Sicherheitskonzept zur DSGVO

(IT, Zutritt, Umgang Bewerbungen, geistiges Eigentum etc.)

ROWA-MOSER

1. Inhalt

1 Einleitung 3
2 Schutzbedarf 4
3 Maßnahmenauswahl 4
4 Personelle Maßnahmen 4
5 Regelungen für Mitarbeiter 4
6 Datenschutz 5
7 Verfahren bei personellen Veränderungen 5
8 Regelungen für den Einsatz von Fremdpersonal 5
9 Sicherheitssensibilisierung und -schulung 6
10 Abwehr von Social Engineering-Angriffen 6
11 Clear Desk/Clear Screen-Policy 7
12 Entsorgung von Datenträgern und Papierdokumenten 7
13 Telearbeit 8
14 Auswahl von Passwörtern 8
15 BIOS-Zugangskontrolle 8
16 Rechtestruktur auf Arbeitsplatzrechnern 8
17 Wechselmedien 9
18 Verschlüsselung von Arbeitsplatzsystemen 9
19 Regelmäßige Software-Aktualisierungen 9
20 Nutzungsverbot nicht-betrieblicher Software 10
21 Mobile IT-Geräte 10
22 Nutzung von Cloud-Speicherdiensten 11
23 Schutz gegen Schadsoftware 12
24 Technische Virenschutzmaßnahmen 12
25 Vermeidung bzw. Erkennung von Viren durch Benutzer 12
26 Notfallmaßnahmen im Fall von Vireninfektionen 13
27 Ransomware und Verschlüsselungstrojaner 13
28 Netzwerksicherheit 13
29 Firewalls 14
30 Personal Firewalls 14
31 Wireless LAN (WLAN) 14

32 Festlegung der Internet-Sicherheitsstrategie 15
33 Soziale Netzwerke 15
34 Logging, Monitoring und Auditing 15
35 Kontinuierliche Verbesserung 15
36 Datensicherung 15
37 Datensicherungskonzept und -planung 16
38 Zutrittskontrolle 16
39 Schlüsselverwaltung 16
40 Sicherer und rechtlich konformer Umgang mit Bewerbungen 16
41 Umgang mit geistigem Eigentum: 17

1 Einleitung

ROWA-MOSER bedient sich einer sehr umfangreichen IT-Infrastruktur.

Die IT-Infrastruktur und alle Daten müssen wir vor Verlust, Diebstahl oder unbefugter Veränderung schützen.

Das vorliegende Sicherheitskonzept beschreibt die getroffenen Maßnahmen zur Risikoreduzierung und damit zur Realisierung und Aufrechterhaltung des angemessenen Sicherheitsniveaus.

In diesem Sicherheitskonzept wurden daher insbesondere auch Maßnahmen beschrieben, die sich aus den Vorgaben der Datenschutzgrundverordnung und dem Datenschutzgesetz ergeben.

2 Schutzbedarf

Grundsätzlich sind alle Daten der Organisation zu schützen. Dabei gilt es jedoch zu beachten, dass manche Daten wichtiger sind als andere und dadurch ein höheres Schutzniveau verlangen.

Schutz gegen Risiken

Durch den Einsatz von IT-Systemen und elektronisch gespeicherten Daten entstehen Risiken, die genauso wie alle anderen betrieblichen Risiken gezielt behandelt werden müssen.

Dazu zählen:

- IT-Systeme (Server, PCs, Notebooks, Smartphones, Tablets, …)
- Software und Lizenzen
- Infrastruktur (z.B. Kommunikationsanlagen)
- Informationen (Daten von ROWA-MOSER; personenbezogene Daten von Kunden&Lieferanten, Partnern, Mitarbeitern; Verträge, Datenbanken, E-Mails usw.)

3 Maßnahmenauswahl

Einem bestehenden Risiko wird daher grundsätzlich mit organisatorischen und technischen, aber auch persönlichen Maßnahmen begegnet. Dabei kommen Maßnahmen aus folgenden Bereichen zum Einsatz:

- Bauliche und infrastrukturelle Sicherheit: z.B. Zutrittskontrolle
- Personell-organisatorische Sicherheit: z.B. Sicherheitsrichtlinien und -konzepte, Berechtigungskonzepte, Notfalldokumentation, Versicherungsschutz.
- Technische Maßnahmen: z.B. Zugangs- und Zugriffsberechtigungen, Datensicherung, Virenschutz

Die umgesetzten Maßnahmen werden in regelmäßigen Abständen (mindestens 1x jährlich) auf ihre Wirksamkeit, Zweckmäßigkeit und Aktualität geprüft und gegebenenfalls angepasst. Diese Überprüfung wird auch bei Auftreten neuer Bedrohungen oder bei größeren Änderungen der IT-Infrastruktur (z.B. beim Erwerb neuer Systeme oder Anwendungen) durchgeführt.

4 Personelle Maßnahmen

IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiter ein ausgeprägtes Sicherheitsbewusstsein besitzen und in der Lage sind, die Vorgaben in der täglichen Praxis umzusetzen.

