Technisch Organisatorische Maßnahmen

HCA Projektinvest GmbH

Bayerhamerstr. 14c
5020 Salzburg
Österreich

1. Zutrittskontrolle

1.1. Absicherung von Eingängen, Fenstern, Serverraum, etc.

Beschreibung:

Insbesondere das Herzstück des NSC ist äußerst gut gesichert und entspricht der ÖVE/ÖNORM EN 50518-1. Diese Norm enthält unter anderem örtliche und bauliche Anforderungen wie Anforderungen gegen Angriffe mit Schusswaffen, Feuer, Blitzschlag, Regelungen für Personenschleusen, Lüftung und vieles mehr. Die Widerstandsfähigkeit von Türen und verglasten Bereichen des NSC muss den Anforderungen der EN 1627, Widerstandsklasse 3 (WK3/en: RC3) entsprechen. Türen und verglaste Bereiche des NSC erfüllen die Anforderungen der EN 1522, FB3, für den Schutz gegen Angriffe mit Schusswaffen. Die Außenhülle des NSC bietet einen Feuerwiderstand gemäß EN 13501-2, jedoch nicht weniger als 30 Minuten.

Risiken:

Zutritt von Unbefugten, Diebstahl

1.2. Alarmanlage

Beschreibung:

Im NSC sind Alarmanlagen installiert, die elektronische Erkennungen für alle wesentlichen Teile des NSC bieten. Die Alarmanlagen sind wie folgt vorhanden:

Einbruchmeldeanlage nach EN50131-1 Sicherheitsgrad 3, die externe Angreifer erkennt.
Feuermelder nach EN 54 / EN 54-14, der im Falle eines Feuers Alarm auslöst.
Personenschleuse zur Kontrolle von Zutritt und Austritt.
Gasmeldeanlage mindestens Kohlenmonoxid, die im Falle von Gaslecks Alarm auslöst.
Störungserkennung EN 50136-1, um Kommunikationsstörungen zu erkennen.
Überfallmelder nach EN 50131-1, um Überfälle zu erkennen.
Überwachungsmaßnahmen zum Schutz des Personals, die mindestens alle 60 Minuten durchgeführt werden.
Meldungen von den elektronischen Schutzanlagen.
Videoüberwachung nach EN 50132-7.

Alle Anlagen werden gemäß den maßgeblichen Normen instandgehalten. In Fällen, wo keine Normen vorhanden sind, erfolgt die Instandhaltung gemäß den Herstellervorgaben, um die Funktionssicherheit jederzeit sicherzustellen.

Risiken:

Zutritt von Unbefugten, Diebstahl

1.3. Automatisches Zugangskontrollsystem

Beschreibung:

Eine zuverlässige Zutrittskontrolle zu Unternehmensgelände und Firmenräumlichkeiten bildet die Grundlage des modernen Sicherheitskonzepts des ÖWD. Mit einer unternehmensweiten Zutrittskontrolle wird festgelegt, wer zu welchen Bereichen wann Zutritt erhält. Die hauseigene Zutrittssoftware Sphinx gewährt dabei jederzeit Einblick in den aktuellen Zutrittsstatus. Unberechtigte Zutrittsversuche werden selbstverständlich dokumentiert, um Unregelmäßigkeiten rechtzeitig zu erkennen.

Risiken:

Zutritt von Unbefugten

1.4. Chipkarten-/Transponder-Schließsystem

Beschreibung:

Das Unternehmen hat ein elektronisches Chip-Schließsystem implementiert, das den Zugang zu seinen Gebäuden, Stockwerken und sensiblen Räumlichkeiten regelt. Jeder Mitarbeiter des Unternehmens, der Zugang zu diesen Bereichen benötigt, erhält einen speziellen Chip, der in der Lage ist, die elektronischen Schließsysteme zu aktivieren und den Zugang zu den jeweiligen Bereichen freizugeben. Diese Chips sind in der Regel personalisiert und nur für den spezifischen Mitarbeiter gedacht, der berechtigt ist, diese Räumlichkeiten zu betreten.

Durch dieses elektronische Schließsystem kann das Unternehmen den Zugang zu seinen sensiblen Bereichen streng kontrollieren und unerwünschte Besucher und unbefugte Mitarbeiter fernhalten. Das System bietet auch eine höhere Sicherheit, da es den Überblick über alle Eintritte und Austritte aus den sensiblen Bereichen ermöglicht. Sollte es zu unerwarteten Vorfällen kommen, können die Ereignisprotokolle des Systems dazu beitragen, die Sicherheitsverantwortlichen des Unternehmens schnell und effektiv zu informieren.

Risiken:

Zutritt von Unbefugten

1.5. Manuelles Schließsystem

Beschreibung:

Manuelle Schließsysteme dienen als zusätzliche Sicherheitsstufe neben den elektronischen automatischen Schließsystemen und tragen so zur weiteren Erhöhung des Sicherheitsniveaus bei.

Risiken:

Zutritt von Unbefugten

1.6. Personenkontrolle beim Pförtner / Empfang

Beschreibung:

Die Zentrale des ÖWD in Salzburg verfügt über einen Portierdienst, der rund um die Uhr, 24/7 besetzt ist, um eine maximale Sicherheit zu gewährleisten. Außerhalb der Geschäftszeiten wird diese Aufgabe von der Einsatzzentrale übernommen, um sicherzustellen, dass jederzeit ein Ansprechpartner zur Verfügung steht.

Das NSC in Wien wird ebenfalls rund um die Uhr, 24/7 besetzt, um eine lückenlose Überwachung zu gewährleisten. Jeder Besucher muss sich in ein Besucherbuch eintragen, um eine Dokumentation der Anwesenheit zu gewährleisten. Darüber hinaus verfügt das NSC über eine Personenschleuse mit gegenseitig verriegelten Türen, die nicht gleichzeitig geöffnet werden können. Die Türen der Schleuse sind mit automatisch selbstschließenden Verschluss- und Entriegelungseinrichtungen ausgestattet, die ausschließlich von innerhalb des NSC bedient werden können, um den Zutritt zu kontrollieren und unerlaubtes Betreten zu verhindern.

Risiken:

Zutritt von Unbefugten

1.7. Protokollierung der Besucher

Beschreibung:

Die Zentrale des ÖWD in Salzburg verfügt über einen Portierdienst, der rund um die Uhr, 24/7 besetzt ist, um eine maximale Sicherheit zu gewährleisten. Außerhalb der Geschäftszeiten wird diese Aufgabe von der Einsatzzentrale übernommen, um sicherzustellen, dass jederzeit ein Ansprechpartner zur Verfügung steht.
Spezielle Sicherheitszonen (Serverräme) dürfen nur unter Aufsicht eines IT-Mitarbeiters betreten werden.

Das NSC in Wien wird ebenfalls rund um die Uhr, 24/7 besetzt, um eine lückenlose Überwachung zu gewährleisten. Jeder Besucher muss sich in ein Besucherbuch eintragen, um eine Dokumentation der Anwesenheit zu gewährleisten. Darüber hinaus verfügt das NSC über eine Personenschleuse mit gegenseitig verriegelten Türen, die nicht gleichzeitig geöffnet werden können. Die Türen der Schleuse sind mit automatisch selbstschließenden Verschluss- und Entriegelungseinrichtungen ausgestattet, die ausschließlich von innerhalb des NSC bedient werden können, um den Zutritt zu kontrollieren und unerlaubtes Betreten zu verhindern.

Risiken:

Zutritt von Unbefugten

1.8. Schlüsselregelung (Schlüsselausgabe etc.)

Beschreibung:

Das ÖWD-Schlüsselmanagement ist eine bedeutende Aufgabe des ÖWD und umfasst die sorgfältige Verwaltung und Aufbewahrung von Schlüsseln für unsere Kunden. Wir stellen sicher, dass autorisierte Personen jederzeit Zugang zu den hinterlegten Schlüsseln haben und bieten auf Wunsch auch einen Service zur Lieferung der Schlüssel direkt zum Objekt an. Unsere sorgfältige Dokumentation bei der Schlüsselaufbewahrung ermöglicht eine lückenlose Rückverfolgung von Schlüsselausgaben und -rückgaben. Mit unserem ÖWD-Schlüsselmanagement bieten wir eine zuverlässige und effektive Lösung für die sichere Aufbewahrung und Verwaltung von Schlüsseln.

Risiken:

Zutritt von Unbefugten

1.9. Sicherheitsschlösser

Beschreibung:

Im NSC sind verschiedene Verschlusseinrichtungen im Einsatz, um eine sichere Umgebung zu gewährleisten.

Die Türen der Personenschleuse werden mittels elektromechanischer Schließeinrichtungen gesichert, die den Anforderungen der EN 14846 in der Klasse 2-R-2-B-0-C-7-H-B-3-E-4-3 entsprechen. Die ÖVE/ÖNORM EN 50518-1 A.1 spezifiziert die Anforderungen an den Schlosscode und gewährleistet somit eine hohe Sicherheitsstufe. Die Befestigungsschrauben der Türen sind im geschlossenen Zustand gegen Sabotage geschützt. Für den Fall eines Notfalls ist eine mechanische Freischaltung zur Notbefreiung vorhanden, die gegen unbeabsichtigte Betätigung gesichert ist.

