TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN DER ARUNA GMBH

Anlage I zum Auftragsverarbeitungsvertrag

Stand: 16.05.2018

1. VERTRAULICHKEIT

1.1 Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte

- Klingelanlage an Haustüren der Büro-Standorte
- Eingang zu den Büroräumen ist immer geschlossen
- Kontrollierter Einlass von Gästen durch Klingelanlage
- Ladenbüros können direkt über den Gehweg betreten werden
    - zusätzlich Rollläden
    - keine von außen bedienbaren Türklinken
- Schlüsselrechtekonzept für Gebäude und Räume
- besonders schützenswerte Komponenten sind separat geschützt/verschlossen
    - Serverräume und -schränke
    - Tresore

1.2 Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

Windows-Server

- Verschlüsselung von internen Datenträgern auf Blockebene
- TPM

Gehostete Server

- Verschlüsselung von internen Datenträgern auf Blockebene
- Copy-on-Write Dateisystem

Clients

- Verschlüsselung von internen Datenträgern auf Blockebene

Backup- und Fileserver

Verschlüsselung auf Datei- / Containerebene

1.3 Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

Windows Server und Clients

- Domäneninfrastruktur mit zentraler Benutzer- und Gruppenverwaltung (Active Directory)
- Passwortkonzept (Konventionen und Komplexität)

- Automatische Bildschirmsperre beim kurzzeitigen Verlassen des Arbeitsplatzes

Andere Systeme

- Datenverarbeitungssysteme, die nicht in die Domäne integriert werden (z.B. Drucker, managed Switches, Root-Server) sind mit „Benutzername und Passwort" bzw. Zertifikaten abgesichert
- Einsatz von zwei unabhängigen Virenscannern
- Auf dem Mailserver
- Auf den Windows-Server und Client Systemen
- Einsatz von Spamfiltern
- Konsequente Verschlüsselung der Client- und Serverfestplatten (s.Datenträgerkontrolle)

1.4 Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

- „Rogue Detection": Erkennung von Endgeräten, die nicht Teil der Domäne sind
- Verschlüsselung des WLAN mit WPA-2 PSK
- Untergliederung des Domänennetzwerks in Subnetze mit Firewallregeln, die den Verkehr der Subnetze einschränken
- Einsatz einer DMZ
- Einsatz eines restriktiv konfigurierten Subnetzes inkl. VLan für die Nutzung von Seminarteilnehmern

1.5 Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben

- Grundlegendes Berechtigungskonzept ist das „Active Directory" innerhalb der Domäneninfrastruktur
    - Ordner- und Dateifreigaben
    - Steuerung von Lese- und Schreibzugriffen
    - Steuerung von Anwendungszugriffen (Terminalserver, internes Postsystem)
    - lediglich Mitarbeiter der IT-Abteilung besitzen Administratorberechtigung
- Einsatz von Aktenvernichtern bzw. Dienstleistern zur Dokumentenvernichtung
- sicheres Löschen wiederbeschreibbarer Datenträger (einfaches Überschreiben mit 0-Bytes auf Blockebene) bzw. deren datenschutzkonforme Vernichtung
- Sichere Aufbewahrung von Datenträgern (Safe) auf denen pbD gespeichert sind
- Konsequente Verschlüsselung aller Datenträger (auf Datei- oder Blockebene)

1.6 Trennbarkeit

Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

- Physische Trennung soweit möglich
- Sonst Logische Trennung
- Testsysteme enthalten lediglich Testdaten ohne Personenbezug

2. INTEGRITÄT

2.1 Datenintegrität

Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

Web- und E-Mailserver (Im Rechenzentrum)

- Einsatz von Prüfsummen auf Ebene des Dateisystems zur Erkennung von Datenfehlern
- RAID zur automatischen Korrektur von Datenfehlern
- Verwendung von ECC-RAM
- regelmäßige Backups auf File- und Backupserver
- Verwendung von USVs und redundanten Netzteilen

File- und Backupserver

- planmäßig automatisierte Durchführung von Konsistenzprüfungen des Dateisystems
- Vorhaltezeiten für Snapshots („Backup vom Backup") von mindestens dem doppelten Intervall zur Konsistenzprüfung
- Verwendung von USVs und redundanten Netzteilen
- regelmäßige automatisierte Backups auf File- und Backupserver
- RAID (vergleichbar Level 6)