5 Regelungen für Mitarbeiter

Bei allen elementaren Gefährdungen ist menschliches Fehlverhalten ein bedeutender Faktor, entweder als Auslöser oder als Maßnahme zur Abwehr. Um die Risiken menschlichen Fehlverhaltens, sei es durch Unwissenheit oder auch durch Vorsatz, zu minimieren, sind für Mitarbeiter verpflichtende Richtlinien einzuhalten, die folgende Bereiche betreffen:

- Datensicherung
- Diebstahlschutz

- Software und Lizenzen
- Hardware
- Zugangsberechtigungen
- Systemzugriffskontrolle
- Passwörter
- Internet
- E-Mail
- Soziale Medien
- Schadsoftware (Malware)
- Bildschirmschoner
- Remote Access
- Drahtlose Verbindungen
- Social Engineering

6 Datenschutz

Der sorgsame Umgang mit personenbezogenen Daten ist einzuhalten. Jeder Mitarbeiter verpflichtet sich durch seine Unterschrift, den Schutz personenbezogener Daten in seiner täglichen Arbeit zu beachten.

7 Verfahren bei personellen Veränderungen

Bei personellen Veränderungen, insbesondere beim Ausscheiden von Mitarbeitern, werden folgende Maßnahmen veranlasst

- Sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. Mobilgeräte, Speichermedien, Dokumentationen) werden zurückgefordert.
- Sämtliche Zugangsberechtigungen und Zugriffsrechte werden angepasst, entzogen oder gelöscht. Dies betrifft unter anderem auch Berechtigungen für eventuelle Telearbeitszugänge, sowie Daten auf privaten Smartphones oder Notebooks.
- Wenn eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt wurde (z.B. mittels eines gemeinsamen Passwortes), wird nach Ausscheiden einer der Personen die Zugangsberechtigung sofort geändert. Wenn Administratoren ausscheiden, so werden alle diejenigen Passwörter geändert, die ihnen bekannt waren.
- Eine Neuvergabe eines bestehenden Benutzerkontos an neue Mitarbeiter wird nicht durchgeführt.

8 Regelungen für den Einsatz von Fremdpersonal

Betriebsfremde Personen, wie z.B. Personal von Reinigungsfirmen, können leicht Zugang zu vertraulichen Daten erhalten und stellen unter Umständen eine Bedrohung dar.

Folgende Regeln wurden aufgestellt, um vertrauliche Informationen zu schützen.

- Externe Mitarbeiter, die über einen längeren Zeitraum für ROWA-MOSER tätig sind und Zugang zu vertraulichen Unterlagen und Daten erhalten, werden schriftlich im Rahmen von

Geheimhaltungsverpflichtungen auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet.

- Für Fremdpersonal, das nur kurzfristig oder einmalig zum Einsatz kommt, gelten die gleichen Regeln wie für Besucher, d.h. dass etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von Mitarbeitern von ROWA-MOSER erlaubt ist.
- Da es manchmal nicht möglich ist, betriebsfremde Personen ständig zu begleiten oder zu beaufsichtigen, müssen die persönlichen Arbeitsbereiche abgeschlossen werden (Schreibtisch, Schrank; Abmeldung/Sperre am PC).

9 Sicherheitssensibilisierung und -schulung

Um die IT-Sicherheit zu verbessern, sollten alle Mitarbeiter über angemessene Kenntnisse im Umgang mit IT-Systemen und den Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet verfügen. Die Geschäftsführung sieht es als ihre Verantwortung, durch geeignete Schulungsmaßnahmen die nötigen Voraussetzungen zu schaffen. Darüber hinaus werden alle Benutzer dazu motiviert, sich auch in Eigeninitiative Kenntnisse anzueignen.

Bei Benutzerschulungen werden folgende Inhalte besonders beachtet

- Der richtige Umgang mit Passwörtern
- Richtiges Verhalten beim Auftreten von Sicherheitsproblemen
- Der verantwortungsbewusste Umgang mit personenbezogenen Daten
- Erkennen eines Befalls mit Schadprogrammen und Sofortmaßnahmen im Verdachtsfall
- Das richtige Verhalten im Internet
- Das richtige Verhalten bei unzulässigen Anfragen
- Risiken bei der Verwendung mobiler IT-Geräte und Datenträger
- Die Bedeutung der Datensicherung und ihrer Durchführung
- Die Bedeutung des Datenschutzes, die gesetzlichen Anforderungen sowie die vom Alpenverein getroffenen Maßnahmen

10 Abwehr von Social Engineering-Angriffen

Als Social Engineering bezeichnet man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten.

Social Engineering-Angriffe werden oft über das Telefon, heutzutage vermehrt über soziale Netzwerke geführt: Angreifer geben sich als Mitarbeiter, Kunden oder IT-Fachkräfte aus und überzeugen ihre Gesprächspartner durch geschickte Täuschung von ihrer vorgetäuschten Identität. Bei geeigneter Gelegenheit – oft erst nach mehrmaligen Telefonaten – gelangen sie so an Informationen, die die Opfer üblicherweise nie herausgeben würden. Social Engineers können unvorbereitete Mitarbeiter zu verschiedensten unerlaubten Handlungen, insbesondere zu Verstößen gegen Sicherheitsauflagen und -richtlinien bewegen.

