LEBER&PARTNER Rechtsanwälte

# Gefährdungsbeurteilung

**für**

## Datenverarbeitung

**erstellt mit Delegatis durch**

Martin Leber

Stand: 19.07.2016

LEBER&PARTNER Rechtsanwälte

# Inhaltsverzeichnis

## Hinweise zum Verständnis der Risikobeurteilung

Locations, Handlungen und Materialien von denen nach dem aktuellen Kenntnisstand keine Gefahren ausgehen, die über das allgemeine Lebensrisiko hinausgehen werden in der Risikobeurteilung nicht mit aufgeführt. Die Risikobewertung erfolgt nach folgenden Kriterien:

| Risiko(maßzahl) R = W x S | | | | | | |
|---|---|---|---|---|---|---|
| Eintritts-Wahrscheinlichkeit ( W ) | | Schadensausmaß ( S ) | | | | |
| | | 1 | 2 | 3 | 4 | 5 |
| | | keine erheblichen Verletzungen | leichte Verletzungen | mittelschwere Verletzungen | schwere Verletzungen | katastrophale/ tödliche Verletzungen |
| 5 | sehr wahrscheinlich | 5 | 10 | 15 | 20 | 25 |
| 4 | wahrscheinlich | 4 | 8 | 12 | 16 | 20 |
| 3 | unwahrscheinlich | 3 | 6 | 9 | 12 | 15 |
| 2 | sehr unwahrscheinlich | 2 | 4 | 6 | 8 | 10 |
| 1 | mit an Sicherheit grenzender Wahr-scheinlichkeit ausge-schlossen | 1 | 2 | 3 | 4 | 5 |

| Wahrscheinlichkeit (W) | |
|---|---|
| **W** | **Beschreibung** |
| 5 - sehr wahrscheinlich | Ohne (weitere) Schutzmaßnahmen ist mit dem Schadenseintritt zu rechnen. |
| 4 - wahrscheinlich | Der Eintritt des Schadensereignisses ist wahrscheinlicher als sein Ausbleiben. |
| 3 - unwahrscheinlich | Das Ausbleiben des Schadensereignisses ist wahrscheinlicher als sein Eintritt. |
| 2 - sehr unwahrscheinlich | Das Ausbleiben des Schadensereignisses ist deutlich wahrscheinlicher als sein Eintritt. |
| 1 - mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen | Mit dem Schadenseintritt ist nicht zu rechnen. |

| Mögliches Schadensausmaß (S) | |
|---|---|
| **G** | **Beschreibung** |
| 5 - katastrophale/tödliche Verletzungen oder Schäden* | Tod, lebensgefährliche Verletzungen (z.B. Rückenmarksverletzungen, Amputation von Gliedmaßen, Schädelbruch mit Gehirnblutung, Polytrauma) |
| 4 - schwere Verletzungen | Verletzungen, die stationär versorgt werden müssen (z.B. komplizierte Knochenbrüche, stumpfe Bauchverletzung, sowie Verletzungen, die irreversibel sind bzw. nicht ausheilen, wie Gelenkversteifungen oder Gehörschaden) |
| 3 - mittelschwere Verletzungen | Verletzungen, die ambulant versorgt werden müssen (z.B. Schnittverletzung, die genäht werden muss, Verstauchung) |
| 2 - leichte Verletzungen | Bagatell-Verletzungen, die nicht ärztlich versorgt werden müssen |
| 1 - keine erheblichen Verletzungen | Keine oder nur minimale Verletzungen |

## Notwendigkeit der Definition und Umsetzung (weiterer) Schutzmaßnahmen

| R | Beschreibung |
|---|---|
| hohes Risiko R = 12...25 | Das Risiko ist zwingend durch Schutzmaßnahmen zu minimieren. Ist das Risiko durch Anwendung von Schutzmaßnahmen nicht weiter minimierbar, kann der Vorgang so nicht durchgeführt werden. |
| mittleres Risiko R = 6....10 | Das Risiko ist durch Schutzmaßnahmen zu minimieren. Ist das Risiko durch Anwendung von Schutzmaßnahmen nicht weiter minimierbar, kann der Vorgang nur unter Beachtung besonderer Sorgfalt durchgeführt werden. |
| geringes Risiko R = 1.....5 | Das Risiko ist tolerabel. Zusätzliche Schutzmaßnahmen sind nicht zwingend erforderlich. |

