Technische und organisatorische Maßnahmen (TOM)

Ziel dieses Dokumentes

Das vorliegend Dokument beschreibt die technischen und organisatorischen Maßnahmen (TOM) nach Artikel 32 DSGVO der Mensch und Maschine Deutschland GmbH.

Die Zutrittskontrollen sind individuell für die diversen Standorte anzugeben.

Zutrittskontrolle:

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

- Perimeterschutz (Zäune, Mauern, Schranken, Tor etc.).
  Für folgende Standorte: Weßling, Düren, Kirchheim, Hamburg, Oldenburg, Hannover, Wiesbaden, Saarbrücken, Stuttgart

- Zugänge zu den Geschäftsräumen erfolgt über mechanisch Schlüssel für alle Standorte. Zusätzlich werden die folgenden durch ein elektronisches Zutrittskontrollsystem geschützt: Weßling, Wiesbaden und Düren
  - Als Schlüssel Schlüsselkarten / codierte Schlüsselchips genutzt.
  - Öffnungs- und Schließereignisse werden für 6 Monate gespeichert. (Zutrittsprotokollierung i.d.R. nur bei elektronischer Zutrittskontrolle)
- Schlüsselvergabe
  - Die Ausgabe von Schlüsseln wird im dokumentiert und quittiert.
  - Schlüssel werden ausschließlich an festangestellte Mitarbeiter ausgegeben, die regelmäßig am Standort tätig sind.
- Besucherkontrolle
  - Empfangsbereich vorhanden
  - Besucher dürfen sich nur in ständiger Begleitung eines Mitarbeiters in den Geschäftsräumen aufhalten.
  - Besucher müssen sich am Empfang anmelden und einen konkreten Ansprechpartner (Mitarbeiter des Unternehmens) nennen. Der genannte Ansprechpartner wird vom Empfang angerufen und muss den Besuchstermin und den Besucher bestätigen. Der Besucher wird im Anschluss von seinem Ansprechpartner am Empfang abgeholt und nach Abschluss des Termins wieder aus den Geschäftsräumen begleitet.
  - An den folgenden Standorten erhalten die Besucher zusätzlich Besucherausweise: Weßling, Friedrichshafen, Düren und Stuttgart
- Eine Einbruchsmeldeanlage mit Aufschaltung auf den zuständigen Wachdienst ist vorhanden. An den folgenden Standorten: Weßling, Wiesbaden und Saarbrücken.
- IT-Räume und technische Versorgungsräume sind entsprechend einer verbindlichen Schließregelung stets verschlossen zu halten.

- Die lokal vorhandenen Netzwerkverteilsysteme (insbesondere Switches) sind sowohl in verschlossenen Räumen als auch in abgesperrten Server-Racks platziert. Zutritt haben ausschließlich das IT-Personal und im Notfall Wachdienst und Feuerwehr.
- Der Zutritt zu den im Rechenzentrum (ISO-27001 zertifiziertes ISMS) erfolgt mit einem separaten Zylinder-Schlüsselsystem (nur zugänglich für IT). Zutritt haben ausschließlich das IT-Personal.

Zugangskontrolle:

Technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung:

- differenziertes Berechtigungskonzept für Systeme, Anwendungen und Daten für normale und privilegierte Nutzer
- Alle Benutzerkonten werden zentral im Active Directory angelegt und verwaltet.
- Single-Sign-On-Verfahren
- Es werden ausschließlich personalisierte Benutzerkennungen verwendet. Es gibt keine Gruppen Accounts.
- Sichere Passwörter werden vom System technisch erzwungen.
    - Passwörter müssen mindestens 12 Zeichen umfassen.
    - Passwort muss Zeichen aus mindestens 3 der 4 folgenden Zeichenkategorien enthalten:
        - Kleinbuchstaben
        - Großbuchstaben
        - Sonderzeichen
        - Zahlen
    - Für den Zugriff auf sämtliche O365 Anwendung, unabhängig ob per lokaler App oder Webapp, ist eine 2 Faktor Authentifizierung notwendig. Diese findet per SMS an das vom Arbeitgeber bereitgestellten Mobiltelefon statt
    - Zugangssperre nach 3 fehlgeschlagenen Anmeldeversuchen
    - Die letzten 5 Passwörter können nicht mehr verwendet werden.
    - Initial-Passwörter und zurückgesetzte Passwörter müssen in gleicher Weise geschützt werden und sind zusätzlich vom Nutzer unverzüglich zu ändern.
    - Passwörter dürfen nur in verschlüsselter Form gespeichert werden. Es darf dafür nur eine freigegebene Software (Passwort-Manager, z.B. Keepass) eingesetzt werden.
- Beim Verlassen des Arbeitsplatzes muss der Sperrbildschirm aktiviert werden.
- Pausenschaltung nach spätestens 5 Minuten.
- Die Zahl der Administratoren ist auf das absolut Notwendigste beschränkt.
- Netzwerksegmentierung mittels V-LANs
- IT-Anlagen werden mit Perimeter-Firewall geschützt.
- Intrusion Detection/Prevention System wird genutzt.
- Mitarbeiter verfügen über keine lokalen Admin-Konten.