Social Engineering-Angriffe sind häufig erfolgreich, weil sie menschliche Eigenschaften und Schwächen gezielt ausnützen: Hilfsbereitschaft und Höflichkeit, Kundenfreundlichkeit, aber auch Autoritätshörigkeit und Angst. Folgende Maßnahmen werden eingesetzt, um das Risiko zu verringern:

- Schulungen über Social Engineering-Strategien und –Methoden. Diese helfen den Mitarbeitern, sich auf Angriffe dieser Art vorzubereiten.
- Alle Mitarbeiter müssen sich regelmäßig den Wert der von ihnen bearbeiteten Daten bewusstmachen, insbesondere hinsichtlich des Schadens, der entstehen kann, wenn sie in falsche Hände geraten.
- Das Anfordern einer Rückrufnummer oder einer schriftlichen Anfrage kann den Social Engineer bereits abschrecken und gibt den betroffenen Mitarbeitern Gelegenheit zur Nachfrage.
- Neuen Mitarbeitern wird empfohlen, Anfragen, bei denen sie unsicher sind, ob deren Beantwortung zulässig ist, an Vorgesetzte oder andere erfahrene Personen weiterzuleiten.
- Mitarbeiterkommunikation ist wichtig: Bei „verdächtigen“ Anfragen werden auch die anderen Mitarbeiter informiert, um zu verhindern, dass ein abgewiesener Angreifer sein Glück bei anderen Kollegen versucht.

11 Clear Desk/Clear Screen-Policy

In ungesicherten Arbeitsumgebungen hilft eine Clear Desk-Policy beim Schutz vertraulicher Dokumente und Daten vor unbefugten Zugriffen.

Alle Mitarbeiter müssen bei Abwesenheit vertrauliche Unterlagen verschließen. Auch ist dafür Sorge zu tragen, dass keine unberechtigten Personen (Besucher, Reinigungspersonal, unbefugte Mitarbeiter, etc.) Zugriff auf Schriftstücke oder Datenträger mit kritischen Inhalten haben.

Analoges gilt auch für die Computer: Beim Verlassen des Arbeitsplatzes muss sich jeder Benutzer vom PC abmelden. Wenn nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann der Computer stattdessen gesperrt werden (STRG-ALT-ENTF -> SPERREN). Eine automatische Sperre des Computers nach 10 Minuten wurde auf jedem Computer eingestellt.

Alle Benutzer wurden über die Tastenkombinationen zum schnellen Sperren des PCs informiert.

Die Durchführung dieser Maßnahmen wird regelmäßig stichprobenartig kontrolliert.

12 Entsorgung von Datenträgern und Papierdokumenten

Datenträger und Dokumente mit vertraulichen Inhalten werden auf sichere Art entsorgt.

Der Umgang mit Dokumenten mit vertraulichen oder personenbezogenen Inhalten stellt ein Sicherheitsrisiko dar. Dies gilt für Papier ebenso wie für nicht mehr gebrauchte Datenträger wie z.B. defekte Festplatten, Sicherungsbänder oder USB-Sticks.

Folgende Sicherheitsmaßnahmen wurden hierzu getroffen:

- Die Mitarbeiter sind über das Entsorgungskonzept informiert und insbesondere darüber in Kenntnis gesetzt, welche Dokumente nicht über das Altpapier entsorgt werden dürfen. Papierdokumente müssen mit einem handelsüblichen Shredder entsorgt werden.
- Es steht eine ausreichende Anzahl von Entsorgungsmöglichkeiten in erreichbarer Nähe der Mitarbeiter, sowie Ansprechpartner für Rückfragen im Zweifelsfall, zur Verfügung.
- Datenträger werden auf sichere Art vernichtet: Festplatten werden sicher gelöscht (DiskWipe), mechanisch zerstört und entsorgt.

- Bei Festplatten und Wechseldatenträgern wird ein Löschprogramm eingesetzt, das ein sicheres Löschen der Daten gewährleistet.

13 Telearbeit

Unter Telearbeit versteht man Tätigkeiten, die räumlich entfernt vom Standort des Arbeitgebers durchgeführt werden und deren Erledigung durch eine kommunikationstechnische Anbindung an die IT-Infrastruktur des Arbeitgebers unterstützt wird.

Vor der Einrichtung und Vergabe von Telearbeitszugängen muss am entfernten Arbeitsplatz eine Versperr Möglichkeit für Datenträger und Dokumente zur Verfügung stehen.

Der Zugang für Mitarbeiter, die von einem Heimarbeitsplatz aus arbeiten, ist über Remote Desktop möglich. Dabei wird über einen verschlüsselten Zugang nur der Bildschirminhalt auf den Heimrechner übertragen. Der Schutz vor Schadsoftware ist gewährleistet, da wir nur firmeneigene Geräte mit Firmen-Virenschutz verwenden.

14 Auswahl von Passwörtern

Passwörter haben grundlegende Bedeutung beim Schutz der IT-Systeme und Daten. Die richtige Auswahl und der richtige Umgang mit Passwörtern können über die Sicherheit vor unbefugten Zugriffen und Manipulationen entscheiden.

Aus Sicherheitsgründen sind Passwörter jährlich zu ändern. Ein Passwort muss aus mindestens 6 Zeichen bestehen, wobei mindestens jeweils 1 Zahl vorkommen muss.

15 BIOS-Zugangskontrolle

Das BIOS der Client-PCs ist durch ein eigenes Passwort geschützt. Dadurch können BIOS-Einstellungen nur vom Administrator geändert werden

16 Rechtestruktur auf Arbeitsplatzrechnern

Zum besseren Schutz gegen Malware und Rechnerausfälle wird streng darauf geachtet, dass administrative Rechte auf PCs nur dann genützt werden, wenn dies tatsächlich nötig ist.

Konten mit Administrator-Rechten dienen zur Administration des Computers, zur Softwareinstallation, zum Ändern grundlegender Einstellungen, zum Anlegen neuer Benutzer etc.

- Konten mit einfachen Benutzerrechten werden für alltägliche Tätigkeiten, d.h. für die eigentliche Arbeitstätigkeit, verwendet.
- Eine zusätzliche Rechtestruktur mittels eines Rollenkonzepts stellt sicher, dass Benutzer nur Daten einsehen können, die für ihren Arbeitsbereich freigegeben sind.

