Security Policy für die Benutzung des Führerscheinregisters über Portal Austria

Version: 2.5

Erstellt am: 12.03.2018

Dokumentenparameter

Allgemeine Informationen	
Dokumententitel	Security Policy Führscheinregister
Vertraulichkeitshinweis	FSR-WT-intern
Beschreibung	Security Policy für die Benutzung des Führerscheinregisters über Portal Austria
Dokumentenverantwortlich	Mag. Wolfgang Schubert bmvit
Dokumentenart	
Review	
Review-Intervall	bei jedem WT
Datum letzter Review	<13.02.2018>
Gültigkeit	
Organisation	**bmvit**
Zielgruppe(n)	■ alle Mitarbeiterinnen und Mitarbeiter ☐ Führungskräfte ☐ Prozessverantwortliche
	☐ freigegeben ■ Entwurf / Überarbeitung ☐ archiviert
Freigabe durch	bmvit
Datum der Inkraftsetzung	12.03.2018

Version	Datum	Autor/in	Änderung
2.0	*17.01.2018*	*Josef Schmid*	*Adaptierung der Initialversion und Einarbeitung der neuesten Vorgaben und*

			Richtlinien
2.1	*29.01.2018*	*Josef Schmid*	*Adaptierung gem. FSR Wartungsteam* *Vorschläge vom 23. 1. 2018*
2.2	*07.02.2018*	*Josef Schmid*	*Änderungswünsche aus Review 31.01.2018 (bmvit, FSR WT)*
2.3	*19.02.2018*	*Josef Schmid*	*Änderungswünsche aus Review 13.02.2018 (bmvit, FSR WT)*
2.4	*09.03.2018*	*Josef Schmid*	*Freigegebene Version (bmvit, FSR WT)*
2.5	*12.03.2018*	*Josef Schmid*	*Finales Review bmvit*

Änderungen im Dokument im Vergleich zur Ursprungsversion aus dem Jahr 2009:

Das vorliegende Dokument wurde grundlegend verändert und an den Stand der Technik angepasst. Eine Referenzierung der Änderungen zum ursprünglichen Dokument ist somit nicht möglich.

Grundsätzliche Änderungen:

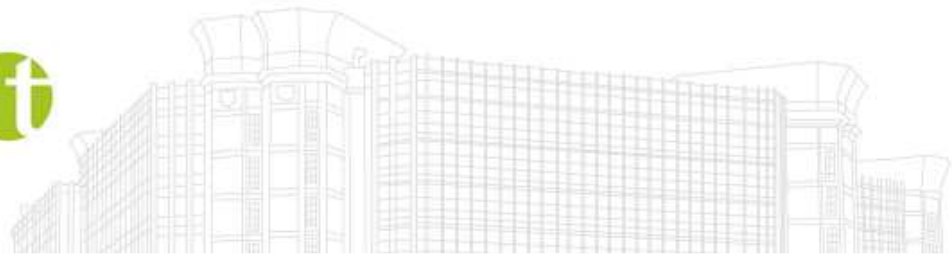
Der Zugriff auf das FSR ist nur mehr über mindestens SecClass 2 möglich.

Es wird keine Unterscheidung zwischen Prüfern und Prüfern mit Heimzugriff gemacht.

Die Regeln für Passwortsicherheit am Portal Austria wurden aufgrund des Zugriffs über SecClass 2 entfernt.

Die Checklisten wurden vereinfacht und sind nun für alle Zielgruppen gültig.

Inhaltsverzeichnis



1 Gültigkeitsbereich und Zielgruppen

Die vorliegende Security Policy ist für die im folgenden genannten Zielgruppen für den Zugriff auf die Applikation Führerscheinregister über das Portal Austria und Portalverbund gültig und durch die genannten Zielgruppen entsprechend umzusetzen

Abkürzung	**Bezeichnung und Beschreibung**
FS	**Fahrschulen**: Hier werden primär die entsprechenden Entscheidungsträger bei der jeweiligen Fahrschule angesprochen. Es ist erforderlich, dass von diesen Personen die Regelungen und Empfehlungen entsprechend aufbereitet den Mitarbeiterinnen / Benutzerinnen / Administratorinnen / Mitarbeitern / Benutzern / Administratoren / etc. zur Kenntnis gebracht werden (z.B. in Form von Schulungen, Merkblättern, etc.)
AC	**Automobilclubs**: Hier werden primär die entsprechenden Entscheidungsträger beim jeweiligen Automobilclub angesprochen. Es ist erforderlich, dass von diesen Personen die Regelungen und Empfehlungen entsprechend aufbereitet den Mitarbeiterinnen / Benutzerinnen / Administratorinnen / Mitarbeitern / Benutzern / Administratoren / etc. zur Kenntnis gebracht werden (z.B. in Form von Schulungen, Merkblättern, etc.)
PR	**Prüferinnen bzw. Prüfer**
AP	Aufsichtspersonen

Das bmvit behält sich das Recht vor, die Einhaltung der Security Policy stichprobenartig zu überprüfen.

Nachfolgende Maßnahmen sind durch das bmvit vorzugeben und in den Checklisten zu verankern:

Der Zugriff auf schützenswerte Daten hat im Rahmen einer Sicherheitsvereinbarung oder -verordnung zu erfolgen, wenn Maßnahmen durch die Anwendung nicht ausreichen. Dies gilt insbesondere für Ausdrucke (z.B.: vorläufige Führerscheine).

Allgemeine Sicherheitsvereinbarungen (wie die Portalverbundvereinbarung)können durch anwendungsspezifische Sicherheitsvereinbarungen ergänzt werden.

Dazu sind die Sicherheitserfordernisse in Sicherheitsklassen zu kategorisieren, welche mit Maßnahmen in folgenden Bereichen zu erfüllen sind:

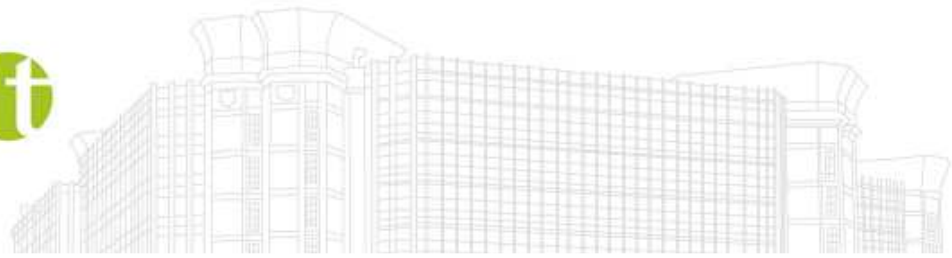
1. Bereich der Benutzer

2. Bereich der Anwendungen,

3. Bereich der Kommunikation vertrauenswürdiger Geräte und Netzwerke.

Trennung zwischen Anwendungs- und Benutzersicherheit:

Die Vereinbarung von Sicherheitsklassen gewährleistet eine adäquate Sicherheit für die Anwendungen bei Auftrennung der Verantwortung für Anwendungs- und Benutzersicherheit.



2 Gültigkeitsbereich und Zielgruppen

Die vorliegende Security Policy behandelt in allgemeiner Form Themen für den sicheren Einsatz von IT-Systemen im Rahmen der Benutzung des Führerscheinregisters und gibt entsprechende Empfehlungen und Mindestanforderungen vor.

