Technische und organisatorische Maßnahmen

· 1. Zutrittskontrolle

Mit der Zutrittskontrolle soll verhindert werden, dass unberechtigte Personen Zutritt zu den informationsverarbeitenden Systemen der unaxus GmbH bekommen. Die Rechenzentren der unaxus GmbH gewährleisten einen hohen Schutz durch moderne Sicherheitstechnik und umfassende Objekt- und Datenschutzmaßnahmen. Der Zutritt zum Rechenzentrum ist dabei nur einem eingeschränkten Kreis von autorisierten Mitarbeitern möglich.

1.1. Organisatorische Maßnahmen

1.1.1. Empfang- und Ausweispflicht

Der Standort des Rechenzentrumgebäudes wird tagsüber zu den normalen Geschäftszeiten per Video überwacht, außerhalb der Geschäftszeiten durch Kontrollgänge eines Sicherheitsdienstes. Auffälligkeiten werden durch die Einbruchmeldeanlage und Kontrollgänge des Sicherheitsdienstes entdeckt. Am Standort des Rechenzentrums besteht für alle Besucher und externen Mitarbeiter die Pflicht, Ausweise zu tragen. Externe Personen dürfen sich grundsätzlich nur in Begleitung eines internen Mitarbeiters innerhalb der Rechenräume aufhalten. Interne Mitarbeiter besitzen durch ihre Zutrittskarten/Codes die entsprechende Berechtigung, Zutritt zu den Geschäftsräumen zu erlangen.

Die Ausweis-Richtlinie sieht folgende Anforderungen beim Ausstellen vor:

- Die Ausweise sowie alle zugehörigen Dokumente und Unterlagen sind verschlossen aufzubewahren.
- Zugänge zu EDV-gestützten Verwaltungstools sind mit Passwörtern zu versehen, sodass Unbefugte keinen Zugriff auf die Arbeitsstationen, über die die Ausweise verwaltet werden, erhalten können.

1.1.2. Schlüsselvergabe

Durch das installierte Zutrittskontrollsystem können nur Personen in die Rechenräume gelangen, die im Vorfeld Berechtigungen im Rahmen ihrer Aufgabenerfüllung (z.B. Systemoperatoren, die Hardware austauschen müssen) erhalten haben. Die Zutrittsberechtigungen werden zentral über ein Zugriffsrechtemanagement, d.h. durch die Einrichtung von Profilen, Vergabe/Sperrung von Berechtigungen eingerichtet. Hierfür existiert ein formaler Genehmigungsprozess. Der Zutritt zum Rechenzentrum erfolgt über eine neutrale

Zutrittskarte, die nach Anforderung und Unterschrift des Empfängers dem Berechtigten ausgehändigt wird. Die Vergabe der Zutrittskarten wird dokumentiert. Bei Verlust der Zutrittskarte wird diese sofort über das installierte Verwaltungssystem gesperrt. Die Berechtigungen können losgelöst von der physischen Verfügbarkeit der Zutrittskarte geändert, gelöscht, oder gesperrt werden.

1.1.3.Technische Maßnahmen

Das Rechenzentrum wird durch folgende technische Maßnahmen vor unberechtigtem Zutritt geschützt:

- ZK-System (Zutrittskontrollsystem)
- EMA (Einbruchmeldeanlage)
- Videokameras
- Zutrittsschleusen

2. Zugangskontrolle

Mit der Zugangskontrolle soll ein Eindringen unberechtigter Personen in die Informationsverarbeitenden Systeme verhindert werden. Hierzu sind technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung implementiert.

