Stellungnahme zu zentralen Datenschutz- und Datensicherheitsthemen der synaforce GmbH

Generischer Ansatz nach Art. 32 DS-GVO zur Sicherheit (Technische und Organisatorische Maßnahmen – TOM)

Ziel und Inhalt:

Die DSGVO fordert von Verantwortlichen und Auftragsverarbeitern in Art. 32 DS-GVO ein Schutzniveau, das dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenen ist.
Dabei sollen zur Gewährleistung der Sicherheit insbesondere die Risiken berücksichtigt werden, die aus einer Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität der personenbezogenen Daten, der an deren Verarbeitung beteiligten IT-Systeme, Dienste und Fachprozesse hervorgehen können.
Ziel ist es, diese Risiken einzudämmen, indem wirksame technische und organisatorische Maßnahmen (TOM) umgesetzt werden.

Zertifizierungen und Testate:
Die synaforce GmbH ist durch folgende, gültige Standards zertifiziert und testiert.

- ISO/IEC 27001:2022
- ISO 9001:2015
- DIN EN 50600 CAT III
- ISAE3402 Type II
- BSI-C5

Diese Zertifizierungen bilden eine fundierte Grundlage für die Umsetzung der TOM, da hier Informationssicherheit, Rechenzentrumssicherheit, Qualitätsmanagement und Datenschutz durch externe Auditoren geprüft werden. Zusätzlich werden regelmäßig Audits und Kontrollen von den internen Beauftragten (ISB, DSB und QMB) durchgeführt.

1 Management und Organisation

Mangelhafte Sicherheitsstrukturen in einer Organisation können den Betriebsablauf erheblich gefährden. Bestehende Fachkompetenzen sind daher zu nutzen. Dabei ist nicht nur der IT-Verantwortliche und der Informationssicherheitsbeauftragte (ISB), sondern auch der Datenschutzbeauftragte (DSB) im Prozess der Umsetzung von Sicherheitsanforderungen einzubinden.

- ☑ Eine geeignete Organisationstruktur für Informationssicherheit ist vorhanden und die Informationssicherheit ist in die organisationsweiten Prozesse und Abläufe integriert
- ☑ Sicherheitsricht- und -leitlinien sind definiert, von der Geschäftsleitung genehmigt und dem Personal kommuniziert
- ☑ Die Rollen der einzelnen Mitarbeiter im Sicherheitsprozess sind eindeutig festgelegt
- ☑ Regelmäßige Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach dem PDCA-Zyklus (Plan-Do-Check-Act)
- ☑ Konzepte und Dokumentationen im Sicherheitsumfeld werden regelmäßig überprüft und aktuell gehalten
- ☑ Einsatz eines geeigneten Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001
- ☑ Die Rollen und Verantwortlichkeiten im Bereich der Sicherheit sind bekannt und besetzt (u. a. Informationssicherheitsbeauftragter (ISB), IT-Leiter, Datenschutzbeauftragter (DSB))
- ☑ Konsequente Einbindung des ISB und DSB bei Sicherheitsfragen
- ☑ Ausreichende fachliche Qualifikation des DSB für sicherheitsrelevante Fragestellungen und Möglichkeiten zur Fortbildung für dieses Thema

- ☑ Durchführung von regelmäßigen Audits des DSB nach Art. 32 DS-GVO zur Sicherheit der Verarbeitung
- ☑ Kenntnis der zuständigen Datenschutzaufsichtsbehörde sowie Wissen über die Meldeverpflichtungen nach Art. 33 und 34 DS-GVO (Verletzung der Sicherheit)
- ☑ Vorhandensein von Eskalationsprozessen bei Sicherheitsverletzungen (Wer ist wann wie zu informieren?), u. a. im Notfallmanagement und konsequente Dokumentation bei Sicherheitsvorkommnissen (Security Reporting)
- ☑ Aktive Unterstützung der Zusammenarbeit des DSB mit dem ISB durch die Unternehmensleitung
- ☑ Erkenntnisse über (neue) digitale Bedrohungen werden stets gesammelt und potenzielle Auswirkungen auf den eigenen Betrieb abgeleitet

2 Physikalische Sicherheit der Infrastruktur

Der persönliche Zugang zu IT-Systemen und personenbezogenen Daten wird Unbefugten erschwert.