Die beschriebenen Sicherheitsmaßnahmen basieren auf geltenden bundesweiten Empfehlungen, insbesondere dem Österreichischen Informationssicherheitshandbuch in der Version 4.0.1 (https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf).

Neben der Erhöhung der Informationssicherheit tragen die aufgezeigten Maßnahmen vor allem zur Wahrung der Rechte auf Geheimhaltung von vertraulichen und personenbezogenen Daten bei und unterstützen somit die Einhaltung wesentlicher Gesetze, wie z.B. des Datenschutzgesetzes.

Der Fokus des Dokuments liegt auf der Benutzung der Applikation "Führerscheinregister". Sicherheitsmaßnahmen für den gesamten operativen IT-Betrieb sind nur soweit enthalten, wie sie die Benutzung des Führerscheinregisters direkt betreffen.

Die Inhalte der Security Policy wurden zielgruppenspezifisch aufbereitet. Jeder Abschnitt enthält einen entsprechenden Zielgruppenvermerk und ist somit nur von den darin genannten Zielgruppen umzusetzen bzw. zu beachten.

Nur so kann eine angemessene Informationssicherheit in allen genannten Bereichen greifen und die unterschiedlichen Zielgruppen können die IT-Systeme für ihre tägliche Arbeit sicher und angemessen einsetzen.

Jene Beteiligte, die bei der Umsetzung der in diesem Dokument angeführten Maßnahmen ihre Mitwirkung beharrlich verweigern, können mit Sanktionen belegt werden.

2.1 Geltende Sicherheitsklassen

Die Sicherheitsklassen beruhen auf den Bestimmungen der E-Government Vorgaben. Aktuell gültige Version SecClass 2.0.0 (https://www.ref.gv.at/fileadmin/_migrated/content_uploads/SecClass_2-0-0_20061218.pdf) aus 2016.

Teilbereich	Si-Klasse	Vertraulichkeit	Verfügbarkeit	Integrität	DSG
Prüfer	2	**hoch**	mittel	mittel	Pers. bez.
Aufsichtsperson	2	**hoch**	mittel	mittel	Pers. bez.
Fahrschulen [1]	3	**sehr hoch**	mittel	mittel	Pers. bez.
ÖAMTC/ARBÖ	2	**hoch**	mittel	mittel	Pers. bez.

Für die Sicherheitsklasse 2 werden für das Führerscheinregister derzeit die Optionen „Authentifizierung durch Wissen und Besitz (Zertifikat)“ oder „Authentifiziert durch Wissen an in einem geschützten Bereich betriebenen Gerät“ eingesetzt.

[1] Für die Fahrschulen gibt es entsprechende Begleitmaßnahmen, welche nachfolgend erläutert werden.

Hinsichtlich der Fahrschulen besteht eine besondere Situation:

Fahrschulen haben im FSR für einen konkreten Anwendungsfall direkten Zugriff auf sensible Daten, nämlich beim Ausdruck des "vorläufigen Führerscheines".

Am "vorläufigen Führerschein" sind Zahlencodes hinterlegt, welche Rückschlüsse auf gesundheitliche Einschränkungen zulassen könnten.

Infolgedessen sind zusätzliche Maßnahmen zur Vermeidung von Datenmissbrauch angebracht.

Dazu gehören unter anderem die Lagerung der Ausdrucke in versperrten Kästen und die Verwendung von Polarisationsfiltern für Bildschirme, um die Einsicht auf die Bildschirme durch Dritte zu unterbinden. Durch diese Maßnahmen soll sichergestellt werde, dass keine unbefugten Personen in den Besitz sensibler Daten kommen können.

Deshalb erscheint es vertretbar, auch für die Fahrschulen die Sicherheitsklasse 2 zur Anwendung zu bringen.

Folgende Maßnahmen sind für die Sicherheitsklasse 2 grundsätzlich erforderlich:

- **Client-Authentifizierung:**
  - Authentifiziert durch Wissen und Besitz (SW-Zertifikat, HW-Token, Bürgerkarte, Einmalpasswort) oder
  - Authentifiziert durch Wissen an in einem geschützten Bereich betriebenen Gerät oder
  - Authentifiziert durch Wissen und Eigenschaft (biometrisch)
- **IT-Grundschutz**
  - Passwortsicherheit
  - Session Timeout
  - Keine (Zwischen-) Speicherung von Anwendungsdaten am Client
  - Schutz vor Schadprogrammen (Viren etc.)
  - Physische Sicherheit
  - Restriktives Gerätemanagement
- **Datensicherheit**
  - Unverfälscht (MAC/Hashwert im SSL
  - Einer Person zuordenbar (über Protokolle)
  - Nicht bestreitbar (über Protokolle oder Signatur)
  - Stark verschlüsselt (SSL, symmetrischer Schlüssel mindestens 100 Bit)
- **Personelle Maßnahmen**
  - Identifikation (Registrierung) entsprechend den Erfordernissen für qualifizierte Zertifikate oder durch persönliche Bekanntschaft
  - Regelungen für Mitarbeiter

3 Kennwortsicherheit und Authentifizierung

Ziele:

- Sichere Gestaltung, Handhabung und Verwaltung von Kennwörtern (Passwörter)
- Schutz von Arbeitsstationen, der Applikation Führerscheinregister sowie darin verarbeiteten vertraulichen Informationen vor unerlaubtem Zugriff

Risiken:

- Unzureichender Schutz von Informationen und deren Missbrauch
- Erraten oder "hacken" von trivialen Kennwörtern
- Unerlaubte Nutzung der Applikation Führerscheinregister bzw. unerlaubte Manipulation von Daten oder Arbeitsstationen

3.1 Authentifizierung und Kennwortsicherheit

Zielgruppen: FS, AC, PR, AP

Für jede Anwenderin, jeden Anwender (Mitarbeiterinnen und Mitarbeiter, Prüferinnen und Prüfer, Aufsichtspersonen, Wartungstechnikpersonal, etc.) von Arbeitsstationen, welche für den Zugriff auf das Führerscheinregister berechtigt werden, soll ein eigenes Benutzerkonto angelegt sein. Es muss jedenfalls die Nachvollziehbarkeit der Nutzung eindeutig gewährleistet sein.

Hierbei kann eine Namenskonvention wie z.B. „1. Buchstabe des Vornamens + Nachname“ verwendet werden. Max Mustermann würde bei dieser Nomenklatur das Benutzerkonto „MMustermann“ erhalten.

Bei der Anmeldung soll sichergestellt sein, dass das Kennwort nicht während der Eingabe ausgespäht werden kann.

Beim Anwender werden folgende Regelungen für Kennwörter empfohlen:

- Kennwörter, welche für den persönlichen Gebrauch bestimmt sind, sollen nicht an andere Personen weitergegeben oder offen gelegt werden.
- Kennwörter sollten mindestens acht Zeichen lang sein.

- Kennwörter sollten aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen.
- Alte Kennwörter sollten nicht wieder verwendet werden.
  Triviale Kennwörter sollten nicht erlaubt sein. Trivial sind z.B. Wörter, die in einem Wörterbuch stehen (unabhängig von der Sprache) oder leicht zu erratende Tastaturfolgen (z.B. 1234, qwertz) sowie Standardausdrücke (z.B. start, führerschein, kfz etc.) aufweisen. Ebenfalls in diese Gruppe fallen Kennwörter mit spezieller Bedeutung, die leicht von Außenstehenden erraten oder bestimmt werden können (z.B. Familienname, Benutzerkennung, Geburtsdatum, KFZ-Kennzeichen etc.)
  Idente Kennwörter für verschiedene Systeme oder Anwendungen sollten unbedingt vermieden werden.
  Sollten Kennwörter aufgeschrieben werden, muss diese Notiz sicher aufbewahrt werden (Behandlung z.B. wie eine Bankomatkarte)
- Kennwörter sollten zumindest alle 90 Tage geändert werden.
  Eine fünfmalige Fehleingabe des Kennworts soll zur Sperrung des Benutzerkontos führen, die ausschließlich durch den zuständigen Benutzerverwalter wieder aufgehoben werden kann.