Benutzer haben grundsätzlich keine Administrationsrechte auf ihren Geräten und kennen auch das Administrator-Passwort nicht.

17 Wechselmedien

Wechselmedien, wie z.B. USB-Sticks, externe Festplatten, Speicherkarten oder CDs, ermöglichen den raschen und einfachen Transfer von Daten und Programmen, bringen aber auch eine Reihe von Risiken mit sich.

Derartige Risiken sind:

- das Starten fremder Betriebssysteme, durch die Schutzmechanismen umgangen werden können;
- die unbefugte Installation nicht freigegebener Software oder Schadsoftware;
- das unberechtigte kopieren von Daten auf Wechselmedien (Datendiebstahl, Verlust der Vertraulichkeit).

Eine völlige Sperre von Wechselmedien ist technisch sehr aufwendig und außerdem aus betrieblichen Gründen nicht möglich. Weiters wird durch das Setzen eines BIOS-Passworts verhindert, dass die Bootreihenfolge durch den Benutzer verändert werden kann.

18 Verschlüsselung von Arbeitsplatzsystemen

Wenn auf einem Computer, der in einer ungeschützten Umgebung betrieben oder aufbewahrt wird, schutzwürdige Daten gespeichert werden, muss Verschlüsselungssoftware eingesetzt werden.

Angesichts der hohen Diebstahls- und Verlustgefahr bei Notebooks müssen diese Geräte immer verschlüsselt werden, um sicherzustellen, dass Daten nur von ihrem rechtmäßigen Eigentümer gelesen werden können.

Bei Notebooks wird eine transparente Verschlüsselung eingesetzt. Dabei wird die gesamte Festplatte des Rechners verschlüsselt, womit alle Dateien geschützt sind. Für die Benutzer ist das bei ihrer Arbeit nicht zu bemerken.

Um zu vermeiden, dass auf wichtige Daten nicht mehr zugegriffen werden kann, weil das Passwort zu ihrer Entschlüsselung verloren gegangen ist, wurde festgelegt, dass Verschlüsselungspasswörter an sicherer Stelle hinterlegt werden.

19 Regelmäßige Software-Aktualisierungen

Durch Software-Updates können Schwachstellen beseitigt oder Funktionen erweitert werden

Updates sind vor allem dann erforderlich, wenn Schwachstellen bekannt werden, die Auswirkungen auf die Sicherheit der Systeme haben oder wenn Fehlfunktionen wiederholt auftauchen. Vor ihrem Einspielen wird die Zuverlässigkeit der neuen Komponenten und das Zusammenwirken mit bestehenden Programmen geprüft.

Auf Serversystemen kann ein fehlerhaftes Update schwerwiegende Konsequenzen hervorrufen. Daher werden auf solchen Systemen Updates erst nach ausführlicheren Tests installiert.

Aus sicherheitstechnischer Sicht besonders wichtig ist das zeitnahe Einspielen von Updates zu Betriebssystemkomponenten und Internet-Browsern, die von den Herstellern regelmäßig angeboten werden. Aber auch verschiedene andere Programme (z.B. Adobe Flash, Adobe Reader, Java…) können als Einfallstore für Schadsoftware dienen. Diese werden daher regelmäßig überprüft, um

sicherzustellen, dass ausschließlich Versionen eingesetzt werden, bei denen alle bekannten Schwachstellen behoben sind.

Da Clientsysteme geringere Verfügbarkeitsanforderungen als Serversysteme haben, sind auf Clients „automatische Updates“ konfiguriert. Diese sorgen für die automatische Durchführung sicherheitskritischer Updates und stellen gleichzeitig sicher, dass dabei ausschließlich vertrauenswürdige Quellen verwendet werden.

20 Nutzungsverbot nicht-betrieblicher Software

Um sicherzustellen, dass keine unerwünschten Programme installiert werden und das System nicht über den vorgesehenen Funktionsumfang hinaus unkontrolliert genutzt wird, ist das Einspielen bzw. die Nutzung nicht-betrieblicher Software verboten und, soweit technisch möglich,

Der Einsatz jeder Hard- und Software, die nicht für den eigentlichen Betriebszweck benötigt wird, erhöht die Gefahr des „Einschleusens“ von Schadprogrammen und verringert die Stabilität der Systeme. Generell ist daher die Nutzung privater Software (Programme, Daten) und Hardware (Notebooks, USB-Sticks, externe Festplatten, Speicherkarten etc.) untersagt.

Weitere Probleme können durch unlizenzierte Software entstehen, die von Benutzern auf Vereinsrechnern installiert wurde. Derartige Lizenzrechtsverletzungen können unter Umständen zu finanziellen Belastungen, aber auch zu Reputationsschäden für ROWA-MOSER führen.

Folgenden Maßnahmen wurden umgesetzt:

- Bei ROWA-MOSER besteht ein Nutzungsverbot für nicht betriebliche Software
- Das unautorisierte einspielen und/oder Nutzen von Software wurde, soweit möglich, mit technischen Mitteln verhindert (keine Administratorrechte).
- In unregelmäßigen Abständen werden die Rechner auf unzulässige Software überprüft; wenn derartige Software gefunden wird, muss sie umgehend deinstalliert werden.
- Die Nutzung bestimmter Programme ist grundsätzlich untersagt (z.B. Filesharing-Software oder Hacker-Tools).