- ☑ Es besteht ein umfassendes Gesamtkonzept zur Gebäudeabsicherung im Allgemeinen (z. B. Brandschutz, Zutrittsbeschränkung und -kontrolle, Videoüberwachung)
- ☑ Es besteht ein Konzept zu Zutrittsregelungen und zur physischen Zugangskontrolle (Perimeterschutz)
- ☑ Klare Regelungen zum Umgang mit Besuchern (z. B. Begleitung, Sicherheitszonen, Protokollierung, Zuständiger Mitarbeiter für Besucher) ist als Bestandteil des Konzepts implementiert
- ☑ Gelebte Regelungen zum Umgang auch mit externen Dienstleistern (z. B. bei Werkverträgen, Handwerker, Wartung von Systemen) – wie Geheimhaltungserklärung, persönliche Begleitung in Sicherheitszonen und Protokollierung
- ☑ Es bestehen verschiedene Sicherheitszonen (z. B. Außenbereiche, Arbeitsbereiche und Besprechungsräume, Datacenterbereiche)
- ☑ Bei Sicherheitszonen:
    - Aktuelle Übersicht zur Berechtigungsverwaltung (Welcher Mitarbeiter darf in welche Zone?)
    - Zugang zu Hochsicherheitszonen durch Token **und** Zweifaktorauthentifizierung (Fingerprint / PIN)
    - Bei Zonenübergang und im Datacenterbereich selbstschließende Türen
    - Beschilderung, welche Zone nicht betreten werden soll/darf
- ☑ Sichere Schließsysteme samt zentraler, dokumentierter Schlüssel-/Tokenverwaltung
- ☑ Es besteht ein Brandschutzkonzept
- ☑ Verwendung von Feuer-/Rauchmeldeanlagen (im Rahmen des Brandschutzkonzepts)
- ☑ Einsatz von automatischen Löschsystemen in Serverräumen (z. B. Stickstoff-Löschung) unter Berücksichtigung von Arbeitsschutzvorschriften
- ☑ Feuerhemmende Schränke/Tresore zur Lagerung essenzieller Komponenten (z. B. Backup-Bänder, wichtige Originaldokumente)
- ☑ Das Gebäude (z. B. Wände, Fenster) und die Infrastruktur (z. B. Leitungen, Gefahrenmeldeanlagen) werden regelmäßig durch Fachpersonal geprüft und gewartet
- ☑ Komplette Umzäunung des Betriebsgeländes
- ☑ Stabile, einbruchshemmende Fenster und Türen im EG
- ☑ Einsatz einer Alarmanlage zur Einbruchserkennung, insbesondere außerhalb der Arbeitszeit
- ☑ Einsatz von Videoüberwachungssystemen unter Berücksichtigung datenschutzrechtlicher Anforderungen (Monitoring des Zugangsschutzes)
- ☑ Ausreichende Klimatisierung von Serverräumen
- ☑ Keine Fenster in Serverräumen

- ☑ Einsatz von Anlagen zur Sicherstellung der Stromversorgung von Serversystemen (redundante USV, NEA), insbesondere bei kurzfristigen Stromausfällen oder Schwankungen
- ☑ Risiken durch Überflutung/Starkregen werden regelmäßig geprüft und Risikobewertungen durchgeführt.

3 Awareness der Mitarbeiter

Beschäftige stehen mittlerweile verstärkt im Fokus von Cyberattacken. Mittels raffinierten Social Engineering Techniken sollen sie dazu verleitet werden, sicherheitskritische Aktionen auszuführen. Mitarbeiter müssen daher gerade in Sicherheitsfragen geschult sein, um solche Angriffe zu vereiteln.

- ☑ Das gesamte Personal der Organisation erhält jährlich eine Schulung für Informationssicherheit und Datenschutz
- ☑ Schulung in Informationssicherheit und Datenschutz für neue Beschäftigte werden zeitnah nach Aufnahme des Beschäftigungsverhältnisses gemacht
- ☑ Regelmäßige Auffrischungsschulungen für bestehendes Personal bei Bedarf (z.B.: Neuerungen oder besondere Bedrohungen / Gefahren) werden durchgeführt
- ☑ Bei Bedarf werden regelmäßig Informationen über Neuigkeiten zum Datenschutz und der Informationssicherheit (z. B. per Mail, Intranet) an alle Mitarbeiter veröffentlicht
- ☑ Relevante Richtlinien, z. B. zur E-Mail-/Internetnutzung, Umgang mit Schadcodemeldungen, Einsatz von Verschlüsselungstechniken, werden aktuell gehalten und sind leicht auffindbar (z. B. im Intranet)
- ☑ Datenschutzinformationen (welches z. B. auch Schulungsinhalte bereitstellt) sind für alle betroffenen Mitarbeiter im Intranet zugänglich
- ☑ Ausgewählte Mitarbeiter, die bei der Erkennung von Sicherheitsverletzungen beteiligt sind (ISB, DSB, Geschäftsführung, Führungskräfte, Rufbereitschaft) kennen die internen Prozesse zum Umgang mit Vorfällen (u. a. Meldung nach Art. 33 DS-GVO, Notfallpläne und -konzepte)
- ☑ Alle Beschäftigten werden über die Gefahren der E-Mail-Kommunikation, insbesondere bei verschlüsselten E-Mail-Anhängen (z. B. Zip-Datei mit Passwort) sensibilisiert
- ☑ Beschäftigte erkennen gefälschte E-Mails (z. B. Absenderadressen, Auffälligkeiten, eingebettete Links)
- ☑ Sensibilisierung des Personals in Bezug auf angemessene Einsatzregeln, Richtlinien, Prozesse und Verhalten (u. a. welche Daten dürfen in welcher Form weitergegeben werden, was kann sicherheitskritisch sein)
- ☑ Sollte Homeoffice zur Verfügung gestellt werden, werden den Mitarbeitern die sichere Nutzung von Home Office Lösungen erläutert und spezifische Gefahren aufgezeigt