Andere Türen im NSC sind mittels mechanischer Schließeinrichtungen gemäß EN 12209, Klasse 2-R-2-1-0-C-7-H-B-3-E gesichert. Auch hier wird durch die Anforderungen an den Schlosscode eine hohe Sicherheitsstufe gewährleistet.

Risiken:

Zutritt von Unbefugten, Diebstahl

1.10. Sorgfältige Auswahl von Reinigungspersonal

Beschreibung:

Eine wichtige Aufgabe des ÖWD ist die Auswahl von zuverlässigem und vertrauenswürdigem Personal, was auch in der Gewerbeordnung festgelegt ist. Es ist daher unerlässlich, dass auch das Reinigungspersonal diesen hohen Anforderungen

entspricht und sorgfältig ausgewählt wird.

§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:

Zutritt von Unbefugten

1.11. Sorgfältige Auswahl von Wachpersonal

Beschreibung:

Der ÖWD hat eine wichtige Aufgabe bei der Sicherstellung von Schutz und Sicherheit in verschiedenen Bereichen, wie z.B. im Objektschutz oder bei Veranstaltungen. Eine entscheidende Voraussetzung für eine erfolgreiche Umsetzung dieser Aufgaben ist die Auswahl von zuverlässigem und vertrauenswürdigem Personal. Diese Anforderung ist nicht nur eine interne Richtlinie des Unternehmens, sondern auch gesetzlich durch die Gewerbeordnung festgelegt. In dieser Vorschrift sind zahlreiche Bestimmungen und Anforderungen an das Personal und die Qualifikationen festgelegt, um sicherzustellen, dass die Mitarbeiter des ÖWD in der Lage sind, ihren Aufgabenbereich sicher und effektiv zu erfüllen.

§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:

Zutritt von Unbefugten

1.12. Videoüberwachung der Zugänge

Beschreibung:

Der ÖWD ist spezialisiert auf Videoüberwachung und bietet eine umfassende Überwachung aller kritischen Bereiche.

Im NSC ist eine CCTV-Überwachung nach der Norm EN 50518-1 implementiert. Dies ermöglicht eine lückenlose Überwachung aller Annäherungen zum Gebäude, in dem das NSC untergebracht ist. Die Überwachung erfolgt nach den Anwendungsrichtlinien der EN 50132-7 und kann von innen gesteuert werden.
Des Weiteren verfügt das NSC über eine Überwachungsmöglichkeit, die es dem Personal ermöglicht, berechtigte Personen zu erkennen, bevor diesen der Zutritt zur Personenschleuse gewährt wird.

Risiken:

Zutritt von Unbefugten

2. Zugangskontrolle

2.1. Einsatz einer Hardware-Firewall

Beschreibung:

Das interne Netzwerk (LAN oder Intranet) wird mittels einer redundant ausgelegten Firewall vom restlichen Netzwerk, insbesondere vom globalen Internet, abgeschottet. Zur Gewährleistung einer hohen IT-Sicherheit werden regelmäßige Wartungsarbeiten und Überprüfungen durchgeführt, um die Aktualität der Firewall sicherzustellen.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen."

Risiken:

Hacking

2.2. Einsatz einer Software-Firewall

Beschreibung:

Auf allen Computern und Servern im System ist eine Sicherheitssoftware installiert, die aus einem Virenschutz und einer personalisierten Firewall besteht. Der Virenschutz wird zentralisiert verwaltet, um eine effektive Überwachung der Aktualität und Aktivität des Virenscanners zu gewährleisten. Dadurch wird eine maximale Kontrolle über die Sicherheit des Systems erreicht.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen."

Risiken:

Hacking

2.3. Einsatz von Anti-Viren-Software

Beschreibung:

Auf allen Computern und Servern im System ist eine Sicherheitssoftware installiert, die aus einem Virenschutz und einer personalisierten Firewall besteht. Der Virenschutz wird zentralisiert verwaltet, um eine effektive Überwachung der Aktualität und Aktivität des Virenscanners zu gewährleisten. Dadurch wird eine maximale Kontrolle über die Sicherheit des Systems erreicht.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen."

Risiken:

Hacking, Trojaner, Viren, Ransomware

2.4. Einsatz von VPN-Technologie

Beschreibung:

Die Filialen sind über LIC+ Leitungen miteinander verbunden und bilden das interne Firmennetzwerk. Der Zugriff von außerhalb auf das Netzwerk wird durch eine redundante Firewall geregelt, die auch ein VPN Gateway zur Verfügung stellt. So können sich Mitarbeiter mit Firmenlaptops über einen VPN-Tunnel sicher mit dem Netzwerk verbinden. Die VPN-Technologie ermöglicht eine verschlüsselte Verbindung zwischen dem Remote-Standort und dem internen Netzwerk, was die Datensicherheit erhöht und Remote-Arbeit erleichtert.

Risiken:

Nutzung von Unbefugten, Hacking

2.5. Erstellen von Benutzerprofilen

Beschreibung:

Alle Benutzer, die IT-Technologie nutzen, werden über das interne Ticketsystem gemeldet und erhalten ein individuelles Benutzerprofil. Die Erstellung der Benutzerprofile erfolgt nach den Vorgaben des Mitarbeiteranmeldeprozesses und wird ausschließlich unter dem Vier-Augen-Prinzip durchgeführt, um die Sicherheit und Integrität des Systems zu gewährleisten.

Risiken:

Nutzung von Unbefugten

2.6. Passwortvergabe

Beschreibung:

Die Vergabe der Passwörter erfolgt unter strikter Berücksichtigung der geltenden Passwortrichtlinie, welche strenge Kriterien für die Passwortkomplexität und -länge vorsieht. Die Benutzer werden aktiv aufgefordert, ihr Passwort nach Erhalt unverzüglich zu ändern und es auf ein individuelles, nur ihnen bekanntes Passwort zu setzen, um die Sicherheit des IT-Systems zu erhöhen.

Risiken:

Nutzung von Unbefugten

Verhaltensregeln:

Die Passwortrichtlinie ist Teil der ÖWD IT-Richtlinie (Absatz 4.6. Kennwortschutz):
Punkt 20
Alle Kennwörter müssen folgende Voraussetzungen erfüllen:
• Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen.
• Jedes Passwort darf nicht länger als 60 Tage verwendet werden.
• Das Kennwort muss mindestens sechs Zeichen lang sein.
• Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten:
- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Zahlen zur Basis 10 (0 bis 9)
- Nicht alphabetische Zeichen (zum Beispiel: !, $, #, %)
Punkt 21:
Jeder Rechner muss sich nach maximal 15 Minuten Untätigkeit automatisch in den Sperrzustand versetzen und bei Reaktivierung ein Kennwort verlangen. Für Telefone und Tablets gilt eine maximale Dauer von einer Minute Untätigkeit.
Punkt 22:
Die Weitergabe oder unverschlüsselte Aufbewahrung der Passwörter von persönlichen Zugängen ist untersagt!

2.7. Verschlüsselung von Datenträgern in Laptops / Notebooks

Beschreibung:

Geräte, die von der IT-Abteilung verwaltet werden, wie Unternehmenslaptops, sind durch TrueCrypt oder BitLocker verschlüsselt, um eine erhöhte Datensicherheit zu gewährleisten. Die Verschlüsselung wird bei jedem Start des Geräts im Unternehmensnetzwerk automatisch überprüft und eventuelle Abweichungen werden gemeldet. Dadurch wird sichergestellt, dass die Verschlüsselung jederzeit ordnungsgemäß funktioniert und das Unternehmensnetzwerk vor unautorisiertem Zugriff geschützt ist.

Im Rahmen der internen IT-Richtlinie ist festgelegt, dass sämtliche Mobiltelefone und andere mobile Datenträger, welche zur Verwendung im Unternehmensnetzwerk zugelassen sind, durch eine Verschlüsselung geschützt werden müssen. Dadurch soll verhindert werden, dass bei Verlust oder Diebstahl der Geräte auf sensible Unternehmensdaten zugegriffen werden kann. Die Verschlüsselungstechnologie wird zentral vorgegeben und ist durch regelmäßige Überprüfungen und Aktualisierungen stets auf dem neuesten Stand.

Risiken:

Nutzung von Unbefugten bei Verlust

2.8. Verschlüsselung von mobilen Datenträgern

Beschreibung:

Die Mitarbeiter sind laut IT Richtlinie dazu verpflichtet alle mobilen Datenträger auf denen sich Unternehmensdaten befinden zu verschlüsseln.

Risiken:

Nutzung von Unbefugten bei Verlust

2.9. Verschlüsselung von Smartphone-Inhalten

Beschreibung:

Im Rahmen der internen IT-Richtlinie ist festgelegt, dass sämtliche Mobiltelefone und andere mobile Datenträger, welche zur Verwendung im Unternehmensnetzwerk zugelassen sind, durch eine Verschlüsselung geschützt werden müssen. Dadurch

soll verhindert werden, dass bei Verlust oder Diebstahl der Geräte auf sensible Unternehmensdaten zugegriffen werden kann. Die Verschlüsselungstechnologie wird zentral vorgegeben und ist durch regelmäßige Überprüfungen und Aktualisierungen stets auf dem neuesten Stand.