21 Mobile IT-Geräte

Smartphones, Tablets und Notebooks sind heute weit verbreitet und werden auch beim ROWA-MOSER eingesetzt.

Mobile Geräte gehen leicht verloren und sind ein beliebtes Ziel für Diebstähle. Dadurch können gespeicherte Daten in falsche Hände geraten und eventuell vorhandene Passwörter und Daten gestohlen werden

Bei unzureichend abgesicherten Schnittstellen von Mobilgeräten (Bluetooth, WLAN, USB) können unter Umständen Daten ausgelesen oder Schadprogramme eingeschleppt werden.

- Schadsoftware, die auf mobilen IT-Geräten ausgeführt wird, kann Dateninhalte auslesen oder Passworteingaben aufzeichnen und versenden. Auch der Versand von Werbe-SMS an Dritte oder die automatische Anwahl kostenpflichtiger Telefonnummern ist möglich.
- Manipulierte Mobilgeräte können dazu genützt werden, vertrauliche Gespräche aufzuzeichnen und abzuhören.

- Über Internetaufrufe oder infizierte E-Mails eingeschleppte Schadsoftware kann in das interne Netzwerk gelangen.
- GPS-Empfänger und Daten des WLAN-Empfängers können dazu verwendet werden, um Bewegungsprofile zu erstellen und automatisch zu versenden.

Da der Großteil dieser Geräte für den privaten Einsatz gedacht ist, ist eine zentrale Kontrolle von Sicherheitseinstellungen nicht möglich. Die Sensibilisierung der Mitarbeiter für den sicheren Umgang mit mobilen IT-Geräten wird daher als besonders wichtig erachtet.

Folgende Regeln wurden erarbeitet:

- Mobile IT-Geräte dürfen nicht unbeaufsichtigt (etwa im Hotel oder im Auto) liegen gelassen oder anderen Personen überlassen werden. Abgesehen von der möglichen Diebstahlgefahr besteht die Möglichkeit, dass darauf gespeicherte Daten eingesehen werden oder Schadsoftware installiert wird.
- Mobilgeräte müssen ebenso wie PCs durch Passwörter vor unbefugter Inbetriebnahme geschützt werden.
- Auf mobilen IT-Geräten müssen Virenschutzprogramme betrieben und regelmäßig aktualisiert werden.
- Alle Schnittstellen, die nicht aktuell benötigt werden, müssen deaktiviert werden
- Der Verlust oder Diebstahl eines mobilen IT-Geräts muss den zuständigen Verantwortlichen sofort gemeldet werden, damit rechtzeitig Sicherheitsmaßnahmen ausgelöst werden können.
- Im Normalfall sollten nur vorher geprüfte und als sicher eingestufte Apps installiert werden. In jedem Fall müssen die Benutzer aber auf ihre Auswahl achten und dürfen nur vertrauenswürdige Programme installieren.
- Das sogenannte „Jailbreaking“, d.h. das Aushebeln der vom Hersteller vorgesehenen Sicherheitsmaßnahmen, darf auf beruflich verwendeten Mobilgeräten keinesfalls ausgeführt werden. Es setzt die Geräte besonderen, zusätzlichen Sicherheitsgefährdungen aus.
- Wenn mobile IT-Geräte weitergegeben oder entsorgt werden, müssen alle darauf gespeicherten Daten und Einstellungen gelöscht werden. Dazu eignet sich am besten ein „Factory Reset“, d.h. das Zurücksetzen des Geräts in den Auslieferungszustand. Danach wird noch manuell nachgeprüft, ob noch Informationen auf den Speichern verblieben sind.

22 Nutzung von Cloud-Speicherdiensten

Cloud-Speicherdienste wie z.B. Dropbox, iCloud oder Google Drive ermöglichen den einfachen Datenaustausch beim Einsatz mehrerer IT-Geräte und sind auch für Online-Backups geeignet. Wenn sie von den Mitarbeitern eigenmächtig eingesetzt werden, besteht aber die Gefahr, dass Daten unbemerkt aus der Organisation abfließen

Für Mitarbeiter liegt es oft nahe, ihren privaten Cloud-Speicher auch für berufliche Zwecke zu nutzen. Das kann dazu führen, dass Daten dem Zugriff der Organisation entzogen und in unsicheren Umgebungen gespeichert werden. Auch der Diebstahl von Daten wird damit erleichtert.

Für Cloud-Speicher, die aus strategischen Gründen zugelassen werden sollen, müssen die Anbieter zuvor eingehend geprüft werden (hinsichtlich Sicherheit, aber auch Datenschutz).

23 Schutz gegen Schadsoftware

Malware ist ein Sammelbegriff für unterschiedliche Arten von Schadsoftware (Viren, Trojaner, Würmer, usw.). Solche Programme können durch Löschen, Versenden oder sonstige Manipulationen unkontrollierbare Schäden an Programmen und Daten bewirken. „Schutz gegen Schadsoftware“ wir oft kurz als „Virenschutz“ bezeichnet, so auch in diesem Dokument.

24 Technische Virenschutzmaßnahmen

Zur Abwehr von Vireninfektionen sind alle Computer der Organisation mit Antivirus-Software ausgestattet. Zusätzlich werden weitere Einstellungen gesetzt, um Gefahren zu reduzieren, die aus noch unbekannter oder vom Virenschutz „übersehener“ Schadsoftware entstehen können

Auch die beste Virenschutzsoftware erzielt nie eine hundertprozentige Trefferquote. Moderne Virentypen setzen verschiedene Methoden der Tarnung ein; es ist auch Fakt, dass Viren sich schneller verändern, als die Hersteller von Antivirus-Software passende Signaturupdates erarbeiten können. Eine weitere Gefahrenquelle sind sogenannte Zero-Day-Attacken, bei denen bisher unbekannte Sicherheitslücken für Angriffe genützt werden, bevor noch Abwehrmaßnahmen verfügbar sind.