4 Authentifizierung

Digitale Zugangsbeschränkungen für Nutzer von IT-Systemen und Diensten werden durch geeignete Mittel beschränkt.

- ☑ Einweisung aller Mitarbeiter in den Umgang mit Authentifizierungsverfahren und -mechanismen
- ☑ Geregelter Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage (z. B. neuer Mitarbeiter), Änderung (z. B. Namenswechsel nach Heirat) und Löschung (z. B. Weggang Mitarbeiter)
- ☑ Vergabe von eindeutigen Kennungen für jeden Nutzer
- ☑ Es werden keine Gruppenkennungen angelegt
- ☑ Verwendung von starken Passwörtern und Veröffentlichung einer Richtlinie dafür – z. B.
    - bei Usern: mind. 10-stellig (inkl. festgelegter Passwortkomplexität)
    - bei Administratoren: mind. 12-stellig (inkl. festgelegter Passwortkomplexität)
    - festgelegt in SOP 11 - Zugriffsberechtigungen

- ☑ Automatische Umsetzung der Passwortrichtlinie für starke Passwörter in den Systemen mit Nutzerkennungen
- ☑ Verhinderung der Auswahl schwacher Passwörter bei Anwendungen (über Richtlinien und technisch erzwungen über das Identity Management System)
- ☑ Passwörter werden nach einem Sicherheitsvorfall, auch im Verdacht, gesperrt und müssen vom Nutzer neu vergeben werden
- ☑ Bei erstmaligem Login eines neuen Nutzers oder Zurücksetzung des Passworts durch IT (z. B. bei Vergessen des Passworts) muss eine Passwortänderung durch den Nutzer erfolgen
- ☑ Passwörter dürfen nicht weitergegeben werden (auch nicht an Kollegen, Vorgesetze oder die IT-Abteilung)
- ☑ Unterrichtung der Beschäftigten, dass Passwörter nicht auf Zettel oder Pinnwänden aufgezeichnet werden dürfen
- ☑ Keine Speicherung von Passwörtern im Browser
- ☑ Keine Passwörter per E-Mail übermitteln (2-Wege-Versand von Userdaten – E-Mail UND SMS/Telefon)
- ☑ Für lokale Admin-Konten besonders starke Passwörter (z. B. mind. 12-stellig, komplex und ohne übliche Wortbestandteile sowie unterschiedlich für jeden PC)
- ☑ Soweit möglich konsequenter Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung für Administratorkonten bei Anwendungen
- ☑ Zwei-Faktor-Authentifizierung durch biometrische Merkmale (z. B. Fingerprint) bei zentralen Systemen (z. B. Zugangssteuerung zu Sicherheitszone Datacenter)
- ☑ Automatische Sperrung von Zugängen bei zu vielen Fehlversuchen durch falsches Passwort: nach 3-maliger Falscheingabe wird das Konto gesperrt (Kontaktaufnahme mit IT notwendig)
- ☑ Zeitverzögerung zwischen einzelnen Login-Versuchen (insbesondere bei über das Internet erreichbaren Anwendungen) zur Erschwerung von automatischen Online-Angriffen
- ☑ Darstellung der Anzahl der fehlgeschlagenen Logins für einen Nutzer, der sich erfolgreich anmeldet.
- ☑ Passwörter werden ausschließlich im zentralen RemoteDesktopManager gespeichert
  - ☑ Standard-Authentifizierungsinformationen durch Hersteller bei Software werden nach der Installation geändert

5 Rollen-/Rechtekonzept

Nutzer können nur auf die personenbezogenen Daten zugreifen können, die für ihre Tätigkeit erforderlich sind. Durch Einführung von Benutzerrechten zu bestimmten Rollen (z. B. Buchhaltung, IT-Administration) werden unterschiedliche Rechte an konkrete Personen zugewiesen.