Risiken:

Nutzung von Unbefugten bei Verlust

2.10. Zuordnung von Benutzerprofilen zu IT-Systemen

Beschreibung:

Die Zuordnung der Benutzerprofile zu den IT-Systemen erfolgt unter dem vier Augen Prinzip. Soweit möglich erfolgt die Anmeldung an den IT-Systemen über SSo (Single Sign on) was nicht nur eine Zeitersparnis darstellt, da nur noch eine einzige Authentifizierung notwendig ist, sondern auch einen Sicherheitsgewinn darstellt, da das Passwort nur einmal übertragen werden muss und da sich der Nutzer anstelle einer Vielzahl meist unsicherer Passwörter nur noch eines merken muss, somit kann dieses eine Passwort dafür komplex und sicher gewählt werden. Auch Phishing-Attacken werden erschwert, da Benutzer UserID und Passwort nur an einer einzigen Stelle eingeben müssen und nicht mehr an zahlreichen, verstreuten Stellen. Diese eine Stelle kann leichter auf Korrektheit (URL, SSL-Serverzertifikat, etc.) überprüft werden.

Risiken:

Nutzung von Unbefugten

2.11. Zuordnung von Benutzerrechten

Beschreibung:

Die Vergabe von Benutzerrechten wird unter Anwendung des Vier-Augen-Prinzips durchgeführt, um maximale Sicherheit zu gewährleisten. Die Zuweisung von Benutzerrechten erfolgt sowohl im Active Directory als auch in den einzelnen Anwendungen durch die Verwendung von Berechtigungsgruppen, die standardisierte und rollenbasierte Zugriffsrechte gewährleisten. Die Verwendung von Berechtigungsgruppen ermöglicht eine einfachere und effektivere Verwaltung der Zugriffsrechte, wodurch das Sicherheitsrisiko bei der Verwaltung von Benutzerrechten verringert wird.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt. Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:

Nutzung von Unbefugten

3. Zugriffskontrolle

3.1. Anzahl der Administratoren auf das „Notwendigste“ reduziert

Beschreibung:

Die Anzahl der Administratoren ist bewusst beschränkt, um das Risiko von Fehlern oder böswilligen Handlungen zu minimieren. Jeder Administrator wird sorgfältig ausgewählt und erhält nur die Rechte, die für die Erfüllung seiner spezifischen Aufgaben erforderlich sind. Durch diese gezielte Einschränkung von Berechtigungen wird sichergestellt, dass nur autorisierte Personen auf vertrauliche Daten oder kritische Systeme zugreifen können. Dadurch wird das Sicherheitsniveau erhöht und die Gefahr von unbefugten Zugriffen oder Systemausfällen verringert.

Domänenadministratoren haben separate Konten für ihre normalen Benutzeraktivitäten und privilegierten Aufgaben. Auf

diese Weise wird eine Trennung der Berechtigungen sichergestellt und das tägliche Arbeiten sicherer gemacht. Wenn ein Administrator eine privilegierte Aufgabe ausführen muss, muss er sich mit seinem separaten Administratorkonto anmelden, um auf die erforderlichen Funktionen zugreifen zu können. Diese Vorgehensweise reduziert das Risiko, dass ein Angreifer durch eine Kompromittierung des normalen Benutzerkontos auch auf die privilegierten Funktionen zugreifen kann.

Risiken:

Datenzugriff von Unbefugten

3.2. Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

Beschreibung:

Für jeden Standort wurde ein individuelles Abfallwirtschaftskonzept erstellt und ein Abfallbeauftragter bestellt. Dieser ist für die Umsetzung des Abfallmanagements verantwortlich. Der Prozess des Abfallmanagements beinhaltet auch die Vernichtung von Akten. Hierbei kommen entweder Aktenvernichter zum Einsatz oder die zertifizierte Vernichtung durch externe Dienstleister wird durchgeführt. Auf diese Weise wird sichergestellt, dass sensible Informationen und Daten ordnungsgemäß und sicher vernichtet werden.

Digitale Daten auf Datenträgern werden ebenfalls entsprechend behandelt und durch zertifizierte Dienstleister vernichtet, um sicherzustellen, dass alle vertraulichen Informationen ordnungsgemäß und dauerhaft gelöscht werden.

Risiken:

Datenzugriff von Unbefugten

3.3. Erstellen eines Berechtigungskonzepts

Beschreibung:

Die Verwaltung der Benutzer erfolgt nach dem A-G-G-P-Prinzip des Microsoft Active Directory Standards. Dabei wird jeder Benutzer einem Account zugewiesen und in globalen oder universellen Domänengruppen zusammengefasst, beispielsweise alle Mitarbeiter aus Wien in einer Gruppe. Für die Vergabe von Berechtigungen im Filesystem wird eine globale Gruppe genutzt, die entweder die globale Gruppe oder im Ausnahmefall auch einzelne Benutzer enthält. Die Vergabe von Berechtigungen in den eingesetzten Anwendungen wird ebenfalls verwaltet. Dabei wird darauf geachtet, Berechtigungsgruppen zu verwenden und Einzelberechtigungen zu vermeiden, um Fehler zu vermeiden und die Administration zu vereinfachen. Die Vergabe von Berechtigungen erfolgt stets nach dem Vier-Augen-Prinzip, um Missbrauch zu verhindern.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt,
die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.
Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und
ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:

Datenzugriff von Unbefugten

3.4. Meldepflicht

Beschreibung:

Es müssen gestohlene oder verloren gegangene Geräte unverzüglich an den ISB, die IT-Abteilung und das Sekretariat der Geschäftsführung gemeldet werden. Wenn ein Benutzer vermutet, dass unbefugte Personen auf Unternehmensdaten zugreifen, muss er dies entsprechend den Meldevorschriften dem ISB und der IT-Abteilung melden.

IT Richtlinien

"Abhanden gekommene oder gestohlene Geräte müssen dem ISB, der IT-Abteilung und dem Sekretariat der GD umgehend am folgenden Werktag gemeldet werden."
"Vermutet ein User, dass ein unbefugter Zugriff über Mobilgeräte auf Unternehmensdaten erfolgt ist, muss er dies der IT-Abteilung in Einklang mit Melderichtlinien des ÖWD mitteilen."

3.5. ordnungsgemäße Vernichtung von Datenträgern

Beschreibung:

Es wurde ein Abfallwirtschaftskonzept pro Standort erstellt und ein Abfallbeauftragter benannt. Das Abfallmanagement regelt den Prozess der Vernichtung, einschließlich der Vernichtung von digitalen Datenträgern. Diese werden gemäß Vernichtungsstufe v5 zertifiziert entsorgt.

Risiken:

Datenzugriff von Unbefugten

3.6. Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

Beschreibung:

Die Passwortrichtlinie ist ein Bestandteil der IT-Richtlinie und enthält unter dem Punkt "Kennwortschutz" Vorschriften bezüglich des Umgangs mit Passwörtern, einschließlich ihrer Komplexität, des Ablaufdatums und des Aussehens.

Risiken:

Datenzugriff von Unbefugten

Verhaltensregeln:

20. Alle Kennwörter müssen folgende Voraussetzungen erfüllen:
• Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen.
• Jedes Passwort darf nicht länger als 60 Tage verwendet werden.
• Das Kennwort muss mindestens sechs Zeichen lang sein.
• Das Kennwort muss Zeichen aus drei der folgenden Kategorien enthalten:
- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Zahlen zur Basis 10 (0 bis 9)
- Nicht alphabetische Zeichen (zum Beispiel: !, $, #, %)

Ausgenommen von der Kennwortrichtlinie sind Geräte welche die technischen Voraussetzungen für die Verwendung sicherer Passwörter nicht erfüllen, wie einfache Telefone. Bei diesen Geräten ist der höchstmögliche technische Schutz zu verwenden (z.B.: vierstelliger PIN).

21. Jeder Rechner muss sich nach maximal 15 Minuten Untätigkeit automatisch in den Sperrzustand versetzen und bei Reaktivierung ein Kennwort verlangen. Für Telefone und Tablets gilt eine maximale Dauer von einer Minute Untätigkeit.

22. Die Weitergabe oder unverschlüsselte Aufbewahrung der Passwörter von persönlichen Zugängen ist untersagt!

3.7. physische Löschung von Datenträgern vor Wiederverwendung

Beschreibung:

Datenträger werden ausschließlich innerhalb des Unternehmens wiederverwendet und niemals an externe Stellen weitergegeben. Bevor ein Datenträger intern weitergegeben wird, wird er sicher gelöscht, um sicherzustellen, dass keine vertraulichen Daten darauf verbleiben.

Risiken:

Datenzugriff von Unbefugten

3.8. Protokollierung der Vernichtung

Beschreibung:

Gemäß der ISO PB_Abfallmanagement_5.00 müssen alle Belege der Vernichtung an eine zentrale Stelle weitergeleitet werden. Nach der Erfassung werden die Belege einschließlich aller Anhänge wie Lieferscheine, Begleitscheine, Zertifikate usw. vom zuständigen Abfallmanagementbeauftragten aufbewahrt.