Aus diesen Gründen werden laufend Maßnahmen implementiert, um das Risiko einer Infektion weiter zu verringern.

25 Vermeidung bzw. Erkennung von Viren durch Benutzer

Alle Benutzer müssen folgende Verhaltensregeln beachten:

- Auch bei E-Mails von vermeintlich bekannten bzw. vertrauenswürdigen Absendern muss geprüft werden, ob der Inhalt der Nachricht zum Absender passt und ob die Mail bzw. das Attachment auch erwartet wurde.
- Als Attachment gesendete Programme (d.h. Dateien mit den Endungen .com, .exe, .bat, .vbs etc.) werden herausgefiltert und dem Benutzer nicht zugestellt. Sollte eine Zustellung irrtümlich passieren, so ist die IT-Abteilung zu informieren. Besondere Vorsicht ist bei doppelten, Dateinamen-Endungen („.jpg.vbs“ oder „gif.exe“) geboten.
- Auch E-Mails im HTML-Format oder Office-Dokumente (.docx, .xlsx, .pptx etc.) sowie Bildschirmschoner (.scr) können Schadfunktionen enthalten. Sie dürfen nur dann geöffnet werden, wenn sie von vertrauenswürdigen Absendern stammen und die Datei erwartet wurde.
- Mehrere E-Mails mit gleichem Betreff sind verdächtig, vor allem, wenn sie von verschiedenen Absendern stammen (Spam, Phishing).
- Phishing-Mails, d.h. Mails, in denen zur Übermittlung von persönlichen Daten oder Passwörtern (z.B. PIN oder TAN) aufgefordert wird, dürfen auf keinen Fall beantwortet werden. Auch darin angegebene Webseiten dürfen nicht geöffnet werden. Bei Erhalt einer derartigen E-Mail sollten auch die anderen Mitarbeiter darauf hingewiesen werden, dass es sich dabei um einen Betrugsversuch handelt.
- Internet-Links in E-Mails dürfen nur dann aufgerufen werden, wenn es sich um vertrauenswürdige Nachrichten handelt, und müssen mit großer Vorsicht behandelt werden: Beim Anklicken kann Schadsoftware, wie z.B. ein Verschlüsselungstrojaner, installiert oder

eine Phishing-Website aufgerufen werden. Die im Link angezeigte Website täuscht oft über die tatsächlich aufgerufene URL hinweg.

- Spam-Mails, Werbemails und andere unaufgefordert erhaltene Zusendungen dürfen nicht beantwortet werden. Die Aufforderung an den Absender, weitere Zusendungen zu unterlassen, ist kontraproduktiv: Diese Rückmeldung bestätigt nur die Gültigkeit der Empfänger-Adresse und erhöht damit das Risiko, weitere Zusendungen zu erhalten. Das Abbestellen von E-Mails ist nur bei seriösen Zustellern sinnvoll.

26 Notfallmaßnahmen im Fall von Vireninfektionen

Für Notfälle, die in Folge einer Virusinfektion auftreten können, wurden Notfallpläne erstellt, um die weitere Ausbreitung der Viren zu verhindern und möglichst rasch die Rückkehr zum Normalbetrieb einleiten zu können. Die Notfallpläne sind in der Zentralablage gespeichert.

Dabei wurden folgende Punkte behandelt:

- Den Benutzern ist eine Ansprechperson bekannt, die sie in Notfällen erreichen können, um die weiteren Maßnahmen einzuleiten und zu koordinieren.
- Es muss sichergestellt sein, dass bei Vorliegen eines neuen Virus die Updates der Virenschutzprogramme möglichst rasch auf allen Rechnern eingespielt werden.
- Falls infizierte E-Mails an andere Unternehmen (Kunden, Partner) versandt wurden, müssen diese Unternehmen umgehend darüber informiert werden, um die weitere Ausbreitung der Schadsoftware zu verhindern.
- Sollte das Virus Daten gelöscht oder verändert haben, so ist durch das Backupkonzept sichergestellt, dass die Daten aus den Datensicherungen rekonstruieren werden können.

27 Ransomware und Verschlüsselungstrojaner

Eine bedeutende Bedrohung im Bereich Internetkriminalität ist die Ransomware. Dabei handelt es sich um Schadsoftware, bei der Benutzer erpresst werden, ein „Lösegeld“ (engl. Ransom) zu zahlen, um ihren Computer weiter benutzen oder ihre Dateien öffnen zu können.

Wenn auf dem befallenen PC Netzlaufwerke verbunden sind, sind auch die Dateien auf diesen Laufwerken betroffen. Der Angriff kann daher weit über den einzelnen Computer hinausreichen und den gesamten Datenbestand der Organisation beschädigen. Verschlüsselungstrojaner können auf diese Weise zu massivem, vielleicht auch existenzbedrohendem Datenverlust führen.

Die folgenden Maßnahmen wurden getroffen, um Schäden durch Ransomware zu vermeiden:

- Das wichtigste Mittel gegen Datenverluste durch Verschlüsselungstrojaner sind regelmäßige und vollständige Datensicherungen. Dazu wurde ein umfangreiches Backup-Konzept erstellt, das regelmäßig getestet wird.