- ☑ Erstellen von Rollenprofilen für die Beschäftigten unter Einbeziehung der Einträge des Verzeichnisses der Verarbeitungstätigkeiten
- ☑ Über das Rollen-/Rechtekonzept werden Zugang zu Informationen und Gebäuden/Bereichen gezielt gesteuert und reglementiert
- ☑ Regelungen zur Verwaltung der Rollen (Zuweisung, Entzug)
- ☑ Regelmäßige Überprüfung (z. B. einmal pro Jahr), ob die Zuweisung der Rollen den Vorgaben entspricht sowie, ob die Rollen noch den Anforderungen der Geschäftstätigkeit entsprechen
- ☑ Keine Administratorkennungen für Nutzer, die keine administrativen Tätigkeiten ausführen
- ☑ Verschiedene administrative Rollen (z. B. Anlage neuer Benutzer, Durchführung von Backups, Konfiguration der Firewall) für die IT-Administration
- ☑ Die Nutzung von Superuser (z. B. root unter Linux) werden nicht verwendet

- ☑ Für Beschäftigte mit IT-Administrationsaufgaben sind zwei Benutzerkennungen eingerichtet: eine Administrationskennung und eine normale Nutzerkennung (für nicht-administrative Zwecke wie z. B. Zeiterfassung)
- ☑ Regelung, dass nicht unter Nutzung von Administratorenrechten im Internet gesurft oder E-Mails gelesen/versendet werden

6 Endgeräte (Clients)

Die für die tägliche Arbeit genutzten Endgeräte der Nutzer müssen dauerhaft abgesichert werden. Keine oder nur unzureichende Regelungen führen meist zu offenen Schwachstellen auf Clientsystemen, von denen dann eine erhebliche Gefährdung für die gesamte Organisation ausgehen kann.

- ☑ Eine Geräte-/Assetverwaltung (Wer setzt welche Geräte in welchem Bereich ein?) ist vorhanden
- ☑ Automatisches Sperren nach einer gewissen Zeitspanne der Inaktivität, falls manuelles Sperren bei Verlassen des Einflussbereichs nicht gewährleistet werden kann bzw. vergessen wurde
- ☑ Blickschutzfolien bei potenzieller unbefugter Einsichtnahme (z. B. im Empfangsbereich) bei Monitoren und Notebookbildschirmen
- ☑ Aktivierung einer Firewall, die unerwünschte Servicedienste auf dem Endgerät blockiert (z. B. bei Private- und Public-Anmeldungen)
- ☑ Verwendung einer Anti-Viren-Lösung bzw. eines Endpoint-Protection-Systems mit regelmäßigen, mindestens tagesaktuellen Signatur-Updates und Regelungen, wie im Falle einer Warnmeldung zu verfahren ist
- ☑ Zentrale Erfassung von Schadcode-Alarmmeldungen durch die IT-Administration
- ☑ Ablaufplan und Konzept der IT-Administration bei Schadcode-Befall
- ☑ Konzept zum Patch Management (u. a. Update-Plan mit Übersicht der eingesetzten Software)
- ☑ Regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Software wie Betriebssysteme, Office-Software und Fachanwendungen (z. B. durch E-Mail-Newsletter, Herstellerveröffentlichungen, Fachmedien, Sicherheitswarnungen)
- ☑ Automatisches Einspielen von Sicherheitsupdates des Betriebssystems, der installierten Software (z. B. PDF-Reader) oder von Softwarebibliotheken (z. B. Java), sofern möglich
- ☑ Personenbezogene Daten werden auf einem Speichermedium gespeichert, das von dem Backup erfasst wird
- ☑ Einbindung von externen Geräten werden durch technische Maßnahmen auf das erforderliche Mindestmaß begrenzt (z. B. bei USB-Sticks, Smartphones, externe Festplatten) und wird zusätzlich organisatorisch geschult
- ☑ Auto-Start von externen Medien (z. B. USB-Sticks) ist deaktiviert
- ☑ Fernwartung für Clients zu IT-Administrationszwecken werden ausschließlich über verschlüsselte Verbindungen nach Authentifizierung durch den Administrator und Freigabe durch den Nutzer durchgeführt
- ☑ Ausschließlicher Einsatz von Betriebssystemen und Software, für die noch Sicherheitsupdates zeitnah zur Verfügung gestellt werden
- ☑ Verhinderung der Ausführung von (aus dem Internet) heruntergeladener Software, deren Quellen als unsicher gekennzeichnet werden – Installation ausschließlich durch Administratoren
- ☑ Der Zugang zu Websites wird restriktiv verwaltet, sodass das Risiko einer Kompromittierung z. B. durch Malware verringert und der Zugriff auf nicht autorisierte Websites verhindert wird
- ☑ Verhinderung der automatischen Ausführung von Programmen aus dem temporären Download-Verzeichnis des Internetbrowsers

- ☑ Anwendungen sind an den Endgeräten ausschließlich mit User-Kennungen (ohne Administratorrechte) auszuführen
- ☑ Prozess zur wirksamen Datenlöschung vor Vergabe eines Endgeräts an einen anderen Mitarbeiter

7 Mobile Datenspeicher

Der Einsatz von USB-Datenträgern, Notebooks und Smartphones wird durch Regelungen zur Nutzung auch für den Verlustfall umgesetzt, um Unbefugten den Zugriff auf sensible Daten zu verwehren.