Risiken:

Datenzugriff von Unbefugten

3.9. Sichere Aufbewahrung von Datenträgern

Beschreibung:

Es ist strengstens untersagt, Firmendaten auf externen Datenspeichern zu speichern, einschließlich Cloud-Drives und ähnlicher Technologien. Ausnahmen bilden lediglich Microsoft Kollaborationstools, die von der IT-Abteilung bereitgestellt werden.
Datenträger, die für die Vernichtung vorgesehen sind, werden in speziell dafür vorgesehenen Behältnissen gesammelt und in einem abgeschlossenen Bereich aufbewahrt, der nur befugtem Personal zugänglich ist.
Datenträger, die zum Zweck der Datensicherung gelagert werden, befinden sich in einem feuerfesten Safe, der ebenfalls in einem abgeschlossenen Bereich aufbewahrt wird, der nur befugtem Personal zugänglich ist.
Datenträger, die sich im Einsatz befinden, werden ständig automatisiert überwacht, um Veränderungen, Tausch oder Diebstahl zu verhindern.

Risiken:

Datenzugriff von Unbefugten

3.10. Verbesserung der Sicherheit

Beschreibung:

Die Wirksamkeit und Aktualität der Informationssicherheitsmaßnahmen werden in regelmäßigen Abständen überprüft. Zusätzlich erfolgt eine regelmäßige Prüfung der Kenntnisse der betroffenen Mitarbeiter bezüglich der Maßnahmen und deren Umsetzbarkeit sowie Integration in den Betriebsablauf.

Auszug aus der LEITLINIE ZUR INFORMATIONSSICHERHEIT DER ÖWD SECURITY & SERVICES:

Die Leitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben. Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheit und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

3.11. Verschlüsselung von Datenträgern

Beschreibung:

Die IT-Abteilung sorgt dafür, dass Arbeitsplatzrechner sowie Laptops (Notebooks) standardisiert und professionell konfiguriert werden, um eine sichere Authentisierung und Anmeldung der Benutzer zu gewährleisten. Hierbei wird insbesondere darauf geachtet, dass eine Verschlüsselung mittels des Programms "Bitlocker" implementiert wird. Darüber hinaus wird die Installation von Updates und Patches zentral gesteuert, um sicherzustellen, dass die Systeme immer auf dem neuesten Stand sind und bekannte Sicherheitslücken geschlossen werden. Es ist dabei untersagt, dass die Mitarbeiter individuelle

Installationen von Anwendungen auf ihren Geräten vornehmen. Dies dient dazu, die Integrität des Systems zu wahren und unerwünschte Anwendungen oder Programme fernzuhalten, die möglicherweise Schwachstellen aufweisen oder unbefugt auf Unternehmensdaten zugreifen können.

Risiken:

Datenzugriff von Unbefugten bei Verlust

3.12. Verwaltung der Rechte durch Systemadministrator

Beschreibung:

Die Vergabe und Verwaltung von IT-Berechtigungen erfolgt ausschließlich durch geschulte Systemadministratoren. Dies dient der Sicherstellung der ordnungsgemäßen Vergabe von Berechtigungen und der Verhinderung von unbefugtem Zugriff auf Systemressourcen. Systemadministratoren sind mit den IT-Richtlinien und den relevanten rechtlichen Anforderungen vertraut und verfügen über das notwendige Fachwissen und die Erfahrung, um eine effektive Vergabe und Verwaltung von IT-Berechtigungen sicherzustellen. Die Vergabe von IT-Berechtigungen erfolgt in der Regel auf der Grundlage von Nutzeranforderungen und wird regelmäßig überprüft, um sicherzustellen, dass sie den aktuellen Geschäftsanforderungen entsprechen.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt. Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:

Datenzugriff von Unbefugten

3.13. Zugriff auf Firmenrechner

Beschreibung:

Der Zugriff auf Unternehmensdaten von externen Standorten aus erfolgt ausschließlich über eine Virtual Private Network (VPN) Verbindung. Diese Technologie gewährleistet einen sicheren, kontrollierten und verschlüsselten Zugriff auf die Daten und Anwendungen des Unternehmens. Alle anderen Zugriffe, insbesondere unverschlüsselte, sind strikt untersagt. Diese Regelungen sind in den IT-Richtlinien des Unternehmens detailliert festgehalten und sind allen Mitarbeitern bekannt.

Der Zugriff auf Firmenrechner erfolgt über das Domänennetzwerk, welches von Microsoft Active Directory (AD) geregelt wird. Durch sichere Passwörter, die den Vorgaben der Passwortrichtlinie entsprechen, wird der Zugriff auf die Firmenrechner kontrolliert und eingeschränkt. Jeder Mitarbeiter besitzt ein eigenes Konto, um einen individuellen Zugriff auf die benötigten Ressourcen zu gewährleisten. So wird gewährleistet, dass jeder Mitarbeiter nur auf die ihm zugewiesenen Ressourcen zugreifen kann und kein unbefugter Zugriff auf Firmendaten stattfindet.

4. Weitergabekontrolle

4.1. Beim physischen Transport: sichere Transportbehälter/-verpackungen

Beschreibung:

Der Österreichische Wachdienst (ÖWD) ist auf den sicheren physischen Transport von Gütern spezialisiert. Dabei ist es von höchster Wichtigkeit, dass die Güter sicher und zeitgerecht von A nach B gelangen. Hierfür setzt der ÖWD auf Transportbehälter und Transportverpackungen, die speziell für den sicheren Transport von Gütern ausgelegt sind. Diese Verpackungen bieten ein hohes Maß an Schutz vor äußeren Einflüssen wie Stößen, Erschütterungen oder Feuchtigkeit, um die Güter unbeschadet ans Ziel zu bringen.

Sofern der Transport von externen Dienstleistern durchgeführt wird, setzt der ÖWD auf Identifikationsnummern zur Nachvollziehbarkeit und Transparenz des Transportprozesses. Dadurch ist jederzeit gewährleistet, dass die Güter den Anforderungen entsprechend transportiert werden. Um eine hohe Qualität und Sicherheit im Transportprozess sicherzustellen, werden regelmäßige Überprüfungen durchgeführt und gegebenenfalls Optimierungen vorgenommen. Der ÖWD stellt sicher, dass die geltenden gesetzlichen Vorgaben sowie die internen Richtlinien und Standards bei jedem Transport eingehalten werden.

Risiken:

Dateneinsicht durch Dritte bei Verlust

4.2. Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

Beschreibung:

Der sichere physische Transport von Gütern ist ein zentrales Geschäftsfeld des ÖWD. Um sicherzustellen, dass die Güter sicher, zeitgerecht und unbeschädigt von A nach B transportiert werden, ist es entscheidend, vertrauenswürdige Mitarbeiter auszuwählen und zu schulen. Diese Maßnahmen sind auch in der Gewerbeordnung verankert.

Es ist wichtig, dass die Mitarbeiter des ÖWD in der Lage sind, sicher und zuverlässig mit den Gütern umzugehen, die ihnen anvertraut wurden. Um sicherzustellen, dass diese Standards eingehalten werden, werden regelmäßig Schulungen angeboten.

§ 130 GewO 1994 Rechte und Pflichten der Berufsdetektive und Bewacher

(3) Gewerbetreibende, die zur Ausübung des Bewachungsgewerbes berechtigt sind, sind auch zur Fahrzeug- und Transportbegleitung berechtigt.
...
(8) Die zur Ausübung des Gewerbes der Berufsdetektive sowie die zur Ausübung des Bewachungsgewerbes berechtigten Gewerbetreibenden dürfen zur Ausübung der ihren Gewerben vorbehaltenen Tätigkeiten (§ 129 Abs. 1 bzw. Abs. 4) nur Arbeitnehmer verwenden, die eigenberechtigt sind und die für diese Verwendung erforderliche Zuverlässigkeit und Eignung besitzen.
(9) Die im Abs. 8 genannten Gewerbetreibenden sind verpflichtet, der Bezirksverwaltungsbehörde, im Gebiet einer Gemeinde, für das die Landespolizeidirektion zugleich Sicherheitsbehörde erster Instanz ist, der Landespolizeidirektion, als Sicherheitsbehörde ein Verzeichnis aller Personen, die für eine der im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogen werden, spätestens zwei Wochen vor dem Beginn ihrer Verwendung vorzulegen; jede Änderung hinsichtlich der für die im § 129 Abs. 1 bzw. Abs. 4 genannten Tätigkeiten herangezogenen Personen ist dieser Behörde binnen zwei Wochen anzuzeigen. Das Verzeichnis oder die Anzeigen von Änderungen dieses Verzeichnisses haben neben dem Vor- und Familiennamen der betreffenden Person auch deren Geburtsdatum, Geburtsort, Staatsangehörigkeit und Unterkunft (Wohnung) zu enthalten.
(10) Ist auf Grund bestimmter Tatsachen die Zuverlässigkeit einer gemäß Abs. 9 bekannt gegebenen Person nicht gegeben, so hat die Sicherheitsbehörde dem Gewerbetreibenden ohne unnötigen Aufschub schriftlich mitzuteilen, dass der Betroffene die erforderliche Zuverlässigkeit nicht besitzt.