## Auswahl von Schutzmaßnahmen

Reichweite der Maßnahmen: weitreichend ↑ / wenig weitreichend ↓

### 1. Gefahrenquelle vermeiden/beseitigen

Durch Arbeitsgestaltung, Auswahl geeigneter Technik und Einsatz geeigneter Arbeitsmittel und Arbeitsstoffe wird die Entstehung von Gefahrenquellen vermieden. (z.B. Hubarbeitsbühnen statt Leitern einsetzen, scharfe Kanten an Kulissen durch entsprechende Konstruktion oder Bearbeitung vermeiden)

### 2. Sicherheitstechnische Maßnahmen

Maßnahmen ergreifen, damit sich Gefahren an Gefahrenquellen nicht realisieren können. Durch sicherheitstechnische Maßnahmen werden vorhandene oder zu erwartende Gefährdungen beherrscht. (z. B. Absturzsicherung wie Geländer oder Fallschutznetz)

### 3. Organisatorische Sicherheitsmaßnahmen

Durch organisatorische Maßnahmen verhindern, dass die Personen einer Gefahrenquelle ausgesetzt werden (zeitliche oder räumliche Trennung von Gefahrenquelle und Person) und Sicherstellen, dass Gefahrenquellen sicher erkannt werden können. (z.B. Arbeitsablauforganisation, freie Bühne bei Rig-Fahrten, Kennzeichnung von Gefahrenbereichen, Qualifikationen definieren)

### 4. Persönliche Schutzausrüstungen (PSA) verwenden

PSA zur Verringerung der Verletzungs- und Erkrankungsrisiken einsetzen. (z.B. Helm, Sicherheitsschuhe, Gehörschutz, Klettergurt)

### 5. Verhaltensbezogene Sicherheitsmaßnahmen

Die Wirkung von Gefahrenquellen durch ein sicherheitsgerechtes Verhalten der beteiligten Personen verringern. (z.B. Unterweisungen, intensives Proben von gefährlichen Abläufen). Voraussetzung ist die durchgeführte Risiko/Gefährdungsbeurteilung, anhand derer Betriebsanweisungen, als Grundlage der Unterweisung, erstellt werden.

T O P

Umsetzung: schwierig ↑ / einfach ↓

LEBER&PARTNER Rechtsanwälte

## Risikobewertung und Schutzmaßnahmen für Handlungen

### Erfassen, speichern und bearbeiten von personenbezogenen Daten

**Phasen:**

| Gefährdungen | Gefährdete Personengruppen | Risiko ohne Schutzmaßnahmen | | | Risiko mit Schutzmaßnahmen | | |
|---|---|---|---|---|---|---|---|
| | | EW | SA | R | EW | SA | R |
| Datenverlust | | 1 | 1 | 1 | 1 | 1 | 1 |
| Unbefugter Zugang - Zugangskontrollmaßnahmen | | 1 | 1 | 1 | 1 | 1 | 1 |
| Unbefugter Zutritt - Zutrittskontrollmaßnahmen | | 1 | 1 | 1 | 1 | 1 | 1 |
| Unbefugte Weitergabe - Weitergabekontrollmaßnahmen | | 1 | 1 | 1 | 1 | 1 | 1 |
| Unbefugter Zugriff - Zugriffskontrollmaßnahmen | | 1 | 1 | 1 | 1 | 1 | 1 |
| Unbefugte Eingabe - Eingabekontrollmaßnahmen | | 1 | 1 | 1 | 1 | 1 | 1 |
| Verstoß gegen das Gebot der Auftragskontrolle | | 1 | 1 | 1 | 1 | 1 | 1 |
| Verstoß gegen das Trennungsgebot | | 1 | 1 | 1 | 1 | 1 | 1 |

