

Anlage

Technische und organisatorische Maßnahmen (TOM)

Version 1.12

Zutrittskontrolle BEWOTEC

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen:

1. Haupt-Eingangstür mit automatischer Verriegelung, Zutritt nur mittels Zahlencode oder ABUS SECCOR Chipschlüssel (elektronisches Türschloss)
2. Bürotüren sind mit elektronischen Türschlössern gesichert, welche abends verriegelt werden
 - a. Der Zutrittsschutz zu den sonstigen Büroflächen wird durch absperrbare Türen realisiert. Sofern Notausgänge vorhanden sind, sind diese so zu verriegeln, dass ein Öffnen von außen nicht möglich ist ohne die Fluchtfunktion zuvor aufzuschließen. Alle Türen sind nach Verlassen der Betriebsflächen abzusperren.
3. Alle Flurtüren mit elektronischer Verriegelung und Alarmanlagen überwacht
 - a. Alle Flurtüren müssen außerhalb der Geschäftszeiten geschlossen und verriegelt sein, da sonst ein scharf schalten der Alarmanlage nicht möglich ist. So ist sicher gestellt das die Alarmanlage außerhalb der Geschäftszeiten immer scharf geschaltet ist.
4. Server-Raum ist durch Stahltür mit elektronischem Codeschloss gesichert
 - a. Der Zutrittsschutz für den Serverraum wird durch eine abgesperrte Stahl Tür realisiert, zu der nur die Geschäftsführung und geschulte Mitarbeiter der IT-Abteilung Schlüssel hat.
 - b. Der Zutrittsschutz für die Server Schränke wird durch abgesperrte Schranktüren realisiert, zu denen wiederum nur geschulte Mitarbeiter Zugang haben.
5. Gebäude durch Alarmanlage gesichert
 - a. 24/7- Überwachung sowie zentralem Wachdienst mittels Anbindung über redundante GSM Module im Server Raum.

6. Gebäude wird per Video überwacht
 - a. Haupteingangstüre und Lieferanten Eingang ist Video überwacht.
7. Glasbruchmelder in der unteren Etage

Organisatorische Maßnahmen:

1. Empfang ist während der Arbeitszeiten stetig durch interne Mitarbeiter besetzt
2. Videoüberwachung des Haupteingangs und des Lieferanten Eingangs.
3. Personenbezogene Schlüsselregelung mit zentraler DB
 - a. Zutrittsberechtigungen zu den verschiedenen Sicherheitszonen (Abteilungen) werden generell durch die Geschäftsleitung oder den Leiter der IT-Abteilung erteilt oder entzogen. Hierbei wird für die Ausgabe von Schlüsseln zu der Zonen eine zentrale Datenbank verwendet, in welchem Name, Datum, Anzahl, Berechtigungen und Art der Chip-Schlüssel festgehalten werden.
 - b. Alle Schließ.-und Öffnungsvorgänge können jederzeit an den elektronischen Türschlössern ausgelesen werden.

Zugangskontrolle BEWOTEC

Unbefugten ist die Nutzung von Datenverarbeitungssystemen zu verwehren.

Technische Maßnahmen:

1. AD-Authentifizierung an allen DV-Systemen mit Benutzernamen und Kennwort
 - a. Zugang zu den Anwendungssystemen per Web-Oberfläche oder Anwendungs-Oberfläche (reguläre Nutzung): jeder Nutzer muss sich zum Zugriff auf personenbezogene Daten authentisieren – normalerweise mittels Benutzername und Passwort, aber auch abweichend davon durch entsprechende per-authentifizierte Links mit Benutzerzuordnung.
 - b. Zugang zu den Servern (z. B. für administrative Aufgaben, Zugang normalerweise per RDP; SSH): alle Server verlangen eine Benutzerauthentifizierung. Dies wird in der Regel durch Benutzername und Passwort realisiert.

2. Regelmäßiger Passwortwechsel mit Windows – Kennwortrichtlinien

- a. Passworte müssen angemessenen BEWOTEC Mindestregeln entsprechen wie z.B. einer minimalen Passwortlänge und Komplexität. (Buchstaben-Sonderzeichen-Zahlen kombiniert; 7Zeichen; keine Wiederholungen)
- b. Passworte müssen in regelmäßigen Abständen geändert werden. Erstpassworte müssen umgehend geändert werden. (alle 90Tage AD und E-Mail-System 90Tage)
- c. Die Umsetzung der Anforderungen an Passwortlänge, Passwortkomplexität und Gültigkeit ist durch organisatorische Einstellungen in den GPO der Domäne realisiert.

Nach dreimaligen Fehlerhaften Login werden die Accounts automatisch gesperrt und können nur durch IT-Verantwortliche wieder freigegeben werden.

3. Einsatz von zentralisierter Anti-Viren Software

- a. Zentralisierte und verwaltete Anti Virus Lösung, zum Schutz gegen Virus, Trojaner etc.

