# IT-Checkliste

# „Datenintegrität“

Spuren sind vorhanden und sichergestellt!


… aber wer kommt als Täter in Frage ?

## 1.1 Inhaltsverzeichnis

## 1.2 Überblick zur Checkliste

**Hintergrund**: IT-Systeme unterstützen uns in zahlreichen Lebensbereichen und bilden einen integralen Bestandteil unserer Gesellschaft. Mit der zunehmenden Verbreitung spielen IT-Systeme jedoch immer häufiger auch eine zentrale Rolle im Zusammenhang mit kriminellen Handlungen, wodurch die Bedeutung von elektronischen Spuren und Beweisen zunimmt. Umfeldabklärungen bei Strafverfolgungen mit IT-Bezug sind (neben der ordnungsgemässen Sicherstellung von digitalen Beweismitteln) eine wesentliche Voraussetzung für eine bessere Einschätzung und erhöhte Aussagekraft vor Gericht.

**Zweck**: Wenn Umfeldabklärungen bei Strafverfolgungen mit IT-Bezug durchgeführt werden, soll die vorliegende Checkliste helfen, die folgende Frage zu beantworten: „Haben unberechtigte Personen die Möglichkeit gehabt, auf das IT-System zuzugreifen und Daten zu manipulieren?“ Dadurch soll besser eingeschätzt und eingegrenzt werden können, wer welche Eingaben / Transaktionen am IT-System durchgeführt hat und welcher Person der digitale Beweis zuzuordnen ist.

**Zielpublikum**: Strafverfolgungsbehörden und Verteidiger – Die Checkliste ist so aufgebaut, dass für eine erste Beurteilung keine vertieften Informatik-Kenntnisse notwendig sind.

**Theorie und Grundlage**: IT-Sicherheit wird häufig unterteilt nach den Zielen „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“. Zur Beantwortung der Frage nach dem eigentlichen Urheber einer Transaktion im IT-System wird primär die „Datenintegrität“ angesprochen, sekundär auch die „Vertraulichkeit“. So gefährden öffentliche Passwörter nämlich indirekt die Datenintegrität. Die Checkliste basiert auf den IT-Grundschutzkatalogen des Deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI; Kataloge im Internet gratis abrufbar unter „http://www.bsi.de“). Aus den über 900 detailliert beschriebenen Massnahmen wurden 61 Massnahmen ausgewählt, wobei die Auswahl aufgrund des Zwecks der Checkliste sowie des Zielpublikums erfolgte. Die Titel wurden übernommen und mit eigenen Fragen, Beispielen und Risikobeschreibungen der Autoren ergänzt. Zudem sind Referenzen zu den konkreten Massnahmen gemäss IT-Grundschutzkatalogen angegeben. (Tipp: Im elektronischen Dokument sind die Hyperlinks aktiviert.)

**Benutzeranleitung**: Die Checkliste sollte verwendet werden, wenn der Ermittlungsauftrag formuliert wird. Ebenso kann die Liste auch im Anschluss an die Sicherstellung von digitalen Beweisen benutzt werden, um weitere Umfeldabklärungen zu machen. Dabei sind die für den konkreten Fall relevanten Module (wie beispielsweise Computer-Basis, mobiler Einsatz, Netzwerkanschluss) gemäss der im nächsten Kapitel aufgeführten Beschreibung auszuwählen. Fragen, welche mit „Nein“ beantwortet werden, geben Hinweise auf Schwachstellen und Risiken. Zudem können sich durch ein „Nein“ einige der nachfolgenden Fragen erübrigen. Mit Stern (★) gekennzeichnete Themen sind besonders wichtig und daher speziell zu beachten.

**Annahme**: Die digitalen Beweise sind ordnungsgemäss erhoben worden.

**Autoren**: Christian de Raemy, Nicole Jerjen, Andreas Löwinger, Daniel Russenberger,
Anita Tschopp

## 1.3 Leporello und Ablauf-Schema

Als Arbeitshilfe stehen zur Verfügung:
- drei Leporellos (Checklisten in Kurzform);
- drei Ablauf-Schemata;
- eine Detail-Checkliste;
- ein Glossar.

Die Vorgehensweise:
a) Auswahl des Leporellos;
b) Festlegen der anwendbaren Module mit Hilfe des dazugehörenden Ablauf-Schemas;
c) Abarbeiten der Prüfpunkte von oben nach unten;
d) Prüfen, ob ein Mangel für den konkreten Sachverhalt relevant ist (bei Nein-Antworten).

Der Leporello dient der Übersicht in Form einer Checkliste. Für die unterschiedlichen Verwendungen von Geräten gibt es drei verschiedene Leporellos:
- Heimarbeitsplatz;
- Geschäftsarbeitsplatz;
- Mobiler Einsatz.

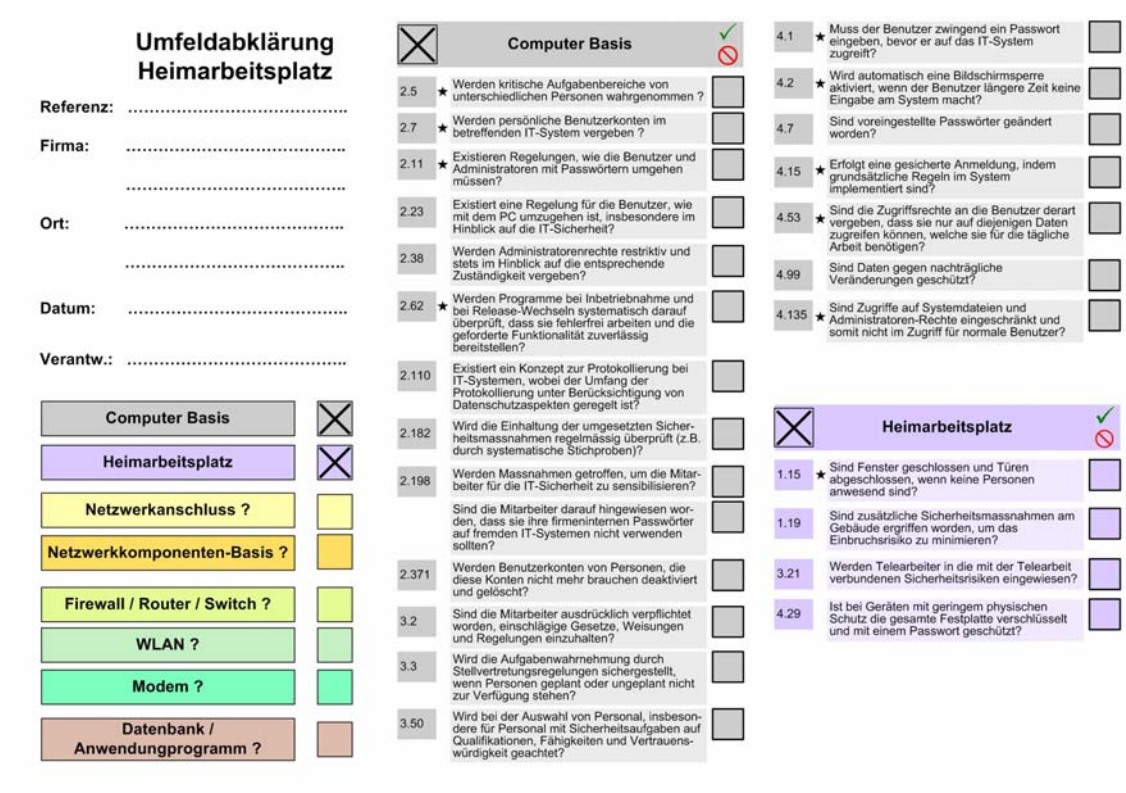
Mit Hilfe des Ablaufschemas kann für den jeweiligen Leporello festgelegt werden, welche Module anwendbar sind.

In der Detail-Checkliste sind zusätzliche Erläuterungen meist in Form von Beispielen enthalten. Zudem wird beschrieben, welche Risiken bestehen, wenn die Frage mit „Nein“ beantwortet wird. Schliesslich wird auf weitere hilfreiche Informationen in den IT-Grundschutz-Katalogen verwiesen. Die Hyperlinks zeigen auf die vollständige Beschreibung der Massnahmen gemäss IT-Grundschutz-Katalogen.

Im Glossar sind die in der Checkliste verwendeten IT-Fachausdrücke kurz erläutert.

## Heimarbeitsplatz

Leporello Vorderseite



**Umfeldabklärung Heimarbeitsplatz**

Referenz: .....

Firma: .....

.....

Ort: .....

.....

Datum: .....

Verantw.: .....

- Computer Basis
- Heimarbeitsplatz
- Netzwerkanschluss ?
- Netzwerkkomponenten-Basis ?
- Firewall / Router / Switch ?
- WLAN ?
- Modem ?
- Datenbank / Anwendungprogramm ?

**Computer Basis**

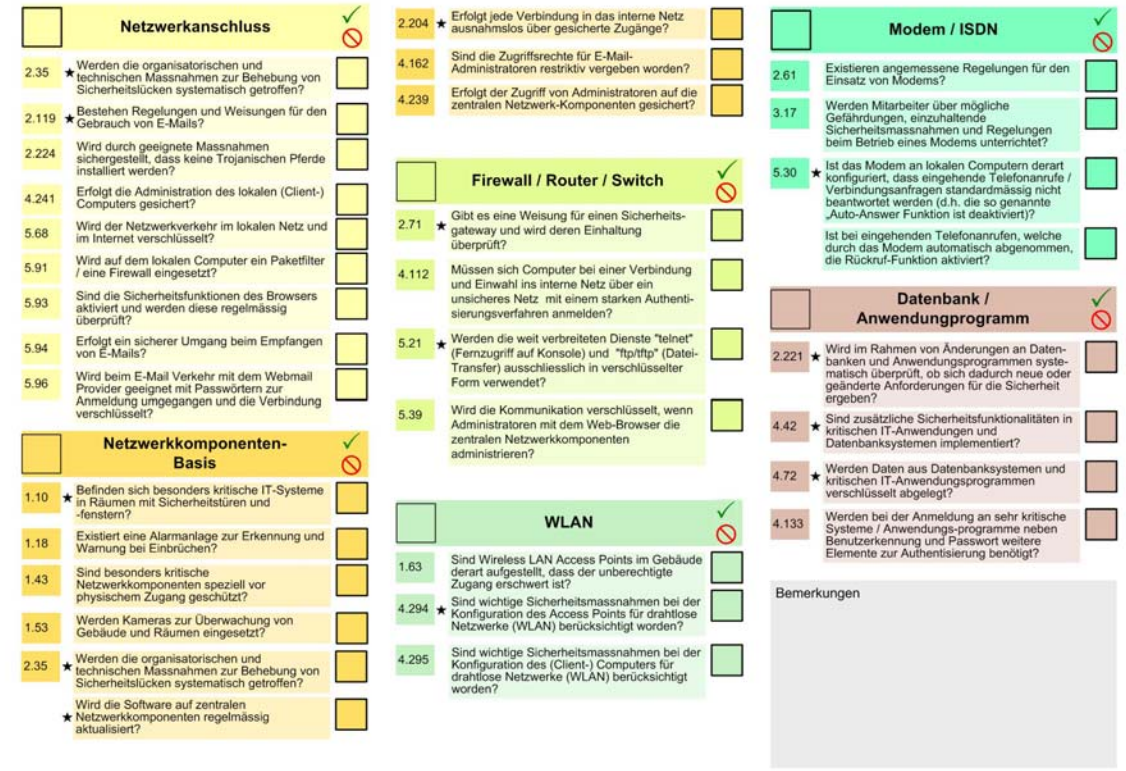
- 2.5 ★ Werden kritische Aufgabenbereiche von unterschiedlichen Personen wahrgenommen ?
- 2.7 ★ Werden persönliche Benutzerkonten im betreffenden IT-System vergeben ?
- 2.11 ★ Existieren Regelungen, wie die Benutzer und Administratoren mit Passwörtern umgehen müssen?
- 2.23 Existiert eine Regelung für die Benutzer, wie mit dem PC umzugehen ist, insbesondere im Hinblick auf die IT-Sicherheit?
- 2.38 Werden Administratorenrechte restriktiv und stets im Hinblick auf die entsprechende Zuständigkeit vergeben?
- 2.62 ★ Werden Programme bei Inbetriebnahme und bei Release-Wechseln systematisch darauf überprüft, dass sie fehlerfrei arbeiten und die geforderte Funktionalität zuverlässig bereitstellen?
- 2.110 Existiert ein Konzept zur Protokollierung bei IT-Systemen, wobei der Umfang der Protokollierung unter Berücksichtigung von Datenschutzaspekten geregelt ist?
- 2.182 Wird die Einhaltung der umgesetzten Sicherheitsmassnahmen regelmässig überprüft (z.B. durch systematische Stichproben)?
- 2.198 Werden Massnahmen getroffen, um die Mitarbeiter für die IT-Sicherheit zu sensibilisieren?
- Sind die Mitarbeiter darauf hingewiesen worden, dass sie ihre firmeninternen Passwörter auf fremden IT-Systemen nicht verwenden sollten?
- 2.371 Werden Benutzerkonten von Personen, die diese Konten nicht mehr brauchen deaktiviert und gelöscht?
- 3.2 Sind die Mitarbeiter ausdrücklich verpflichtet worden, einschlägige Gesetze, Weisungen und Regelungen einzuhalten?
- 3.3 Wird die Aufgabenwahrnehmung durch Stellvertretungsregelungen sichergestellt, wenn Personen geplant oder ungeplant nicht zur Verfügung stehen?
- 3.50 Wird bei der Auswahl von Personal, insbesondere für Personal mit Sicherheitsaufgaben auf Qualifikationen, Fähigkeiten und Vertrauenswürdigkeit geachtet?