| Zum Schutz gegen | Schutzmaßnahmen | Ausführungsverantwortliche | Kontrollverantwortliche |
|---|---|---|---|
| Datenverlust | Es exitiert eine Gebäudealarmanlage | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es exitiert eine Feuer- und Rauchmeldeanlage im Rechenzentrum | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es exitiert ein Notfallkonzept. Dieses wird kontinuierlich weiterentwickelt | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es sind Mitarbeiter 24 Stunden pro Tag vor Ort, vom 24.-26.12. sowie am 31.12. in Rufbereitschaft. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es existieren Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen sowie Feuerlöschgeräte getrennte Brandabschnitte (Büro/Rechenzentrum) | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es exitieren Klimaanlagen in Serverräumen | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es werden mindestens zwei mal jährlich Notfallübungen im Rechenzentrum durchgeführt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Zum Schutz vor Wasserschäden liegen Serverräume nicht unter sanitären Anlagen. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Die Stromversorgung ist über eine Netzersatzanlage (24 Stunden Überbrückung mit beliebig häufiger Nachbetankung) inkl. einer unterbrechungsfreien Stromversorgung (15 Minuten Autonomiezeit) und Schutzsteckdosenleisten in Serverräumen gewährleistet. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| Unbefugter Zugang - Zugangskontrollmaßnahmen | Für alle Benutzer werden Benutzerprofile mit Zugangsberechtigungen erstellt und den einzelnen IT-Systemen zugeordnet. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Jedes System ist durch Authentifikationsmaßnahmen, wie Benutzername und Passwort und/oder Clientzertifikate, SSH-Schlüssel und Firewalls vor unberechtigten Zugriffen geschützt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Fernzugriff wird ausschließlich über VPN gestattet. Zugriffe werden protokolliert. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Der Fernzugriff auf die IT-Systeme zu Wartungszwecken erfolgt nur über passwortgeschützte VPN-Verbindungen und ist nur durch einen beschränkten Mitarbeiterkreis möglich. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |

| Zum Schutz gegen | Schutzmaßnahmen | Ausführungsverantwortliche | Kontrollverantwortliche |
|---|---|---|---|
| | Identifikation von Benutzern erfolgt :<br>Client: Username / User ID<br>Server: Username / User ID | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Der Fernzugriff auf die IT-Systeme zu Wartungszwecken erfolgt nur über passwortgeschützte VPN-Verbindungen und ist nur durch einen beschränkten Mitarbeiterkreis möglich. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Passwortrichtlinien Server: Serverpasswörter werden durch das System generiert und haben eine Entropie von 128 bit (Entspricht: 340.282.366.920.938.463.463.374.607.431.768.211.456 Möglichkeiten) | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Direkte SSH Verbindungen sind nicht zugelassen. Konkret ist eine Zugangsberechtigung für die Accelerated nur dann notwendig, wenn diese im Rahmen ihrer Leistungen die Administration von Betriebssystemen oder Applikationen übernimmt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Die IT-Systeme sind durch Hardware- und Softwarefirewalls geschützt. Zugriffe auf die ITSysteme werden im Zugriffslogfile protokolliert. Die Logfiles werden entsprechend den Projektvorgaben aufbewahrt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Der Fernzugriff auf die IT-Systeme zu Wartungszwecken erfolgt nur über passwortgeschützte VPN-Verbindungen und ist nur durch einen beschränkten Mitarbeiterkreis möglich. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Der Fernzugriff auf die IT-Systeme zu Wartungszwecken erfolgt nur über passwortgeschützte VPN-Verbindungen und ist nur durch einen beschränkten Mitarbeiterkreis möglich. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Protokollierung der Systemzugriffe erfolgt auf Systemebene, gesichert durch Backups. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| Unbefugter Zutritt - Zutrittskontrollmaßnahmen | Es existiert ein Wachdienst. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Zentrales Schließsystem. Es existieren Sicherheitsschlösser, elektronisches Chipkarten-/Transponder-Schließsystem. Regulierte Vergabe von Schlüsseln bzw. im wesentlichen Zutrittskarten auf RFID Basis. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Das Service-Personal ist rund um die Uhr, also 24 x 7 x 360, vor Ort. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Zutritt zu den Racks und Zugriff auf deren Schließtechnik haben nur autorisierte und namentlich benannte Personen. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es existiert ein Empfangsbereich mit Personenkontrolle und Protokollierung aller Besucher durch personenbezogene Zutrittslisten. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Dritte, also beispielsweise Techniker oder Reinigungskräfte, haben nur Zutritt in Begleitung von autorisierten Mitarbeitern der Accelerated IT Services GmbH. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es existiert ein Videoüberwachung der Zutrittspunkte und übrigen Flächen. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es existiert eine Einbruchmeldeanlage nach VdS Klasse C mit Lichtschranken, Bewegungsmeldern und Überwachung sämtlicher Türen. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | IT-Systeme werden ausschließlich in den Betriebsstätten der Accelerated IT Services GmbH betrieben und befinden sich in abgeschlossenen Racks (Serverschränken). | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Der Zutritt zu den Serverräumen erfolgt durch Chipkarte und biometrischer Zutrittskontrolle. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Die Schutzmaßnahmen werden fortlaufend überprüft. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |

