Wird das Generationenprinzip angewendet?		
• Ist der Sicherungs-Speicher nur während der Speicherung online?		
• Erfolgt vor der Speicherung ein Virenscan des Primärspeichers?		
Software für die Sicherung		
• Update der Sicherungs-Software geregelt?		
Kontrolle der Sicherung		
• Wird die Sicherung systematisch überprüft (Lesbarkeit)		
• Wird das Restore regelmässig geübt?		

2.4 Archiv (Sekundärspeicher)

Thema	Status	Bemerkung
Aufbau und Örtlichkeiten		
• Ist es örtlich getrennt vom Primärspeicher und von der Sicherung?		
Speicherorganisation		
• Ist die Aufbewahrungsdauer (Archivierung) für die Daten (Belegpflicht) erfüllt?		
• Ist das Intervall für die Daten-archivierung festgelegt?		
• Sind die Datenträger beschriftet (Datum, Inhalt)		

3 Applikationen

Thema	Status	Bemerkung
Wird für alle Applikationen regelmässig überprüft, ob ein Update ansteht		

4 PC-Clients

Thema	Status	Bemerkung
Gibt es Benutzer*innen (ausser IT-Administratoren), welche Administratorrechte auf dem PC-Client haben?		
Wurden diese Benutzer*innen speziell geschult?		
Arbeiten die Benutzer*innen mit festgelegten Gruppenrichtlinien (GPO)?		
Werden die Laufwerke für die Datenspeicherung nicht genutzt (d.h. die Benutzer*innen speichern alles im Primärspeicher ab)?		
Ist der Flashplayer deaktiviert?		
Ist (kann) JavaScripct deaktiviert (werden)?		
Ist gewährleistet, dass keine lokalen Laufwerke freigegeben wurden (GPO)?		

Ist gewährleistet, dass die Benutzer*innen keine Programme installieren können (GPO)?		
Ist gewährleistet, dass die Benutzer*innen keine Browser-Plug-Ins installieren können (GPO)?		
Ist gewährleistet, dass sicherheitsrelevante Updates des Betriebssystems möglichst rasch installiert werden?		
Ist gewährleistet, dass die Clients regelmässig auf Viren gescannt werden?		

5 MS Office

Thema	Status	Bemerkung
Sind die Einstellungen im Trust-Center korrekt (Makros) und für den Benutzer nicht änderbar?		

6 WEB Dienste

Falls Sie WEB Dienste zur Verfügung stellen:

Thema	Status	Bemerkung
Gibt es 2 Firewalls mit einer DMZ (Demilitarisierte Zone) Server.		
Sind alle nicht benötigten Dienste im Server inaktiv?		
Ist die Administration nur über ein starkes Passwort möglich?		
Wird die Software regelmässig aufdatiert?		
Gibt es eine WEB Application Firewall?		
Ist das GEO-Blocking aktiv?		
Gibt es einen Aktionsplan im Falle einer DDoS (Distributed Denial of Service)? https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html#par_text		

7 Lokales Netzwerk

Thema	Status	Bemerkung
Sind grössere Netzwerke in Subnetze aufgeteilt?		
Sind grössere Netzwerke in VLANs aufgeteilt?		
Gibt es einen Firewall ins Internet?		
Wird das Netzwerk regelmässig überprüft (z.B. mit arp, nmap usw.)		

8 IT-Abteilung

Thema	Status	Bemerkung
Gibt es Stellenbeschreibungen für die IT- Mitarbeitenden?		
Orientieren sich die IT-Mitarbeitenden regelmässig über die aktuelle Virenlage (z.B. über NCSC, SW-Lieferanten usw.)		
Werden gemeldete Sicherheitslücken sofort geschlossen.		

9 Mitarbeitende

Thema	Status	Bemerkung
Wurden die Mitarbeitenden in IT-Sicherheit geschult (Phishing, Trojaner …?		
Ist den Mitarbeitenden das Passwortkonzept bekannt		
Gibt es Richtlinien über das Surfen im Internet?		
Gibt es Richtlinien wie lange Mitarbeitende Dateien auf ihren PCs behalten dürfen?		
Sind sich die Mitarbeitenden den Gefahren von Makroviren bewusst.		

10 Mobile Computing

Thema	Status	Bemerkung
Können die Mitarbeitenden über eine Cloud auf die Daten in der Firma zugreifen?		
Falls Daten lokal gespeichert werden müssen, gibt es eine Verschlüsselung?		
Sind die Mitarbeitenden geschult im Erkennen von speziellen Gefahren des Mobile Computing (Virenschutz, WLAN, E-Mail usw.)		

11 Home-Office

Thema	Status	Bemerkung
Können die Mitarbeitenden über eine Cloud auf die Daten in der Firma zugreifen?		
Falls Daten lokal abgespeichert werden, ist es den Mitarbeitenden bewusst, dass Sie für den Datenschutz zuständig sind?		

12 WEB-Seite

Thema	Status	Bemerkung
Werden E-Mail-Adressen auf der WEB-Seite zurückhaltend aufgeführt?		
Gibt es ein Zertifikat für die WEB-Seite?		
Wird für die Administration ein sicheres Passwort verlangt (Passwortkonzept)		
Wird die verwendete CMS Software regelmässig aufdatiert (inkl. allfälliger Plugins)		
Wird die verwendete CMS Software regelmässig auf Schadsoftware überprüft (z.B. scan auf .exe Dateien)		

13 SaaS (Software as a Service)

Thema	Status	Bemerkung
Sind die Geschäftsbeziehungen in AGBs festgehalten?		
Sind die Geschäftsbeziehungen in einem Vertrag festgehalten?		
Sind folgenden Themen klar geregelt:		
• Gibt es keine Auswertung oder Weitergabe der Daten durch den Anbieter?		
• Sind die Mitarbeitenden des Anbieters zur Geheimhaltung verpflichtet?		
Erfolgt der Zugriff über eine 2-Faktor Authentifizierung?		
Erfolgt der Datenverkehr verschlüsselt und verfügt der Anbieter über ein entsprechendes Zertifikat?		