Windowsserver

- Virtualisierung der produktiven Windowsserver-Betriebsumgebungen mit Snapshotfunktion
- Verwendung von ECC-RAM
- Verwendung von USVs und redundanten Netzteilen

Clients

- regelmäßige automatisierte Backups auf File- und Backupserver

2.2 Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

- Führung einer Inventarliste für Clients
- Datenübertragungen von E-Mailsystemen werden protokolliert
- Datenträger werden an einem bestimmten Ort verwahrt
- Externe Zugriffe zum Zwecke der Wartung werden durch ein VPN mit benutzerspezifischen Zertifikaten realisiert

- nicht mehr benötigte (defekte, veraltete, etc.) Datenträger, werden überschrieben oder mechanisch zerstört

2.3 Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind

- Einschränkung des Zugriffs auf bestimmte Datensätze im CRM
- Protokollierung von Änderungen und Löschung im CRM
- Vergabe von Lese- und Schreibrechten auf Dateiebene und per Netzwerkfreigabe (Berechtigungskonzept)

2.4 Transportkontrolle

Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden

- konsequente Verschlüsselung von Datenträgern
- Einsatz von verschlüsselten Verbindungen bei externen Datenübertragungen
- Zur Übermittlung von E-Mailanhängen setzen wir im elektronischen Postfach nach Einrichtung geschützte/verschlüsselte Zip-Dateien sowie PGP/GPG und S/Mime ein
- Wartungs-Zugriffe und Vernetzung der Büro-Standorte über zertifikatsbasierte VPN-Zugänge

3. VERFÜGBARKEIT

3.1 Verfügbarkeitskontrolle

Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind

Zu schützende Systeme

- Webserver, Mailserver (Standort: Rechenzentrum)
- Clients, File- und Backupserver, Windowsserver (Standort: Büroräume)

Webserver

- alle Daten liegen in einem zu RAID-6 vergleichbaren Level (Ausfall von 2 Festplatten gleichzeitig möglich ohne Datenverlust)
- verschlüsselte Partitionen für personenbezogene Daten
- verschlüsselter Auslagerungsspeicher (Swap)

Mailserver

- alle Daten liegen in einem zu RAID-1 vergleichbaren Level (Spiegelung)
- verschlüsselte Partitionen für personenbezogene Daten
- verschlüsselter Auslagerungsspeicher (Swap)

Clients

- Datensicherheit durch Verschlüsselung auf Blockebene

Backup- und Fileserverserver

- alle Daten liegen in einem zu RAID-6 vergleichbaren Level (Ausfall von 2 Festplatten gleichzeitig möglich ohne Datenverlust)
- Verschlüsselung auf Datei- / Containerebene

Windowsserver

- Datensicherheit durch RAID (Level 1, 5 und 6) mit Hot-Spare-Festplatte
- Laufwerksverschlüsselung auf Blockebene (mit TPM)

Sonstige Maßnahmen

- Betriebssysteme auf den Windows-Clients und Windows-Servern werden über den WSUS automatisiert aktualisiert und dokumentiert
- Linux und FreeBSD und die darauf laufenden Anwendungen werden nach Bedarf manuell aktualisiert
- Virenscanner kommen in zwei Bereichen zum Einsatz. Direkt auf dem E-Mail-Server und auf Dateiebene der Clients und Domainserver. Es handelt sich um zwei unterschiedliche Antivirenhersteller
- Einsatz von Firewalls
- Einsatz von USVs in den Serverräumern

- Klimatisierte Serverräume

4. BELASTBARKEIT DER SYSTEME

4.1 Zuverlässigkeit

Belastbarkeit bedeutet im engeren Sinne, wie die IT-Systeme vor internen und externen Einflüssen abgesichert ist und im weiteren Sinne die Widerstandsfähigkeit der IT im Fehlerfall, bei Störungen, bei hoher Beanspruchung. Zuverlässigkeit ist die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