Risiken:

Dateneinsicht durch Dritte

4.3. Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

Beschreibung:

Um die Dokumentation der Empfänger von Daten sowie die geplanten Überlassungszeiträume und Löschfristen von Daten sicherzustellen, schließt unser Unternehmen Geheimhaltungsvereinbarungen mit externen Empfängern ab. Hierbei wird streng darauf geachtet, dass alle Sicherheitsstandards eingehalten werden. Unsere Outsourcing-Leitlinie dient dazu, Entscheidungsträger bei der Einhaltung unserer hohen Sicherheitsstandards zu unterstützen. Diese Sicherheitsleitlinie gilt für alle Betriebsteile und muss bei der Konzeption von Outsourcing-Vorhaben berücksichtigt werden, die

Informationsverarbeitung betreffen. Vor jeder Outsourcing-Entscheidung werden bereits Sicherheitsaspekte berücksichtigt und bei der Ausschreibung entsprechend einbezogen. Unsere Leitlinie dient als Prüfungsgrundlage gegenüber dem Outsourcing-Dienstleister und ist den Verträgen mit Dienstleistern zugrunde zu legen.

Risiken:

Dateneinsicht durch Dritte

4.4. E-Mail-Verschlüsselung

Beschreibung:

Die Sicherheit und Vertraulichkeit der internen Unternehmenskommunikation via Mail hat für jedes Unternehmen höchste Priorität. Um diese zu gewährleisten, wurden alle Exchange-Server entsprechend konfiguriert. So ist standardmäßig sichergestellt, dass alle internen Clients eine Verschlüsselung einfordern. Dadurch wird eine verschlüsselte Übertragung von E-Mails im Unternehmensnetzwerk erreicht und unerlaubte Zugriffe von außen verhindert. Die geltende IT-Richtlinie sieht vor, dass vertrauliche oder geheime Inhalte und Dokumente nur verschlüsselt via Mail an unternehmensexterne E-Mailkonten versandt werden dürfen. Dabei gilt es auch zu beachten, dass das Verbot automatisierter Weiterleitungen von E-Mails an externe Konten oder private mobile Geräte besteht. Ein solches Verhalten könnte die Sicherheit der Unternehmenskommunikation gefährden und ist daher strikt untersagt.

Für die externe Kommunikation bietet unser Unternehmen verschiedene Möglichkeiten, um eine sichere Übertragung von Daten und Informationen zu gewährleisten. Dabei wurden zwei Standard-Protokolle für verschlüsselte E-Mail-Kommunikation etabliert: S/MIME und OpenPGP.
S/MIME (Secure/Multipurpose Internet Mail Extensions) ist ein Verschlüsselungsprotokoll, das digitale Signaturen und Verschlüsselung von E-Mails ermöglicht. Dabei wird eine digitale Signatur verwendet, um die Authentizität des Absenders zu überprüfen und eine verschlüsselte Verbindung zwischen Sender und Empfänger aufzubauen. Die Verschlüsselung erfolgt dabei auf der Client-Seite, das heißt der Absender verschlüsselt die E-Mail mit einem privaten Schlüssel und der Empfänger kann die E-Mail nur mit dem entsprechenden öffentlichen Schlüssel entschlüsseln.
OpenPGP (Pretty Good Privacy) ist ein weiteres Verschlüsselungsprotokoll, das auf asymmetrischer Verschlüsselung basiert und eine Ende-zu-Ende-Verschlüsselung von E-Mails ermöglicht. Dabei wird eine Kombination aus privatem und öffentlichem Schlüssel verwendet, um eine sichere Übertragung von Daten zu gewährleisten. Die Verschlüsselung erfolgt dabei ebenfalls auf der Client-Seite und ermöglicht es dem Empfänger, die E-Mail nur mit dem entsprechenden privaten Schlüssel zu entschlüsseln.
Durch die Verwendung dieser beiden Standard-Protokolle wird eine sichere und verschlüsselte Kommunikation zwischen unserem Unternehmen und externen Partnern gewährleistet.

Risiken:

Dateneinsicht durch Dritte

4.5. Einrichtungen von Standleitungen bzw. VPN-Tunneln

Beschreibung:

Das interne Firmennetzwerk wird durch LIC+ Leitungen verbunden, wodurch alle Filialen miteinander kommunizieren können. Um den Zugriff auf das Firmennetzwerk von außen zu regeln, ist eine redundante Firewall implementiert, die auch ein VPN Gateway bereitstellt. Auf diese Weise ist es möglich, sichere Verbindungen zum Firmennetzwerk von Firmenlaptops aus aufzubauen, indem ein VPN-Tunnel genutzt wird. Die Firewall bietet zusätzliche Sicherheit, indem sie den Datenverkehr auf unerwünschte oder unsichere Zugriffsversuche überwacht und blockiert. Das VPN-Gateway ermöglicht autorisierten Benutzern den Zugriff auf das Netzwerk von außerhalb der Firmenumgebung, während eine Zwei-Faktor-Authentifizierung sicherstellt, dass nur autorisierte Benutzer auf die Terminalserver des Unternehmens zugreifen können. Die redundante Auslegung der Firewall und des VPN Gateways stellt sicher, dass die Verbindungen zum Firmennetzwerk jederzeit verfügbar und geschützt sind.

Risiken:

Dateneinsicht durch Dritte

4.6. Kopieren von Dateien

Beschreibung:

Das unbefugte Kopieren von Dateien zum Zwecke der Heimarbeit oder zu privaten Zwecken ist gemäß den IT-Richtlinien des Unternehmens strikt untersagt. Das Abspeichern von Firmendaten auf externen Datenspeichern, einschließlich Cloud-Speicher und ähnlicher Technologien, ist ebenfalls ausdrücklich verboten. Diese Maßnahme dient dazu, die Sicherheit und Integrität der Firmendaten zu schützen und unbefugten Zugriff auf vertrauliche Informationen zu verhindern.

5. Eingabekontrolle

5.1. Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Beschreibung:

Um die Nachvollziehbarkeit von Aktivitäten auf den IT-Systemen sicherzustellen, wird jedem neuen Benutzer ein persönlicher IT-Account mit individuellem Passwort zugewiesen. Um den Zugriff auf das Unternehmensnetzwerk sicher und konsistent zu gestalten, wird der IT-Account für jeden neuen Benutzer im Rahmen des Mitarbeitermeldeprozesses angelegt. Die zentrale Verwaltung des Zugriffs auf das Netzwerk erfolgt über den Active Directory (AD) von Microsoft. Durch die Verwendung des AD wird sichergestellt, dass alle Benutzeridentitäten konsistent und sicher verwaltet werden.

Für den Zugriff auf bestimmte Programme innerhalb des Netzwerks werden oft eigene Benutzeraccounts erstellt. Der Einstieg in diese Programme erfolgt in der Regel über eine Single-Sign-On (SSO) Authentifizierung, die es den Benutzern ermöglicht, sich nur einmal mit ihrem IT-Account anzumelden und dann auf verschiedene Programme und Dienste innerhalb des Netzwerks zuzugreifen. Dadurch wird nicht nur die Sicherheit erhöht, sondern auch die Benutzerfreundlichkeit verbessert.

Die Zuweisung von IT-Accounts und die Verwendung von Passwörtern sind wichtige Bestandteile des Identitäts- und Zugriffsmanagements, um sicherzustellen, dass nur autorisierte Benutzer auf IT-Systeme zugreifen und Aktivitäten nachvollziehbar sind.

Risiken:

Verfälschung von Daten, Datenverlust

5.2. Protokollierung der Eingabe, Änderung und Löschung von Daten

Beschreibung:

Die Verwendung von Systemen, die die Protokollierung von Aktivitäten in Logfiles ermöglichen, ist Standard. Dadurch können alle Aktionen von Benutzern auf den IT-Systemen verfolgt und bei Bedarf nachvollzogen werden. Diese Protokollierungsdaten können auch zur Erkennung von Sicherheitsverletzungen oder Fehlern in der Systemkonfiguration verwendet werden. Die Logfiles werden in der Regel regelmäßig gesichert und archiviert, um eine spätere Analyse zu ermöglichen. Durch die individuellen Benutzerkonten und die Protokollierung von Aktivitäten kann eine angemessene Datensicherheit und -integrität gewährleistet werden.

Risiken:

Verfälschung von Daten, unberechtigter Zugriff

5.3. Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

Beschreibung:

Um die Sicherheit und Integrität des IT-Systems des Unternehmens zu gewährleisten, sind die Vergabe von Zugriffsrechten für jeden Benutzer genau geregelt und vorwiegend in Rechtegruppen organisiert. Die Vergabe von Zugriffsrechten ist ein Teil

des zentralen Mitarbeitermeldeprozesses und erfolgt immer im Vier-Augen-Prinzip. Jeder Mitarbeiter erhält nur die Zugangsrechte, die für die Erfüllung seiner Aufgaben im Unternehmen notwendig sind, um den unbefugten Zugriff auf sensible Unternehmensdaten zu verhindern. Zusätzlich werden auch die Rechte zur Eingabe, Änderung und Löschung von Daten durch Software-Accounts geregelt, um die Nachvollziehbarkeit und Kontrolle der Datenzugriffe zu gewährleisten.

Auszug aus der ÖWD Leitlinie zur Informationssicherheit:
"Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.
Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können."