- 4.1 ★ Muss der Benutzer zwingend ein Passwort eingeben, bevor er auf das IT-System zugreift?
- 4.2 ★ Wird automatisch eine Bildschirmsperre aktiviert, wenn der Benutzer längere Zeit keine Eingabe am System macht?
- 4.7 Sind voreingestellte Passwörter geändert worden?
- 4.15 ★ Erfolgt eine gesicherte Anmeldung, indem grundsätzliche Regeln im System implementiert sind?
- 4.53 ★ Sind die Zugriffsrechte an die Benutzer derart vergeben, dass sie nur auf diejenigen Daten zugreifen können, welche sie für die tägliche Arbeit benötigen?
- 4.99 Sind Daten gegen nachträgliche Veränderungen geschützt?
- 4.135 ★ Sind Zugriffe auf Systemdateien und Administratoren-Rechte eingeschränkt und somit nicht im Zugriff für normale Benutzer?

**Heimarbeitsplatz**

- 1.15 ★ Sind Fenster geschlossen und Türen abgeschlossen, wenn keine Personen anwesend sind?
- 1.19 Sind zusätzliche Sicherheitsmassnahmen am Gebäude ergriffen worden, um das Einbruchsrisiko zu minimieren?
- 3.21 Werden Telearbeiter in die mit der Telearbeit verbundenen Sicherheitsrisiken eingewiesen?
- 4.29 Ist bei Geräten mit geringem physischen Schutz die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt?

Leporello Rückseite



**Netzwerkanschluss**

- 2.35 ★ Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen?
- 2.119 ★ Bestehen Regelungen und Weisungen für den Gebrauch von E-Mails?
- 2.224 Wird durch geeignete Massnahmen sichergestellt, dass keine Trojanischen Pferde installiert werden?
- 4.241 Erfolgt die Administration des lokalen (Client-) Computers gesichert?
- 5.68 Wird der Netzwerkverkehr im lokalen Netz und im Internet verschlüsselt?
- 5.91 Wird auf dem lokalen Computer ein Paketfilter / eine Firewall eingesetzt?
- 5.93 Sind die Sicherheitsfunktionen des Browsers aktiviert und werden diese regelmässig überprüft?
- 5.94 Erfolgt ein sicherer Umgang beim Empfangen von E-Mails?
- 5.96 Wird beim E-Mail Verkehr mit dem Webmail Provider geeignet mit Passwörtern zur Anmeldung umgegangen und die Verbindung verschlüsselt?

**Netzwerkkomponenten-Basis**

- 1.10 ★ Befinden sich besonders kritische IT-Systeme in Räumen mit Sicherheitstüren und -fenstern?
- 1.18 Existiert eine Alarmanlage zur Erkennung und Warnung bei Einbrüchen?
- 1.43 Sind besonders kritische Netzwerkkomponenten speziell vor physischem Zugang geschützt?
- 1.53 Werden Kameras zur Überwachung von Gebäude und Räumen eingesetzt?
- 2.35 ★ Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen?
- ★ Wird die Software auf zentralen Netzwerkkomponenten regelmässig aktualisiert?

- 2.204 ★ Erfolgt jede Verbindung in das interne Netz ausnahmslos über gesicherte Zugänge?
- 4.162 Sind die Zugriffsrechte für E-Mail-Administratoren restriktiv vergeben worden?
- 4.239 Erfolgt der Zugriff von Administratoren auf die zentralen Netzwerk-Komponenten gesichert?

**Firewall / Router / Switch**

- 2.71 ★ Gibt es eine Weisung für einen Sicherheits-gateway und wird deren Einhaltung überprüft?
- 4.112 Müssen sich Computer bei einer Verbindung und Einwahl ins interne Netz über ein unsicheres Netz mit einem starken Authentisierungsverfahren anmelden?
- 5.21 ★ Werden die weit verbreiteten Dienste "telnet" (Fernzugriff auf Konsole) und "ftp/tftp" (Datei-Transfer) ausschliesslich in verschlüsselter Form verwendet?
- 5.39 Wird die Kommunikation verschlüsselt, wenn Administratoren mit dem Web-Browser die zentralen Netzwerkkomponenten administrieren?

**WLAN**

- 1.63 Sind Wireless LAN Access Points im Gebäude derart aufgestellt, dass der unberechtigte Zugang erschwert ist?
- 4.294 ★ Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des Access Points für drahtlose Netzwerke (WLAN) berücksichtigt worden?
- 4.295 Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des (Client-) Computers für drahtlose Netzwerke (WLAN) berücksichtigt worden?

**Modem / ISDN**

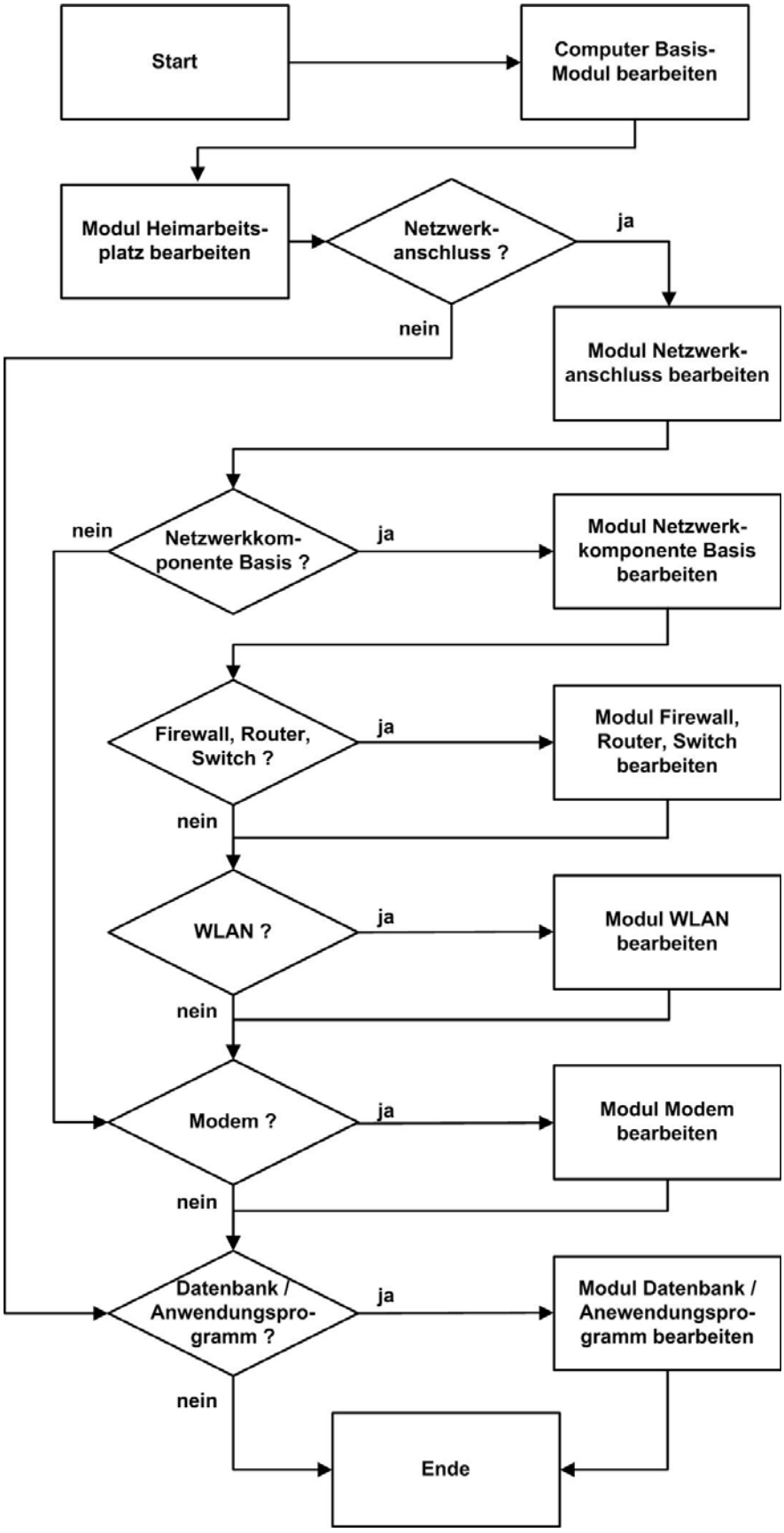
- 2.61 Existieren angemessene Regelungen für den Einsatz von Modems?
- 3.17 Werden Mitarbeiter über mögliche Gefährdungen, einzuhaltende Sicherheitsmassnahmen und Regelungen beim Betrieb eines Modems unterrichtet?
- 5.30 ★ Ist das Modem an lokalen Computern derart konfiguriert, dass eingehende Telefonanrufe / Verbindungsanfragen standardmässig nicht beantwortet werden (d.h. die so genannte „Auto-Answer Funktion ist deaktiviert)?
- Ist bei eingehenden Telefonanrufen, welche durch das Modem automatisch abgenommen, die Rückruf-Funktion aktiviert?

**Datenbank / Anwendungprogramm**

- 2.221 ★ Wird im Rahmen von Änderungen an Datenbanken und Anwendungsprogrammen systematisch überprüft, ob sich dadurch neue oder geänderte Anforderungen für die Sicherheit ergeben?
- 4.42 ★ Sind zusätzliche Sicherheitsfunktionalitäten in kritischen IT-Anwendungen und Datenbanksystemen implementiert?
- 4.72 ★ Werden Daten aus Datenbanksystemen und kritischen IT-Anwendungsprogrammen verschlüsselt abgelegt?
- 4.133 Werden bei der Anmeldung an sehr kritische Systeme / Anwendungs-programme neben Benutzerkennung und Passwort weitere Elemente zur Authentisierung benötigt?