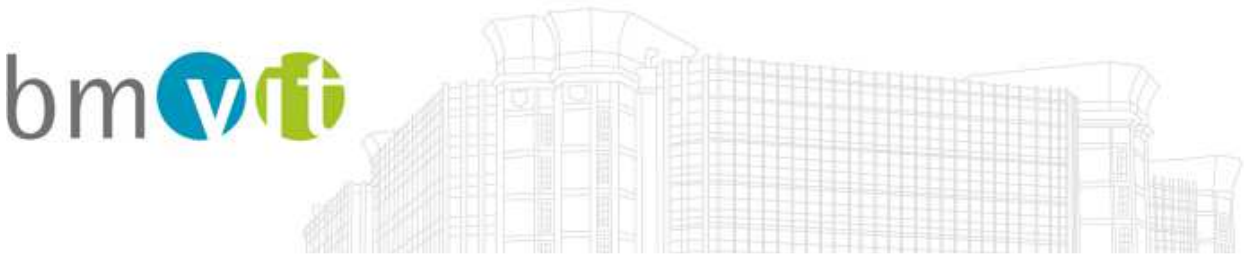
Ein Kennwort sollte sofort, d.h. außerhalb des regulären Änderungsintervalls, geändert werden, wenn

- der Verdacht besteht, dass es bekannt geworden ist,
- jemandem das Kennwort bewusst bekannt gegeben wurde (z.B. Wartungsarbeiten),
- jemand anderer das Kennwort unter besonderen Umständen verwendet hat (z.B. Vertretung oder Notfall).

In der Praxis haben sich oft Passphrasen zur Generierung von sicheren Kennwörtern bewährt.

Beispiel: „Die Fahrschule ist im 1. Bezirk und hat 13 Autos.“

Dieser Satz wird zur Erzeugung des Passwortes verwendet. Man nimmt von jedem Wort den ersten Buchstaben und sämtliche Sonderzeichen als Passwort. Daraus ergibt sich das Passwort:



Die Fahrschule ist im 1. Bezirk und hat 13 Autos.

DFii1.Buh1A.

(Anmerkung: Diese Passphrase dient als Beispiel und sollte nicht verwendet werden)

3.2 Kennwortsicherheit am Portal Austria

Zielgruppen: FS, AC, PR, AP

Für die Nutzung der Anwendung Führerscheinregister ist je nach Einrichtung der Portalumgebung eine Anmeldung am Portal Austria notwendig. Hierbei müssen die unter folgendem Link angeführten allgemeinen Nutzungsbedingungen für das Portal Austria eingehalten werden:

http://www.portal.at/Content.Node2/public/navigation/BRZG_Allgemeine_Nutzungsbedingungen.pdf

Für die Authentifizierung am Portal Austria bzw. die anschließende Nutzung des Führerscheinregisters ist ab 1 .4. 2018 zwingend eine starke Authentifizierung mittels Bürgerkarte bzw. Handysignatur notwendig.

3.3 Berechtigungsvergabe durch Administratoren

Zielgruppen: FS, AC, PR

Berechtigungen für Benutzer von Arbeitsstationen, welche als Zugangspunkt für die Applikation Führerscheinregister genutzt werden, sollten möglichst restriktiv vom Systemadministrator bzw. Berechtigungsverwalter vergeben werden. Das bedeutet, dass Benutzerinnen und Benutzern nur jene Rechte zugeteilt werden sollten, die sie zur Erfüllung ihrer Aufgaben benötigen (restriktiver Umgang mit Administrator-Rechten wird empfohlen).

Weiters wird empfohlen, die tägliche Arbeit nicht unter der Administratorkennung durchzuführen.

Benutzerkonten bzw. Berechtigungen sind zu deaktivieren, wenn die jeweilige Person die Funktion nicht mehr ausübt.

4 Informationssicherheit am Arbeitsplatz

Ziele / Grundlagen:

- Schutz von Arbeitsstationen, der Applikation Führerscheinregister sowie von vertraulichen Informationen vor unerlaubtem Zugriff bzw. unerlaubter Einsichtnahme

Risiken:

- Zugriff durch nicht berechtigte Personen
- Verlust oder Verfälschung von Informationen
- Unerwünschte Offenlegung von vertraulichen Informationen
- Einschleppung von Schadsoftware (Viren, Würmer, Trojaner, etc.)
- Aushebelung der Schutz- und Kontrollmaßnahmen des Betriebssystems

4.1 Generelle Handhabung von Informationen

Zielgruppen: FS, AC, PR, AP

Nicht öffentlich zugängliche Informationen aus dem Führerscheinregister dürfen nicht in die Hände Unbefugter gelangen sowie in Gesprächen an Unbefugte weitergegeben oder von Unbefugten mitgehört werden (siehe auch Kapitel Social Engineering).

Auf Papier gebrachte bzw. gedruckte Informationen aus dem Führerscheinregister dürfen nicht unbeaufsichtigt oder frei zugänglich liegengelassen werden (z.B. unbeaufsichtigte Ausdrucke am Drucker, vergessene Dokumente im Kopierer). Monitore müssen so aufgestellt werden, dass keine unbefugte Einsichtnahme möglich ist bzw. muss falls dies nicht möglich ist darauf geachtet werden, dass bei Arbeiten im Führerscheinregister keine unberechtigten Personen die Bildschirmeinhalte einsehen können.

Diese Maßnahmen gelten insbesondere bei der Handhabung und Verarbeitung von "vorläufigen Führscheinen".

4.2 Clean Desktop

Zielgruppen: FS, AC, PR, AP

Sollten nicht öffentlich zugängliche Informationen aus dem Führerscheinregister in Papierform vorhanden sein (z.B. Ausdrucke), müssen diese Informationen vor Beendigung der Arbeit in Schreibtischen oder Schränken zu verschließen.

4.3 Verlassen des Arbeitsplatzes

Zielgruppen: FS, AC, PR, AP

Die Arbeitsstation muss auch während kurzer Abwesenheit vom Arbeitsplatz gesperrt werden, um unbefugten Zugriff zu vermeiden.

In der Praxis wird dies häufig durch Aktivierung eines kennwortgeschützten Bildschirmschoners umgesetzt. Bei längerer Inaktivität muss der Computer automatisch den Bildschirm sperren (z.B. nach 10 Minuten).

4.4 Internetnutzung

Zielgruppen: FS, AC, PR, AP

Die Benutzerin bzw. der Benutzer der Applikation Führerscheinregister müssen über die sichere Nutzung des Internets informiert sein.