- um neue Konfigurationen und Anwendungen auf ihre Funktion und den verbundenen Ressourcen zur testen, kommen virtualisierte Testumgebungen zum Einsatz
- Wartungen, bei denen mit Ausfallzeiten zu rechnen ist, werden außerhalb der Geschäftszeiten durchgeführt
- Backups, bei denen größere Datenmengen über das Intranet bzw. zwischen den einzelnen Standorten über das Internet laufen, werden über Nacht, also außerhalb der Geschäftszeiten ausgeführt
- zentrale Verwaltung der Antivirensoftware auf Windows-Clients und -servern (mehrfache Aktualisierung der Signaturdatenbank, zentrales Monitoring/Reporting)
- Firewall (im Router) an jedem Standort (IDS, DoS, IP-Filter; Standardregel: Paket verwerfen)
- klimatisierte Serverräume

5. VERFAHREN ZUR WIEDERHERSTELLUNG DER VERFÜGBARKEIT PERSONENBEZOGENER DATEN NACH EINEM PHYSISCHEN ODER TECHNISCHEN ZWISCHENFALL

5.1 Wiederherstellbarkeit

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können

Webserver

- tägliches, verschlüsseltes Datenbankbackup auf Backup- und Fileserver in den Büroräumen
- manuelles Anfertigen von Dateisystem-Snapshots vor Systemeingriffen

Mailserver

- manuelles Anfertigen von Dateisystem-Snapshots vor Systemeingriffen
- Mailserveranwendung fertigt automatisiert ein rotierendes Backup an:
- wöchentlich vollständiges Backup
- täglich differentielles Backup
- wöchentlich manueller Transfer der Backupdateien auf Backup- und Fileserver in den Büroräumen

Clients

- Windows 7
  - monatlich vollständiges Backup
  - wöchentlich inkrementelles Backup
- Windows 8
  - monatlich vollständiges Backup
  - wöchentlich inkrementelles Backup
  - verschlüsselter Dateiversionsverlauf auf Backup- und Fileserver
- MacOS
  - Verschlüsseltes Time Machine-Backup

File- und Backupserver

- Mehrere File- und Backupserver, die untereinander derart automatisiert Backups anfertigen, dass je ein Backup vom Datenbestand eines jeden File- und Backupservers besteht

Windowsserver

- automatisiertes, tägliches und rotierendes vollständiges Backup der virtuellen Maschinen

Sonstige Maßnahmen

- Einsatz von Virtualisierungenstechnologien
- Vorhalten von Ersatzteilen
- IT-Dienstleister auf Abruf
- Business-Notfallhotline der Telekom bei Störungen oder Ausfällen der Telefonanlage

6. VERFAHREN REGELMÄßIGER ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER WIRKSAMKEIT DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

6.1 Überprüfung

- automatisierte Berichte über:
  - erfolgte und fehlgeschlagene Backups
  - Zusammenfassungen der Patchlevel (WSUS)
  - monatliche Berichte über Festplattenstatus der Fileserver
  - verfügbare Updates des Webserver

6.2 Auftragskontrolle

Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können

- eindeutige Vertragsgestaltung gemäß individueller Leistungsvereinbarung
- formalisierte Auftragserteilung durch schriftliche und unterzeichnete Auftragsverarbeitungsvereinbarung
- Möglichkeit der Durchführung von Kontrollen durch den Auftraggeber zur Vertragsausführung
- Führung eines Verzeichnisses aller Auftragnehmer
- Verpflichtungen der Mitarbeiter/innen des Auftragnehmers auf das Datengeheimnis bzw. zur Vertraulichkeit
- Durchführung von regelmäßigen Unterweisungen zum Datenschutz
- schriftliche Bestellung eines externen Datenschutzbeauftragten

7. SCHRIFTLICHE DOKUMENTATION VON SONSTIGEN MAßNAHMEN

- Verfahrensverzeichnis
- Schlüsselmanagement
- IT-Richtlinie (Administratorhandbuch)
- Nachweise Schulung der Mitarbeiter
- AVVs
- Strukturanalyse
- Grundrisse
- Netzwerkplan
- Beauftragung einer externen Brandschutzfirma