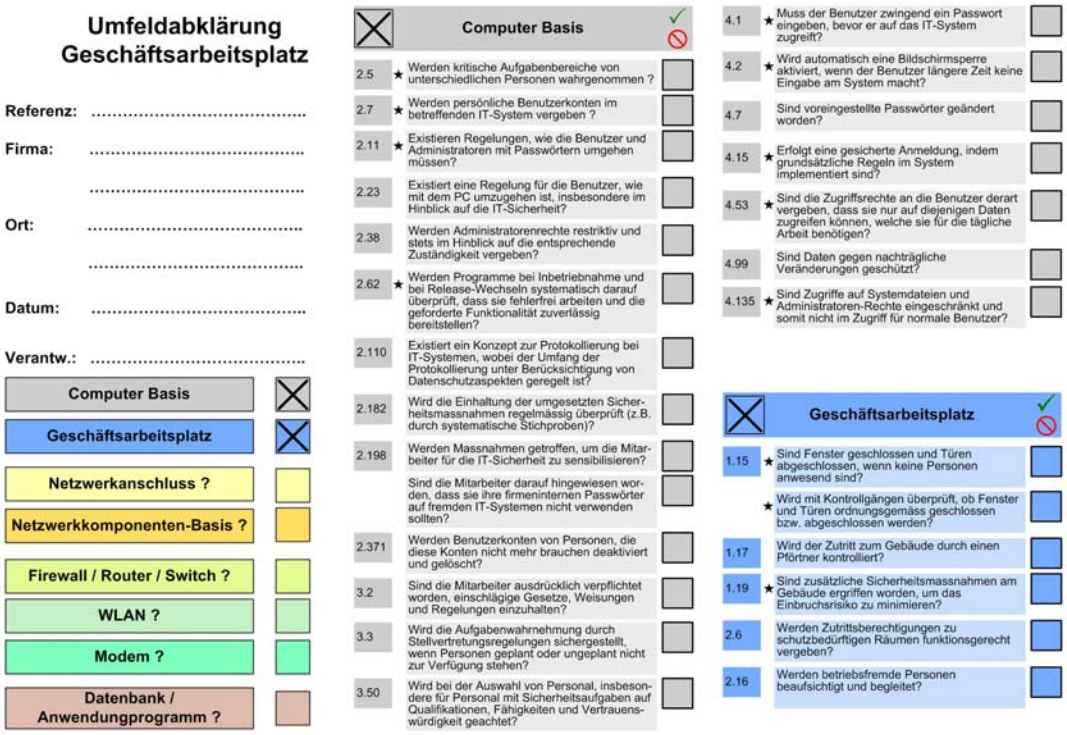
Bemerkungen

**Heimarbeitsplatz - Ablaufschema**

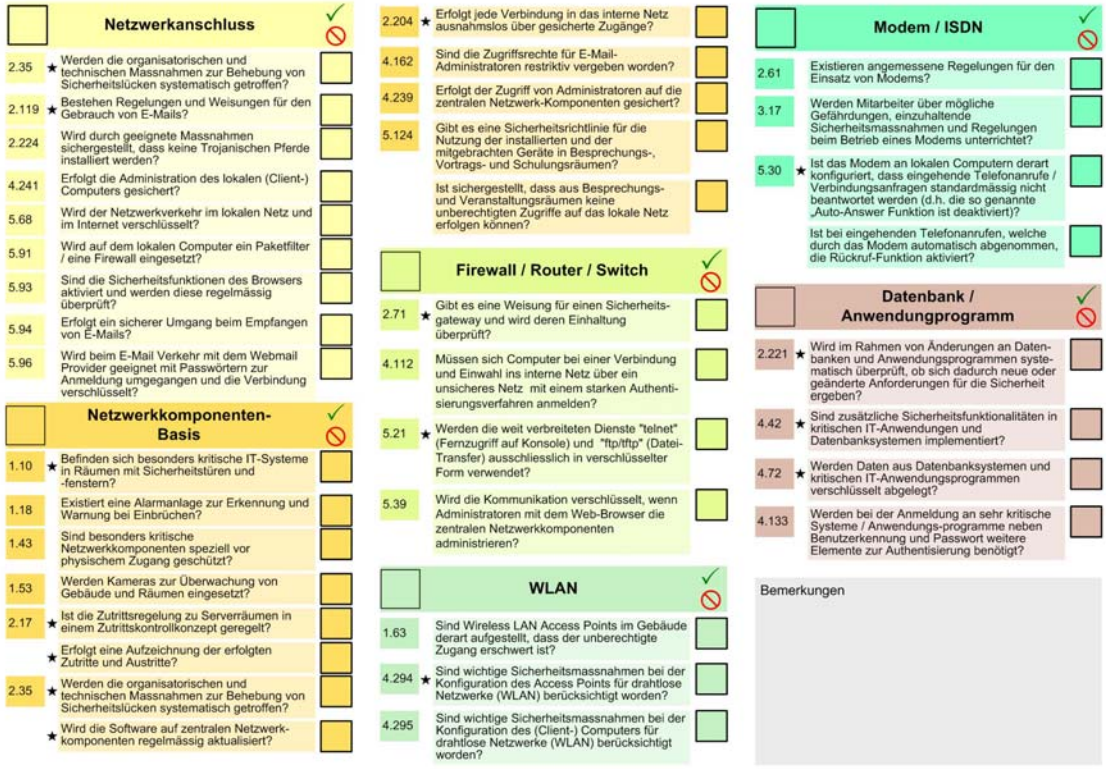


## Geschäftsarbeitsplatz

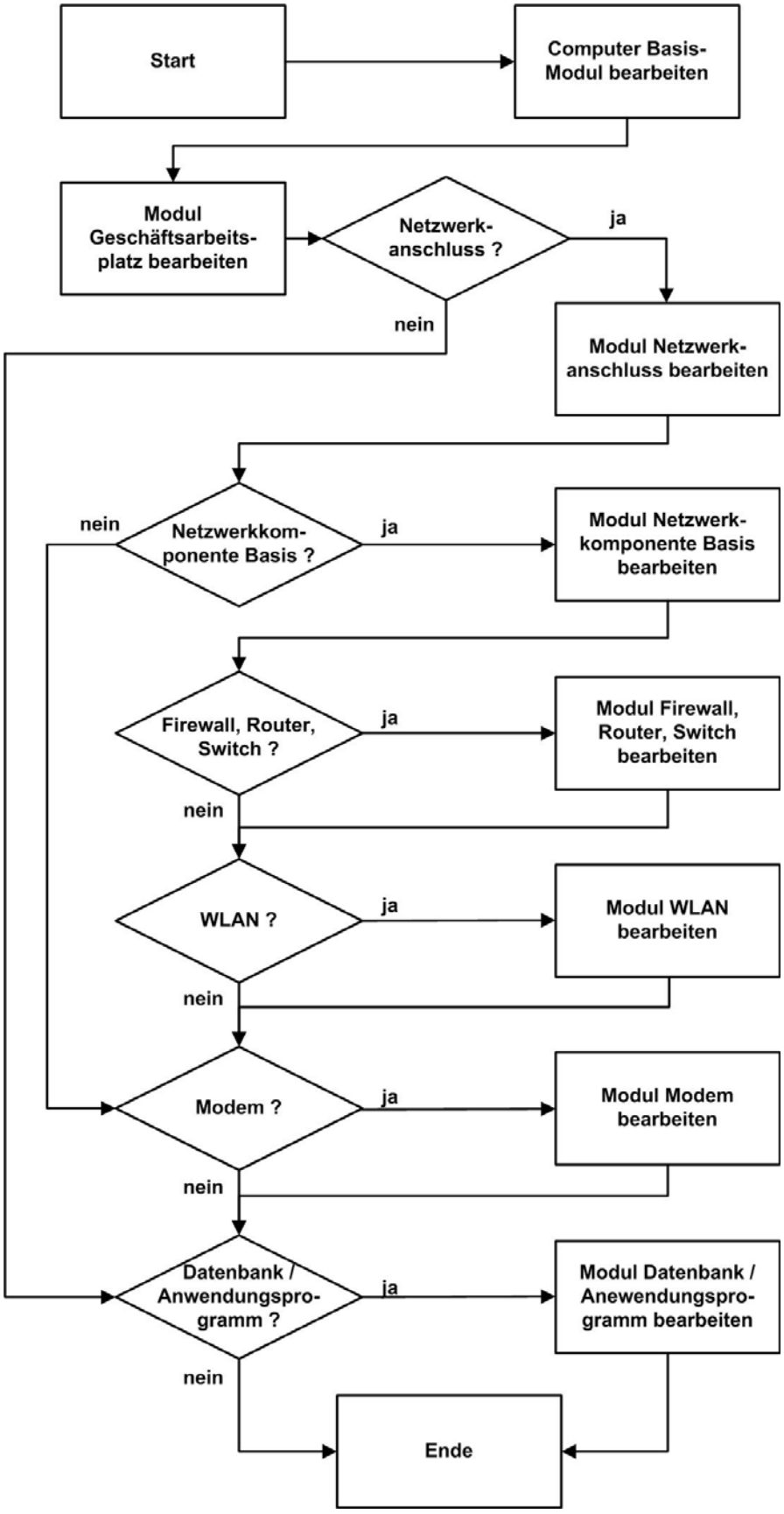
Leporello Vorderseite




Leporello Rückseite

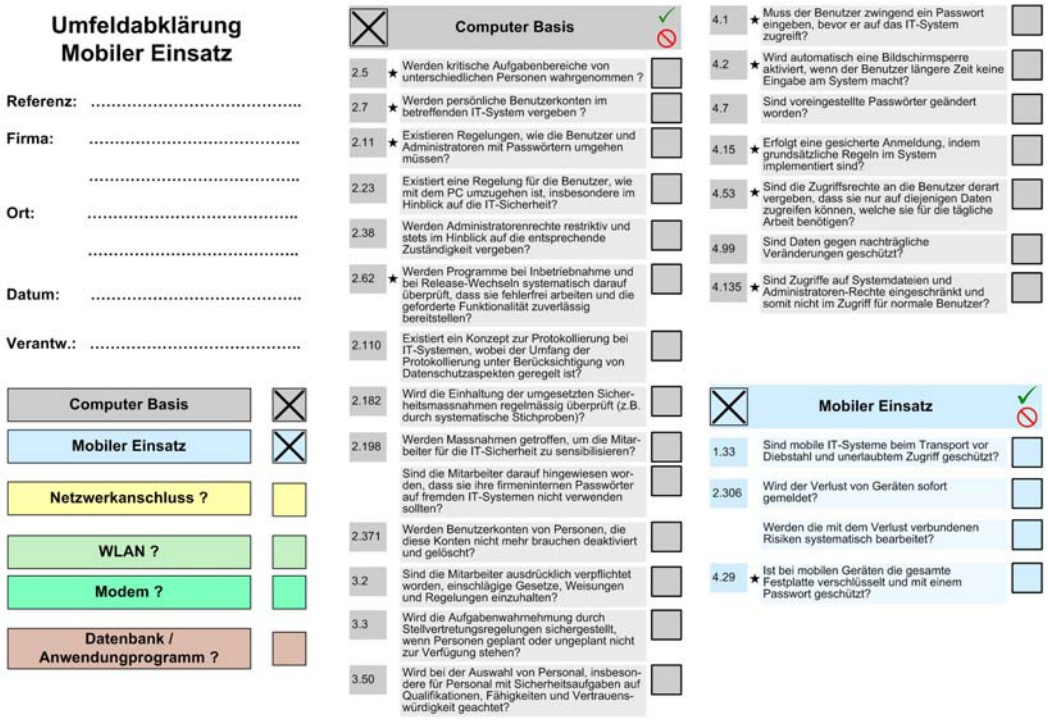


**Geschäftsarbeitsplatz - Ablaufschema**



## Mobiler Einsatz

Leporello Vorderseite



**Umfeldabklärung Mobiler Einsatz**

Referenz: .....