- ☑ Einsatz starker Verschlüsselung der mobilen Endgeräte (z. B. Festplattenverschlüsselung aller Clients)
- ☑ Einsatz von Backup- und Synchronisierungsmechanismen zur Verhinderung eines größeren Datenverlusts bei Verlust und Diebstahl
- ☑ Bei Smartphones: Zugang ausschließlich nach Authentifizierung (z. B. PIN, Passwort)
- ☑ Regelungen, dass bei Nutzung mobiler Arbeitsplätze (z. B. Notebook auf Dienstreise) ausschließlich per Remote (2-Faktor) auf Unternehmensdaten zugegriffen werden darf. Lokale Datenspeicherung auf dem Endgerät ist verboten.
- ☑ Diebstahlsicherungen (z. B. Anbringung von verschließbaren Stahlkabeln) werden für Notebooks bei Bedarf zur Verfügung gestellt
- ☑ Keine Privatnutzung bei Notebooks und Smartphones
- ☑ Die Mitarbeiter kennen die Regelungen bei Verlust eines mobilen Endgerätes, z. B. Verlustmeldung beim Unternehmen und/oder Polizei
- ☑ Bei mobilen Datenträgern: Es gibt die SOP 05 – Mobile Geräte zum sicheren Umgang mit mobilen Datenträgern. Die Mitarbeiter kennen diese Richtlinie und sind im Umgang mit mobilen Datenträgern geschult
- ☑ Bei mobilen Datenträgern: Sicheres Löschen der Datenträger vor und nach der Verwendung ist organisatorisch sichergestellt

8 Serversysteme

Serversysteme werden mit besonderer Sorgfalt abgesichert, da Sicherheitsverletzungen dort i. d. R. aufgrund der großen Menge personenbezogener Daten enorme Auswirkungen haben könnten.

- ☑ Nur kompetent geschulte Personen dürfen Administrationstätigkeiten auf den Servern durchführen
- ☑ Es werden verschiedene Administrationsrollen mit Rechten nach dem Least-Privileg-Prinzip für unterschiedliche Administrationsaufgaben (z. B. Softwareupdates, Konfiguration, Backup, Firewall) eingesetzt
- ☑ Geregelter Prozess zum zeitnahen Einspielen von Sicherheitsupdates der Server – kritische Updates werden unverzüglich eingespielt
- ☑ Soweit möglich, konsequenter Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung bei Anwendungen, die dies insbesondere für Administratoren unterstützen
- ☑ Deaktivierung/Deinstallation von Standard Server-Diensten, die nicht benötigt werden (z. B. Webserver, Printserver)
- ☑ Serverlokale Dienste werden über Firewall auf Servern vor Außenzugriff geblockt
- ☑ Weitere Härtungsmaßnahmen für das eingesetzte Serverbetriebssystem (z.B. Mimikatz)

9 Websites und Webanwendungen

Webseiten und Webanwendungen werden mit Best-Practice-Ansätzen abgesichert.

- ☑ Verwendung des HTTPS-Protokolls nach Stand der Technik (TLS1.2 bzw. TLS1.3)
- ☑ Absicherung von Datenbanken auf dem Webserver mittels Firewalls

- ☑ Fernzugang zu eigenen Webservern nur mit verschlüsselter Verbindung und Zwei-Faktor-Authentifizierung
- ☑ Nur geschulte bzw. kompetente Personen dürfen Administrationstätigkeiten auf den Servern durchführen
- ☑ Geregelter Prozess zur Information über Sicherheitsupdates und zeitnahes Einspielen derselben, insbesondere bei gängigen Content-Management-Systemen (CMS)

10 Netzwerk

Angriffe über das Internet auf das eigene Netzwerk wird aktiv durch Maßnahmen geschützt.