- WLAN-Authentication mittels RADIUS
    - Protokollierung der Anmeldungen

Zugriffskontrolle:

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

- Berechtigungen werden auf Grundlage eines Rollenkonzepts nach dem „Need-to-Know"-Prinzip, bzw. „Least Priviledge"-Prinzip vergeben.
- Vergabe, Entzug und Änderungen von Berechtigungen (Onboarding-, Offboarding und Wechselprozesse) erfolgen nach einem dokumentierten Antrags- und Genehmigungsverfahren.
- Jeder Zugriff auf personenbezogene Daten wird, sofern technisch möglich, protokolliert.
- Malware-Schutz
    - Auf allen Mitarbeitergeräten ist Sophos Protection aktiv, welches Angriffe von innen und außen zentral reportet
    - Auf allen Servern kommen Sophos Protection zum Einsatz.
- Firewall-Konfiguration nach dem Prinzip „Default-Deny"
    - Es werden jeweils nur die zur Aufgabenerfüllung notwendigen Ports freigeschaltet.

Weitergabekontrolle:

Maßnahmen bei Transport, Übertragung, Übermittlung oder Speicherung auf Datenträger sowie bei der nachträglichen Überprüfung:

- Akten- und Datenträgervernichtung:
    - Vernichtung erfolgt durch einen spezialisierten Dienstleister.
    - Die internen Aktenvernichter entsprechen der Stufe P-4 gemäß DIN 66399-2.
    - Akten werden physisch zerstört
    - CDs und DVDs werden physisch zerstört
    - Funktionsfähige Festplatten werden sicher gelöscht
    - Defekte Festplatten werden mechanisch vernichtet
    - Akten und Datenträger werden bis zur Vernichtung in sicher verschlossenen Sammeltonnen aufbewahrt.
- Datenübermittlung
    - Vertrauliche und personenbezogene Daten werden via SSL, TLS (Version 1.2 oder höher) oder IPSEC-VPN sicher übertragen.
    - E-Mails werden in jedem Fall mindestens der Transportweg zwischen den Servern mittels TLS verschlüsselt.
- Der Fernzugriff von Remote-Arbeitsplätzen erfolgt via IPSEC-VPN.
- Umfangreiche Protokollierung
    - Drucker-Protokolle

    - Einzelverbindungsnachweise bei Telefonie
    - Firewall-Logs
- Die WLAN-Schnittstelle darf nur für die Dauer der Nutzung aktiv gehalten werden.
- Es gilt die Clean-Desk-Policy.

Eingabekontrolle:

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt worden sind:

- Es werden ausschließlich personalisierte Benutzerkennungen verwendet.
- Alle Benutzerkonten werden zentral im Active Directory angelegt und verwaltet.
- Zugänge für das CRM-System Salesforce werden in Salesforce verwaltet
- Jede Veränderung (inkl. Administrator-Tätigkeiten) von personenbezogenen Daten wird, sofern technisch möglich, protokolliert.