Firma: .....

.....

Ort: .....

.....

Datum: .....

Verantw.: .....

Computer Basis

Mobiler Einsatz

Netzwerkanschluss ?

WLAN ?

Modem ?

Datenbank / Anwendungsprogramm ?

**Computer Basis**

2.5 ★ Werden kritische Aufgabenbereiche von unterschiedlichen Personen wahrgenommen ?

2.7 ★ Werden persönliche Benutzerkonten im betreffenden IT-System vergeben ?

2.11 ★ Existieren Regelungen, wie die Benutzer und Administratoren mit Passwörtern umgehen müssen?

2.23 Existiert eine Regelung für die Benutzer, wie mit dem PC umzugehen ist, insbesondere im Hinblick auf die IT-Sicherheit?

2.38 Werden Administratorenrechte restriktiv und stets im Hinblick auf die entsprechende Zuständigkeit vergeben?

2.62 ★ Werden Programme bei Inbetriebnahme und bei Release-Wechseln systematisch darauf überprüft, dass sie fehlerfrei arbeiten und die geforderte Funktionalität zuverlässig bereitstellen?

2.110 Existiert ein Konzept zur Protokollierung bei IT-Systemen, wobei der Umfang der Protokollierung unter Berücksichtigung von Datenschutzaspekten geregelt ist?

2.182 Wird die Einhaltung der umgesetzten Sicherheitsmassnahmen regelmässig überprüft (z.B. durch systematische Stichproben)?

2.198 Werden Massnahmen getroffen, um die Mitarbeiter für die IT-Sicherheit zu sensibilisieren?

Sind die Mitarbeiter darauf hingewiesen worden, dass sie ihre firmeninternen Passwörter auf fremden IT-Systemen nicht verwenden sollten?

2.371 Werden Benutzerkonten von Personen, die diese Konten nicht mehr brauchen deaktiviert und gelöscht?

3.2 Sind die Mitarbeiter ausdrücklich verpflichtet worden, einschlägige Gesetze, Weisungen und Regelungen einzuhalten?

3.3 Wird die Aufgabenwahrnehmung durch Stellvertretungsregelungen sichergestellt, wenn Personen geplant oder ungeplant nicht zur Verfügung stehen?

3.50 Wird bei der Auswahl von Personal, insbesondere für Personal mit Sicherheitsaufgaben auf Qualifikationen, Fähigkeiten und Vertrauenswürdigkeit geachtet?

4.1 ★ Muss der Benutzer zwingend ein Passwort eingeben, bevor er auf das IT-System zugreift?

4.2 ★ Wird automatisch eine Bildschirmsperre aktiviert, wenn der Benutzer längere Zeit keine Eingabe am System macht?

4.7 Sind voreingestellte Passwörter geändert worden?

4.15 ★ Erfolgt eine gesicherte Anmeldung, indem grundsätzliche Regeln im System implementiert sind?

4.53 ★ Sind die Zugriffsrechte an die Benutzer derart vergeben, dass sie nur auf diejenigen Daten zugreifen können, welche sie für die tägliche Arbeit benötigen?

4.99 Sind Daten gegen nachträgliche Veränderungen geschützt?

4.135 ★ Sind Zugriffe auf Systemdateien und Administratoren-Rechte eingeschränkt und somit nicht im Zugriff für normale Benutzer?

**Mobiler Einsatz**

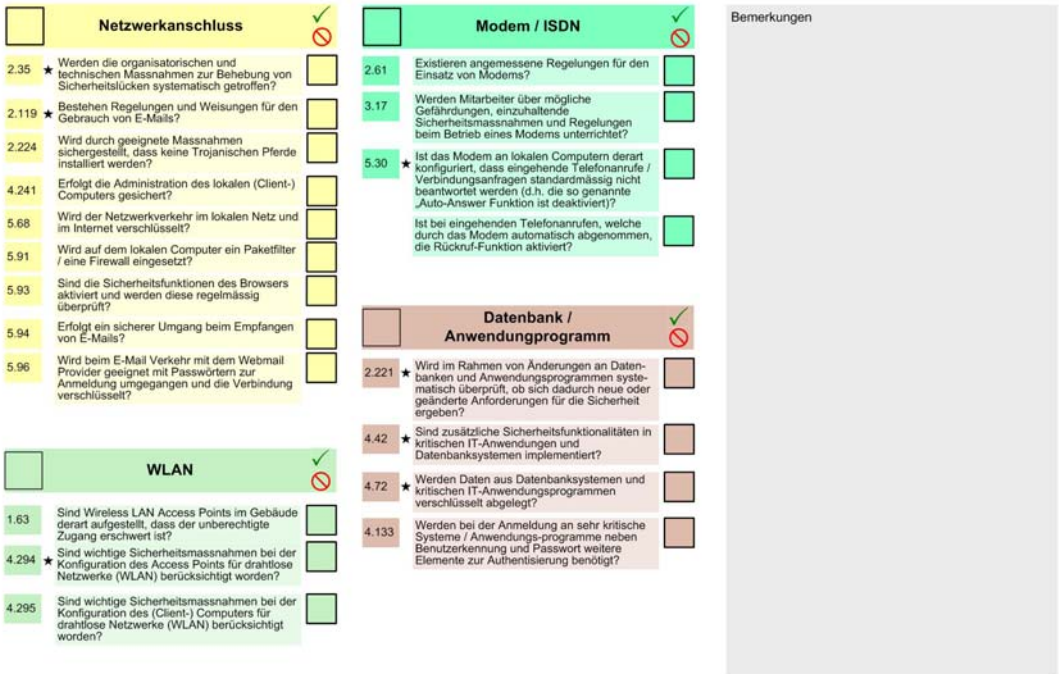
1.33 Sind mobile IT-Systeme beim Transport vor Diebstahl und unerlaubtem Zugriff geschützt?

2.306 Wird der Verlust von Geräten sofort gemeldet?

Werden die mit dem Verlust verbundenen Risiken systematisch bearbeitet?

4.29 ★ Ist bei mobilen Geräten die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt?

Leporello Rückseite



**Netzwerkanschluss**

2.35 ★ Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen?

2.119 ★ Bestehen Regelungen und Weisungen für den Gebrauch von E-Mails?

2.224 Wird durch geeignete Massnahmen sichergestellt, dass keine Trojanischen Pferde installiert werden?

4.241 Erfolgt die Administration des lokalen (Client-) Computers gesichert?

5.68 Wird der Netzwerkverkehr im lokalen Netz und im Internet verschlüsselt?

5.91 Wird auf dem lokalen Computer ein Paketfilter / eine Firewall eingesetzt?

5.93 Sind die Sicherheitsfunktionen des Browsers aktiviert und werden diese regelmässig überprüft?

5.94 Erfolgt ein sicherer Umgang beim Empfangen von E-Mails?

5.96 Wird beim E-Mail Verkehr mit dem Webmail Provider geeignet mit Passwörtern zur Anmeldung umgegangen und die Verbindung verschlüsselt?

**WLAN**

1.63 Sind Wireless LAN Access Points im Gebäude derart aufgestellt, dass der unberechtigte Zugang erschwert ist?

4.294 ★ Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des Access Points für drahtlose Netzwerke (WLAN) berücksichtigt worden?

4.295 Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des (Client-) Computers für drahtlose Netzwerke (WLAN) berücksichtigt worden?

**Modem / ISDN**

2.61 Existieren angemessene Regelungen für den Einsatz von Modems?

3.17 Werden Mitarbeiter über mögliche Gefährdungen, einzuhaltende Sicherheitsmassnahmen und Regelungen beim Betrieb eines Modems unterrichtet?

5.30 ★ Ist das Modem an lokalen Computern derart konfiguriert, dass eingehende Telefonanrufe / Verbindungsanfragen standardmässig nicht beantwortet werden (d.h. die so genannte „Auto-Answer Funktion ist deaktiviert)?

Ist bei eingehenden Telefonanrufen, welche durch das Modem automatisch abgenommen, die Rückruf-Funktion aktiviert?

**Datenbank / Anwendungsprogramm**

2.221 ★ Wird im Rahmen von Änderungen an Datenbanken und Anwendungsprogrammen systematisch überprüft, ob sich dadurch neue oder geänderte Anforderungen für die Sicherheit ergeben?

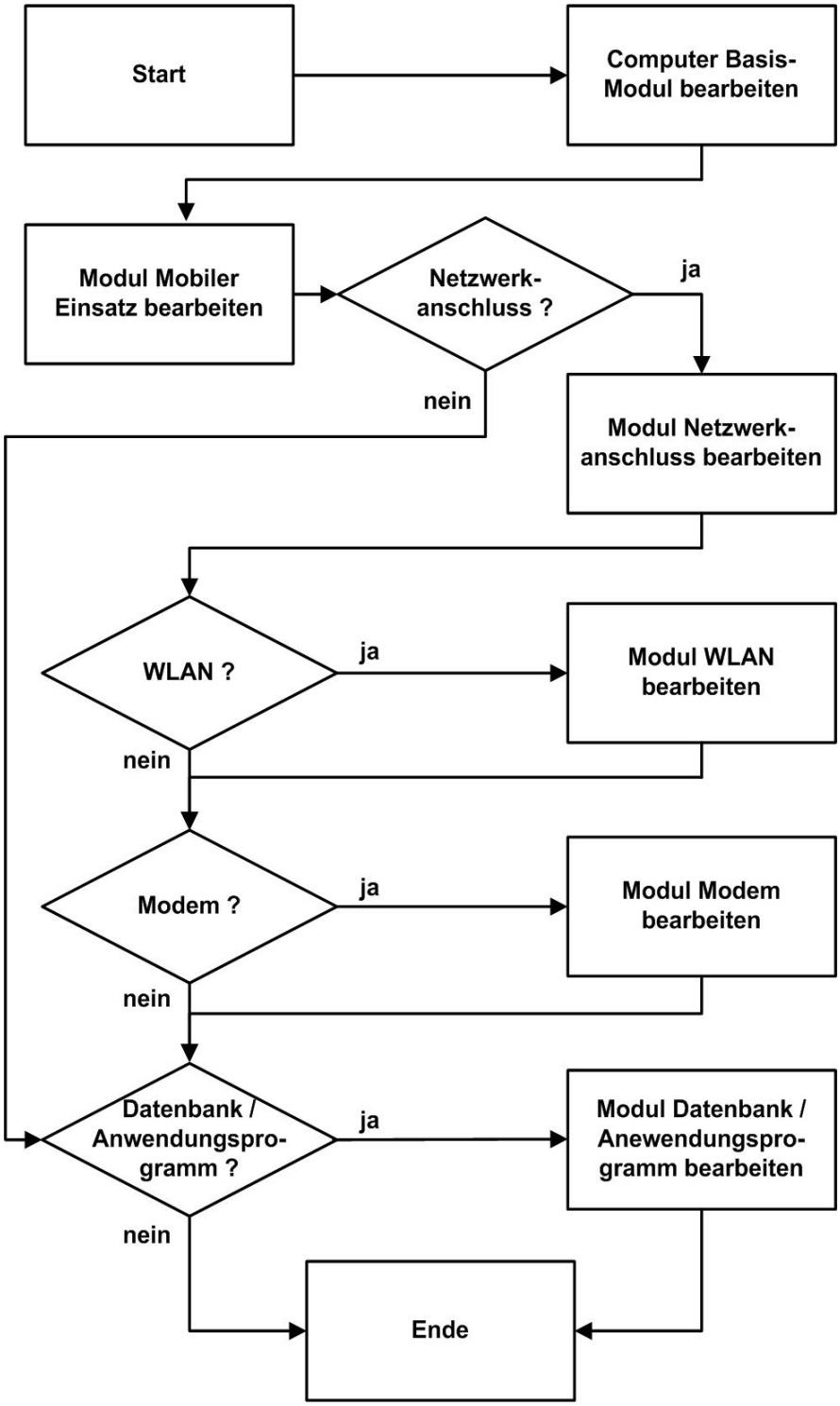
4.42 ★ Sind zusätzliche Sicherheitsfunktionalitäten in kritischen IT-Anwendungen und Datenbanksystemen implementiert?