| Zum Schutz gegen | Schutzmaßnahmen | Ausführungsverantwortliche | Kontrollverantwortliche |
|---|---|---|---|
| Unbefugte Weitergabe - Weitergabekontrollmaßnahmen | Es exitieren Regelungen für die Übertragung personenbezogener Daten | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Die E-Mail-Kommunikation zur Bearbeitung von Aufträgen und zur Kommunikation mit Kunden ist sowohl unverschlüsselt als auch verschlüsselt. Eine Unterstützung für PGPVerschlüsselung ist aber vorhanden und wird auf Kundenwunsch genutzt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Personenbezogene Daten werden in kennwortgeschützten Datenbanken gespeichert. Die Übertragung und der Fernzugriff auf diese Daten findet nur über gesicherte verschlüsselte Verbindungen statt (VPN, SSL/TLS). | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Defekte Datenträger werden zerstört. Diese werden anschließend durch ein Fachunternehmen entsorgt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Datenträger aus Kundenservern werden vor deren Wiederverwendung sicher gelöscht, sodass deren Daten anschließend nicht wiederhergestellt werden können. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Dokumente mit personenbezogenen Daten werden durch die Vernichtung in Aktenvernichtungsgeräten „gelöscht“. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| Unbefugter Zugriff - Zugriffskontrollmaßnahmen | Es erfolgt eine Auswertung von Protokollen durch die Geschäftsleitung. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Die Administration und der Zugriff auf Logfiles erfolgt nach dem "Vier-Augen-Prinzip" | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Nicht benötigte Dienste, Ports und Accounts werden standardmäßig deaktiviert oder gesperrt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es erfolgt eine Protokollierung der Benutzerzugriffe. Dabei wird differenziert nach: Schreiben von Daten, Lesen von Daten, Datenbankzugriffe, Programmausführung, Terminalzugriff, Schellzugriff , Löschen, An/Abmeldeversuche, Richtlinienverstöße | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es sind abgestufte Administratorrrechte vorhanden. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Für den Zugriff auf einzelne IT-Systeme ist der Kreis der berechtigten Mitarbeiter beschränkt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Der Zugriff auf die IT-Systeme erfolgt ausschließlich durch autorisierte, namentlich benannte Personen, mit einer Limitierung im Hinblick auf den jeweiligen Zuständigkeitsbereich dieser Person. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| Unbefugte Eingabe - Eingabekontrollmaßnahmen | Formulare, deren Daten in automatisierte Verarbeitungen übernommen wurden, werden den gesetzlichen Regelungen entsprechend aufbewahrt | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Die Aufbewahrungsfrist für die Logfiles wird im Regelfall individuell mit den Kunden vereinbart und beträgt in allen anderen Fällen zumindest 4 Wochen. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Um nachträglich festzustellen und überprüfen zu können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, werden alle Dienste in Form von Logfiles protokolliert. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| Verstoß gegen das Gebot der Auftragskontrolle | Im Regelfall bedient sich die Accelerated keiner Unterauftragnehmer, die direkten Zugriff auf die Daten des Kunden innehaben. Ausnahmen sind jeweils explizit mit dem Kunden zu vereinbaren. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Die Auswahl von Unterauftragnehmern erfolgt nach deren Sorgfältigkeit und Zuverlässigkeit im Umgang mit personenbezogenen Daten, sowie der Datensicherheit. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Es wird ein schriftlicher Vertrag mit Auftragsdatenverarbeitern gemäß § 11 BDSG geschlossen | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |

| Zum Schutz gegen | Schutzmaßnahmen | Ausführungsverantwortliche | Kontrollverantwortliche |
|---|---|---|---|
| Verstoß gegen das Trennungsgebot | Es werden nur Daten im Rahmen und Umfang der vertraglichen Vereinbarungen erhoben. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Zuordnungsdatei werden in einem getrennten, abgesicherten System aufbewahrt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Produktiv- und Testsysteme sind voneinander getrennt. Daten auf Testsystemen werden nach Abschluss der Tests gelöscht. Soweit möglich werden für Testsysteme anonymisierte oder pseudonymisierte Daten verwendet. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Mandanten werden innerhalb der Systeme logisch voneinander abgetrennt | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |
| | Soweit möglich und vertraglich vereinbart, werden Mandantensysteme voneinander getrennt. | Accelerated IT Service GmbH | Leber & Partner Rechtsanwälte |