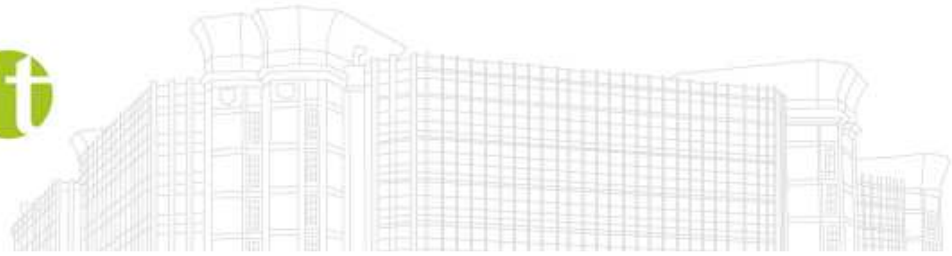
Der Webbrowser, der für den Zugriff auf das Internet verwendet wird, muss sicher konfiguriert und automatisch aktualisiert werden. Es ist darauf zu achten, dass nur aktuelle Webbrowser verwendet werden, die nach wie vor laufend mit Sicherheitsaktualisierungen (Updates) versorgt werden

In der Praxis kann in den meisten Fällen eine sichere Konfiguration rasch umgesetzt werden, indem man in den Optionen des Webbrowsers die Sicherheitseinstellungen auf „hoch“ setzt.

Unbedingt umzusetzen ist das Löschen des Webbrowser-Caches (im Microsoft Internet Explorer sind dies die temporären Internetdateien) beim Schließen des Webbrowsers.

Umsetzungshinweise für den Webbrowser „Microsoft Internet Explorer 11.x“:

- *Menüpunkt "Extras" – "Internetoptionen" – "Allgemein" – "Temporäre Internetdateien" – "Einstellungen“ - Checkbox "Bei jedem Zugriff auf die Webseite" aktivieren.*
- *Menüpunkt "Extras" – "Internetoptionen" – "Erweitert" – Kategorie Sicherheit: Checkbox*



"Leeren des Ordners für temporäre Internetdateien beim Schließen des Browsers" aktivieren. Erfolgt der Zugriff auf das Internet über Wireless LAN (WLAN) wird empfohlen, den gesamten Verkehr über eine WPA2[2] Verschlüsselung mit mindestens 128 Bit Schlüssellänge zu verschlüsseln. Eine WEP[3] Verschlüsselung ist nicht mehr zeitgemäß und sollte vermieden werden.

4.5 Software-Nutzung

Zielgruppen: FS, AC, PR, AP

4.5.1 Organisatorische Maßnahmen

Es wird empfohlen, ausschließlich die Installation jener Software zu erlauben, die durch Ihr Unternehmen freigegeben wurde und jegliche Installation von unbekannten Programmen zu verbieten. Die Benutzerinnen und Benutzer des Systems müssen über die Auswirkungen der Installation nicht freigegebener Software informiert sein.

4.5.2 Technische Umsetzung

Benutzerkonten mit Superuser- bzw. Administratorberechtigungen sollen ausschließlich für administrative Tätigkeiten des Arbeitsgerätes oder zur Softwareinstallation verwendet werden. Benutzern für laufende Tätigkeiten sollten im System nur einfache Benutzerrechte (z.B. bei Windows 10 eingeschränkte Benutzer) zugeordnet werden, die nicht berechtigen, Software auf dem System zu installieren.

[2] Wi-Fi protected Access - WPA ist eine Verschlüsselungsmethode für ein Wireless LAN. Auch hierbei ist die Sicherheit sehr stark von der Wahl und Länge der sogenannten „Pre-Shared-Keys“ abhängig.

[3] Wired Equivalent Privacy - WEP ist der ehemalige Standard-Verschlüsselungsalgorithmus für Wireless LAN und gilt heutzutage als unsicher.

4.6 PC-Konfiguration

Zielgruppen: FS, AC, PR,AP

Unkontrollierte Änderungen der Betriebsumgebung stellen ein hohes Risiko für die Sicherheit der Arbeitsstation und aller davon betroffenen Daten dar. Die Konfiguration der Arbeitsstation sollte nur durch lokal zuständige Personen (z.B. Administratoren, Wartungstechniker) verändert werden. Im Besonderen sollte dies bei Sicherheitseinstellungen, Schutzmechanismen oder ähnlichem gelten.

Updates und Patches des Betriebssystems (z.B. Windows 10) müssen in regelmäßigen Abständen (möglichst rasch nach Verfügbarkeit) eingespielt werden, um potentielle Sicherheitslöcher zu schließen. Dies kann z.B. durch automatische Updates umgesetzt werden.

Betriebssysteme, welche seitens des Herstellers keine laufenden Sicherheitsupdates mehr erhalten, dürfen für den Zugriff auf das Führerscheinregister nicht verwendet werden.

4.7 E-Mail

Zielgruppen: FS, AC, PR, AP

Durch die Nutzung von E-Mail ist die Benutzerin bzw. der Benutzer einer Reihe von Risiken ausgesetzt. Der Absenderadresse ist als Urheber der E-Mail für den Inhalt und die korrekte Empfängeradresse verantwortlich. Die Installation bzw. Aktivierung eines Spam-Filters wird empfohlen. Dieser filtert viele der unerwünschten Werbe-Mails bzw. löscht diese im Bedarfsfall. Hier muss jedoch auf falsch klassifizierte Mails geachtet werden (Mails, die von legitimen Absendern stammen, aber irrtümlich als Spam klassifiziert wurden).

5 Virenschutz

Ziele / Grundlagen:

- Schutz von Arbeitsstationen, der Applikation Führerscheinregister sowie von vertraulichen Informationen vor unerlaubtem Zugriff
- Schutz vor Datenmanipulation und Denial of Service Attacken[4]
- Gewährleistung der Verfügbarkeit der Arbeitsstation bzw. der Möglichkeit des Zugriffs auf das Führerscheinregister
- Verhalten und Vorgehen bei Virenbefall Risiken:
- Zugriff durch nicht berechtigte Personen
- Ausfall von Arbeitsstationen und somit Verlust der Möglichkeit des Zugriffs auf das Führerscheinregister
- Verlust oder Verfälschung von Informationen
- Unerwünschte Offenlegung von vertraulichen Informationen
- Schadsoftware (Viren, Würmer, Trojaner, etc.)
- Unerlaubte Nutzung der Arbeitsstation bzw. Missbrauch des Internetzugangs

5.1 Grundlagen

Zielgruppen: FS, AC, PR, AP

Viren können harmlos sein oder bösartig Daten zerstören sowie fremden Personen den Zugriff auf Arbeitsplatzsysteme ermöglichen. Auswirkungen von Computerviren oder ähnlicher schädlicher Software aller Art beeinträchtigen die Integrität bzw. Verfügbarkeit von Daten oder Arbeitsstationen. Daneben können Computerviren auch gezielt zur Offenlegung vertraulicher Daten genutzt werden.

Computerviren werden von außen oder innen in Arbeitsstationen oder Unternehmensnetzwerke eingeschleust und können sich bei mangelndem Schutz schnell verbreiten. Das Risiko, Computerviren zu erhalten, besteht insbesondere durch

[4] Angriff auf eine Arbeitsstation, mit dem Ziel einen oder mehrere Dienste „arbeitsunfähig“ zu machen

- das Öffnen infizierter E-Mail Anhänge,
- die Nutzung infizierter Speichermedien (CDs, DVD, USB-Speicher, Wechselfestplatte, Speicherkarten),
- das Zugreifen auf infizierte oder speziell präparierte Webseiten bei Arbeiten im Internet

5.2 Technische Umsetzung

Zielgruppen: FS, AC, PR, AP

Um den Befall von Viren und ähnlicher schädlicher Software zu vermeiden, muss auf allen Arbeitsstationen von denen auf das Führerscheinregister zugegriffen wird, der betriebssysteminterne Schutzmechanismus (z.B. Windows Defender) aktiviert werden.