4. Einsatz von Hardware Firewalls im Cluster

- a. WatchGuard Firewall Cluster mit Intrusion Detektion

5. Fernzugriff nur über VPN-Technologie möglich

6. Sperrungen von nicht benötigten Schnittstellen (USB etc.)

7. Datenträger Verschlüsselung von mobilen Geräten wie Notebooks und Tablets

8. Automatisches Sperren von Benutzer Account

- a. Nach wiederholter fehlerhafter Authentisierung wird der Benutzer Zugang automatisch gesperrt. Ein Prozess zum Rücksetzen bzw. Entsperrung von gesperrten Zugangskennungen ist nicht verfügbar, sondern muss persönlich in der IT-Abteilung durchgeführt werden.

9. Automatische Zugangssperre am Arbeitsplatz

- a. Bei mehr als fünf Minuten Inaktivität der Arbeitsstation bzw. des Terminals werden die angemeldeten Benutzer automatisch in den Anmelde-Modus per AD GPO versetzt und damit der Kennwortschutz automatisch aktiviert.

Organisatorische Maßnahmen:

1. Verwaltung und Festlegung der Zugriffe auf befugte Personen

- a. Der Kreis der Personen, die befugt Zugang zu den BEWOTEC DV-Anlagen auf oder mit denen Daten verarbeitet und/oder gespeichert werden, ist auf das zur jeweiligen Aufgaben- bzw. Funktionserfüllung im Rahmen der laufenden Betriebsorganisation notwendige Minimum beschränkt.

Zugänge für temporär beschäftigte Personen (Berater, Praktikanten, Auszubildende) werden individuell vergeben.

Bei der BEWOTEC GmbH wird die Anzahl der Personen mit Zugang zu vorgenannten DV-Anlagen auf ein Minimum reduziert. Hierbei werden verschiedene Personengruppen unterschieden: System- Administratoren, Datenbank-Administratoren, normale Benutzer, und Personen ohne Zugang zu solchen DV-Systemen.

System-Administratoren können die von der Geschäftsführung erteilten Zugangs- und Zugriffsberechtigungen in das System einpflegen und entsprechende Berechtigungsmerkmale protokolliert ausgeben, System-Wartungen und Updates durchführen, Server-Logs einsehen, und ganz allgemein serverbezogene administrative Aufgaben durchführen.

Datenbank-Administratoren können sich auf Datenbank-Ebene direkt in die jeweiligen Kundendatenbanken einloggen und dort administrative Arbeiten durchführen und Backups erstellen. Normale Benutzer können sich nur über die jeweiligen Web-Oberflächen oder Anwendungen in die Anwendungssysteme einloggen, und dort die ihren jeweiligen Zugriffsberechtigungen entsprechenden Aufgaben durchführen.

2. Sorgfältige Auswahl des Reinigungspersonals

Zugriffskontrolle BEWOTEC

Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen:

1. Einsatz von Aktenvernichtern
2. Ordnungsgemäße Vernichtung von Datenträgern
3. Protokollierung von Zugriffen auf alle Server basierten Anwendungen und Datenbestände
 - a. Zugriffe der System-Administratoren werden nur insoweit protokolliert, dass ihre jeweiligen Anmelde-Vorgänge und die von ihnen auf den Server-Shells gestarteten Befehle erfasst werden. Alle anderen (z. B. in grafischen Konsolen gestarteten) Befehle werden nicht erfasst. Die Anmelde-Vorgänge werden für die Dauer von 3 Monaten aufgehoben. Zugriffe der System-Administratoren dienen nicht der Verarbeitung oder dem aktiven Zugriff auf personenbezogene Daten, sondern der Pflege, Wartung und Aktualisierung der Server-Systeme an sich.
 - b. Für alle anderen (regulären) Nutzer, die die entsprechenden Anwendungsprogramme zur Verarbeitung der personenbezogenen Daten nutzen, wird eine üblicherweise eine Anwendungs-Historie vorgehalten, die erfasst, welcher Nutzer wann welche Aktion ausgeführt hat, sofern diese Aktion persönliche Daten modifiziert. Darüber hinaus werden noch viele weitere Aktionen protokolliert, um in der Anwendung selbst Änderungsverläufe etc. darstellen zu können.

Organisatorische Maßnahmen:

1. Einsatz von Dienstleistern zur Aktenvernichtung
2. Datenträger Löschung und Daten-Vernichtung
 - a. Datenträger werden aus Sicherheitsgründen vor deren internen Wiederverwendung (z.B. Wechsel des Hauptnutzers) oder Weitergabe datenschutzgerecht gelöscht.
3. BEWOTEC Berechtigungs-Konzept
4. Sichere Aufbewahrung von Datenträgern wie z.B. Backup-Medien
5. Verwaltung der Benutzerrechte nur durch BEWOTEC Administratoren

Weitergabekontrolle BEWOTEC

Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Grundsätzlich werden keine Daten aus den BEWOTEC Systemen weitergegeben. Falls dies ausnahmsweise erforderlich sein sollte, so erfolgt die Weitergabe nur auf Anfrage in besonderen Fällen.