4.72 ★ Werden Daten aus Datenbanksystemen und kritischen IT-Anwendungsprogrammen verschlüsselt abgelegt?

4.133 Werden bei der Anmeldung an sehr kritische Systeme / Anwendungs-programme neben Benutzerkennung und Passwort weitere Elemente zur Authentisierung benötigt?

Bemerkungen

**Mobiler Einsatz - Ablaufschema**



## 1.4 Detail-Checkliste

## Computer-Basis

*Modul: Computer-Basis*

### ★ M 2.5 – Aufgabenverteilung und Funktionstrennung

Werden kritische Aufgabenbereiche von unterschiedlichen Personen wahrgenommen? ○ ja ○ nein

Beispiele kritischer Aufgabenbereiche: Programmierung und Überführung der Programme in die Produktion, Arbeit in der IT und im Fachbereich, Zahlungserfassung und Zahlungsfreigabe

Wenn keine angemessene Funktionstrennung stattfindet (d.h. eine Person übernimmt mehrere kritische Aufgaben und Funktionen gleichzeitig), besteht das Risiko, dass bestehende Kontrollen umgangen werden und unerlaubte Handlungen von Schlüsselpersonen unentdeckt bleiben. Es besteht das erhöhte Risiko, dass Schlüsselpersonen andere Login-Daten kennen (z.B. Passwort) und generell zu weitreichende Zugriffsrechte (beispielsweise Administrator-Rechte) besitzen.

### ★ M 2.7 – Vergabe von Zugangsberechtigungen

Werden persönliche Benutzerkonten im betreffenden IT-System vergeben? ○ ja ○ nein

Beispiele: Jeder Benutzer erhält ein persönliches Benutzerkonto, und es werden keine Benutzerkonten von mehreren Personen geteilt.

Wenn Zugangsberechtigungen nicht oder unvollständig verwaltet werden, besteht das Risiko, dass unerlaubte Handlungen keiner Person oder keinem eingegrenzten Personenkreis zugeordnet werden können.

Weitere Informationen sind beim BSI zu finden unter M 2.8 , M 2.30, M 2.31, M 2.63, M 2.94, M 4.53, M 4.135.

### ★ M 2.11 – Regelung des Passwortgebrauchs

Existieren Regelungen, wie die Benutzer und Administratoren mit Passwörtern umgehen müssen? ○ ja ○ nein

Beispiele: Passwörter nicht auf Zettel schreiben, dem Stellvertreter nicht weitergeben, regelmässig wechseln, Mindestlänge wählen etc.

Es besteht das Risiko, dass die Benutzer das Passwort nicht vertraulich behandeln und dadurch eine andere Person in den Besitz des Passworts kommt. Dadurch kann diese Person unter einer anderen Benutzerkennung arbeiten.

### M 2.23 – Herausgabe einer PC-Richtlinie

Existiert eine Regelung für die Benutzer, wie mit dem PC umzugehen ist, insbesondere im Hinblick auf die IT-Sicherheit? ○ ja ○ nein

Beispielsweise wird geregelt: Installation von fremden Programmen, Bildschirmsperre beim Verlassen des Arbeitsplatzes etc.

Es besteht das Risiko, dass aufgrund von Mängeln in der Handhabung von IT-Systemen unberechtigte Personen auf Daten zugreifen und diese verändern können (entweder direkt über ein fremdes Benutzerkonto oder indirekt über das Erlangen eines fremden Passworts).

## M 2.38 – Aufteilung der Administrationstätigkeiten

Werden Administratorenrechte restriktiv und stets im Hinblick auf die entsprechende Zuständigkeit vergeben? ○ ja ○ nein

Beispielsweise wird zwischen Netzwerkadministrator und Datenbankadministrator unterschieden. Zudem erhalten normale Benutzer keine Administratorenrechte.

Administratoren besitzen in der Regel weitreichende Zugriffsrechte. Wenn solche Zugriffsrechte nicht restriktiv vergeben werden, besteht das erhöhte Risiko, dass die Administratoren auf vertrauliche Daten (wie Hinweise zu Passwörtern) zugreifen. Zudem besteht stets das Risiko von Fehlmanipulationen, die sich bei Administratoren besonders gravierend auswirken können und dadurch die Datensicherheit generell gefährdet wird.

Weitere Informationen sind beim BSI zu finden unter M 2.26.

## ★ M 2.62 – Software-Abnahme- und Freigabe-Verfahren

Werden Programme bei Inbetriebnahme und bei Release-Wechseln systematisch darauf überprüft, dass sie fehlerfrei arbeiten und die geforderte Funktionalität zuverlässig bereitstellen? ○ ja ○ nein

Beispiele: Programme werden mit Testfällen systematisch überprüft, und es existiert ein dokumentiertes Freigabeverfahren unter Einbezug der Fachstellen.

Wenn die systematische Prüfung des fehlerfreien und zuverlässigen Funktionierens der Programme nicht durchgeführt wird, besteht das Risiko, dass die neuen Programme Sicherheitslücken beinhalten und diese nicht erkannt werden. Dadurch wird die Systemsicherheit generell gefährdet.

Weitere Informationen sind beim BSI zu finden unter M 2.86, M 2.221.

## M 2.110 – Datenschutzaspekte bei der Protokollierung

Existiert ein Konzept zur Protokollierung bei IT-Systemen, wobei der Umfang der Protokollierung unter Berücksichtigung von Datenschutzaspekten geregelt ist? ○ ja ○ nein

Beispielsweise wird protokolliert: An- und Abmeldungen am System, Lese- und Schreibzugriffe auf sehr vertrauliche Daten, Einrichten von Benutzern durch Administratoren, Datensicherungen.

Wenn die Protokollierung nicht, nicht regelmässig oder nicht umfassend erfolgt, ist jede davon betroffene Massnahme nicht nachvollziehbar und damit in Frage gestellt.

Weitere Informationen sind beim BSI zu finden unter M 2.340.

## M 2.182 – Regelmässige Kontrollen der IT-Sicherheitsmassnahmen

Wird die Einhaltung der umgesetzten Sicherheitsmassnahmen regelmässig überprüft (z.B. durch systematische Stichproben)? ○ ja ○ nein

Wenn die Einhaltung der Sicherheitsmassnahmen nicht regelmässig überprüft wird, besteht das Risiko, dass der durch die Massnahme gewährte Schutz der Vertraulichkeit und der Integrität der Daten nicht mehr wirksam ist.

## M 2.198 – Sensibilisierung der Mitarbeiter für IT-Sicherheit

Werden Massnahmen getroffen, um die Mitarbeiter für die IT-Sicherheit zu sensibilisieren? ○ ja ○ nein

z.B. regelmässige Informationen, interne Weiterbildungen

Wenn die Mitarbeiter nicht auf die IT-Sicherheit sensibilisiert sind, besteht das Risiko, dass vertrauliche Daten durch unsachgemässe Handhabung Unbefugten zugänglich gemacht werden.

Sind die Mitarbeiter darauf hingewiesen worden, dass sie ihre firmeninternen Passwörter auf fremden IT-Systemen nicht verwenden sollten? ○ ja ○ nein

z.B. kein Gebrauch im Internet-Cafe, beim Mailprovider, beim Arbeitskollegen etc.

Es besteht das Risiko, dass die fremden IT-Systeme Sicherheitslücken aufweisen oder dass bereits Abhörprogramme (Sniffer) installiert sind. Bei der Verwendung von firmeninternen Passwörtern (bzw. Wahl des gleichen Passworts auf verschiedenen Systemen) auf fremden Systemen kann das Passwort somit gestohlen werden.

Weitere Informationen sind beim BSI zu finden unter M 3.26, M 3.5, M 4.251.

## M 2.371 – Geregelte Deaktivierung und Löschung ungenutzter Konten

Werden Benutzerkonten von Personen, die diese Konten nicht mehr brauchen, deaktiviert und gelöscht? ○ ja ○ nein

Beispiele: regelmässige Überprüfung der Zugriffsrechte; standardisierte Austrittsmeldungen durch die Personalabteilung. Ebenso können beispielsweise Benutzerkonten, welche längere Zeit nicht verwendet wurden, automatisch vom System deaktiviert werden.

Wenn die Konten nicht deaktiviert und gelöscht werden, besteht das Risiko, dass mit Hilfe dieser Konten unerkannt Daten eingesehen und manipuliert werden.

Weitere Informationen sind beim BSI zu finden unter M 4.17.

## M 3.2 – Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen

Sind die Mitarbeiter ausdrücklich verpflichtet worden, einschlägige Gesetze, Weisungen und Regelungen einzuhalten? ○ ja ○ nein

z.B. mittels schriftlicher Bestätigung bei der Neueinstellung von Mitarbeitern

Es besteht das Risiko, dass Mitarbeiter sich ihrer Verantwortung zur Einhaltung von Gesetzen, Weisungen und Regelungen nicht (bzw. zuwenig) bewusst sind. Dadurch wird unter anderem die Datensicherheit gefährdet, wie beispielsweise die Vertraulichkeit von Passwörtern oder die Datenintegrität generell.

## M 3.3 – Vertretungsregelungen

Wird die Aufgabenwahrnehmung durch Stellvertretungsregelungen sichergestellt, wenn Personen geplant oder ungeplant nicht zur Verfügung stehen? ○ ja ○ nein

Beispielsweise besitzt der Stellvertreter die notwenigen Zugriffsrechte, so dass die Weitergabe von persönlichen Passwörtern nicht notwendig ist.

Wenn Stellvertretungsregelungen fehlen, besteht das Risiko, dass die Aufgaben nicht in der gleichen Zuverlässigkeit (bezüglich der Sicherheitsmassnahmen) wahrgenommen werden. Bei der Weitergabe von Passwörtern an Stellvertreter besteht das Risiko, dass Datenabfragen und -manipulationen später nicht zugeordnet werden können.

## M 3.50 – Auswahl von Personal

Wird bei der Auswahl von Personal, insbesondere für Personal mit Sicherheitsaufgaben, auf Qualifikationen, Fähigkeiten und Vertrau- ○ ja ○ nein

enswürdigkeit geachtet?

Es besteht das Risiko, dass Mitarbeiter die Anforderungen für eine ordnungsgemässe Umsetzung der Sicherheitsmassnahmen nicht erfüllen können und sich dadurch generell erhöhte Sicherheitsrisiken ergeben. Bei fehlender oder unklarer Vertrauenswürdigkeit besteht ein erhöhtes Risiko von unerlaubten Handlungen.