# Hinweise zum Alarm- und Gefahrenabwehrplan

**Hinweise zum Alarm- und Gefahrenabwehrplan**

1. Die im Folgenden beschriebenen Handlungen beschreiben die für den Fall des Schadenseintritts oder unmittelbar drohenden Schadenseintritt definierten Prozesse der Alarmierung und Gefahrenabwehr.
2. Es sind die Gefahren aufgeführt, für die im System ein Notfallplan erstellt wurde.
3. Die beschriebenen Handlungen, ihre Ablaufreihenfolge und die definierten Zuständigkeiten sind verbindlich, es sei denn, dass Gefahr im Verzug ein abweichendes Handeln erforderlich macht.
4. Sie können auch durch Weisung des Veranstaltungsleiters oder des Einsatzleiters abgeändert oder außer Kraft gesetzt werden.

LEBER&PARTNER Rechtsanwälte

## Alarm und Gefahrenabwehrplan

| Datenverlust | | Phasen: | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Im Zusammenhang mit** | **Gefährdete Personengruppen** | **Risiko ohne Schutzmaßnahmen** | | | **Risiko mit Schutzmaßnahmen** | | | |
| | | EW | SA | R | EW | SA | R | |
| Erfassen, speichern und bearbeiten von personenbezogenen Daten | [] | 1 | 1 | 1 | 1 | 1 | 1 | |

| Alarmierungs- und Gefahrenabwehrmaßnahme | Hinweis | Ausführung | Kontrolle | Erledigt |
|---|---|---|---|---|
| 1.0 Meldung an Administrator | | Kunde | Administrator | |
| 1.1 Auswertung der Serverprotokolle um heraus zu finden, welche Daten betroffen sind und wie es zum Datenverlust kam | Prüfung zumindest folgender Szenarien:<br>–> Menschliche Ursache (Daten wurden ausversehen durch Kunden gelöscht)<br>–> Technisches Problem (Festplattenfehler) | Ausführende Techniker und Dienstleister | Administrator | |
| 2.0 Abstimmung mit dem Kunden bezüglich des Zeitpunkt zum Einspielen eines Backups | –> Der Kunde soll entscheiden, von welchem Zeitpunkt das Backup eingespielt werden soll. –> Der Kunde soll entscheiden, wann das Backup eingespielt werden soll. –> Der Kunde soll auch über das Ergebnis der Auswertung der Serverprotokolle informiert werden. | Leber & Partner Rechtsanwälte | Kunde | |
| 3.0 Überspielen des vom Kunden gewünschten Serverbackups | | Administrator | Leber & Partner Rechtsanwälte | |
| 4.0 Protokoll anfertigen | | Administrator | Leber & Partner Rechtsanwälte | |
| 5.0 Protokoll an Leber & Partner übersenden | | Administrator | Leber & Partner Rechtsanwälte | |
| 6.0 Protokoll an Kunden übersenden | | Leber & Partner Rechtsanwälte | Kunde | |

LEBER&PARTNER Rechtsanwälte

## Unbefugter Zugang - Zugangskontrollmaßnahmen

**Phasen:**

| Im Zusammenhang mit | Gefährdete Personengruppen | Risiko ohne Schutzmaßnahmen | | | Risiko mit Schutzmaßnahmen | | |
|---|---|---|---|---|---|---|---|
| | | EW | SA | R | EW | SA | R |
| Erfassen, speichern und bearbeiten von personenbezogenen Daten | [] | 1 | 1 | 1 | 1 | 1 | 1 |

Gemeint sind Maßnahmen um zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können, wobei allerdings das Wort "nutzen" sich nicht auf die Legaldefinition des § 3 Abs. 5 BDSG beschränkt. Maßnahmenziele: Das Eindringen in die Datenverarbeitungssysteme durch Unbefugte soll verhindert werden. Die Accelerated IT Services GmbH setzt ausschließlich Serversysteme ein, deren Zugang geschützt ist. Dies geschieht im Regelfall durch Benutzername und Passwort, sowie durch weitere technische Schutzmaßnahmen, wie z.B. Firewalls.

