CyberWehr

RISK MANAGEMENT SOLUTIONS GMBH

Monika Wehr ▪ Alte Landstrasse 109 ▪ 8803 Rüschlikon ▪ Telefon +41 (0) 79 348 55 63

**IAM Identity and Access Management**

Zugangsdaten gehören zu den grossen Sicherheitsrisiken in Unternehmen. Ein ordentliches Identitäts- und Zugriffsmanagement reicht von der Zugangskontrolle zu Gebäuden, den Netzwerksystemen über Software-Applikationen bis hin zur Passwortverwaltung. Der Schutz der Informationen (Daten) vor unbefugtem Zugriff und Missbrauch ist durch technische und juristisch-organisatorische Massnahmen sicherzustellen. Die folgenden Bereiche sollen Ihnen einen Überblick ermöglichen; nicht alles ist für Ihr Unternehmen von Relevanz. Das entscheidet im Ergebnis die individuell auf Ihr Unternehmen abgestimmte Risikoanalyse und der «Risikoappetit» Ihrer Organisation.

Ist Datensicherheit gegeben zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich von Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der System und der IT-Infrastruktur? Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

## Allgemeine Informationen

***KONTROLLE – Dokumentieren Sie die Massnahmen?***

Liegen Richtlinien sowie **Arbeitsanweisungen vor,** in denen Verfahrens- und Vorgehensweisen beschrieben sind zur
- privaten **E-Mail- und Internetnutzung**
- der **Vernichtung von Papierdokumenten**
- Elektronische Speichermedien
- dem sorgfältigen Umgang mit Benutzerkonten sowie Passwörtern?

[Hier weitere allgemeinen Informationen beschreiben]

## Vertraulichkeit / Zutritts-, und Zugangskontrolle zum Gebäude gemäss Art. 32 Abs. 1 lit. b DSGVO:

- Transportkontrolle
- Übermittlungs- und Übertragungskontrolle
- Weitergabe Kontrolle (Logmechanismen bei elektrischem Datentransport)
- Zugangs- und Benutzerkontrolle (PC mit Passwortschutz)
- Zugriffskontrolle (Zugriff auf Daten nur gemäss Berechtigungskonzept)
- Zutrittskontrolle (verschlossene Türen), Speicher- und Datenträgerkontrolle etc.

## Auswahl geeigneter Zutrittskontrollverfahren

- Absicherung durch Zutrittskontrollsystem (nur mit entsprechenden Schlüsseln/Ausweisen)
- Ausweiskontrollen (Identifikation)
- Begrenzen der Zutrittsberechtigungen auf bestimmte Gebäudebereiche/Räume/Zeitfenster
- Ausweise mit Kodierung, fälschungssichere Ausweise
- Zutritt zum Gebäude z.B. Alarmanlagen, bauliche Maßnahmen wie die Sicherung von Fenstern und Türen oder einfach auch nur der Zaun um das Gelände
- Örtliche Zugangssicherheit erhöhen gegen Diebstahl durch: Schlüssel, Magnetkarte, Chipkarte, RFID-Badge, Kombinierte Verfahren
- Sabotageschutz auch auf IoT-Geräten

*[Hier ggfs. weitere Massnahmen beschreiben]*

## PHYSISCHE ZUGANGSKONTROLLE (Absicherung der Zugänge):

- Umzäunung des Betriebsgeländes, Mauer, Aufstellen von Hinweisschildern
- Wachpersonal/Pförtner
- keine Wegweiser/Beschilderung zu sensiblen Bereichen (Serverraum, ...)
- Einbruchhemmende Sicherheitstüren mit zusätzlichen Sicherungen (stabile Sicherheitsschlösser)
- Sicherheitsschränke für Rechner, verschließbare Racks
- Türen aller Gebäudezugänge  sollten die gleiche Widerstandsfähigkeit haben
- Kellerlichtschächte: Rollenrost oder Gitterrostsicherung (abschließbar)
- Abschließbare Fenstergriffe, vergitterte Fenster, durchbruchhemmende Verglasung
- Alarmanlage, Sicherheits-Kamera-Anlagen, Bewegungsmelder und weitere Sensoren
- Wandschutzschränke und Tresore mit elektronischem Schließsystem
- elektronische Schließanlage
- Server in Rechenzentren, Absicherung der Arbeitsstationen, IoT-Geräte sind überall verteilt