2.1. Organisatorische Maßnahmen

2.1.1. Benutzer- und Berechtigungsverfahren

Benutzer, die im Rahmen ihrer Aufgabenerfüllung zu einem System Rechte erlangen sollen, müssen diese Berechtigungen über einen formalen Benutzer- und Berechtigungsprozess beantragen. Die Anforderungen zur Benutzer- und Berechtigungsvergabe sind durch die interne Sicherheitsrichtlinie zum Identity- und Accessmanagement beschrieben und die Berechtigungsvergabe in einer Verfahrensanweisung dokumentiert. Im Benutzer- und Berechtigungs-Verwaltungssystem werden die Benutzerkennungen und Berechtigungen von Benutzern geführt. Technisch erfolgt die Genehmigung für das Erteilen und Löschen von Zugriffsrechten über Ticketsysteme, in denen der Vorgang dokumentiert wird. Im Verwaltungssystem werden Berechtigungen von Benutzern gesperrt, sobald der Benutzer das Unternehmen verlässt, bzw. wenn die Berechtigungen nicht mehr benötigt oder unberechtigt benutzt werden. Auch im Rahmen der Systemdiagnose werden obsolete Zugriffsrechte gelöscht. Technisch ist jeder berechtigte Benutzer auf eine einzelne Benutzer-ID auf dem Zielsystem beschränkt.

2.2. Technische Maßnahmen

2.2.1. Authentisierungsverfahren

Zugangsberechtigungen sind so feingranular wie möglich konfiguriert, sodass Personen nur dort Zugang haben, wo sie diesen auf Grund ihrer Funktion und ihrer Aufgabenerfüllung benötigen. Die Zugangskontrollverfahren gelten für alle Mitarbeiter der unaxus GmbH. Alle Systeme sind durch zweistufige Authentifizierungsverfahren (z.B. Benutzer-ID und Passwort) geschützt, die unberechtigte Zugriffe unterbinden. Werden im Rahmen des Authentifizierungsverfahrens Passwörter eingesetzt, müssen diese den internen Passwortrichtlinien für Mitarbeiter und Systeme entsprechen. Passwörter, die nach den Richtlinien nicht der Qualität entsprechen, sind nicht erlaubt. Die Systeme werden nach einer bestimmten Zeit der Inaktivität automatisch gesperrt. Zusätzlich werden Accounts automatisch deaktiviert, wenn deren Passwörter nicht geändert werden.

Ein Fernzugriff auf interne Systeme ist nur in authentifizierter Form möglich, bei dem z.B. asymmetrische Authentisierungsverfahren (Public-/Private-Key-Verfahren) eingesetzt werden, die zusätzlich zur Nachweisbarkeit protokolliert werden. Der Zugriff auf interne Systeme wird nur Geräten gewährt, die sich im Besitz der unaxus GmbH befinden und administriert werden. Der Zugriff auf interne Systeme über WLAN-Verbindungen kann nur durch einen zusätzlichen VPN-Tunnel erfolgen.

2.2.2. Verschlüsselung

Daten mit hohen Schutzbedarfen werden nach aktuellem Stand der Technik mit verschlüsselten Verfahren analog der internen IT-Sicherheitsrichtlinie zur Kryptographie gesichert. Werden Daten anhand Datenträger ausgetauscht, wird dokumentiert, wer zu welchem Zeitpunkt zu welchem Zweck von wem einen Datenträger erhält. Datenträger, die nicht mehr zum produktiven Einsatz kommen, werden durch sichere Lösch- und Überschreib-Verfahren entsorgt. Es gelten hier die Regelungen der internen Sicherheitsrichtlinie zur Entsorgung von Medien.

3. Zugriffskontrolle

Mit der Zugriffskontrolle sollen unerlaubte Handlungen in den informationsverarbeitenden Systemen verhindert werden, indem Maßnahmen zur Überwachung und Protokollierung der Zugriffe implementiert werden.