28 Netzwerksicherheit

Durch eine Netzwerkverbindung zum Internet entstehen Gefahren: Würden keine zusätzlichen Schutzmaßnahmen eingerichtet, so wäre die Verbindung in beiden Richtungen offen und es könnte vom Internet auf das ROWA-MOSER Netz und dessen Daten zugegriffen werden

29 Firewalls

IT-Systeme im internen Netzwerk dürfen nur unter Verwendung ausreichender Sicherheitseinrichtungen mit dem Internet verbunden werden. Dazu werden Firewalls eingesetzt.

Die Firewall ist so konfiguriert, dass sie die Netzwerkverbindungen zwischen Netzwerken mit unterschiedlichem Sicherheitsbedarf kontrolliert und standardmäßig alle jene Verbindungen blockiert, die nicht explizit als „erlaubt“ deklariert wurden.

Zum Einsatz kommt eine Fortinet-Firewall. Diese prüft den Datenverkehr im Detail auch auf Applikationsebene. Sie erlaubt gezielte Eingriffe in den Internetzugriff, indem z.B. einzelne Anwendungen gesperrt oder nur für bestimmte Benutzer freigegeben werden.

Jede Firewall muss richtig installiert und konfiguriert werden, um wirksam Schutz zu bieten. Sie muss außerdem laufend administriert werden. Folgende grundlegende Regeln wurden dafür erstellt:

- Jede Kommunikation zwischen internem Netz und dem Internet muss ausnahmslos über die Firewall geführt werden. Die Firewall darf nicht durch Modem-, WLAN- oder Mobile Internet-Verbindungen umgangen werden.
- Sicherheitsrelevante Updates der Firewall-Software müssen regelmäßig eingespielt werden, um zu verhindern, dass durch eine Schwachstelle der Firewall das gesamte Netzwerk gefährdet wird.
- Die Konfiguration und Administration der Firewall ist nur über eine sichere Verbindung möglich. Angreifern aus dem Internet darf es nicht möglich sein, die Konfiguration der Firewall zu verändern oder auszulesen. Auch aus dem internen Netzwerk ist der Zugang nur befugten Personen möglich.
- Eigene Audits der Firewall-Regeln werden regelmäßig durchgeführt.

30 Personal Firewalls

Beim Internetzugang unterwegs vom Notebook über WLAN oder Mobile Internet, werden Personal Firewalls eingesetzt, um einen grundlegenden Schutz gegen Fremdzugriffe zu gewährleisten.

31 Wireless LAN (WLAN)

Bei ROWA-MOSER werden sowohl kabelgebundene LANs als auch drahtlose Netzwerke eingesetzt. Sicherheitstechnisch entstehen durch WLANs neue Gefährdungen und es sind zusätzliche Maßnahmen zu beachten, um nicht die Sicherheit des gesamten Netzwerks zu gefährden.

Neben dem Ausspionieren von Daten besteht auch die Gefahr, dass Eindringlinge illegale Aktivitäten über das WLAN durchführen, für die dann der Betreiber verantwortlich gemacht wird. Ein ungesichertes WLAN kann daher auch zu rechtlichen Problemen führen.

Folgende Maßnahmen wurden daher bei der Implementierung und beim Betrieb des WLANs beachtet:

- Geeignete Positionierung und Ausrichtung der Zugriffspunkte und Antennen, um außerhalb des AV-Hauses den WLAN-Empfang möglichst zu verhindert;
- Verschlüsselungsoptionen sind aktiviert; es wird ausschließlich WPA2 eingesetzt;
- Eine Änderung der Standardeinstellungen (insbes. der Passwörter) am WLAN-Access-Point wurde vorgenommen;

- Der DHCP-Server am WLAN-Access-Point wurde deaktiviert;

32 Festlegung der Internet-Sicherheitsstrategie

Eine WWW-Sicherheitsstrategie dient zur Klärung grundlegender sicherheitsrelevanter Fragestellungen.

Die WWW-Sicherheitsstrategie von ROWA-MOSER beinhaltet folgende Grundsätze:

- WWW-Zugang ist allen Mitarbeitern gestattet
- Es werden keine Einschränkungen durch URL-Filter gemacht
- Benutzer werden regelmäßig in den Awareness-Trainings auf die Gefahren hingewiesen
- Technische Hilfestellung bei sicherheitsrelevanten Benutzerfragen findet über die IT-Abteilung statt.

Das richtige Benutzerverhalten hat wesentlichen Anteil bei der Abwehr der Gefahren, die aus der Internet-Nutzung entstehen. Jeder Mitarbeiter wird deshalb verpflichte, die einschlägigen Sicherheitsrichtlinien einzuhalten.

Beim Herunterladen von Dateien oder Programmen kann eine Vielzahl von Sicherheitsproblemen auftreten, etwa Viren, Würmer oder Trojaner. Die Benutzer müssen daher immer die Möglichkeit in Betracht ziehen, dass heruntergeladene Dateien oder Programme Schadsoftware enthalten.

33 Soziale Netzwerke

Soziale Netzwerke (Facebook, Xing, Twitter, ...) können potenzielle Risiken mitbringen:

- Einschleusen und Verbreitung von Schadsoftware über soziale Netzwerke
- Kontrollverlust über die transportierten Inhalte
- Cyber-Mobbing, d.h. öffentliches Bloßstellen und Herabwürdigen von Personen
- Produktivitätsverlust aufgrund intensiver privater Nutzung durch Mitarbeiter

Die Arbeitsplatzrechner sind durch technische Maßnahmen abgesichert, sodass möglichst verhindert wird, dass Schadsoftware von infizierten Webseiten in das interne Netzwerk gelangen kann.