Sollte dies nach aktuellem Stand der Technik keinen geeigneten Schutz bieten, muss ein Programm zum automatischen Erkennen und Beseitigen von Computerviren (Antiviren-Software) installiert sein. Weiters müssen die erforderlichen Virensignaturen zeitgerecht (möglichst täglich) aktualisiert werden.

Die Antiviren-Software soll sämtliche Kommunikationskanäle (Netzwerkverkehr) sowie Datenschnittstellen (z.B. USB-Stick, Internet, E-Mail, CD-ROM, DVD, etc.) überwachen. Bei Programmen sollten, soweit möglich, Makrofunktionen[5] deaktiviert werden, um die Infektion durch Makroviren zu verhindern.

Sollte in der Praxis eine Arbeitsstation ungewohnt reagieren (z.B. selbständig größer werdende Dateien, längere Reaktionszeiten), kann eine Infektion durch Computerviren die Ursache sein.

Besteht der Verdacht des Virenbefalls, muss unverzüglich die lokal zuständige Person (Systemadministrator, Wartungstechniker) informiert werden, damit gemeinsam eine Problemanalyse erfolgen kann.

[5] Makrofunktionen werden benutzt, um häufig wiederkehrende Aufgaben zu automatisieren, können jedoch auch schädlichen Code enthalten. Insbesondere für Applikationen im Microsoft Office-Umfeld (Textverarbeitung, Tabellenkalkulation) existieren häufig Makrofunktionen.

Die Antiviren-Software sollte mit einem Passwort geschützt werden und als Dienst[6] im Hintergrund permanent laufen. Dies gewährleistet, dass der Virenscanner ständig aktiv ist und auch nicht von Schadsoftware ohne weiteres deaktiviert werden kann.

Regelmäßig (möglichst rasch nach Verfügbarkeit) sollten alle Arbeitsstationen, von denen auf das Führerscheinregister zugegriffen wird, komplett auf Viren untersucht werden (vollständiger System-Scan).

[6] Dienste laufen im Hintergrund der Arbeitsstation und werden beim Hochfahren automatisch gestartet.

6 (Personal) Firewalls

Ziele / Grundlagen:

- Schutz von Arbeitsstationen, der Applikation Führerscheinregister sowie von vertraulichen Informationen vor unerlaubten Zugriff
- Gewährleistung der Verfügbarkeit der Arbeitsstationen bzw. der Möglichkeit des Zugriffs auf das Führerscheinregister

Risiken:

- Zugriff durch nicht berechtigte Personen
- Ausfall von Arbeitsstationen und somit Verlust der Möglichkeit des Zugriffs auf das Führerscheinregister
- Auspionieren des Benutzerverhaltens
- Unerwünschte Offenlegung von vertraulichen Informationen
- Schadsoftware (Viren, Würmer, Trojaner, etc.)
- Unerlaubte Nutzung der Arbeitsstation bzw. Missbrauch des Internetzugangs

6.1 Grundlagen

Zielgruppen: FS, AC, PR

Firewalls sind Programme oder Hardware, die nicht benötigte Verbindungskanäle, so genannte Ports, zu Arbeitsstationen blockieren, um Angreifern so wenig Angriffspunkte wie möglich zu bieten. Weiters bieten sie die Möglichkeit, genutzte Verbindungskanäle laufend zu prüfen. Eine Personal Firewall prüft die Aktivitäten und den Datenverkehr auf einer einzelnen Arbeitsstation. Viele Personal Firewalls kontrollieren auch den Zugang zum Internet so, dass sie nur erlaubten Programmen Zugang gewähren und alle anderen Programme blockieren.

Im Gegensatz zu Personal Firewalls, welche direkt auf der Arbeitsstation als Programm

installiert und betrieben werden, gibt es Hardware Firewalls. Solche Hardware Firewalls sind im Gegensatz zu Personal Firewalls eigene Systeme und überwachen grundsätzlich die gesamten

Netzwerkzugänge. Hinter einer Hardware Firewall kann also beispielsweise ein gesamtes Unternehmensnetzwerk abgesichert werden.

6.2 Technische Umsetzung

Zielgruppen: FS, AC, PR

Der Einsatz von Personal Firewalls kann Risiken wie das Ausbreiten von Würmern oder ähnlicher Schadsoftware erheblich minimieren. Daher müssen Personal Firewalls (z.B. aktivierte Windows Firewall unter Windows 10) auf Arbeitsstationen, von denen auf das Führerscheinregister zugegriffen wird, eingesetzt werden sofern diese nicht zumindest durch eine Hardware-Firewall geschützt sind. der Mehrstufige Schutz beim Einsatz einer Hardware-Firewall mit zusätzlichen Personal Firewalls wird dringend empfohlen.

Sind mehrere Arbeitsstationen durch Firewalls zu schützen, so wird der Einsatz von einer Hardware Firewall empfohlen. Die z.B. in Windows 10 integrierten Personal Firewalls sollten aber auch in diesem Fall weiterhin aktiv bleiben um ein zweistufiges Schutzkonzept umzusetzen.

Eine Firewall sollte nur die erlaubten Applikationen und Ports zulassen und jede andere Kommunikation unterbinden. Es ist ratsam, die Standard-Policy auf „deny“[7] zu stellen und nur die erlaubten Ports und Applikationen freizuschalten („white listing“).

[7] deny = ablehnen

7 Wartung und Entsorgung von Hard- und Software

Ziele / Grundlagen:

- Schutz von Arbeitsstationen, der Applikation Führerscheinregister sowie von vertraulichen Informationen vor unerlaubten Zugriff Risiken:
- Zugriff durch nicht berechtigte Personen
- Unerwünschte Offenlegung von vertraulichen Informationen
- Schadsoftware (Viren, Würmer, Trojaner, etc.)
- Unerlaubte Nutzung der Arbeitsstation bzw. Missbrauch des Internetzugangs

7.1 Grundlagen

Zielgruppen: FS, AC, PR

Um den ordnungsgemäßen Betrieb der Arbeitsstationen zu gewährleisten, müssen diese in regelmäßigen Abständen gewartet werden. Hierzu zählen vor allem die Installation der Updates und Bugfixes für die eingesetzte Software und der Austausch defekter Hardware (Festplatten, Lüfter, etc.)

7.2 Fernwartung/Remote Wartung

Zielgruppen: FS, AC, PR

Eine Fernwartung / Remote Wartung an Arbeitsstationen, von denen auf das Führerscheinregister zugegriffen wird, darf grundsätzlich nur unter Einhaltung folgender Regelungen durchgeführt werden:

- Der Aufbau der Verbindung für eine Fernwartung sollte immer von der lokalen Arbeitsstation
- initiiert werden, im Normalbetrieb sollte die Fernwartung gesperrt sein und nur nach expliziter Freigabe für eine genau definierte Zeitspanne aktiviert werden.
- Fernwartungstätigkeiten müssen von lokalen Benutzerinnen / Systembetreuerinnen bzw. Benutzern / Systembetreuern überwacht werden.
- Das externe Wartungspersonal muss sich zu Beginn der Wartung authentifizieren.
- Die lokale Benutzerinnen / Systembetreuerin bzw. Benutzer / Systembetreuer muss jeder einzelnen Fernwartungstätigkeit explizit zustimmen.
- Der Aufbau einer Fernwartungsverbindung muss für die Benutzerin bzw. den Benutzer deutlich sichtbar sein (z.B. Meldung, die bestätigt werden muss).
- Den lokalen Benutzerinnen / Systembetreuerinnen bzw. Benutzern / Systembetreuern muss jederzeit die Möglichkeit gegeben sein, die Fernwartung zu unterbrechen bzw. abzubrechen.
- Fernwartungsverbindungen müssen verschlüsselt werden (mind. 128 Bit Schlüssellänge).