- ☑ Geeignete Netzwerksegmentierung: Restriktive (logische) Trennung sensitiver Netze von Verwaltungsnetzen (mittels Firewall-Systeme)
- ☑ Einsatz einer Firewall am zentralen Internetübergang
- ☑ Blockierung aller nicht benötigten Dienste (z. B. VoIP, Peer-to-Peer, Telnet)
- ☑ Einsatz geeigneter Firewall-Architekturen zur Absicherung rein interner Systeme (z. B. Arbeitsplatz, Drucker) zu den über das Internet erreichbaren Servern (z. B. Mail-Server, Web-Server, VPN-Endpunkt) - Konzept einer DMZ (Demilitarisierten Zone)
- ☑ Einsatz von Funkzugängen per WLAN nur auf aktuellen WLAN-Routern mit wirksamen Zugangsmechanismen (z. B. WPA-Enterprise 802.1x)
- ☑ Nutzung eines WLAN-Gastzugang ohne Zugangsmöglichkeit zum internen Netzwerk
- ☑ Geregelter Prozess zur ordnungsmäßigen Konfiguration der Firewalls und regelmäßige Überprüfung der selbigen (z. B. zu der Notwendigkeit von Freigaben)
- ☑ Protokollierungen auf Firewall-Ebene, um auch unbefugte Zugriffe zwischen den Netzen festzustellen und zu analysieren
- ☑ Einsatz von ausreichend qualifiziertem Personal zur Konfiguration der Firewall
- ☑ Prüfung eingehender E-Mails mittels Anti-Malwareschutz
- ☑ Blockieren von gefährlichen E-Mail-Anhängen (z. B. .exe, .doc, .cmd)
- ☑ Vermeiden von unverschlüsselten Protokollen (z. B. FTP, Telnet)
- ☑ Einsatz von Intrusion-Detection-Systemen (IDS) und Intrusion-Prevention-Systemen (IPS)
- ☑ Anbindung von Niederlassungen oder Homeoffice über stark verschlüsselte VPN-Verbindungen mit Client-Zertifikatsauthentifizierung bzw. Citrix (ausschließlich über 2-Faktor-Authentifizierung)

11 Archivierung

Archivdaten werden aufgrund gesetzlicher Aufbewahrungsfristen eine bestimmte Zeit lang weiterhin aufbewahrt. Eine Absicherung der enthaltenen personenbezogenen Daten ist daher auch gewährleistet.

- ☑ Es sind Regelungen etabliert, welche Daten auf welcher Rechtsgrundlage aufbewahrt werden müssen und wie lange die Aufbewahrungsfrist ist (Löschkonzept)
- ☑ Zugänge zu den Archivdateien sind festgelegt
- ☑ Archivdaten werden nach Ablauf der Aufbewahrungsfrist wirksam gelöscht
- ☑ Keine Archivierung auf Datenträgern, die für eine lange Speicherdauer ungeeignet sind (z. B. wiederbeschreibbare DVDs)
- ☑ Keine Aufbewahrung von Archivdaten in Produktivdatenbanken, sondern Überspielen von Archivdaten aus Produktivsystemen in die Archivsysteme
- ☑ Geeignete Datenformate für die Archivierung von Dokumenten wurden ausgewählt, damit eine langfristige Lesbarkeit der Daten gewährleistet ist

12 Wartung durch Dienstleister

Die Tätigkeiten von externen IT-Dienstleistern, insbesondere bei Wartung, werden überwacht und dokumentiert. Um eine ungewollte Datenweitergabe zu verhindern, werden personenbezogene Daten auf ausgemusterter Hardware sorgfältig gelöscht/vernichtet.

- ☑ Aufzeichnung aller Tätigkeiten von externen Dienstleistern
- ☑ Verschwiegenheitsverpflichtung im Dienstleistungsvertrag und zusätzlich die Geheinhaltungserklärung vom externen Mitarbeiter unterzeichnen lassen
- ☑ Es wird ein interner Mitarbeiter festgelegt, der die Tätigkeiten des externen Dienstleisters überwacht (bzw. ggf. begleitet)
- ☑ Regelungen zur wirksamen Datenlöschung auf Hardware (z. B. PCs, Drucker, Smartphones), die vom Dienstleister oder Hersteller zurückgenommen werden (z. B. bei Defekten, Abschreibung)
- ☑ Bei Einsatz von Fernwartungssoftware werden regelmäßig Sicherheitsupdates eingespielt und auf Informationen über bekannte Schwachstellen oder Fehlkonfigurationen geachtet
- ☑ Fernwartung externer Dienstleister werden protokolliert und der Zugang nur auf das zu wartende System begrenzt – ein Mitarbeiter verfolgt aktiv am Bildschirm des gewarteten Systems die Tätigkeiten

13 Protokollierung

Mittels geeigneter Protokollierungen können Sicherheitsverletzungen nach Art. 33 DS-GVO auch im Nachhinein erkannt und aufgearbeitet werden. Ohne Auflistung von Benutzeraktivitäten kann dagegen meist keine valide Bewertung stattfinden, ob und in welchem Umfang ein unbefugter Datenzugriff erfolgte.