## PC – ZUGANGSKONTROLLE - Datenverarbeitungsanlagen

- Berechtigungskonzept
- Zugriffsprotokollierung
    - Passwort
    - Pin & Benutzername
    - Schlüssel
    - Magnetkarte
    - Chipkarte
    - RFID-Badge
    - Kombinierte Verfahren

## Identifikation und Authentisierung auf BIOS-, Betriebssystem- und Anwendungsebene

- Persönliche Zugangsdaten
- Mindestlänge des Passworts
- Komplexität des Passwortes
- regelmäßige Passwortwechsel
- Verschlüsselte Ablage des Speichers
- Verfremdung des Passworts

- Passworthistorie
- Single-Sign on
- Sperren des Benutzerkontos bei Falscheingabe
- Umfangreiche Protokollierung unabhängig von Anmeldevorgängen in maximal möglicher Detailtiefe
- Automatisierter Passwort Manager (Kee Pass/Dashlane u.a.)? dieselben PW überall?
- Wer benötigt direkten Zugang zum Internet? Desktop-Computer von Ingenieuren und Maschinenarbeitern, die industrielle Kontrollsysteme (ICS) verwenden, sicher nicht.
  Andere Nutzer benötigen beides, Zugang zum Internet und zum ICS-System

## Zugangskontrolle PC

- Hardwareschloss
- BIOS-Passwort / Boot-Passwort
- Verschlüsselte Festplatte, Verschlüsselungssoftware installiert
- System-Login
- Betriebssystemstart nur von Festplatte/internem Datenträger
- Automatisches Sperren des PC nach Untätigkeitsphase
- Timed Log-In

## Zugang zu Ressourcen für Mitarbeiter(gruppen) festlegen

- Arten: lesen, schreiben, umbenennen, löschen, ausführen, anlegen, protokollieren
- Geräte
- Laufwerke, z.B. Zugriff auf Diskettenlaufwerk nur durch Systemadministrator
- Partitionen, (z.B. direkte Zugriffs-, Schreib- und Leserechte auf Plattenbereiche nur für Systemadministrator)
- Dateien/Verzeichnisse
- Schnittstellen, Datenbanken - Zugangsrechte - Authentifizierung gesteuert? Absicherung von Webschnittstellen oder der Software zur Verwaltung. In großen Umgebungen kann es sinnvoll sein, die Authentifizierung an Verzeichnisdienste wie Active Directory zu übergeben bzw. erweiterte Funktionen, wie die Multifaktor-Authentifizierung (MFA) - MFA nutzt die Kombination von zwei oder mehr Berechtigungsnachweisen für die Prüfung der Identität -> Sicherheit von Anmeldeverfahren und Erschwerung des Identitätsdiebstahl

## ZUGANGSKONTROLLE – externe Personen (Kunden, Lieferanten, Dienstleister, Besucher)

Regelungen für zeitl. und in den Berechtigungen stark eingeschränkter Zugangstoken

- zeitl. und in den Berechtigungen stark eingeschränkter Zugangstoken
- Protokoll über Zutritt und Verlassen
- ständige Begleitung
- Zutritt zu sensiblen Bereichen nur wenn unumgänglich

## Reinigungs- und Wartungsarbeiten

- Einsatz nur von autorisiertem Wartungspersonal
- Authentifizierung des Wartungspersonals
- Verpflichtung auf Datengeheimnis
- Protokollierung der Wartungsarbeiten
- Auch: Festlegungen zu Heimarbeitsplätze