| Alarmierungs- und Gefahrenabwehrmaßnahme | Hinweis | Ausführung | Kontrolle | Erledigt |
|---|---|---|---|---|
| 1.0 Meldung an Administrator | | Ausführende Techniker und Dienstleister | Administrator | |
| 1.1 Auswertung der Serverprotokolle um heraus zu finden, welche Daten betroffen sind und ob es zum Datenverlust kam | Prüfung zumindest folgender Szenarien: –> Menschliche Ursache (PW Weitergabe) –> Technisches Problem (Hackerangriff) | Ausführende Techniker und Dienstleister | Administrator | |
| 1.2 Abstimmung mit Leber & Partner über weiteres Vorgehen und welche Personen/Kunden informiert werden müssen. | | Ausführende Techniker und Dienstleister | Administrator | |
| 2.0 Information an die Kunden über Vorfall und getätigte bzw. geplante Maßnahmen | | Leber & Partner Rechtsanwälte | Kunde | |
| 3.0 Automatische Neuvergabe der Serverpasswörter für den kompromittierten Server | | Ausführende Techniker und Dienstleister | Administrator | |
| 3.1 ggf. Verlagerung des Kundenservers auf einen anderen Node | | Ausführende Techniker und Dienstleister | Administrator | |
| 4.0 Protokoll anfertigen | | Administrator | Leber & Partner Rechtsanwälte | |
| 5.0 Protokoll an Leber & Partner übersenden | | Administrator | Leber & Partner Rechtsanwälte | |
| 6.0 Protokoll an Kunden übersenden | | Leber & Partner Rechtsanwälte | Kunde | |

## Unbefugter Zugriff - Zugriffskontrollmaßnahmen

**Phasen:**

| Im Zusammenhang mit | Gefährdete Personengruppen | Risiko ohne Schutzmaßnahmen | | | Risiko mit Schutzmaßnahmen | | |
|---|---|---|---|---|---|---|---|
| | | EW | SA | R | EW | SA | R |
| Erfassen, speichern und bearbeiten von personenbezogenen Daten | [] | 1 | 1 | 1 | 1 | 1 | 1 |

Es muss gewährleistet werden, dass die zur Benutzung von DV-Anlagen berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind und das personenbezogene Daten bei der Verarbeitung, Nutzung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

| Alarmierungs- und Gefahrenabwehrmaßnahme | Hinweis | Ausführung | Kontrolle | Erledigt |
|---|---|---|---|---|
| 1.0 Meldung an Administrator | | Ausführende Techniker und Dienstleister | Administrator | |
| 1.1 Auswertung der Serverprotokolle um heraus zu finden, welche Daten betroffen sind und ob es zum Datenverlust kam | Prüfung zumindest folgender Szenarien: –> Menschliche Ursache (PW Weitergabe) –> Technisches Problem (Hackerangriff) | Ausführende Techniker und Dienstleister | Administrator | |
| 1.2 Abstimmung mit Leber & Partner über weiteres Vorgehen und welche Personen/Kunden informiert werden müssen. | | Ausführende Techniker und Dienstleister | Administrator | |
| 2.0 Information an die Kunden über Vorfall und getätigte bzw. geplante Maßnahmen | | Leber & Partner Rechtsanwälte | Kunde | |
| 3.0 Automatische Neuvergabe der Serverpasswörter für den kompromittierten Server | | Ausführende Techniker und Dienstleister | Administrator | |
| 3.1 ggf. Verlagerung des Kundenservers auf einen anderen Node | | Ausführende Techniker und Dienstleister | Administrator | |
| 4.0 Protokoll anfertigen | | Administrator | Leber & Partner Rechtsanwälte | |
| 5.0 Protokoll an Leber & Partner übersenden | | Administrator | Leber & Partner Rechtsanwälte | |
| 6.0 Protokoll an Kunden übersenden | | Leber & Partner Rechtsanwälte | Kunde | |

LEBER&PARTNER Rechtsanwälte

## Unbefugter Zutritt - Zutrittskontrollmaßnahmen

**Phasen:**

| Im Zusammenhang mit | Gefährdete Personengruppen | Risiko ohne Schutzmaßnahmen | | | Risiko mit Schutzmaßnahmen | | |
|---|---|---|---|---|---|---|---|
| | | EW | SA | R | EW | SA | R |
| Erfassen, speichern und bearbeiten von personenbezogenen Daten | [] | 1 | 1 | 1 | 1 | 1 | 1 |