Risiken:

Verfälschung von Daten, Datenverlust

6. Auftragskontrolle

6.1. Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Beschreibung:

Das Unternehmen verfügt über eine umfassende Outsourcing-Leitlinie, die spezifische Vorschriften zur Sicherung der Informationssicherheit und des Datenschutzes festlegt, die bei der Auslagerung von IT-Dienstleistungen eingehalten werden müssen. Die Leitlinie enthält detaillierte Anweisungen zur Auswahl und Überwachung von Drittanbietern sowie zur Erfüllung rechtlicher und behördlicher Anforderungen. Darüber hinaus wird bei der Auswahl von Outsourcing-Partnern ein besonderes Augenmerk auf deren Sicherheitsstandards und deren Fähigkeit zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten gelegt. Die Leitlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Sicherheits- und Datenschutzbestimmungen entspricht.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.1. Auswahl eines Outsourcing- Dienstleisters

Es ist selten erfolgversprechend, eine Geschäftsbeziehung lediglich auf Verträge und Regressansprüche zu begründen. Daher ist der Outsourcing-Dienstleister sorgfältig auszuwählen und eine vertrauensvolle und kooperative Zusammenarbeit anzustreben.
Bei der Auswahl ist zu prüfen, ob der Auftragnehmer als makellos, unbescholten und unbestechlich einzuschätzen ist (Zuverlässigkeit) und ob ein ernsthaftes und fachkundiges Betreiben der Dienstleistung gewährleistet ist (Seriosität).

Zu diesem Zweck sind folgende Punkte zu hinterfragen:
• Referenzen
• Kompetenz und Verfügbarkeit des Ansprechpartners
• Vertrauenswürdigkeit der Mitarbeiter
• Notfallplanung
• Zertifizierungen
• Dauer des Bestehens des Unternehmens
• finanzielle Situation des Unternehmens
• garantierte Verfügbarkeit (maximale Ausfallzeit)
• Sicherheitskonzept und Sicherheitsrichtlinien.
Für die Beurteilung sollte bei größeren Vorhaben eine Besichtigung des Outsourcing-Dienstleisters erfolgen.

Risiken:

Mißbräuchliche Verwendung der Personendaten

6.2. schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag)

Beschreibung:

Das Unternehmen verfügt über eine umfassende Outsourcing-Leitlinie, die spezifische Vorschriften zur Sicherung der Informationssicherheit und des Datenschutzes festlegt, die bei der Auslagerung von IT-Dienstleistungen eingehalten werden müssen. Die Leitlinie enthält detaillierte Anweisungen zur Auswahl und Überwachung von Drittanbietern sowie zur Erfüllung rechtlicher und behördlicher Anforderungen. Darüber hinaus wird bei der Auswahl von Outsourcing-Partnern ein besonderes Augenmerk auf deren Sicherheitsstandards und deren Fähigkeit zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten gelegt. Die Leitlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Sicherheits- und Datenschutzbestimmungen entspricht.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.2. Vertragsspezifische Regelungen

Externen darf generell erst dann Zugang zu IT-Systemen und Anwendungen gewährt werden, wenn ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert.
Im Vertrag ist schriftlich zu vereinbaren:
• Weisungsgebundenheit des Outsourcing-Dienstleisters
• Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen
• Stillschweigen über alle bekanntwerdenden Informationen
• technische und organisatorische Maßnahmen im Einflussbereich des Outsourcing-Dienstleisters und deren Kontrolle
• Melde- und Kommunikationswege
• Notfallvorsorgemaßnahmen
• Personaleinsatz durch den Outsourcing-Dienstleister
• Zutritts- und Zugangsrechte
• Regelungen für den Fall der nicht- oder mangelhaften Erfüllung
• Verfügbarkeitsanforderungen
• Rechte und Pflichten des externen Personals
• Regelungen zur Haftung
• Verfahren bei Beendigung des Vertrags (siehe Kapitel 4.5.5)

Risiken:

Mißbräuchliche Verwendung der Personendaten

6.3. Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Beschreibung:

Das Unternehmen verfügt über eine umfassende Outsourcing-Leitlinie, die spezifische Vorschriften zur Sicherung der Informationssicherheit und des Datenschutzes festlegt, die bei der Auslagerung von IT-Dienstleistungen eingehalten werden müssen. Die Leitlinie enthält detaillierte Anweisungen zur Auswahl und Überwachung von Drittanbietern sowie zur Erfüllung rechtlicher und behördlicher Anforderungen. Darüber hinaus wird bei der Auswahl von Outsourcing-Partnern ein besonderes Augenmerk auf deren Sicherheitsstandards und deren Fähigkeit zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten gelegt. Die Leitlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Sicherheits- und Datenschutzbestimmungen entspricht.

Auszug aus der Outsourcing Leitlinie des ÖWD:

4.5.5 Regelungen zum Ende der Tätigkeiten
Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse und der erhaltenen Unterlagen und Betriebsmittel erfolgen.
Es ist die ordnungsgemäße Funktion von gewarteten IT-Systemen zu überprüfen. Bei entsprechend gefährdeten IT-Systemen ist eine Virenüberprüfung durchzuführen.
Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Außerdem sind ausscheidende Mitarbeiter explizit darauf hinzuweisen, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.
Daten, die im Rahmen des Outsourcings extern gespeichert wurden, sind nach Abschluss des Auftrags vollständig und sicher zu löschen. Dies ist zu kontrollieren.

Risiken:

Mißbräuchliche Verwendung der Personendaten

6.4. Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Beschreibung:

Das Unternehmen verfügt über eine umfassende Outsourcing-Leitlinie, die spezifische Vorschriften zur Sicherung der Informationssicherheit und des Datenschutzes festlegt, die bei der Auslagerung von IT-Dienstleistungen eingehalten werden müssen. Die Leitlinie enthält detaillierte Anweisungen zur Auswahl und Überwachung von Drittanbietern sowie zur Erfüllung rechtlicher und behördlicher Anforderungen. Darüber hinaus wird bei der Auswahl von Outsourcing-Partnern ein besonderes Augenmerk auf deren Sicherheitsstandards und deren Fähigkeit zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten gelegt. Die Leitlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Sicherheits- und Datenschutzbestimmungen entspricht.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.3. Organisation
...
Externe Mitarbeiter sind vor Beginn ihrer Tätigkeit einzuweisen und über hausinterne Regelungen und Vorschriften zur Informationssicherheit sowie die organisationsweite Leitlinie zur Informationssicherheit zu unterrichten.
Externe Mitarbeiter, die (eventuell) Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen und zur Verschwiegenheit zu verpflichten.
...

Risiken:

Mißbräuchliche Verwendung der Personendaten

6.5. Vertragsstrafen bei Verstößen

Beschreibung:

Bei der Zusammenarbeit mit externen Dienstleistern wird jeder Vertrag mit einer Non-Disclosure Agreement (NDA) ergänzt, in welcher auch das Strafmaß bei Verletzung der Vertragsbedingungen festgelegt wird. Dabei werden unter anderem Regelungen zur Geheimhaltung von vertraulichen Informationen und Daten getroffen, um die Vertraulichkeit der Geschäftsbeziehungen zu schützen. Die NDA ist ein wichtiges Instrument zur Sicherstellung des Datenschutzes und der Informationssicherheit bei der Zusammenarbeit mit externen Dienstleistern.

Auszug aus der NDA:
§ 6 Ansprüche aus der Geheimhaltungsvereinbarung

6.1 Sofern ein Vertragspartner diese Geheimhaltungsvereinbarung nachweislich und schuldhaft verletzt, ist er zur Zahlung einer Konventionalstrafe in Höhe von EUR _____ für jeden Fall einer Vertragsverletzung an den jeweils anderen Vertragspartner verpflichtet.
6.2 Diese Pflicht zur Konventionalstrafe nach Punkt 6.1 besteht auch, wenn ein Dritter die Geheimhaltungsvereinbarung nachweislich und schuldhaft verletzt, sofern ihm die Informationen durch einen Vertragspartner zugänglich gemacht wurden.
6.3 Die Geltendmachung darüberhinausgehender Ansprüche bleibt den Vertragspartnern vorbehalten.

Risiken:

Mißbräuchliche Verwendung der Personendaten

6.6. vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Beschreibung:

Das Unternehmen verfügt über eine umfassende Outsourcing-Leitlinie, die spezifische Vorschriften zur Sicherung der Informationssicherheit und des Datenschutzes festlegt, die bei der Auslagerung von IT-Dienstleistungen eingehalten werden müssen. Die Leitlinie enthält detaillierte Anweisungen zur Auswahl und Überwachung von Drittanbietern sowie zur Erfüllung rechtlicher und behördlicher Anforderungen. Darüber hinaus wird bei der Auswahl von Outsourcing-Partnern ein besonderes Augenmerk auf deren Sicherheitsstandards und deren Fähigkeit zur Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmensdaten gelegt. Die Leitlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Sicherheits- und Datenschutzbestimmungen entspricht.