## Festlegung der Zutrittsrechte

- Schlüssel für begrenzten festgelegten Personenkreis
- Befristen der Ausweise, Sperrmöglichkeiten bei Verlust
- Sofortiges Löschen von Berechtigungen ausscheidender Mitarbeiter
- Festlegungen, z.B. für Verlust von Ausweis/Schlüssel, Zugang außerhalb der zugewiesenen Seiten
- Protokoll über Zutritt und Verlassen - Schutz der Integrität des Netzwerkes
- ständige Begleitung
- Zutritt zu sensiblen Bereichen, nur wenn unumgänglich
- Reinigungs- und Wartungsarbeiten
  Einsatz nur von autorisiertem Wartungspersonal
- Authentifizierung des Wartungspersonals
- Verpflichtung auf Datengeheimnis
- Protokollierung der Wartungsarbeiten
- Auch: Festlegungen zu Heimarbeitsplätze

## ZUGRIFFSKONTROLLE

Ist ein Rollenkonzeptes mit differenzierten Benutzerrechten (Auswertung, Verarbeitung) erarbeitet?

- Einrichtung für einzelne Benutzer/Benutzergruppen
  Rechtevergabe entsprechend dem Aufgabenbereich:
  - physischer und logischer Zugriff auf IKT Betriebsmittel und Anlagen ist nur für autorisierte Personen und Prozesse und nur für definierte Aktivitäten möglich
  - Definition von Berechtigungsstufen
  - Prozesse zur Verwaltung von Remote-Zugriffen, auch von Mobilegeräten?
- Beachtung von „besonderen" Accounts/Rollen (Wartung, Azubi,...)
- Keine Zugriffsrechte auf streng vertrauliche Daten
- Delegierung von Benutzerrechten; nicht jeder Benutzer braucht Zugriff auf alle Daten oder Funktionen eines IoT-Gerätes.
  Account nach Ausscheiden/Aufgabenerledigung löschen
- Besonderer Schutz für bestimmte Dateien, z.B. Systemdateien
- Sperren bestimmter DV-Operationen außerhalb festgelegter und kontrollierbarer Zeiten und bei unbefugten Zugriffsversuchen
  sind Bildschirme und damit möglicherweise auch vertrauliche Informationen geschützt in Pausenzeiten vor dem Einsehen durch Unbefugte?
- Aktuelle Rechtestruktur periodisch oder stichprobenweise überprüfen
- Überwachung von wachsenden Dateien, außergewöhnlicher Inanspruchnahme des Speicherplatzes oder von Zugriffen auf bestimmte Dateien
- Löschung nicht mehr benötigter bzw. unzulässig gespeicherter Daten bzw. Sperren aufbewahrungspflichtiger Daten gegen anderweitige Nutzung
- Protokollierung der Zugriffsversuche auf Anwendungen und Daten
- Dokumentation: Benutzerverzeichnis
- Klare Handlungsanweisungen und Verbote: durch private Datenträger (eine DVD) kann Schadsoftware in das Unternehmensnetz gelangen
- Anpassungen an die Konfiguration oder den Betrieb der IoT-Geräte durch unberechtigte Personen ausschliessen?
- Absicherung des Internetzugriffs
  - Filterung durch Firewall
  - Sperrliste für unerwünschte URLs
  - Sperrung unerwünschter Inhalte (per Proxy)

## Fernwartung durch externen Dienstleister

- Verschlüsselter Verbindungsaufbau (VPN), nur durch Auftraggeber regelbar (Abschalten der Zugänge und Berechtigung außerhalb der definierten Wartungszeit)
- Identifizierung des Wartungstechnikers als Berechtigter
- Sicherstellen, dass Wartungsunternehmen nicht - oder nur kontrolliert - auf personenbezogene Daten zugreifen können

*[Hier ggfs. weitere Massnahmen beschreiben]*

## WIEDERHERSTELLBARKEIT

**Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können**

- Redundante Systeme
- Backup
- Raid/ Spiegelung des Rechenzentrums, zwei separate Standorte
- System-Cluster
- Testen von Failover-Szenarien
- Testung der Backup Rückspielung