Weitere Informationen sind beim BSI zu finden unter M 3.10, M 3.33.

### ★ M 4.1 – Passwortschutz für IT-Systeme

Muss der Benutzer zwingend ein Passwort eingeben, bevor er auf das IT-System zugreift? ○ ja ○ nein

z.B. Anmeldung am Betriebssystem, Anmeldung bei einem Anwendungsprogramm

Ohne Passwortschutz besteht das Risiko, dass sich Benutzer unter einer anderen Benutzerkennung anmelden und dadurch nicht mehr nachvollziehbar ist, welcher Benutzer effektiv am System gearbeitet hat.

### ★ M 4.2 – Bildschirmsperre

Wird automatisch eine Bildschirmsperre aktiviert, wenn der Benutzer längere Zeit keine Eingabe am System macht? ○ ja ○ nein

z.B. Aktivierung des Bildschirmschoners und Wiedereinstieg durch erneute Passworteingabe

Ohne automatische Bildschirmsperre besteht das Risiko, dass Benutzer beim Verlassen des Arbeitsplatzes (z.B. in der Mittagspause oder nach Büroschluss) den Computer nicht sperren und dadurch unberechtigte Personen unter der fremden Benutzerkennung auf das System zugreifen. Zudem besitzen die Personen in einem solchen Fall möglicherweise mehr Zugriffsrechte als im Normalfall.

Weitere Informationen sind beim BSI zu finden unter M 4.16.

### M 4.7 – Änderung voreingestellter Passwörter

Sind voreingestellte Passwörter geändert worden? ○ ja ○ nein

Viele Betriebssysteme, Datenbanken, Netzwerk-Geräte etc. werden mit allgemein bekannten Standard-Passwörtern ausgeliefert oder verwenden überhaupt keine Passwörter.

Es besteht das Risiko, dass durch die Benutzung eines voreingestellten Passworts, welches allgemein bekannt ist, Zugriff aufs System möglich wird. Weil es sich dabei oft um Administratoren-Konten handelt, sind damit weitreichende Zugriffsrechte verbunden. Unter anonymer Benutzerkennung können unberechtigte Transaktionen durchgeführt und gegebenenfalls kann auf vertrauliche Daten zugegriffen werden.

### ★ M 4.15 – Gesichertes Login

Erfolgt eine gesicherte Anmeldung, indem mindestens die folgenden Regeln im System implementiert sind? ○ ja ○ nein

1) Jeder Benutzer besitzt ein eigenes Benutzerkonto;
2) Jeder Benutzer besitzt ein eigenes Passwort, welches frei wählbar ist;
3) Passwörter besitzen eine Mindestlänge von 8 Zeichen und können nicht aus trivialen Wörtern bestehen;
4) Passwörter müssen regelmässig geändert werden (mindestens alle 90 Tage);
5) Mehrere erfolglose Anmeldeversuche werden verhindert (z.B.

durch Sperren des betreffenden Benutzerkontos oder zeitlicher Verzögerung bei Fehlversuchen).

Es besteht das Risiko, dass Benutzer ein Benutzerkonto oder Passwort gemeinsam verwenden, wodurch die Nachvollziehbarkeit der Transaktionen nicht mehr gegeben ist. Bei kurzen oder trivialen Passwörtern und der Möglichkeit von zahlreichen Anmeldeversuchen besteht das Risiko, dass eine andere Person das Passwort errät (durch systematisches Ausprobieren, manuell oder automatisiert). Wenn das System die Benutzer nicht regelmässig zur Passwortänderung zwingt, kann sich eine unberechtigte Person, die über ein fremdes Passwort verfügt, über einen längeren Zeitraum unter einer falschen Benutzerkennung anmelden.

## ★ M 4.53 – Restriktive Vergabe von Zugriffsrechten auf Dateien und Verzeichnisse

Sind die Zugriffsrechte an die Benutzer derart vergeben, dass sie nur auf diejenigen Daten zugreifen können, welche sie für die tägliche Arbeit benötigen? ○ ja ○ nein

Beispielsweise besitzen Benutzer keine Zugriffe auf die persönlichen Verzeichnisse ihrer Kollegen, Mitarbeiter der Zahlungsabteilung besitzen keine Zugriffe zu den Personaldaten und umgekehrt.

Es besteht das Risiko, dass Benutzer bei zu vielen Berechtigungen Zugang zu vertraulichen Daten erhalten (unter anderem Hinweise zu Passwörtern).

Weitere Informationen sind beim BSI zu finden unter M 2.7, M 2.8, M 2.30, M 2.31, M 2.63, M 2.94, M 4.135, M 5.10.

## M 4.99 – Schutz gegen nachträgliche Veränderungen von Informationen

Sind Daten gegen nachträgliche Veränderungen geschützt? ○ ja ○ nein

Beispielsweise bieten digitale Signaturen einen hohen Schutz gegen nachträgliche Veränderungen. In abgeschwächter Form kann mittels Read-only Medien und Dateiformaten wie PDF gegen nachträgliche Veränderung geschützt werden.

Wenn Daten nicht mittels digitalen Signaturen geschützt werden, besteht das Risiko, dass diese Daten nachträglich von unberechtigten Personen geändert werden und dies nicht erkannt wird - insbesondere bei Schwachstellen im physischen und logischen Zugriffsschutz. Der Einsatz von digitalen Signaturen kann in einem solchen Umfeld teilweise Abhilfe schaffen. Es besteht aber auch hier ein Rest-Risiko, dass digitale Schlüssel und dazugehörende Passwörter gestohlen werden (z.B. Kopie des Schlüssels und Diebstahl/Ausprobieren des Passworts).

## ★ M 4.135 – Restriktive Vergabe von Zugriffsrechten auf Systemdateien

Sind Zugriffe auf Systemdateien und Administratoren-Rechte eingeschränkt und somit nicht im Zugriff für normale Benutzer? ○ ja ○ nein

Bei weitreichenden Zugriffsrechten für normale Benutzer besteht das Risiko, dass Sicherheitseinstellungen geändert und Schutzmassnahmen dadurch abgebaut werden. Zudem können Administratoren auf Dateien mit verschlüsselten Passwörtern zugreifen, welche in einem zweiten Schritt bei einfachen Passwörtern relativ einfach geknackt werden können. Weiter besitzen Administratoren häufig Schreib-Zugriffe auf Log-Files, wodurch die Protokolleinträge manipuliert werden können.

*M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.*

### ★ M 1.15 – Geschlossene Fenster und Türen

Sind Fenster geschlossen und Türen abgeschlossen, wenn keine Personen anwesend sind? ○ ja ○ nein

Es besteht das Risiko, dass unberechtigte Personen über offene Fenster oder Türen physischen Zutritt zum IT-System erlangen. Dadurch können beispielsweise gewisse Sicherheitsmechanismen des Betriebssystems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.23.

### M 1.19 – Einbruchsschutz

Sind zusätzliche Sicherheitsmassnahmen am Gebäude ergriffen worden, um das Einbruchsrisiko zu minimieren? ○ ja ○ nein

Beispiele: Schliesszylinder, Sicherung von Kellerlichtschächten, Verschluss von nicht benutzten Nebeneingängen.

Es besteht das Risiko, dass unberechtigte Personen relativ einfach physischen Zutritt ins Gebäude und zu IT-Systemen erlangen. Bei physischem Zugriff auf ein IT-System können anschliessend gewisse Sicherheitsmechanismen des IT-Systems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.40.

### M 3.21 – Sicherheitstechnische Einweisung und Fortbildung des Telearbeiters

Werden Telearbeiter in die mit der Telearbeit verbundenen Sicherheitsrisiken eingewiesen? ○ ja ○ nein

z.B. Schulung über IT-Sicherheitsmassnahmen

Es besteht das Risiko, dass Mitarbeiter sich der Sicherheitsrisiken nicht (bzw. zuwenig) bewusst sind und notwendige Massnahmen nicht ergriffen werden. Dies kann unter anderem zu einem Verlust der Datenintegrität und Datenvertraulichkeit führen.

Weitere Informationen sind beim BSI zu finden unter M 2.113.

### ★ M 4.29 – Einsatz eines Verschlüsselungsproduktes für tragbare PCs

Ist bei Geräten mit geringem physischen Schutz die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt? ○ ja ○ nein

z.B. mit eingebautem BIOS-Festplattenschutz oder gängigen Verschlüsselungsprogrammen

Der physische Schutz ist bei IT-Systemen am Heimarbeitsplatz häufig gering. Es besteht somit ein erhöhtes Risiko, dass das Gerät gestohlen wird und dass der Dieb Zugang zu vertraulichen Daten (wie beispielsweise Passwörtern) erlangt. Im Extremfall können Anmeldungen unter fremder Benutzerkennung und Datenänderungen erfolgen.

*M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.*

## ★ M 1.15 – Geschlossene Fenster und Türen

Sind Fenster geschlossen und Türen abgeschlossen, wenn keine Personen anwesend sind? ○ ja ○ nein

Wird mit Kontrollgängen überprüft, ob Fenster und Türen ordnungsgemäss geschlossen bzw. abgeschlossen werden? ○ ja ○ nein

Es besteht das Risiko, dass unberechtigte Personen über offene Fenster oder Türen physischen Zutritt zum IT-System erlangen. Dadurch können beispielsweise gewisse Sicherheitsmechanismen des Betriebssystems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.23, M 2.18.

## M 1.17 – Pförtnerdienst

Wird der Zutritt zum Gebäude durch einen Pförtner kontrolliert? ○ ja ○ nein

Ohne einen Pförtnerdienst besteht das Risiko, dass unberechtigte Personen einfach physischen Zugang zu IT-Systemen erlangen.

## ★ M 1.19 – Einbruchsschutz

Sind zusätzliche Sicherheitsmassnahmen am Gebäude ergriffen worden, um das Einbruchsrisiko zu minimieren? ○ ja ○ nein

Beispiele: Schliesszylinder, Sicherung von Kellerlichtschächten, Verschluss von nicht benutzten Nebeneingängen, Zaunanlage, Mauerwerk, Zufahrtssperren.

Es besteht das Risiko, dass unberechtigte Personen relativ einfach physischen Zutritt ins Gebäude und zu IT-Systemen erlangen. Bei physischem Zugriff auf ein IT-System können anschliessend gewisse Sicherheitsmechanismen des IT-Systems umgangen werden (siehe M 1).

Weitere Informationen sind beim BSI zu finden unter M 1.10, M 1.12, M 1.16, M 1.40, M 1.53, M 1.55.

## M 2.6 – Vergabe von Zutrittsberechtigungen

Werden Zutrittsberechtigungen zu schutzbedürftigen Räumen funktionsgerecht vergeben? ○ ja ○ nein

z.B. Serverraum nur mit Badge, Datensicherungsraum nur mit Pin-Code

Wenn unbestimmte Personenkreise Zutritt zu schutzbedürftigen Räumen haben, besteht das Risiko, dass unerlaubte Handlungen keinem bestimmten Personenkreis zugeordnet werden können. Es besteht das erhöhte Risiko, dass Personen Zugang zu Daten erhalten, die nicht ihrer Aufgabenstellung entsprechen (z.B. Administrator-Passwort) oder dass Personen Manipulationsmöglichkeiten erhalten, die sie an ihrem Arbeitsplatz nicht haben.

Weitere Informationen sind beim BSI zu finden unter M 2.14, M 2.17, M 2.97.