Auftragskontrolle:

Technische und organisatorische Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- Mit Auftraggebern und Auftragnehmern werden Verträge zur Auftragsdatenverarbeitung geschlossen.
    - Es werden alle vorgeschriebenen Kontrollrechte vereinbart.
    - Datenverarbeitung erfolgt ausschließlich nach Maßgabe des vereinbarten Vertrags zur Auftragsdatenverarbeitung und nach Weisung des Auftraggebers.
    - Unterauftragnehmer (sofern vorhanden) werden stets im gleichen Umfang vertraglich verpflichtet, wie der Auftragnehmer selbst.
    - ISMS des Rechenzentrumsbetreibers ist nach ISO27001 zertifiziert.
    - Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers unterliegen einer regelmäßigen Prüfung durch den Auftraggeber.
- Alle Mitarbeiter wurden auf das Datengeheimnis verpflichtet. Freie Mitarbeiter werden ebenfalls auf Vertraulichkeit und Datenschutz verpflichtet.
- Regelmäßige (mind. jährlich) Schulung der Mitarbeiter zu den Themen Datenschutz und Informationssicherheit.
- externer Datenschutzbeauftragter

Home-Office Regelungen:

- Es gelten die Home-Office Richtlinien.
- Es gilt die Clean-Desk-Policy.
- Der Home-Office Arbeitsbereich kann vom Auftraggeber vor Ort geprüft werden.

- Mobile Endgeräte wie z.B. Laptops, Smartphone und Tablets sowie Speichermedien dürfen außerhalb der Büroräume nie unbeaufsichtigt bleiben. Bei Verlust oder Diebstahl erfolgt eine unverzügliche Meldung an Vorgesetzten, um die Frist zur Meldung einer möglichen Datenschutzverletzung zu wahren und schnellstmögliche schadensbegrenzende Maßnahmen einzuleiten.
- Öffentliche WLAN-Netze und private Heimnetze werden als nicht vertrauenswürdig eingestuft und daher ist der Zugriff auf IT-Systeme außerhalb des Unternehmensnetzwerkes nur mittels verschlüsselter Verbindung zulässig.

Verfügbarkeitskontrolle:

Maßnahmen zur Datensicherung:

- Es darf nur Software installiert bzw. genutzt werden, die von der IT freigegeben wurde. Es darf nur die Softwareversion genutzt werden, welche von der IT bereitgestellt wird.
- Formalisiertes Freigabeverfahren für neue oder zu ändernde DV-Verfahren.
    - Ein Gremium (IT Architecture Board) bestehend aus COO, IT-Leiter, Business Solution Architekt und je einem Vertreter aus den operativen Einheiten.
- Separate Backup-Konzepte für unterschiedliche Bereiche
    - Komplettsystem:
        - Nächtliche Voll-Backups auf Festplatten. Speicherung der Datensicherungen in einem separaten Brandabschnitt
        - 12 Wochen Vorhaltezeit
    - Exchange und SharePoint:
        - Nächtliche Voll-Backups auf Festplatten
    - SQL-Datenbanken:
        - Stündliche Inkrementell-Backups und nächtliche Voll-Backups auf Festplatten
    - Geo-Redundanz
        - Office 365 Backups werden in verschiedenen Rechenzentren gesichert
- Redundante Datenhaltung im Rechenzentrum
- Unterbrechungsfreie Stromversorgung (USV)
- Die Klimaanlage und Klima Sensorik sind redundant ausgelegt
- Brandschutz
    - Brandmeldeanlage mit Brandfrüherkennungssystem und Aufschaltung auf eine Brandmeldezentrale
    - Brandhemmende Wände
    - Brandhemmende Tür (T90)
    - keine Brandlasten im Serverbereich

Trennungskontrolle:

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- Trennung von Test-, Entwicklungs- und Produktivsystemen
- Logische Mandantentrennung
- Separation of Duties

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Auswertung von Protokollen auf sicherheitsrelevante Ereignisse und Alarmierung bei potenziellen Hackerangriffen oder Verstößen gegen die Richtlinien
- Regelmäßige Penetrationstest
- Regelmäßige Durchführung von netzwerkbasierten Sicherheits-Scans

Richtlinien zur Informationssicherheit

Es liegt eine `Information Security Policy` vor

Die vorliegenden technisch und organisatorischen Maßnahmen (TOM) werden regelmäßig überprüft.