- ☑ Konzept zur Protokollierung von Benutzeraktivitäten, technischen Systemereignissen, Fehlerzuständen und Internetaktivitäten unter Berücksichtigung datenschutzrechtlicher An-forderungen (u. a. auch Beschäftigtendatenschutz)
- ☑ Die Uhren der verwendeten Informationsverarbeitungssysteme (PCs, Notebooks, etc.) sind mit geeigneten Zeitquellen synchronisiert, damit eine gezielte Analyse bei Sicherheitsereignissen möglich ist
- ☑ Einhaltung der Zweckbindung der Log-Dateien ist sichergestellt: Die Personalvertretung und der DSB sind hier eingebunden

14 Business Continuity

Die Verfügbarkeit der Geschäftsprozesse und der damit verbundenen IT-Systeme und Daten ist gewährleistet. Im Rahmen des Backup-Konzepts ist ein geordnetes Zusammenspiel beim Wiedereinspielen gespeicherter Datenbestände vorgesehen, um im Notfall weiter betriebsfähig zu bleiben.

- ☑ Notfallplan Business Continuity: Regelungen, welche Systeme in welcher Reihenfolge wieder instandgesetzt werden, welche (externen) Personen/Dienstleister im Notfall zu Rate gezogen werden können sowie welche Meldeverpflichtungen es gibt
- ☑ Der Notfallplan wird regelmäßig überprüft
- ☑ Schriftlich fixiertes Backup-Konzepts
- ☑ Die Backups werden auf einen hochverfügbaren, vor unbefugter Manipulation durch Dritte (z.B. durch Ransomware) geschützten und verschlüsselten Backupspeicher geschrieben und über zwei Rechenzentren mit einer Distanz von mindestens 150 km synchron gehalten
- ☑ Geeignete physische Aufbewahrung von Backupmedien (z. B. Tresor, unterschiedliche Brandabschnitte, …)
- ☑ Regelmäßige Überprüfung, ob mindestens ein Backup werktäglich durchgeführt wird
- ☑ Regelmäßige Tests, ob alle relevanten Daten im Backup-Prozess enthalten sind und die Wiederherstellung funktioniert
- ☑ Mindestens ein Backup-System ist durch Schadcode nicht verschlüsselbar

- ☑ Makros in Office-Dokumenten im Betriebsalltag werden zum Schutz vor Ransomware unterbunden
- ☑ Verhinderung einer automatischen Ausführung von heruntergeladenen Programmen (z. B. Software Restriction Policy)
- ☑ Deaktivierung von Windows Script Hosts (WSH) auf Clients (sofern nicht zwingend benötigt)
- ☑ Notfallplan beinhaltet den Umgang mit Verschlüsselungstrojanern – dieser liegt auch in Papierform vor

15 Kryptographie

Mittels kryptographischen Verfahren nach Stand der Technik wird die Vertraulichkeit, Integrität und Authentizität von Daten, Systemen und Entitäten sichergestellt.

- ☑ Regeln für die effektive Nutzung der Kryptographie, einschließlich der Schlüsselverwaltung, sind definiert
- ☑ Mit Hash-Verfahren wird die Integrität von Daten, Software und IT-Systemen erreicht
- ☑ Passwortspeicherung nur dann mit „normalen“ Hashfunktionen (z. B. SHA-Klasse), wenn Passwort mind. 12-stellig ist und die Komplexität gem. Vorgaben erfüllt sind
- ☑ Symmetrische Verschlüsselung nach Stand der Technik
- ☑ Asymmetrische Verschlüsselung nach Stand der Technik mit z. B. RSA-2048 Bit (oder höher)
- ☑ Wirksame Schlüsselverwaltung (Generierung, Ausgabe, Sperrung) bei Einsatz kryptographischer Verfahren
- ☑ Schutz von geheimen Schlüsseln durch starke Passwörter mit mindestens 12 Stellen
- ☑ SSL-Zertifikate werden ausschließlich bei vertrauenswürdigen Zertifizierungsstellen beschafft
- ☑ Einsatz von HTTPS nach Stand der Technik (z. B. mind. 2048-Bit RSA, Perfect Forward Secrecy, HSTS)
- ☑ Es werden keine kryptographischen Verfahren mit bekannten Schwachstellen oder zu kurzer Schlüssellänge verwendet. Falls Altsysteme diese doch noch erfordern, ist eine individuelle Risikoanalyse durchzuführen

16 Datentransfer

Sowohl der Datenaustausch mit anderen Stellen über elektronische Kommunikationsnetze als auch der physikalische Transport von mobilen Datenträgern und Dokumenten wird derart abgesichert, dass die Vertraulichkeit und Integrität der personenbezogenen Daten nicht beeinträchtigt wird.