## M 2.16 – Beaufsichtigung oder Begleitung von Fremdpersonen

Werden betriebsfremde Personen beaufsichtigt und begleitet? ○ ja ○ nein

z.B. Besucher, Handwerker, Servicetechniker, Reinigungspersonal

Wenn sich Personen unbeaufsichtigt oder unbegleitet bewegen können, besteht das Risiko, dass sie unberechtigten Zugang zu vertraulichen Daten erhalten. In Kombination mit anderen organisatorischen Mängeln (z.B. kein geregelter Passwortgebrauch) können betriebsfremde Personen zudem Manipulationen an Systemen und an Daten vornehmen.

Weitere Informationen sind beim BSI zu finden unter M 2.4.

# Mobiler Einsatz



*M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.*

## M 1.33 – Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz

Sind mobile IT-Systeme beim Transport vor Diebstahl und unerlaubtem Zugriff geschützt? ○ ja ○ nein

Ohne angemessenen Schutz mobiler IT-Systeme besteht das Risiko, dass unberechtigte Personen Zugriff aufs IT-System erhalten (siehe M 1). Kompensierende Kontrollen wie beispielsweise Festplattenverschlüsselung und Bildschirmsperre können das Risiko minimieren.

Weitere Informationen sind beim BSI zu finden unter M 1.61.

## M 2.306 – Verlustmeldung

Wird der Verlust von Geräten sofort gemeldet? ○ ja ○ nein

Werden die mit dem Verlust verbundenen Risiken systematisch bearbeitet? ○ ja ○ nein

z.B. Ändern aller Passwörter

Wenn der Verlust nicht gemeldet oder nicht systematisch bearbeitet wird, besteht das Risiko, dass unberechtigte Dritte sich mit Hilfe von Informationen aus dem mobilen Gerät Zugang zum IT-System verschaffen.

## ★ M 4.29 – Einsatz eines Verschlüsselungsproduktes für tragbare PCs

Ist bei mobilen Geräten die gesamte Festplatte verschlüsselt und mit einem Passwort geschützt? ○ ja ○ nein

z.B. mit eingebautem BIOS-Festplattenschutz oder gängigen Verschlüsselungsprogrammen

Der physische Schutz ist bei IT-Systemen am Heimarbeitsplatz häufig gering. Es besteht somit ein erhöhtes Risiko, dass das Gerät gestohlen wird und dass der Dieb Zugang zu vertraulichen Daten (wie beispielsweise Passwörtern) erlangt. Im Extremfall können Anmeldungen unter fremder Benutzerkennung und Datenänderungen erfolgen.

Weitere Informationen sind beim BSI zu finden unter M 4.27.

# Netzwerkanschluss

*Modul: Netzwerkanschluss*

## ★ M 2.35 – Informationsbeschaffung über Sicherheitslücken des Systems

Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen? ○ ja ○ nein

Beispiele: regelmässige Informationsbeschaffung über bekannte Sicherheitslücken, schnellstmögliches Einspielen von verfügbaren Patches und Updates.

Wird die Software auf den IT-Systemen regelmässig aktualisiert? ○ ja ○ nein

z.B. mittels neuen Software-Releases, Updates bei Tools etc.

Regelmässig werden Schwachstellen in Betriebssystemen, Datenbanken, Tools und Anwendungsprogrammen gefunden und im Internet veröffentlicht und sind dadurch einschlägig bekannt. Wenn die Schwachstellen durch das Einspielen neuer Software/Patches nicht geschlossen werden, besteht das Risiko, dass unberechtigte Personen diese Schwachstelle ausnützen und auf das IT-System zugreifen. Dadurch kann auf vertrauliche Daten zugegriffen, Netzwerk-Verkehr abgehört und Daten sowie Konfigurationen verändert werden. In einem fortgeschrittenen Stadium kann unter falscher Benutzerkennung oder als Administrator auf das System zugegriffen werden. Sehr ausgeprägt ist das Risiko bei Systemen, welche direkt im Zugriff des Internets stehen.

Weitere Informationen sind beim BSI zu finden unter M 2.273, M 4.152.

## ★ M 2.119 – Regelung für den Einsatz von E-Mail

Bestehen Regelungen und Weisungen für den Gebrauch von E-Mails? ○ ja ○ nein

z.B. Verschlüsselung von Mail-Anlagen, Regeln zur Adressierung, Archivierung von E-Mails, Stellvertreter-Regelung etc.

Wenn das Mail-System ohne begleitende Regelungen genutzt wird, besteht das Risiko, dass unberechtigte Personen auf vertrauliche E-Mails zugreifen können. So kann beispielsweise der Stellvertreter Kenntnis von Passwörtern nehmen, die via E-Mail übermittelt werden, und sich anschliessend unter fremder Benutzerkennung anmelden.

Weitere Informationen sind beim BSI zu finden unter M. 2.118, M 2.274.

## M 2.224 – Vorbeugung gegen Trojanische Pferde

Wird durch geeignete Massnahmen sichergestellt, dass keine Trojanischen Pferde installiert werden? ○ ja ○ nein

Beispiele von geeigneten Massnahmen sind: Unterbinden der Installationsmöglichkeit für die Benutzer, Führen einer Liste von freigegebenen Programmen, Sensibilisierung der Benutzer, Installation von Firewalls auf lokalen Computern der Benutzer, Installation von Software zum Erkennen von schadhaften Programmen etc.

Über Trojanische Pferde können Passwörter ermittelt werden. Ebenso besteht das Risiko, dass über das Trojanische Pferd direkt unter fremder Benutzerkennung auf das System zugegriffen wird.

Weitere Informationen sind beim BSI zu finden unter M 2.235, M 4.253.

## M 4.241 – Sicherer Betrieb von Clients

Erfolgt die Administration des lokalen (Client-) Computers gesichert? ○ ja ○ nein

Beispiel: Administration erfolgt mittels Fernzugriff über eine verschlüsselte Verbindung, über ein zentrales Netzwerkmanagement-System oder lokal, wobei die Administratoren-Passwörter nur einer

kleinen Anzahl von Personen zur Verfügung stehen und regelmässig gewechselt werden.

Ohne sichere Administration des lokalen Computers besteht das Risiko, dass sich unberechtigte Personen als Administrator anmelden und dadurch Zugriff auf vertrauliche Daten erlangen (Abhören von Passwörtern, Missbrauch von Administrationsrechten aufgrund einer zu hohen Anzahl an berechtigten Administratoren etc.). Bei Zugriff auf vertrauliche Daten kann unter anderem auch das Passwort von "normalen" Benutzern ermittelt und anschliessend unter der entsprechenden Benutzerkennung gearbeitet werden.

## M 5.68 – Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

Wird der Netzwerkverkehr im lokalen Netz und im Internet verschlüsselt? ○ ja ○ nein

z.B. erfolgt eine Verschlüsselung bei Client-Server-Anwendungen im LAN, beim Transport von Firmendaten zwischen zwei Standorten der Firma über das Internet (mit VPN), bei Abruf von Maildaten beim öffentlichen Provider etc.

Betriebssysteme senden die Passwörter üblicherweise in verschlüsselter Form über das Netz, so dass sie bei einem Lauschangriff nur geknackt werden können, wenn Sicherheitslücken im Produkt bestehen oder schwache Passwörter (Mindestlänge, Komplexität) gewählt werden; von solchen Schwachstellen ist jedoch auszugehen. Bei Anwendungsprogrammen ohne Passwort-Verschlüsselung (beispielsweise beim Webmail Provider im Internet) besteht ebenfalls das Risiko, dass das Passwort im LAN oder Internet abgehört und für unberechtigte Anmeldungen unter falscher Benutzerkennung verwendet wird. Wenn nicht der gesamte Netzwerkverkehr verschlüsselt wird, besteht das oben genannte Risiko bezüglich Passwörter. Vertrauliche Daten sollten mindestens bei Kommunikation im/durch das Internet verschlüsselt werden.

Weitere Informationen sind beim BSI zu finden unter M 5.66.

## ★ M 5.91 – Einsatz von Personal Firewalls für Internet-PCs

Wird auf dem lokalen Computer ein Paketfilter / eine Firewall eingesetzt? ○ ja ○ nein

Es kann zum Beispiel eine lokale Firewall verwendet werden, welche den Netzwerkverkehr vom und zum Computer analysiert - neben beispielsweise einer zentralen Firewall im Firmennetz oder einer Firewall beim Internetprovider im privaten Umfeld.

Falls der Computer weder von einer lokalen noch von einer zentralen Firewall geschützt ist, besteht das sehr hohe Risiko, dass der Computer vom Internet angegriffen wird und die Datensicherheit generell nicht gegeben ist. Falls der Computer zwar von einer zentralen Firewall geschützt ist, aber keine lokale Firewall vorhanden ist, besteht das Risiko von Angriffen aus dem lokalen Netz (was jedoch gewisse IT-Kenntnisse für einen erfolgreichen Angriff voraussetzt). Zudem besteht das Risiko, dass ohne Einsatz von lokalen Firewalls ausgehende Verbindungen nicht kontrolliert werden und deshalb beispielsweise Trojanische Pferde unentdeckt bleiben können.

Weitere Informationen sind beim BSI zu finden unter M 4.238.

## ★ M 5.93 – Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs

Sind die Sicherheitsfunktionen des Browsers aktiviert und werden diese regelmässig überprüft? ○ ja ○ nein

Beispielsweise sind in den Browsereinstellungen die folgenden Optionen zu deaktivieren: aktive Inhalte (ActiveX, Java-Skripts), Plug-Ins und automatische Passwortspeicherung bei Formularen.

Es besteht das Risiko, dass ein Angreifer aus dem Internet die Schwäche in der Browser-Konfiguration ausnutzt und Zugriff auf das lokale System erlangt. Dadurch kann der Angreifer unter der lokalen Benutzerkennung Transaktionen durchführen. Weiter besteht das Risiko, dass automatisch abgespeicherte Formulardaten von einer unberechtigten Person erlangt werden (mit Software-Tools unterstützt, insbesondere bei direktem physischen Zugriff).

Weitere Informationen sind beim BSI zu finden unter M 5.69.

## M 5.94 – Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs

Erfolgt ein sicherer Umgang beim Empfangen von E-Mails? ○ ja ○ nein

Beispiele für einen sicheren Umgang beim Empfang von E-Mails sind: E-Mail Anhänge werden gefiltert (.exe Dateien blockiert), Passwörter werden nicht via E-Mails an die Benutzer verschickt oder als Alternative werden die E-Mails verschlüsselt.

Wenn gefährliche E-Mail Anhänge (wie .exe) von eingehenden E-Mails nicht gefiltert werden, besteht das erhöhte Risiko, dass Trojanische Pferde installiert werden, welche beispielsweise Passwörter abhören. Alternativ oder zusätzlich können Mitarbeiter im Umgang mit E-Mail-Anhängen geschult werden, so dass sich das Risiko verringert. Beim Versand von Passwörtern in unverschlüsselten E-Mails besteht das Risiko, dass Administratoren, E-Mail-Stellvertreter etc. in den Besitz von Passwörtern von fremden Benutzern kommen und anschliessend unberechtigt die entsprechende Benutzerkennung annehmen.

## M 5.96 – Sichere Nutzung von Webmail

Wird beim E-Mail Verkehr mit dem Webmail Provider geeignet mit Passwörtern zur Anmeldung umgegangen und die Verbindung verschlüsselt? ○ ja ○ nein

Beispiel für eine sichere Nutzung von Webmail: Das E-Mail Passwort für die Anmeldung zum Webmail-Provider wird regelmässig gewechselt, ist mindestens 8 Zeichen lang und wird bei keiner anderen Webseite verwendet. Zudem erfolgt der Zugriff auf die E-Mails beim Webmail-Provider über eine verschlüsselte Verbindung (SSL, https).