Auszug aus der Outsourcing Leitlinie des ÖWD:
4.2. Vertragsspezifische Regelungen

Externen darf generell erst dann Zugang zu IT-Systemen und Anwendungen gewährt werden, wenn ein Vertrag unterschrieben wurde, der die Bedingungen für die Verbindung oder den Zugang definiert.
Im Vertrag ist schriftlich zu vereinbaren:
• Weisungsgebundenheit des Outsourcing-Dienstleisters
• Einhaltung der einschlägigen Gesetze, Vorschriften und internen Regelungen
• Stillschweigen über alle bekanntwerdenden Informationen
• technische und organisatorische Maßnahmen im Einflussbereich des Outsourcing-Dienstleisters und deren Kontrolle
• Melde- und Kommunikationswege
• Notfallvorsorgemaßnahmen
• Personaleinsatz durch den Outsourcing-Dienstleister
• Zutritts- und Zugangsrechte
• Regelungen für den Fall der nicht- oder mangelhaften Erfüllung
• Verfügbarkeitsanforderungen
• Rechte und Pflichten des externen Personals
• Regelungen zur Haftung
• Verfahren bei Beendigung des Vertrags (siehe Kapitel 4.5.5)

Risiken:

Mißbräuchliche Verwendung der Personendaten

7. Verfügbarkeitskontrolle

7.1. Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Beschreibung:

Das Unternehmen setzt moderne Backup-Strategien ein, um die Verfügbarkeit und Integrität seiner Daten sicherzustellen. Dabei wird das sogenannte 3-2-1-Backup-Prinzip angewendet, welches besagt, dass drei Kopien der Daten auf zwei verschiedenen Medien gespeichert werden sollten, wovon eine Kopie an einem externen Ort aufbewahrt werden sollte.

Um die Backup-Prozesse zu optimieren und eine schnelle Wiederherstellung im Ernstfall zu gewährleisten, werden verschiedene Technologien eingesetzt. So erfolgt das Backup beispielsweise auf Festplatten (Disk-to-Disk-Backup) und zusätzlich auf Bänder (Disk-to-Tape-Backup). Dadurch wird eine hohe Geschwindigkeit beim Backup erreicht und eine lange Aufbewahrungszeit durch die Band-Speicherung ermöglicht.

Die Backup-Prozesse werden regelmäßig getestet und optimiert, um eine hohe Zuverlässigkeit und Verfügbarkeit der Daten zu gewährleisten. Zudem werden auch automatisierte Backup-Pläne genutzt, um sicherzustellen, dass alle Daten regelmäßig und zuverlässig gesichert werden.

Risiken:

Datenverlust

7.2. Feuer- und Rauchmeldeanlagen

Beschreibung:

Das Unternehmen legt großen Wert auf den vorbeugenden Brandschutz und hat deshalb in allen Gebäuden behördlich vorgeschriebene Brandmeldeanlagen nach ÖNORM F1000 installiert, die den Anforderungen des Feuerwehr- und Brandschutzwesens entsprechen. Zudem werden die technischen Richtlinien TRVB O 120, TRVB S114, TRVB N116 und TRVB N 106 strikt eingehalten.

Um im Brandfall effektiv handeln zu können, hat das Unternehmen eine Brandschutzordnung erstellt. Diese Brandschutzordnung regelt Zuständigkeiten, gibt Verhaltensregeln vor, während und nach einem Brandfall vor und enthält detaillierte Evakuierungspläne sowie Informationen zu Sammelplätzen und Fluchtwege. Das Ziel ist es, im Ernstfall schnell und sicher reagieren zu können und die Sicherheit aller Personen und auch Daten im Gebäude zu gewährleisten.

Risiken:

Datenverlust

7.3. Feuerlöschgeräte in Serverräumen

Beschreibung:

In den Rechenzentren Salzburg und Wien sind Feuerlöscher nach den behördlichen Vorschriften und Normen vorhanden. Die Standorte der Feuerlöscher sind gut sichtbar gekennzeichnet und jederzeit leicht zugänglich. Zudem wurden bei der Auswahl der Feuerlöscher deren Verträglichkeit mit den IT-Systemen berücksichtigt, um im Falle eines Brandes Schäden an den IT-Systemen möglichst gering zu halten.

Die Feuerlöscher sind regelmäßig von qualifiziertem Personal auf ihre Funktionsfähigkeit und Betriebsbereitschaft geprüft. Darüber hinaus wurden im Vorfeld Brandrisikoanalysen durchgeführt, um die optimale Anordnung und Anzahl der Feuerlöscher sicherzustellen.

Neben den Feuerlöschern werden auch weitere Brandbekämpfungssysteme eingesetzt, wie zum Beispiel automatische Feuerlöschanlagen und Brandmelder, die bei Ausbruch eines Feuers ein akustisches Signal auslösen und das Sicherheitspersonal benachrichtigen.

Um im Ernstfall schnell und effektiv reagieren zu können, sind Evakuierungspläne und Fluchtwege in den Rechenzentren vorhanden. Die Mitarbeiter wurden im Umgang mit Feuerlöschern und anderen Brandbekämpfungssystemen geschult und sind in der Lage, im Falle eines Brandes schnell und sicher zu handeln. Durch die Einhaltung der technischen Richtlinien vorbeugenden Brandschutzes wird das Risiko eines Brandes minimiert und im Ernstfall kann schnell und gezielt reagiert werden.

Risiken:

Datenverlust

7.4. Klimaanlage in Serverräumen

Beschreibung:

Die Serverräume stellen einen essentiellen Teil unserer IT-Infrastruktur dar und müssen daher in höchstem Maße verfügbar und zuverlässig sein. Um eine hohe Verfügbarkeit und Ausfallsicherheit zu gewährleisten, sind die Serverräume mit voneinander unabhängigen Klimaanlagen ausgestattet, die eine redundante Kühlung der Serverinfrastruktur sicherstellen. Dadurch kann im Falle eines Ausfalls einer Klimaanlage die andere Klimaanlage den Betrieb aufrechterhalten.

Um die kontinuierliche Funktionsfähigkeit und Effizienz der Klimaanlagen zu gewährleisten, werden diese jährlich einer Wartung unterzogen. Dabei werden alle wichtigen Bauteile der Klimaanlagen überprüft, gereinigt und bei Bedarf ausgetauscht. Durch diese regelmäßige Wartung wird sichergestellt, dass die Klimaanlagen in einem optimalen Zustand sind und im Falle von Störungen schnell reagiert werden kann.

Zusätzlich zu diesen technischen Maßnahmen sind unsere Serverräume auch mit einem umfassenden Überwachungssystem ausgestattet, das in Echtzeit wichtige Parameter wie Temperatur, Luftfeuchtigkeit und Stromversorgung überwacht und bei

Abweichungen umgehend Alarm schlägt. Durch diese Kombination aus redundanter Kühlung, regelmäßiger Wartung und Überwachung sind wir in der Lage, eine höchstmögliche Verfügbarkeit und Ausfallsicherheit unserer IT-Infrastruktur zu gewährleisten.

Risiken:

Datenverlust

7.5. Schutzsteckdosenleisten im NSC Serverraum

Beschreibung:

Die im Einsatz befindlichen Verteiler sind in Übereinstimmung mit der Norm VDE 0185-305 gefertigt worden und erfüllen somit alle Anforderungen an einen sicheren Betrieb. Die Norm stellt sicher, dass alle elektrischen Verteileranlagen für den Einsatz in Gebäuden und Anlagen ausgelegt und konstruiert sind, bei denen der Schutz von Personen und Sachwerten gewährleistet ist.
Die Verteiler sind mit allen erforderlichen Schutzmaßnahmen ausgestattet, wie z.B. mit einem Schutzleiter, einer Fehlerstromschutzeinrichtung und einem Überlastschutz.
Die Norm VDE 0185-305 bezieht sich auch auf die Planung und Errichtung von Verteileranlagen und definiert die erforderlichen Schutzmaßnahmen sowie die Leitungsauswahl und -dimensionierung. Somit gewährleistet die Norm einen standardisierten und sicheren Einsatz der Verteiler und minimiert das Risiko von Fehlern oder Störungen im Betrieb.

Risiken:

Datenverlust

7.6. Testen von Datenwiederherstellung

Beschreibung:

Das Unternehmen setzt moderne Backup-Strategien ein, um die Verfügbarkeit und Integrität seiner Daten sicherzustellen. Dabei wird das sogenannte 3-2-1-Backup-Prinzip angewendet, welches besagt, dass drei Kopien der Daten auf zwei verschiedenen Medien gespeichert werden sollten, wovon eine Kopie an einem externen Ort aufbewahrt werden sollte.

Um die Backup-Prozesse zu optimieren und eine schnelle Wiederherstellung im Ernstfall zu gewährleisten, werden verschiedene Technologien eingesetzt. So erfolgt das Backup beispielsweise auf Festplatten (Disk-to-Disk-Backup) und zusätzlich auf Bänder (Disk-to-Tape-Backup). Dadurch wird eine hohe Geschwindigkeit beim Backup erreicht und eine lange Aufbewahrungszeit durch die Band-Speicherung ermöglicht.

Zusätzlich wird bei den Backups das sogenannte Immutable Backup-Prinzip umgesetzt. Hierbei handelt es sich um eine Technologie, bei der die Backup-Daten unveränderlich gespeichert werden, so dass keine nachträgliche Änderung oder Löschung der Daten möglich ist. Dadurch wird eine höhere Sicherheit der Backup-Daten gegenüber Ransomware-Angriffen und anderen Manipulationsversuchen gewährleistet.