- Werden während der Wartung Daten oder Programme auf dem lokalen PC-System installiert bzw. angelegt, so muss dies deutlich erkennbar und nachvollziehbar sein (z.B. darf dies nur in besonders markierten Verzeichnissen oder unter bestimmten Benutzerkonten erfolgen).
- Fernwartungstechniker dürfen keinesfalls auf Daten des Führerscheinregisters oder auf das Führerscheinregister selbst zugreifen

7.3 Wartungsarbeiten im Haus

Zielgruppen: FS, AC, PR

Für Wartungsarbeiten durch externes Personal im Hause an Arbeitsstationen, von denen Zugriff auf das Führerscheinregister besteht, sind folgende Vorkehrungen und Regelungen zu treffen:

- Ankündigung der Maßnahme gegenüber den betroffenen Mitarbeiterinnen / Systembetreuerinnen Mitarbeitern / Systembetreuern.
- das Wartungspersonal muss sich auf Verlangen ausweisen.
- Arbeiten sind so weit zu beaufsichtigen, dass beurteilt werden kann, ob während der Arbeit unautorisierte Handlungen vollzogen werden und ob der Wartungsauftrag ausgeführt wurde.
- Der Zugriff auf Daten durch das Wartungspersonal ist so weit wie möglich zu vermeiden.
- Auf den betroffenen Arbeitsstationen sollte für das Wartungspersonal ein eigenes Benutzerkonto existieren, unter der alle Wartungsarbeiten durchgeführt werden (Details siehe Kap. 3). Die dem das Wartungspersonal eingeräumten Zugriffsrechte sind auf das notwendige Minimum zu beschränken und nach den Arbeiten zu widerrufen bzw. zu löschen oder zu deaktivieren.
- Nach der Durchführung von Wartungsarbeiten im PC-Bereich sollte eine vollständige Virenprüfung durchgeführt werden.
- Die durchgeführten Wartungsarbeiten sind zu dokumentieren (Datum, betroffene Arbeitsstationen, Fehlerbeschreibung, Name des das Wartungspersonal).

Folgende Regelungen sollten vertraglich festgelegt werden:

- Verpflichtung zur Geheimhaltung von Daten.
- Einhaltung aller Vorschriften gemäß Datenschutzgesetz in der geltenden Fassung, insbesondere Verpflichtung auf §15 Datenschutzgesetz (DSG 2000), BGBl. I Nr. 165/1999idgF,
- das Wartungspersonal darf keinesfalls auf Daten des Führerscheinregisters oder auf das Führerscheinregister selbst zugreifen
- Verpflichtung, dass ersetzte defekte Datenträger (z.B. Festplatten) nicht an das Wartungspersonal zurückgegeben sondern entsprechend Abs. 7.5 behandelt werden.
- Verpflichtung, Daten, die im Rahmen der Wartung extern gespeichert wurden, nach Abschluss der Arbeiten sicher zu löschen.

- Festlegung der Pflichten und Kompetenzen des externen Wartungspersonals.

7.4 Externe Wartungsarbeiten

Zielgruppen: FS, AC, PR

Zusätzlich zu den in Abs. 7.3 – Wartungsarbeiten im Haus – angeführten Maßnahmen, die sinngemäß auch für die Wartung von Arbeitsstationen außer Haus gelten, sind eine Reihe von weiteren Maßnahmen zu treffen, die im Folgenden kurz angeführt werden:

Werden Arbeitsstationen, von denen auf das Führerscheinregister zugegriffen wird, zur Wartung außer Haus gegeben, so sind die Datenträger (z.B. Festplatten) zuvor zu entfernen bzw. sicher durch mehrmaliges Überschreiben zu löschen (eine entsprechende Datensicherung wird davor dringend empfohlen). Ist dies nicht möglich, weil der Defekt z.B. den Datenträger selbst betrifft, so dürfen defekte Datenträger nicht zur Wartung bzw. im zur Reparatur vorgesehenen Gerät verbleiben sondern sind, wie im Abs. 7.5 beschrieben, zu vernichten bzw. zu entsorgen. Da eine Reparatur von Datenträgern wie z.B. Festplatten ohnedies kaum möglich ist, wird ein Tausch durch einen neuen Datenträger empfohlen.

Weiters ist zu beachten:

- Bei Versand oder Transport der zu reparierenden Arbeitsstationen ist darauf zu achten, dass Beschädigungen und Diebstahl vorgebeugt wird.
- Bei Arbeitsstationen, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten und der Art der Passwortabsicherung alle oder einige Passwörter entweder bekannt gegeben oder auf festgelegte Einstellungen wie z.B. "REPARATUR" gesetzt werden, damit das Wartungspersonal auf die Geräte zugreifen kann. Diese müssen vor produktiver Inbetriebnahme abgeändert bzw. deaktiviert werden.
- Nach der Rückgabe der Arbeitsstationen oder Komponenten sind alle Passwörter zu ändern. Es wird empfohlen, elektronische Datenträger nach der Rückgabe auf Viren zu prüfen.

7.5 Entsorgung bzw. Ausscheidung von Arbeitsstationen und Datenträgern

Zielgruppen: FS, AC, PR

Bei Entsorgung bzw. Ausscheidung von Speichermedien sind diese zuvor durch mehrmaliges Überschreiben sicher zu löschen.

Liegt ein Defekt des Datenträgers vor und können die im Vorfeld erwähnten Programme nicht mehr angewandt werden, muss der Inhalt durch physische Vernichtung (z.B. durch Shreddern) des Datenträgers durchgeführt werden.

Weder das Löschen von Dateien, noch das Formatieren oder Partitionieren einer Festplatte beseitigt die darauf enthaltenen Daten wirklich, so dass Daten mit geeigneten Programmen wiederhergestellt werden können. Das liegt daran, dass Windows Dateien bei der „Löschung“ nicht überschreibt. Die Dateiinhalte bleiben so lange erhalten, bis sie zufällig von neuen Daten überschrieben werden.

Am einfachsten lassen sich einzelne Dateien oder auch ganze wieder beschreibbare Datenträger durch mehrmaliges Überschreiben mit zufälligen Zeichenfolgen nachhaltig löschen.

Kostenlose Programme zur sicheren Löschung sind im Internet erhältlich. Liegt ein Defekt des Datenträgers vor und können die im Vorfeld erwähnten Programme nicht mehr angewandt werden, muss der Inhalt durch physische Vernichtung (z.B. durch Shreddern) des Datenträgers durchgeführt werden.

Bei der Weitergabe an Dritte zur Entsorgung (wie auch bei einem Austausch oder bei einer Reparatur von Festplatten) ist durch entsprechende Absicherung zu gewährleisten, dass die ausgetauschte, defekte Festplatte nicht an einen Verwerter für gebrauchte Platten weitergeleitet wird und so Daten evtl. durch eine Drittperson wieder rekonstruiert werden können.