## Fernwartung durch externen Dienstleister

- Verschlüsselter Verbindungsaufbau (VPN), nur durch Auftraggeber regelbar (Abschalten der Zugänge und Berechtigung außerhalb der definierten Wartungszeit)
- Identifizierung des Wartungstechnikers als Berechtigter
- Sicherstellen, dass Wartungsunternehmen nicht - oder nur kontrolliert - auf personenbezogene Daten zugreifen können

## DATENTRÄGERKONTROLLE

- Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern
- (Datenträgerkontrolle), Zum Beispiel: Verschlüsselung der Datenträger,
- Zentrale Smartphone Administration
- Schutzvorrichtung für Hardware-Schnittstellen

## SPEICHERKONTROLLE

Verhinderung der unbefugten Eingabe sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten pbD - Beispiele für die Umsetzung beim Verantwortlichen/Auftragnehmer:

Datenträger und Datensicherungsbänder

- Verschlüsselungstechnik einsetzen
- Aufbewahrungsregeln und -fristen festlegen
- Zentrale Lagerung (verschlossener Sicherungsschrank, geregelte Schlüsselvergabe, besser dedizierter Verantwortlicher)
- Dokumentation: Bestandsverzeichnis und regelmäßige Datenträgerbestandskontrollen
- Kennzeichnung / Unterscheidung, keine Rückschlüsse auf Inhalt

- Kontrollierte Entsorgung: Löschen von Datenträgern (Disketten, Festplatten, …) durch Systemadministrator, Vernichtung durch zertifizierte Fachfirma
- Datensicherung: Sensitive Datenbestände auch im Backup verschlüsseln

## BENUTZERKONTROLLE

Beispiele für die Umsetzung beim Verantwortlichen/Auftragnehmer:

- Netzwerkzugriffskontrolle: Server in speziellen Rechenzentren, Absicherung der Arbeitsstationen, IoT-Geräte sind aber überall verteilt
- Benutzerzugriffsregelungen nach dem Need-to-Know-Prinzip
- Automatische Aktivierung eines Bildschirmschoners bei Inaktivität verbunden mit einer Passworteingabe zur erneuten Aktivierung des Rechners

## TRANSPORTKONTROLLE

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

- Verschlüsselung der Datenträger; getrennte Schlüsselübertragung
- Sichere (versiegelte) Transportbehälter
- Zuverlässigkeit des Transporteurs
- Verwendung von eindeutigen Datenträgern mit Mehrfachschreibschutz
- Dokumentation/Quittierung von Datenträgern
- Transportprotokoll
- Transport-Überwachung
- Vollständigkeits- und Richtigkeitsprüfung
- Dokumentation des Datenträgertransports durch Absender/Empfänger
- Mitarbeiterunterweisung und -verpflichtung

## DATEN-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

- Direktverbindung / Standleitung
- VPN-Tunnel
- SSH-Tunnel

## 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

- Protokollierung
- Revisionssichere E-Mail-Archivierung
- Revisionssichere Daten- und Dokumentensicherung

## DATENINTEGRITÄT / ZUVERLÄSSIGKEIT

Gewährleistung, dass alle Funktionen des Systems sowie gespeicherte personenbezogene Daten zur Verfügung stehen und nicht durch Fehlfunktionen des Betriebssystems beschädigt werden können

- Penetrationstests
- Test- und Freigabeverfahren
- vorrausschauende Ressourcenplanung
- Redundante Systeme/Komponenten
- Sicherheitskonzept
- Redundante Speichersysteme
- Prüfsummenbildung

*[Hier ggfs. weitere Massnahmen beschreiben]*

**TRENNBARKEIT**

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

- Logische Mandantentrennung
- Festlegung von Datenbankrechten
- Verwendung mehrerer Datenbankinstanzen

[Hier ggfs. weitere Massnahmen beschreiben]