3.1. Berechtigungsvergabe

Die Systeme wurden in der Weise konfiguriert, dass ein regulärer Zugriff mit administrativen Rechten nur für interne, autorisierte Mitarbeiter aus gesicherten Netzsegmenten möglich ist. Hier wurden bedarfsorientierte Berechtigungskonzepte ausgestaltet, die die Zugriffsrechte, sowie deren Überwachung und Protokollierung definieren. Eine Berechtigungsvergabe wird stets nach dem Need-to-know-Prinzip vergeben. Je nach Autorisierung werden differenzierte Berechtigungen, untergliedert nach Rollen und Profilen von Benutzern eingerichtet. Weitere Autorisierungen an Systemen bedürfen der Einrichtung von Berechtigungen nach dem implementierten Benutzer- und Berechtigungsprozess.

3.2. Auswertungen

Zugriffe auf System-lDs und auffällige Zugriffsversuche werden auf einem zentralen Protokollierungsserver protokolliert. Der Zugriff auf die Protokollierungsserver ist nur lesend durch autorisierte Administratoren möglich. Beim auffälligen Zugriffsversuch wird zusätzlich eine Alarmierung (Security Monitoring) an den zuständigen Systemverantwortlichen ausgelöst.

3.3. Veränderungen

Modifikationen an Zugriffsrechten können lediglich von Systemadministratoren des operativen Fachbereichs vorgenommen werden, die die Freigabe des Vorgesetzten erhalten haben. Veränderungen der Zugriffsrechte und Berechtigungen geschehen in der Regel innerhalb eines Arbeitstages, wenn nicht sogar bei Bedarf sofort. Netzwerkgeräte oder Systeme mit voreingestellten Zugriffsmöglichkeiten dürfen nicht im Produktivbereich verwendet werden. Näheres regeln die internen Sicherheitsrichtlinien.

3.4. Löschung

Das Löschen von Benutzerberechtigungen (z.B. Nach dem Austritt eines Mitarbeiters) erfolgt zeitnah, spätestens jedoch innerhalb eines Arbeitstages. Das Löschen von Zugriffsrechten geschieht auch im Rahmen der Systemdiagnose. Hier werden obsolete Zugriffsrechte bereinigt. Im Verwaltungssystem werden Berechtigungen von Benutzern gesperrt, sobald der Benutzer das Unternehmen verlässt bzw. wenn die Berechtigungen nicht mehr benötigt oder unberechtigt benutzt werden. Im Rahmen der Systemdiagnose werden obsolete Zugriffsrechte, die z.B. über einen längeren Zeitraum inaktiv waren, gelöscht.

4. Weitergabekontrolle

Im Rahmen der Weitergabekontrolle werden Maßnahmen beim Transport, der Übertragung und Übermittlung, sowie bei der nachträglichen Überprüfung von personenbezogenen Daten definiert.

4.1. Organisatorische Maßnahmen

4.1.1. Schulungsmaßnahmen

Alle Mitarbeiter sind auf das Fernmeldegeheimnis hin verpflichtet worden. Neue Mitarbeiter erhalten bei Eintritt eine Sicherheitsschulung. Für verschiedene Fachbereiche gibt es speziell abgestimmte Sicherheitssensibilisierungsprogramme;

4.1.2. Klassifizierung der Informationen

Jede Information muss nach ihrem Schutzbedarf eingestuft werden. Handelt es sich um vertrauliche Informationen, müssen diese besonders behandelt werden. Vertrauliche, dienstliche Informationen dürfen nur über sichere Kommunikationswege übertragen werden. Der Umgang mit Informationen wurde in der Richtlinie „Datenklassifikation" und deren Anhang geregelt. Es sind insbesondere folgende Regeln einzuhalten:

- Es müssen spezielle Verfahren und Regelungen zum Schutz der Informationen und Datenträger beim Transport insbesondere über Unternehmensgrenzen hinweg definiert und dokumentiert werden (z.B. Verfahrensanweisung für den Einsatz von Boten).
- Es müssen so weit wie möglich kryptographische Verfahren (z-B. Verschlüsselung bei der Übertragung vertraulicher Daten) eingesetzt werden. Die Anforderungen aus der IT-Sicherheitsrichtlinie Kryptographie sind zu berücksichtigen.
- Bei der Übergabe an externe Empfänger ist die erfolgte vollständige und sichere Übergabe nachweisbar zu dokumentieren.