Die Backup-Prozesse werden regelmäßig getestet und optimiert, um eine hohe Zuverlässigkeit und Verfügbarkeit der Daten zu gewährleisten. Zudem werden auch automatisierte Backup-Pläne genutzt, um sicherzustellen, dass alle Daten regelmäßig und zuverlässig gesichert werden.

Risiken:

Datenverlust

7.7. Unterbrechungsfreie Stromversorgung (USV)

Beschreibung:

Der ÖWD legt besonderen Wert auf die kontinuierliche Verfügbarkeit der Server in den Serverräumen. Hierzu werden umfangreiche Maßnahmen zur Gewährleistung der Stromversorgung getroffen. Alle Serverräume sind mit einer ausreichend dimensionierten und jährlich gewarteten USV (unterbrechungsfreie Stromversorgung) ausgestattet. Im Falle eines Stromausfalls springt die USV ein und gewährleistet den Stromfluss an die angeschlossenen Geräte, um einen

unterbrechungsfreien Betrieb der Server zu gewährleisten. Zusätzlich zu den USV-Anlagen sind in den beiden Rechenzentren in Salzburg und Wien Dieselaggregate im Einsatz, die bei einem längeren Stromausfall die Stromversorgung sicherstellen.

Alle Notstromgeneratoren sind mit einer unabhängigen Startvorrichtung ausgestattet, die automatisch aktiviert wird, wenn die Netzversorgung ausfällt. Das bedeutet, dass die Notstromgeneratoren sofort einsatzbereit sind, wenn der Strom ausfällt. Dies verhindert Ausfallzeiten und stellt sicher, dass die Server und anderen wichtigen Einrichtungen im Rechenzentrum immer in Betrieb sind.

Darüber hinaus verfügt das NSC (Netzwerk- und Sicherheitszentrum) über eine Notstromversorgung, die eine ausreichende Kapazität für den ununterbrochenen Betrieb von allen Kommunikations-, Meldungs-, Überwachungs-, Aufzeichnungs-, wichtigen Belüftungs- und Beleuchtungs-Einrichtungen einschließlich der Überwachungsanlagen für die Zeitdauer von mindestens 24 Stunden bietet. Das bedeutet, dass bei einem Stromausfall alle wichtigen Systeme im NSC weiterhin betriebsbereit bleiben und das NSC jederzeit einsatzbereit ist.

Ein Umschalten von oder zur Notstromversorgung beeinträchtigt den normalen Betrieb nicht. Dies bedeutet, dass der Betrieb der Server und anderer Einrichtungen im Falle eines Stromausfalls ohne Unterbrechung fortgesetzt wird. Die Notstromversorgung bietet daher eine zuverlässige und sichere Stromversorgung, um sicherzustellen, dass alle wichtigen Systeme und Einrichtungen im Rechenzentrum kontinuierlich in Betrieb bleiben.

Risiken:

Datenverlust

8. Trennungsgebot

8.1. Erstellung eines Berechtigungskonzepts

Beschreibung:

Das Berechtigungskonzept ist Bestandteil des Mitarbeitermeldeprozesses. Jeder Benutzer erhält dabei genau die Rechte, die er zur Erbringung seiner Arbeit benötigt. Hierbei wird ein granulares Rechtesystem angewendet, das auf der Vergabe von Berechtigungen in Berechtigungsgruppen basiert. Durch diese Vorgehensweise wird eine hohe Administrierbarkeit gewährleistet.

Um sicherzustellen, dass jeder Mitarbeiter nur auf die benötigten Ressourcen zugreifen kann, werden im Vorfeld genau die notwendigen Berechtigungen ermittelt. Hierbei werden die individuellen Aufgaben und Verantwortlichkeiten des Mitarbeiters berücksichtigt. Die Berechtigungen werden dann in entsprechenden Berechtigungsgruppen zusammengefasst, die bestimmten Rollen oder Funktionen im Unternehmen entsprechen.

Durch die Verwendung von Berechtigungsgruppen wird eine einfache und effektive Verwaltung von Berechtigungen gewährleistet. So können beispielsweise alle Mitarbeiter einer Abteilung mit ähnlichen Aufgaben und Verantwortlichkeiten in derselben Gruppe zusammengefasst werden. Bei Änderungen an den Aufgaben oder der Position des Mitarbeiters können die Berechtigungen schnell und einfach angepasst werden.

Das granulare Rechtesystem stellt sicher, dass jeder Benutzer nur auf die Ressourcen zugreifen kann, die für ihn freigegeben wurden. Auf diese Weise wird eine unerlaubte Nutzung von Ressourcen vermieden und die Sicherheit der Systeme gewährleistet.

Die Vergabe von Berechtigungen erfolgt dabei unter Berücksichtigung von Rollen und Funktionen im Unternehmen. Die hohe Administrierbarkeit des Berechtigungskonzepts stellt sicher, dass Änderungen schnell und effektiv umgesetzt werden können.

Risiken:

Datenverlust, Datenpanne

8.2. Festlegung von Datenbankrechten

Beschreibung:

Der Zugriff auf die Datenbank ist ausschließlich über die vorgelagerten Softwareanwendungen möglich, welche über eine integrierte Rechteverwaltung verfügen. Normale Benutzer haben keinen direkten Zugriff auf die Datenbank und können ausschließlich über die zugewiesenen Berechtigungen in den Softwareanwendungen auf die benötigten Daten zugreifen.
Der direkte Zugriff auf die Datenbank ist ausschließlich den Administratoren gestattet. Durch die Einrichtung separater administrativer und regulärer Konten wird sichergestellt, dass administrative Aktivitäten von normalen Benutzeraktivitäten strikt getrennt bleiben. Dies dient dazu, mögliche Missbräuche oder Sicherheitsrisiken zu minimieren und die Integrität der Datenbank zu gewährleisten. Die Trennung der Konten reduziert das Risiko von unautorisierten Zugriffen auf sensitive Daten und verhindert, dass Unbefugte die Administrationsrechte missbrauchen können.

Risiken:

Datenverlust, Datenpanne, unberechtigter Zugriff

8.3. Logische Mandantentrennung (softwareseitig)

Beschreibung:

Um eine fehlerhafte oder missbräuchliche Zugriff auf die Daten von anderen Mandanten zu verhindern, ist auf dem Datenbankserver eine logische Mandantentrennung implementiert. Hierfür werden mandantenspezifische Accounts für den Datenzugriff genutzt und ein geeignetes Berechtigungskonzept umgesetzt. Dies gewährleistet, dass nur mandanteneigene Daten gelesen oder verändert werden können.
Die logische Mandantentrennung sorgt somit für eine klare Trennung zwischen den Daten der einzelnen Mandanten und minimiert die Möglichkeit von Datenverlust oder Datenschutzverletzungen.

Risiken:

Datenverlust, Datenpanne

8.4. physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Beschreibung:

Das Unternehmen setzt moderne Backup-Strategien ein, um die Verfügbarkeit und Integrität seiner Daten sicherzustellen. Dabei wird das sogenannte 3-2-1-Backup-Prinzip angewendet, welches besagt, dass drei Kopien der Daten auf zwei verschiedenen Medien gespeichert werden sollten, wovon eine Kopie an einem externen Ort aufbewahrt werden sollte.

Um die Backup-Prozesse zu optimieren und eine schnelle Wiederherstellung im Ernstfall zu gewährleisten, werden verschiedene Technologien eingesetzt. So erfolgt das Backup beispielsweise auf Festplatten (Disk-to-Disk-Backup) und zusätzlich auf Bänder (Disk-to-Tape-Backup). Dadurch wird eine hohe Geschwindigkeit beim Backup erreicht und eine lange Aufbewahrungszeit durch die Band-Speicherung ermöglicht.

Die Backup-Prozesse werden regelmäßig getestet und optimiert, um eine hohe Zuverlässigkeit und Verfügbarkeit der Daten zu gewährleisten. Zudem werden auch automatisierte Backup-Pläne genutzt, um sicherzustellen, dass alle Daten regelmäßig und zuverlässig gesichert werden.

Risiken:

Datenverlust, Datenpanne

8.5. Trennung von Produktiv- und Testsystem

Beschreibung:

Um sicherzustellen, dass die Test- und Schulungssysteme die Produktivsysteme und deren Daten nicht beeinflussen können, werden separate Datenbanken für diese Zwecke eingesetzt. Dies bedeutet, dass die Test- und Schulungssysteme nicht auf die Produktivdatenbanken zugreifen, sondern auf ihre eigenen spezifischen Datenbanken.

Durch diese Trennung können potenzielle Probleme, die bei Tests oder Schulungen auftreten können, isoliert werden und haben keine Auswirkungen auf die Produktivsysteme. Gleichzeitig ermöglicht die Nutzung von separaten Datenbanken auch eine bessere Verwaltung von Test- und Schulungsdaten, da diese von den Produktivdaten getrennt sind und separat behandelt werden können.

Diese Maßnahme bietet auch einen zusätzlichen Schutz gegenüber Angriffen oder Fehlern in Test- und Schulungsumgebungen, da diese nicht auf die Produktivdatenbanken zugreifen können. Dies hilft dabei, die Integrität der Produktivdaten und die Sicherheit des gesamten Systems zu gewährleisten.

Risiken:

Datenverlust, Datenpanne