8 Physikalische Sicherheit

Ziele / Grundlagen:

- Physikalischer Schutz betriebswichtiger IT-Komponenten
- Gewährleistung der Verfügbarkeit der Arbeitsstationen bzw. der Möglichkeit des Zugriffs auf das Führerscheinregister Risiken:
- Unbefugte verschaffen sich Zugang zu den Arbeitsstationen oder IT-Komponenten und greifen in unerwünschter und schädlicher Weise unbemerkt zu
- Diebstahl der IT-Komponenten
- Unerwünschte Offenlegung von vertraulichen Informationen

8.1 Grundlagen

Zielgruppen: FS, AC

Dieses Kapitel behandelt das Thema Zutrittsschutz bei Arbeitsstationen und zentrale Netzwerk und Telekommunikationskomponenten. Neben den technischen Maßnahmen zur Erhöhung der Informationssicherheit ist es wesentlich, dass ein unberechtigter Zugang zu den Arbeitsstationen unterbunden ist.

Folgende Regelungen sind zu beachten:

- Der Zugang zu Arbeitsstationen, von welchen auf das Führerscheinregister zugegriffen werden kann und der Zugang zu anderen schützenswerten IT-Komponenten (z.B. Netzwerkverteiler) darf möglichst nur befugten Personen ermöglicht werden.

8.2 Sichere Handhabung von gedruckten oder kopierten Unterlagen

Zielgruppen: FS, AC, PR

Nicht öffentlich zugängliche Informationen aus dem Führerscheinregister dürfen nicht in die Hände Unbefugter gelangen oder an Unbefugte weitergegeben werden. Auf Papier gebrachte, gedruckte oder kopierte Informationen aus dem Führerscheinregister dürfen nicht unbeaufsichtigt oder frei zugänglich liegengelassen werden. Nach dem Kopieren solcher Unterlagen mit vertraulichen bzw. personenbezogenen Daten des Führerscheinregisters muss darauf geachtet werden, dass Vorlagen nicht im Kopierer zurückgelassen werden.

Es muss sichergestellt sein, dass Fehlkopien, Fehldrucke bzw. nicht mehr benötigte Dokumente sicher durch einen Aktenvernichter oder andere geeignete Maßnahmen vernichtet werden (z.B. mind. Sicherheitsstufe 2 laut ÖNORM S2109).

9 Social Engineering

Ziele / Grundlagen:

- Mitarbeiterinnen und Mitarbeiter sollen Social Engineering Attacken auf Personen im Vorfeld erkennen und angemessen reagieren

Risiken:

- Zugriff auf Informationen durch nicht berechtigte Personen
- Unerwünschte Offenlegung von vertraulichen Informationen
- Unerlaubte Nutzung der Arbeitsstation bzw. Missbrauch des Internetzugangs

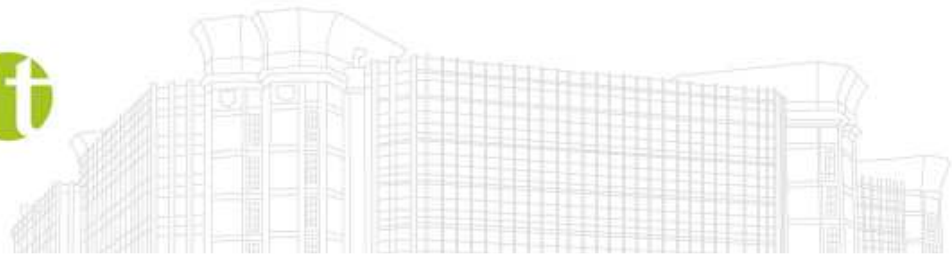
Zielgruppen: FS, AC, PR, AP

Unter Social Engineering werden Angriffe auf Unternehmen mit nicht-technischen Hilfsmitteln verstanden. Ziel von Angriffen ist es, unberechtigten Zugriff auf Informationen oder IT-Systeme zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z.B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Typische Fälle von Angriffen mit Hilfe von Social Engineering sind das Erfragen von Informationen über das Telefon oder das Durchsuchen des Abfalls nach brauchbaren Informationen (Passwörter, nicht mehr benötigte Ausdrucke usw.). Häufig verläuft ein Social Engineering Angriff mehrstufig. Der Angreifer gibt sich als Mitarbeiterin, Kundin oder IT-Technikerin bzw. Mitarbeiter, Kunde oder IT-Techniker aus und überzeugt eine Benutzerin bzw. einen Benutzer durch geschickte Täuschung von seiner Identität. Oft wird über einen längeren Zeitraum ein Vertrauensverhältnis aufgebaut, indem die Angreifer wiederum unproblematische Anfragen über das Telefonat stellen. Hat der Angreifer ausreichend Informationen gesammelt und wurde die Vertrauensstellung gefestigt, geht der Angreifer zu seinem eigentlichen Ziel über und bittet sein Opfer um einen entscheidenden „Gefallen“. Der Angreifer erhält häufig Informationen, die die Mitarbeiterin bzw. der Mitarbeiter einem Unbekannten nie zukommen lassen würde.

Häufig wird der Angriff vom Opfer nicht einmal registriert. Statistisch gesehen sind neue Mitarbeiterinnen und Mitarbeiter, die mit den Verhältnissen noch nicht vertraut sind sowie Mitarbeiter mit direktem Kundenverkehr am häufigsten betroffen.

Der beste Schutz gegen diese Art von Angriff ist die Schulung der Mitarbeiterinnen und Mitarbeiter. Hierdurch wird ein Bewusstsein für die Gefahr geschaffen, wodurch die Mitarbeiter in die Lage versetzt werden, Gefahren zu erkennen zu vermeiden. Bestimmte Verhaltensregeln erleichtern den Mitarbeiterinnen und Mitarbeiter diese Gefahrenvermeidung. Konkret sollten Mitarbeiterinnen und Mitarbeiter:

- Keine Auskunft an unbekannte Personen erteilen.
- Aufpassen, dass sie bei der Eingabe von Passwörtern nicht beobachtet werden (Shouldersurfing).



- Vertrauliche Daten dauerhaft zerstören
- Vertrauliche Papierdokumente in Aktenvernichtern zerstören
- Mitarbeiterinnen und Mitarbeiter ist infolge des dauernden Umgangs mit sensiblen Informationen nicht mehrbewusst, dass diese geheim sind. Bei sozialen Aktivitäten in öffentlichen Räumen sollte nicht über sensible Angelegenheiten gesprochen werden (Personen auf Nebentischen hören mit).
- Keine vertraulichen Informationen über anonyme Kanäle (Telefon, E-Mail) weitergeben.

Mitarbeiterinnen und Mitarbeiter sollten auf jeden Fall auffällige oder unzulässige Anfragen oder Handlungsweisen mit den Kollegen besprechen und dokumentieren – so weiß man, ob der Anrufer es schon bei anderen Kollegen versucht hat. In solchen Gesprächen können auch neue Gegenmaßnahmen gefunden werden und ein Gefühl für den Wert der Informationen entwickelt werden.

10 Sicherheitssensibilisierung und Schulung

Ziele / Grundlagen:

- Regelmäßige Vermittlung einer angemessenen Kenntnis im sicheren Umgang mit Arbeitsstationen und durchzuführende Maßnahmen, um Informationssicherheit zu erhöhenbzw. hoch zu halten.