4.2. Technische Maßnahmen

4.2.1. Zugriffs- und Transportsicherung

Grundsätzlich können auf die Systeme, die personenbezogene Daten verarbeiten, nur autorisierte Nutzer zugreifen. Die Übertragung von Daten erfolgt ausschließlich durch das System selbst an autorisierte Empfänger, über kryptographisch stark gesicherte Wege. Die Übertragung wird in Logfiles protokolliert.

Um das System vor unberechtigten Zugriffen von Desktop-PCs der Mitarbeiter und somit vor einer unautorisierten Weitergabe von Daten zu schützen, gelten die internen Sicherheitsrichtlinien für Mitarbeiter.

Die Integrität von wichtigen Systemdateien wird durch regelmäßige Überprüfung deren kryptografischer Prüfsumme sichergestellt.

Der Zugriffsschutz auf Systeme mit sensiblen Informationen wird auf mehreren Ebenen realisiert: Auf Dateisystem-, auf Betriebssystem- und auf Netzwerkebene. Die Schutzmechanismen erlauben nur speziell autorisierten Administratoren den Zugriff auf die jeweilige Ebene. Um Datenverlust vorzubeugen, müssen alle arbeitsrelevanten Daten auf Servern gespeichert werden. Diese Daten werden regelmäßig gemäß den definierten Backup-Konzepten gesichert, sodass ein Datenverlust dadurch weitestgehend ausgeschlossen ist.

4.2.2. Protokollierung

Der Zugriff und die Aktivitäten der Administratoren werden in speziellen Protokolldateien aufgezeichnet. Die Protokollierung der Zugriffe erfolgt auf einen zentralen, dedizierten Protokollierungsserver, der von den zu protokollierenden Systemen getrennt installiert ist. Der Zugriff auf die Protokolle und auf den zentralen Protokollierungsserver ist geschützt und nur autorisierten Administratoren gestattet. Systemadministratoren dürfen dabei die Protokolle auf den Protokollierungsserver einsehen, aber nicht verändern. Der Transport der Protokollierungsdaten geschieht über eine verschlüsselte Verbindung. Auf den Protokollierungsserver werden verschiedene Verletzungen von Sicherheitskontrollen protokolliert, wie z.B. nicht berechtigte Zugangsversuche oder signifikante Schutzverletzungen. Bei besonders sensiblen Systemen ist der Zugriff nur nach dem 4-Augen-Prinzip möglich.

5. Eingabekontrolle

Um die Nachvollziehbarkeit und Dokumentation der Datenverwaltung und -pflege sicherzustellen, werden Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder gelöscht worden sind, implementiert.

5.1. Protokollierungs- und Protokollauswertung

Durch die Einhaltung der oben aufgeführten Regeln zu Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle wurde die Grundlage für die Eingabekontrolle der Systeme geschaffen, die personenbezogenen Daten verarbeiten. Grundsätzlich wird im Rechte- und Rollen-Konzept zwischen Systemusern, Prozessusern und personalisierten Usern unterschieden.

Angaben zur Protokollierung sind in Kapitel 4.2.2 zu finden.

Protokollauswertungen werden stichprobenartig von den Systemadministratoren vorgenommen, insbesondere jedoch, wenn Auffälligkeiten oder der Verdacht auf eine Kompromittierung (z.B. durch eine Alarmierung / Triggering eines Events) aufgetreten ist. Die Protokollauswertungen sind als Informationen klassifiziert, die nur innerhalb des Unternehmens im Rahmen der Aufrechterhaltung und Sicherstellung der Systemstabilität und -Sicherheit zu verwenden sind.

6. Auftragskontrolle

Alle Weisungen des Auftraggebers zum Umgang mit personenbezogenen Daten werden dokumentiert und an zentraler Stelle für die mit der Datenverarbeitung befassten Mitarbeiter der unaxus GmbH hinterlegt.