34 Logging, Monitoring und Auditing

Zentrales Überwachungssystem mit Alert für Hardware, Netzwerk und Komponentencheckup doppelt. (automatisch PRTG, manuell durch IT-Abteilung)

35 Kontinuierliche Verbesserung

Aufarbeiten von Sicherheitsrelevanten Vorfällen. Organisation (Qualitätsverbesserung) wird durch Abweichungsblätter und den KVP der ISO Zertifizierung sichergestellt.

36 Datensicherung

Datensicherung und Notfallwiederherstellungsmaßnahmen helfen bei der Schadensbegrenzung nach Systemausfällen, dem Verlust einzelner Dateien oder im schlimmsten Fall der Zerstörung der gesamten IT-Infrastruktur. Verschiedene, miteinander verknüpfte Maßnahmen sind nötig, um

sicherzustellen, dass die IT-Systeme innerhalb eines definierten Zeitraums wieder funktionsfähig sind.

Durch die Datensicherungen werden auch weitere Risiken abgedeckt. So können bestimmte Datenstände zu Beweisführungszwecken wiederhergestellt werden oder Daten gerettet werden, die von Schadsoftware verfälscht oder zerstört wurden. Außerdem ermöglichen Backups, die Daten nach schwerwiegenden Vorfällen, wie z.B. einem Brand im Serverraum oder dem Diebstahl von Rechnern, wiederherzustellen.

37 Datensicherungskonzept und -planung

Voraussetzung regelmäßiger Datensicherungen ist die zentrale Speicherung aller wichtigen Daten, die auch hinsichtlich der Datensicherheit erforderlich ist. Benutzer wurden dazu verpflichtet, ihre Daten auf Netzlaufwerken der dafür vorgesehenen Server (und nicht den Festplatten ihrer Arbeitsplatzrechner) abzuspeichern.

Um eine größtmögliche Ausfallsicherheit zu gewährleisten wird gegenwärtig eine verschlüsselte Online-Datensicherung bei Tirol-Cloud genutzt.

38 Zutrittskontrolle

Die Überwachung des Zutritts zum Gebäude bzw. zu sensiblen Bereichen zählt zu den wichtigsten Schutzmaßnahmen. Ein Zutrittskontrollsystem vereinigt verschiedene bauliche, organisatorische und personelle Vorkehrungen:

Einige Bereiche sind besonders Schützenswert (Serverräume, Archive, Buchhaltung).

Aus diesen Festlegungen wurden die Anforderungen für Zutrittskontrollmaßnahmen abgeleitet, die bei der Auswahl einer Schließlösung und der Schlüsselvergabe beachtet wurden.

39 Schlüsselverwaltung

Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral geregelt. Reserveschlüssel werden vorgehalten und gesichert aufbewahrt. Schlüssel werden nur an berechtigte Personen ausgegeben.

Über die Aus- und Rückgabe aller Schlüssel werden schriftliche Aufzeichnungen geführt. Anhand dieser Listen ist es jederzeit möglich nachzuvollziehen, wer zu welchem Zeitpunkt Zutritt zu welchen Bereichen hatte. Aus diesem Grund ist es auch den Mitarbeitern verboten, ihre Schlüssel anderen zu überlassen; jede Schlüsselausgabe muss über die zentrale Ausgabestelle erfolgen.

Für den Verlust von Schlüsseln wurde ebenfalls vorgesorgt: Jedem Mitarbeiter ist bekannt, wer in diesem Fall zu verständigen ist.

40 Sicherer und rechtlich konformer Umgang mit Bewerbungen

Alle Bewerbungen müssen an die zuständige Person übermittelt werden.
Es wurde auch ein eigenes E-Mail-Postfach angelegt, auf dem Bewerbungen zentral gespeichert werden. (bewerbung@rowa-moser.at)

Dieser E-Mail-Account wird von der zuständigen Person überwacht. Diese Person stellt sicher, dass gesetzliche Löschfristen eingehalten werden.

Bewerbungen, die ausgedruckt werden und an zuständige Fachabteilungen weitergegeben werden, werden nach der Verwendung vernichtet. Das Shreddern hat allerspätestens nach 6 Monaten zu erfolgen.

Bewerbungen, die über Dritte kommen (z.B. Jobs Experts) werden unverzüglich gelöscht, wenn es zu keinem Vertragsverhältnis kommt.

Wenn Bewerbungen an Niederlassungen geschickt werden, dürfen sie nur an Niederlassungsleiter direkt gesendet werden. Die jeweiligen Niederlassungsleiter stellen die Vernichtung der Bewerbung spätestens nach 6 Monaten sicher.

41 Umgang mit geistigem Eigentum:

Geistiges Eigentum von Partnerunternehmen darf ohne Zustimmung der Geschäftsführung nicht für sich selbst genutzt, oder an unbefugte Dritte weitergegeben werden.

Zum geistigen Eigentum gehören sämtliche Marken, Kennzeichen, Warenzeichen, Gebrauchs- und Geschmacksmusterrechte, geschäftliche Bezeichnungen, Logos, Produktfotografien, Produktbeschreibungen, Datenblätter, technische Informationen und sonstige Produktinformationen und -präsentationen, unabhängig ob in digitaler Form oder körperlicher Form.