- ☑ Regelungen für alle Arten von Datentransfers sowohl innerhalb der Organisation als auch zwischen der Organisation und anderen Parteien bestehen
- ☑ Verschlüsselung von mobilen Datenträgern (wie DVD, USB-Sticks, Festplatte) nach Stand der Technik
- ☑ Bei E-Mail: Transportverschlüsselung von personenbezogenen Daten nach Stand der Technik bei normalem Risiko
- ☑ Bei E-Mail: Transportverschlüsselung und Inhaltsverschlüsselung von personenbezogenen Daten nach Stand der Technik bei hohem Risiko
- ☑ Sicherstellung der Integrität von personenbezogenen Daten durch digitale Signaturen zumindest bei hohem Risiko
- ☑ Verschlüsselte Nutzung von DNS-Diensten (DNSSec, DNS-over-TLS)

17 Entwicklung und Auswahl von Software

Datenschutz und Sicherheit werden frühzeitig bei der Entwicklung von eigenen Softwaresystemen bzw. bei der Auswahl von Softwareprodukten im eigenen Betrieb berücksichtigt.

- ☑ Alle betroffenen Mitarbeiter sind darüber geschult, dass Security-by-Design (Sicherstellung der Vertraulichkeit, Verfügbarkeit und Integrität) als Teilmenge von Data-Protection-By-Design eine gesetzliche Datenschutzanforderung ist und Einfluss auf zentrale Designentscheidungen (Produktauswahl, zentral vs. dezentral, Pseudonymisierung, Verschlüsselung, Land eines Dienstleisters) hat
- ☑ Es findet eine Trennung von Produktivsystem zu Entwicklungs-/Testsystem statt
- ☑ Der Zugang zum Source-Code bei der Entwicklung von Software ist beschränkt
- ☑ Es werden keine personenbezogenen Daten oder Zugangsdaten in der Source-Code-Verwaltung abgelegt
- ☑ System- und Sicherheitstests, wie z. B. Code-Scan werden durchgeführt
- ☑ Ausreichende Testzyklen werden berücksichtigt
- ☑ Fortlaufende Inventarisierung der Versionen von Software oder Komponenten (z. B. Frameworks, Bibliotheken) sowie deren Abhängigkeiten
- ☑ Standardsoftware und entsprechende Updates werden nur aus vertrauenswürdigen Quellen bezogen
- ☑ Sicherstellung, dass ein fortlaufender Plan zur Überwachung, Bewertung und Anwendung von Updates oder Konfigurationsänderungen für die gesamte Lebenszeit einer Softwareanwendung besteht

18 Auftragsverarbeiter / Unterauftragnehmer

Dienstleister, die personenbezogene Daten im Rahmen einer Auftragsverarbeitung behandeln, benötigen geeignete Garantien, damit auch die Sicherheit der Verarbeitung gewährleistet werden kann.

- ☑ Es werden nur Dienstleister (hier Unterauftragnehmer) verwendet, die
  - die Garantien (in Form von Dokumenten) zur Verfügung stellen können
  - Sicherheitsmaßnahmen implementiert haben, die nach Art. 32 DS-GVO als Bestandteil eines AV-Vertrags zur Dienstleistung passen
  - Die Wirksamkeit der Garantien durch geeignete Zertifizierungen (ansatzweise) nachweisen können oder ein ISMS implementiert haben und dies auch nachweislich umsetzt – Bsp.: ISO 27001 bei Rechenzentrum mit Scope Physikalische Sicherheit ist meist aussagekräftig
- ☑ Vor-Ort-Kontrolle durch den Verantwortlichen wird nicht ausgeschlossen
- ☑ Der Auftragsverarbeiter darf keine weiteren Subdienstleister ohne Information des Auftraggebers aufnehmen – dieser hat dann ein Widerspruchsrecht
- ☑ Jeder Auftragsverarbeiter muss Prozesse bei der Erkennung von Datenschutzverletzungen haben und diese unverzüglich dem jeweiligen Verantwortlichen im Sinne der DS-GVO melden
- ☑ Transfers in unsichere Drittländer sind nur mit weiteren technischen Schutzmaßnahmen, primär dem Einsatz von kryptographischen Verfahren erlaubt. Eine Zustimmung des Verantwortlichen muss erfolgen.
- ☑ Daten werden bei Auftragsverarbeitung (spätestens) nach Vertragsende wirksam gelöscht
- ☑ Regelmäßige Überprüfung des Auftragsverarbeiters bezüglich Sicherheitspraktiken und Dienstleistungserbringung