Maßnahmen, um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten, mit welchen personenbezogene Daten verarbeitet werden.
Maßnahmenziele: Als Zutritt ist das physische Betreten von Räumlichkeiten zu verstehen – insbesondere von Räumen, in denen Daten aufbewahrt oder verarbeitet werden. Dazu zählen im wesentlichen die von der Accelerated betriebene Rechenzentren. Um Unbefugten den Zutritt zu den dort untergestellten Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

| Alarmierungs- und Gefahrenabwehrmaßnahme | Hinweis | Ausführung | Kontrolle | Erledigt |
|---|---|---|---|---|
| 1.0 Meldung an Administrator | | Ausführende Techniker und Dienstleister | Administrator | |
| 1.1 Auswertung der Protokolle des Schließsystems | Prüfung zumindest folgender Szenarien: –> Menschliche Ursache (Karten-Weitergabe) –> Technisches Problem (Hackerangriff) | Ausführende Techniker und Dienstleister | Administrator | |
| 1.2 Abstimmung mit Leber & Partner über weiteres Vorgehen und welche Personen/Kunden informiert werden müssen. | | Ausführende Techniker und Dienstleister | Administrator | |
| 3.0 Änderung des Zutrittscodes und ggf. Neuausgabe der Zutrittskarten | | Ausführende Techniker und Dienstleister | Administrator | |
| 4.0 Protokoll anfertigen | | Administrator | Leber & Partner Rechtsanwälte | |
| 5.0 Protokoll an Leber & Partner übersenden | | Administrator | Leber & Partner Rechtsanwälte | |

## Unbefugte Weitergabe - Weitergabekontrollmaßnahmen

**Phasen:**

| Im Zusammenhang mit | Gefährdete Personengruppen | Risiko ohne Schutzmaßnahmen | | | Risiko mit Schutzmaßnahmen | | |
|---|---|---|---|---|---|---|---|
| | | EW | SA | R | EW | SA | R |
| Erfassen, speichern und bearbeiten von personenbezogenen Daten | [] | 1 | 1 | 1 | 1 | 1 | 1 |

Schutzziel: Es muss verhindert werden, dass personenbezogenen Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und damit festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.

| Alarmierungs- und Gefahrenabwehrmaßnahme | Hinweis | Ausführung | Kontrolle | Erledigt |
|---|---|---|---|---|
| 1.0 Meldung an Administrator | | Ausführende Techniker und Dienstleister | Administrator | |
| 1.1 Auswertung der Serverprotokolle um heraus zu finden, welche Daten betroffen sind und ob es zum Datenverlust kam | Prüfung zumindest folgender Szenarien: –> Menschliche Ursache (PW Weitergabe) –> Technisches Problem (Hackerangriff) | Ausführende Techniker und Dienstleister | Administrator | |
| 1.2 Abstimmung mit Leber & Partner über weiteres Vorgehen und welche Personen/Kunden informiert werden müssen. | | Ausführende Techniker und Dienstleister | Administrator | |
| 2.0 Information an die Kunden über Vorfall und getätigte bzw. geplante Maßnahmen | | Leber & Partner Rechtsanwälte | Kunde | |
| 3.0 Automatische Neuvergabe der Serverpasswörter für den kompromittierten Server | | Ausführende Techniker und Dienstleister | Administrator | |
| 3.1 ggf. Verlagerung des Kundenservers auf einen anderen Node | | Ausführende Techniker und Dienstleister | Administrator | |
| 4.0 Protokoll anfertigen | | Administrator | Leber & Partner Rechtsanwälte | |
| 5.0 Protokoll an Leber & Partner übersenden | | Administrator | Leber & Partner Rechtsanwälte | |
| 6.0 Protokoll an Kunden übersenden | | Leber & Partner Rechtsanwälte | Kunde | |

LEBER&PARTNER Rechtsanwälte

## Unterschriften

Mit meiner Unterschrift bestätige ich die Risikobeurteilung zur Kenntnis genommen zu haben. Ich nehme die Delegation der mir, meiner Person, Funktion, Gruppe oder dem Unternehmen, das ich vertrete, übertragenen Ausführungs- und Kontrollverantwortung an. Für die Erfüllung der Aufgaben wurde ich hinreichend unterwiesen. Die notwendigen Unterlagen und Hilfsmittel stehen mir zur Verfügung.