Sämtliche BEWOTEC Server liegen netztopologisch hinter entsprechenden Gateways bestehend aus Router und Firewall, der Zugriff auf die Systeme kann nur über diese erfolgen. Die Gateways lehnen Verbindungen, die aus einem nicht explizit freigeschalteten Netz kommen ab.

Technische Maßnahmen:

1. Einrichtung von VPN-Tunneln
 - a. Daten werden überwiegend in VPN-Netzen mit entsprechenden Protokollen ausgetauscht. Authentisierung und Verschlüsselung sind unsere Maßnahmen, um das Risiko des unbefugten Kopierens und Änderns personenbezogener Daten zu reduzieren.
 - b. Die Datenübertragungen zwischen Clients und Servern werden generell verschlüsselt via VPN durchgeführt.
2. E-Mail-Verschlüsselung
 - a. Für eine nahtlose Integration im Bereich Datenschutz haben wir die Office 365-Nachrichtenverschlüsselung mit vielseitigen neuen Funktionen für die E-Mail-Verschlüsselung und den Rechteschutz in Betrieb. Die Neuerungen basieren auf Azure Information Protection und erleichtern die Freigabe geschützter E-Mails für Personen innerhalb und außerhalb des Unternehmens.
3. Sicherer Postversand
 - a. Soweit Datenträger durch Transportunternehmen übermittelt werden, werden die Datenträger nur nach vorheriger Authentisierung des Transportunternehmens Deutsche Post AG, Spediteur, Kurierdienst, Taxifahrer, etc.), notfalls durch telefonische Rückversicherung beim Transportunternehmen, herausgegeben. Die Herausgabe der Datenträger an das Transportunternehmen ist zu dokumentieren.

4. Verschlüsselte Datenübermittlung
5. Netzwerksicherheit durch Hard- und Software Sicherheitskomponenten

Organisatorische Maßnahmen:

1. Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
2. Geheimhaltungserklärung intern / extern
3. Regelungen zur Nutzung von Internet und E-Mail

Eingabekontrolle BEWOTEC

Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen:

1. Protokollierung der Eingabe, Änderung und Löschung von Daten
 - a. Zugriffe der System-Administratoren werden nur insoweit protokolliert, dass ihre jeweiligen Anmelde-Vorgänge und die von ihnen auf den Server-Shells gestarteten Befehle erfasst werden. Alle anderen (z. B. in grafischen Konsolen gestarteten) Befehle werden nicht erfasst. Die Anmelde-Vorgänge werden für die Dauer von 3 Monaten aufgehoben. Zugriffe der System-Administratoren dienen nicht der Verarbeitung oder dem aktiven Zugriff auf personenbezogene Daten, sondern der Pflege, Wartung und Aktualisierung der Server-Systeme an sich.
 - b. Für alle anderen (regulären) Nutzer, die die entsprechenden Anwendungsprogramme zur Verarbeitung der personenbezogenen Daten nutzen, wird eine üblicherweise eine Anwendungs-Historie vorgehalten, die erfasst, welcher Nutzer wann welche Aktion ausgeführt hat, sofern diese Aktion persönliche Daten modifiziert. Darüber hinaus werden noch viele weitere Aktionen protokolliert, um in der Anwendung selbst Änderungsverläufe etc. darstellen zu können.

Organisatorische Maßnahmen:

1. Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
2. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
3. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Auftragskontrolle BEWOTEC

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

Technische Maßnahmen:

1. entfällt

Organisatorische Maßnahmen:

1. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
2. Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG
3. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
4. Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
5. Eindeutige Vertragsgestaltung, insbesondere Abgrenzung der Verantwortlichkeiten zwischen Auftraggeber und Auftragnehmer und Festlegung der durchzuführenden Kontrollmaßnahme

Verfügbarkeitskontrolle BEWOTEC

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

Technische Maßnahmen:

1. Feuerlöschgeräte in Serverräumen und Fluren
2. Brandschutzmeldeanlage
3. Redundante Klima-Anlage in den Server Räumen
4. Temperatur Überwachung im Server Raum
5. Überspannungsschutz für alle Schutzkontaktsteckdosen im Server Raum
6. Unterbrechungsfreie Stromversorgung für Produktiv relevante System

Organisatorische Maßnahmen:

1. Alarmmeldung bei unberechtigten Zutritten zu Serverräumen und Gebäude
2. Tägliche Datensicherung sowie Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
3. Backup- & Recovery-Konzept
4. Notfallplan
5. Testen von Datenwiederherstellung
6. Ständige Netzwerküberwachung

Trennungsgebot BEWOTEC

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können

Technische Maßnahmen:

1. Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
2. Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
3. Trennung von Produktiv- und Testsystemen

Organisatorische Maßnahmen:

1. Erstellung eines Berechtigungskonzepts
2. Festlegung von Datenbankrechten
3. Logische Mandantentrennung (softwareseitig)
4. Versehen der Datensätze mit Zweckattributen/Datenfeldern