Die unaxus GmbH verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung erfolgt nur nach schriftlicher Einwilligung des Auftraggebers. Der Datenschutzbeauftragte des Auftraggebers hat das jederzeitige Recht, nach Absprache die Umsetzung seiner Weisungen bei der unaxus GmbH zu kontrollieren. Die unaxus GmbH wird den Auftraggeber bei der Durchführung von Kontrollen durch den Auftraggeber unterstützen und an der vollständigen Abwicklung der Kontrolle mitwirken.

Die unaxus GmbH wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach ihrer Auffassung gegen gesetzliche Regelungen verstößt, sowie dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist. Die unaxus GmbH ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Fernmeldegeheimnisses verpflichtet. Sie verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien werden erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet.

7. Verfügbarkeitskontrolle

Alle Dienste der unaxus GmbH sind hochsensibel in Bezug auf deren Verfügbarkeit und müssen vor zufälliger Zerstörung oder Verlust geschützt werden. Die Kunden erwarten eine hochverfügbare Bereitstellung aller Netzwerk- und Rechenzentrums-Dienstleistungen. In diesem Zusammenhang werden Maßnahmen zur Datensicherung und -erhaltung umgesetzt.

7.1. Organisatorische Maßnahmen

7.1.1. Notfallhandbücher und Backup-Verfahren

Zur Sicherstellung der Notfallhandbücher und Backup-Verfahren werden in den als für notwendig erachteten Abteilungen Notfallhandbücher erstellt. Die Notfallhandbücher definieren Verantwortlichkeiten (z.B. Notfallverantwortlicher), sowie Eskalations-, Informations- und Alarmierungspfade, legen Wiederanlaufpläne und Verfahren für einen Shutdown für einen Mangelfall fest, regeln Ersatzbeschaffung von Hard- und Software und dokumentieren, wie Daten gesichert und archiviert werden müssen. Die Notfallhandbücher sind damit ein wesentlicher Bestandteil für den Umgang und der Behandlung der Systeme und Daten im Notfall, die insbesondere auf die Backup-Strategien und Backup-Dokumentationen verweisen. Alle Daten werden in regelmäßigen Abständen gesichert, wobei die Sicherung dokumentiert an einem anderen Ort als das zu sichernde System verwahrt wird. Die Backups verlassen jedoch nicht eines der Rechenzentren der unaxus GmbH. Zum Schutz der Archive und Backups sind die zuvor genannten Zutrittskontrollen implementiert. Der Zugang auf die Backup-Software ist limitiert auf dedizierte Backup-Administratoren. Die Häufigkeit von Datenbackups richtet sich nach der Kritikalität der Informationen und ist individuell anpassbar. Funktionalitätstests von Datenbackups werden stichprobenartig von den zuständigen Systemadministratoren vorgenommen.

Im Wiederherstellungsprozess wird beschrieben, wie und in welcher Reihenfolge die Systeme und Daten installiert und wiederhergestellt werden müssen.

Alle Prozesse zur Wiederherstellung der Daten, der Wiederanlaufplan der Systeme, sowie die Notfallsituation müssen in regelmäßigen Abständen in einer Übung durchgeführt und getestet

werden. Die Tests und Übungen werden protokolliert und dokumentiert. Die bei Notfällen und Incidents benötigten Eskalationspfade wurden im Praxisbetrieb erprobt.

7.2. Technische Maßnahmen

7.2.1. Firewall

Die Netze und Systeme der unaxus GmbH sind mit einer Firewall gegen Hackerangriffe geschützt, die regelmäßig von autorisierten Systemadministratoren gewartet und aktualisiert werden. Die Firewall- Regeln sind so ausgelegt, dass nur benötigte Dienste erlaubt sind und in der Grundeinstellung jeden Netzwerkverkehr blockieren. Alle Internetverbindungen sind durch mindestens eine Firewall geschützt. Die Kontrolle sicherheitsrelevanter Konfigurationen erfolgt hierbei im Rahmen von Sicherheitsaudits und Penetrationstests, die u.a. von der internen Sicherheitsabteilung durchgeführt wird.