Risiken:

- Sicherheitsmaßnahmen werden nicht effizient eingesetzt bzw. nicht genutzt
- Informationssicherheit kann nicht auf einem hohen Niveau gehalten werden
- Zugriff auf Informationen durch nicht berechtigte Personen
- Unerwünschte Offenlegung von vertraulichen Informationen

Zielgruppen: FS, AC

Jeder Mitarbeiter ist für die ordnungsgemäße Handhabung der zur Verfügung gestellten Daten und für ein adäquates sicherheitsbewusstes Verhalten („Awareness“) verantwortlich. Letzteres muss durch geeignete Maßnahmen gefördert werden. Dies kann durch regelmäßige Schulungen (zumindest jährlich) erreicht werden, bei denen den Mitarbeiterinnen und Mitarbeiter die bestehenden Sicherheitsmaßnahmen erläutert werden sowie ein Überblick über Gefahren und Angriffstechniken gegeben wird, damit sie diese später auch erkennen können.

Besonders sollte der sichere Einsatz von Arbeitsstationen, das rasche Erkennen von Sicherheitslücken sowie das richtige Verhalten und präventive Setzen von Schutzmaßnahmen regelmäßig allen Mitarbeiterinnen und Mitarbeitern näher gebracht werden.

Anmerkung: PR und AP sind selbst für die Einhaltung der in dieser Policy gelisteten Maßnahmen und Regelungen verantwortlich.

11 Regelungen für Sicherheitsvorfälle

Ziele / Grundlagen:

Allen Mitarbeiterinnen und Mitarbeitermuss ein klares Verständnis darüber entstehend, wie mit einem Sicherheitsvorfall richtig umgegangen werden soll, um

- die Information über potentielle Sicherheitsvorfälle rasch zur Verfügung zu stellen
- einen geregelten Ablauf von der Meldung bis hin zur Behebung zu etablieren
- notwendige Maßnahmen zur Verbesserung der IT-Sicherheit abzuleiten

Risiken:

- Sicherheitsvorfälle werden nicht erkannt bzw. nicht rechtzeitig erkannt
- Sicherheitsvorfälle werden nicht angemessen behandelt
- Zugriff auf Informationen durch nicht berechtigte Personen
- Unerwünschte Offenlegung von vertraulichen Informationen
- Unerlaubte Nutzung der Arbeitsstation bzw. Missbrauch des Internetzugangs

Zielgruppen: FS, AC, PR, AP

Entdeckt eine Mitarbeiterin bzw. ein Mitarbeiter (Zielgruppen FS, PR, AC, AP) eine Anomalie im Betrieb eines Computersystems oder erkennt sonstige Verdachtsmomente auf einen möglichen Sicherheitsvorfall, muss dies unverzüglich an den zuständigen Systemadministrator oder Wartungstechniker melden.

Auf Basis der gemeldeten Sicherheitsvorfälle sollten geeignete Maßnahmen zur Behebung bestehender, aber auch zur Vermeidung möglicher zukünftiger Sicherheitsmängel abgeleitet werden.

Bei kritisch erscheinenden Sicherheitsvorfällen (z.B. Diebstahl einer Arbeitsstation, von der auf das Führerscheinregister zugegriffen wird) ist eine Meldung an die zuständige Behörde durchzuführen (Zielgruppen FS, AC, PR, AP)

12 Nutzung der Applikation „Führerscheinregister“

Ziele / Grundlagen:

Den Benutzerinnen und Benutzern soll die Gefahr von gefälschten Internetseiten vor Augen geführt und gezeigt werden, wie man die besuchten Seiten auf ihre Echtheit prüfen kann. Auch der sichere Umgang bei der Verwendung der Applikation soll vermittelt werden.

Risiken:

- Benutzerkonto und Kennwort werden in einer gefälschten Maske eingegeben
- Nicht beendete Sitzungen werden gestohlen
- Zugriff auf Informationen durch nicht berechtigte Personen
- Unerwünschte Offenlegung von vertraulichen Informationen

Zielgruppen: FS, AC, PR, AP

Die Kommunikation über das Internet zwischen der Applikation Führerscheinregister und der Benutzerin bzw. dem Benutzer erfolgt über eine sichere, verschlüsselte Verbindung. Dies soll gewährleisten, dass niemand die Kommunikation abhören und so an Daten, Benutzerkonto und Kennworte der Benutzerinnen bzw. Benutzer gelangen kann. Für diese Verschlüsselung wird ein Zertifikat verwendet, das sicherstellt, dass man tatsächlich mit dem Server des BRZ verbunden ist.

Benutzerinnen bzw. Benutzer der Applikation Führerscheinregister sollten bei der Verwendung darauf achten, dass die Verbindung verschlüsselt ist. Dies ist durch ein Sicherheitssymbol im Webbrowser, wie etwa einen Schlüssel oder ein Vorhängeschloss, erkennbar. Klickt man auf dieses Symbol, werden Details bezüglich des verwendeten Zertifikats angezeigt. Hierbei sollte darauf geachtet werden, dass der Name des Zertifikatsbesitzers korrekt ist.

Benutzt man z.B. das Führerscheinregister über das Portal Austria, muss als Organisation „Bundesrechenzentrum GmbH“ sowie signon.portal.at aufscheinen. Damit eine sichere Verschlüsselung möglich ist, sollte stets die aktuellste Version des bevorzugten Webbrowsers verwendet werden.

Bei der weiteren Verwendung des Führerscheinregisters sind folgende Punkte zu beachten:

- Jede Benutzerin bzw. jeder Benutzer bekommt einen eigenen Zugang durch Benutzerkonto und Kennwort.
- Abgerufene Daten dürfen nicht explizit gespeichert werden (z.B. bei Downloads nicht „Speichern unter“ sondern „Öffnen“ auswählen).
- Bevor das Webbrowserfenster geschlossen wird, ist die aktive Sitzung durch das Klicken des „Abmeldebuttons“ zu beenden.

Wird der personalisierte Zugang nicht mehr benötigt (z.B. Austritt der Mitarbeiterin bzw. des Mitarbeiters, Pensionierung, etc.) müssen die zuständigen Personen entsprechende Löschung bzw. Deaktivierung des Benutzerkontos veranlassen.

13 Erläuterungen der Begriffe

Arbeitsstation:

Subsumierter Begriff für Personal Computer (PC), Laptop, Server, Tablet-PC.

Benutzerin bzw. Benutzer:

Der Begriff Benutzerin bzw. Benutzer (von Arbeitsstationen) bezieht sich auf die im jeweiligen Kapitel gelisteten Zielgruppen bzw. deren Mitarbeiterinnen und Mitarbeitern.

Bildschirmschoner:

Ein kennwortgeschützter Bildschirmschoner ist ein Hilfsmittel des Zugangsschutzes, wenn er so eingerichtet ist, dass er nach einer kurzen Zeit der Inaktivität den Client sperrt und den Zugang zum IT-System erst nach erneuter Authentifizierung ermöglicht.

Computerviren:

Sind Programme oder Programmteile, die über Datenträger, Netze oder Einrichtungen zur Datenübertragung auf einen Rechner gelangen. Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware (zum Beispiel Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion).

IT-Ressourcen:

Zusammenfassender Begriff für Anwendung, System, Dateien und Verfahren.

Kennwort:

Ein Kennwort ist eine Zeichenfolge, die ein berechtigter Benutzer für den Systemzugang oder für den Zugang zu Daten wissen muss.