7.2.2. Hochverfügbarkeit und Stromversorgung

Aus der Hochverfügbarkeitsanforderung ergibt sich am Standort Zürich, an dem das System aufgestellt ist, eine grundsätzliche hochredundant ausgelegte Netzwerk-Infrastruktur, die Einzelfehler in fast allen Bereichen und Doppelfehler in vielen Bereichen abfangen kann. Sensible Dienste werden georedundant an verschiedenen Standorten betrieben. Die Stromversorgungen sind mehrfach unabhängig voneinander ausgelegt. Das Rechenzentrum in Glattbrugg und Zürich ist mit einer unterbrechungsfreien Stromzufuhr ausgestattet. Die zentrale Elektrotechnik in Glattbrugg ist in drei (N+1) Blöcke aufgeteilt. In jedem Block ist die Technik Mittelspannung, Niederspannung, USV und Netzersatzanlage (NEA) enthalten. Ein Betriebsblock dient zur Redundanz. Die zentrale Elektrotechnik in Zürich ist in zwei (N) Blöcke aufgeteilt. Sowohl in Glattbrugg wie auch in Zürich ist die Klimatisierung in zwei Blöcke aufgeteilt (N+1)

Die Versorgungsblöcke in Zürich sind räumlich voneinander getrennt, um eine gegenseitige Beeinflussung im Schadens- oder Störfall zu verhindern. Jeder Block hat einen eigenen mittelspannungsseitigen Abgang. Um sich vor einem Totalausfall in der Versorgung durch die zu schützen, ist in zweiter Instanz in Zürich zwischen Verbraucher und Versorger eine redundant ausgelegte, unterbrechungsfreie Stromversorgung (USV) installiert. Die gesamte Anlage in Zürich wird über eine zentrale, redundant aufgebaute Netzleittechnik überwacht und gesteuert. Zusätzlich wird permanent die Netzqualität von allen Ein- und Ausgängen der USV Anlagen überwacht.

7.2.3. Brandschutz

Eine Löschanlage schützt die Sicherheitsräume in Zürich im Brandfall. Das ungiftige Gas bewirkt bei einem Brandfall eine Sauerstoffverdrängung im Raum, wodurch dem Brandherd die Grundlage Sauerstoff entzogen wird. Die Server werden durch den Löschvorgang nicht beeinträchtigt und können normal weiter betrieben werden.

Um einen Brandfall im Vorfeld zu verhindern ist des Weiteren eine Brandfrüherkennungsanlage in Zürich installiert, die ständig die Luftpartikel anhand eines vorgegebenen Soll-Kalibrierungszeitraumes überwacht. Ändert sich die Zusammensetzung der Luftpartikel oder steigt die Zahl der für eine Brandentstehung typischen Partikel, schlägt die Früherkennung Alarm. Zur ersten Bekämpfung von Bränden sind Handfeuerlöscher installiert.

8. Trennungskontrolle

Durch die getroffenen Maßnahmen zur Trennungskontrolle sind der softwareseitige Ausschluss im Sinne einer Mandantentrennung, die Trennung von Test- und Routineprogrammen, die Trennung durch getroffene Zugriffsregelungen, sowie Dateiseparierung.

Beispielsweise müssen alle Produktivsysteme getrennt von den Entwicklungs- und Testsystemen betrieben werden. Technisch wird das durch eine Segmentierung von Netzen mit einem aktivierten Firewall-Regelwerk realisiert. Produktivdaten dürfen nicht als Kopie für Testzwecke verwendet werden, ebenso dürfen Testdaten nicht in Produktivumgebung eingesetzt werden. Details regeln die internen Sicherheitsrichtlinien zum sicheren Betrieb.