Beim unsicheren Umgang mit Webmail besteht das Risiko, dass die Passwörter abgehört oder durch Ausprobieren gefunden werden. Dadurch können E-Mails unter einer falschen Benutzerkennung über Webmail verschickt werden.

Weitere Informationen sind beim BSI zu finden unter M 5.66.

*M 1 – Allgemeine Bemerkung zu Massnahmen M 1.x: Wenn physischer Zugang zu IT-Systemen besteht (z.B. Zutritt zum Server-Raum), können gewisse logische Zugriffskontrollen (z.B. Passworteingabe) umgangen werden. Beispielsweise kann bei Windowssystemen in der Regel ab CD gebootet werden und mit Spezialprogrammen auf sämtliche Daten der Festplatte zugegriffen werden. Dadurch können beispielsweise Passwörter der Benutzer gestohlen werden, welche anschliessend für eine Anmeldung unter einer fremden Benutzerkennung verwendet werden können. Deshalb ist es wichtig, dass bei einer Beurteilung der Zugriffskontrollen zum IT-System stets auch berücksichtigt wird, ob die Systeme physisch vor unberechtigtem Zugriff geschützt sind.*

### ★ M 1.10 – Verwendung von Sicherheitstüren und -fenstern

Befinden sich besonders kritische IT-Systeme in Räumen mit Sicherheitstüren und -fenstern? ○ ja ○ nein

Beispiele solcher kritischen IT-Systeme sind Netzwerk-Server mit zentraler Ablage von vertraulichen Daten.

Ohne Sicherheitstüren und -fenster besteht das Risiko, dass unberechtigte Personen relativ einfach physischen Zutritt zu IT-Systemen mit erhöhtem Schutzbedarf erlangen. Dadurch können gewisse Sicherheitsmechanismen des IT-Systems umgangen werden (siehe M 1). Es kann möglicherweise auf wichtige, zentrale Daten zugegriffen werden (z.B. verschlüsselte Passwörter sämtlicher Netzwerkbenutzer, wobei mehrere Passwörter auf dieser Stufe häufig relativ leicht geknackt werden können).

Weitere Informationen sind beim BSI zu finden unter M 1.49, M 1.58, M 2.18.

### M 1.18 – Gefahrenmeldeanlage

Existiert eine Alarmanlage zur Erkennung und Warnung bei Einbrüchen? ○ ja ○ nein

Ohne Alarmanlage besteht das Risiko, dass Einbrüche nicht erkannt werden und unentdeckt bleiben.

### M 1.43 – Gesicherte Aufstellung aktiver Netzkomponenten

Sind besonders kritische Netzwerkkomponenten speziell vor physischem Zugang geschützt? ○ ja ○ nein

Beispielsweise werden Netzwerk-Server, Firewall-Systeme und Router in Serverräumen aufbewahrt, teilweise sogar in abschliessbaren Racks/Schränken.

Bei Zugang zu kritischen Netzwerkkomponenten besteht das Risiko, dass gewisse Sicherheitsmechanismen des Systems umgangen werden können (siehe M 1). Insbesondere ist an dieser Stelle ein einfacherer Zugang zu Passwörtern (Abhören und Manipulation des Netzverkehrs, Erlangen und Knacken von verschlüsselten Passwörtern) möglich.

### M 1.53 – Videoüberwachung

Werden Kameras zur Überwachung von Gebäude und Räumen eingesetzt? ○ ja ○ nein

Es besteht das Risiko, dass Einbrüche nicht erkannt und Abläufe nicht nachvollzogen werden können. Zusammen mit weiteren Schwachstellen beim Zutrittsschutz kann dies dazu führen, dass unberechtigte Personen relativ einfach physischen Zugang zu IT-Systemen erlangen.

### ★ M 2.17 – Zutrittsregelung und -kontrolle

Ist die Zutrittsregelung zu Serverräumen in einem Zutrittskontroll- ○ ○

konzept geregelt? ja nein

z.B. Verantwortlichkeit für die Kontrolle, Listen von Zutrittsberechtigten, sichtbares Tragen von Zutrittsausweisen

Erfolgt eine Aufzeichnung der erfolgten Zutritte und Austritte? ○ ja ○ nein

z.B. Aufzeichnung der durch Badge gesicherten Zutritte, Besucherliste mit Ausweisnummer und Visum für Zutritt und Austritt

Wenn Zutrittsregelungen nicht kontrolliert und dokumentiert werden, besteht das Risiko, dass Personen oder Personenkreise Daten unentdeckt einsehen oder manipulieren.

## ★ M 2.35 – Informationsbeschaffung über Sicherheitslücken des Systems

Werden die organisatorischen und technischen Massnahmen zur Behebung von Sicherheitslücken systematisch getroffen? ○ ja ○ nein

z.B. regelmässige Informationsbeschaffung über bekannte Sicherheitslücken, schnellstmögliches Einspielen von verfügbaren Patches und Updates

Wird die Software auf zentralen Netzwerkkomponenten regelmässig aktualisiert? ○ ja ○ nein

z.B. mittels neuen Software-Releases, Updates bei Tools etc.

Regelmässig werden Schwachstellen in Betriebssystemen, Datenbanken, Tools und Anwendungsprogrammen gefunden und im Internet veröffentlicht und sind somit einschlägig bekannt. Wenn die Schwachstellen durch das Einspielen neuer Software/Patches nicht geschlossen werden, besteht das Risiko, dass unberechtigte Personen diese Schwachstelle ausnützen und auf das IT-System zugreifen. Dadurch kann auf vertrauliche Daten zugegriffen, kann Netzwerk-Verkehr abgehört und können Daten sowie Konfigurationen verändert werden. In einem fortgeschrittenen Stadium kann unter falscher Benutzerkennung oder als Administrator auf das System zugegriffen werden. Dieses Risiko besteht insbesondere bei zentralen Netzwerk-Komponenten. Sehr ausgeprägt ist das Risiko bei Systemen, welche direkt im Zugriff des Internets stehen.

Weitere Informationen sind beim BSI zu finden unter M 2.273, M 4.152.

## ★ M 2.204 – Verhinderung ungesicherter Netzzugänge

Erfolgt jede Verbindung in das interne Netz ausnahmslos über gesicherte Zugänge? ○ ja ○ nein

Beispiel: zentrale Firewall, ohne die Möglichkeit, diese Firewall mit WLAN oder Modem zu umgehen.

Wenn Verbindungen über ungesicherte Zugänge möglich sind, besteht das Risiko, dass Unbefugte von aussen einfacher und unbemerkt ins Netz eindringen können.

## M 4.162 – Sichere Konfiguration von Exchange 2000 Servern

Sind die Zugriffsrechte für E-Mail-Administratoren restriktiv vergeben worden? ○ ja ○ nein

Die Administrations-Rechte für das E-Mail System sollten restriktiv vergeben werden an Personen, welche die Berechtigungen für ihre tägliche Arbeit benötigen.

Es besteht das Risiko, dass vertrauliche Daten (wie Passwörter) über E-Mail verschickt werden und die E-Mail-Administratoren davon Kenntnis erlangen. Dieses Risiko erhöht sich, je mehr Personen diese Administrationsrechte besitzen.

## M 4.239 – Sicherer Betrieb eines Servers

Erfolgt der Zugriff von Administratoren auf die zentralen Netzwerk-Komponenten gesichert? ○ ja ○ nein

Beispiele:
1) Administrationszugang zu zentralen Netzwerk-Komponenten ist ausschliesslich über die lokale Konsole am Server möglich (technisch so eingeschränkt) oder
2) Administrationszugang zu zentralen Netzwerk-Komponenten erfolgt mittels Fernzugriff über eine verschlüsselte Verbindung.

Bei ungesichertem Zugriff auf zentrale Netzwerk-Komponenten ist die Datenintegrität im lokalen Netz generell gefährdet, z.B. durch unberechtigten Administrationszugang und anschliessendem Ermitteln von Benutzerpasswörtern.

Weitere Informationen sind beim BSI zu finden unter M 4.80.

## M 5.124 – Netzzugänge in Besprechungs-, Veranstaltungs- und Schulungsräumen

Gibt es eine Sicherheitsrichtlinie für die Nutzung der installierten und der mitgebrachten Geräte in Besprechungs-, Vortrags- und Schulungsräumen? ○ ja ○ nein

Ist sichergestellt, dass aus Besprechungs- und Veranstaltungsräumen keine unberechtigten Zugriffe auf das lokale Netz erfolgen können? ○ ja ○ nein

Beispiele von angemessenen Sicherheitsmassnahmen sind: Installation von firmeneigenen Computern in Besprechungs- und Veranstaltungsräumen mit sehr eingeschränkten Zugriffsberechtigungen im lokalen Netz sowie Verbot zum Anschliessen von fremden Computern; Installation eines Firewall-Rechners zur Trennung und Kontrolle des lokalen Teilnetzes bei Besprechungs- und Veranstaltungsräumen; technische Einschränkungen für den Anschluss von Computern ans Netz (z.B. Authentisierung über die so genannte MAC-Adresse oder Deaktivierung der automatischen Adress-Zuweisung an fremde Computer (kein DHCP)).

Es besteht das Risiko, dass aus Besprechungs-, Veranstaltungs- und Schulungsräumen auf das lokale Netz unberechtigt zugegriffen wird und somit Besucher auf vertrauliche Daten zugreifen beziehungsweise sich im Extremfall sogar mit den ermittelten Passwörtern unter einer fremden Benutzerkennung einwählen. Kompensierende Sicherheitsmassnahme kann eine ständige Begleitung und Überwachung von Besuchern sein.

Weitere Informationen sind beim BSI zu finden unter M 2.333.

## ★ M 2.71 – Festlegung einer Policy für ein Sicherheitsgateway

Gibt es eine Weisung für einen Sicherheitsgateway und wird deren Einhaltung überprüft? ○ ja ○ nein

Beispielsweise regelt die Weisung für einen Sicherheitsgateway, welche technischen Kommunikationsprotokolle zwischen dem sicheren und dem unsicheren Netz zugelassen sind. So könnte beispielsweise ausgehender Web-Verkehr zugelassen werden. Weiter kann der Umfang der Protokollierung auf einem solchen System geregelt werden.

Wenn es keine Weisung für einen Sicherheitsgateway gibt, besteht das Risiko, dass der Gateway falsch konfiguriert und ungewollter Netzwerkverkehr zugelassen wird. Dadurch wird die Sicherheit im Netz generell gefährdet. Zudem besteht das Risiko, dass auf dem Sicherheitsgateway wichtige Informationen nicht protokolliert werden, wodurch die Nachvollziehbarkeit von Verbindungen und Transaktionen nicht gegeben ist.

Weitere Informationen sind beim BSI zu finden unter M 2.279, M 2.299, M 4.225.

## M 4.112 – Sicherer Betrieb des RAS-Systems

Müssen sich Computer bei einer Verbindung und Einwahl ins interne Netz über ein unsicheres Netz (z.B. über Telefonlinie mittels Modem oder übers Internet) mit einem starken Authentisierungsverfahren anmelden? ○ ja ○ nein

Starke Authentisierungsverfahren beruhen auf mindestens 2 der folgenden 3 Faktoren: Authentisierung mit 1) etwas, das man weiss (z.B. Passwort); 2) etwas, das man hat (z.B. Streichliste); 3) etwas, das man ist (z.B. Fingerabdruck).

Zugriffe aus unsicheren Netzen ins interne Netz sind den Angriffen von (externen) Hackern ausgesetzt. Wenn ein schwaches Authentisierungsverfahren angewendet wird, besteht das Risiko, dass sich eine unberechtigte Person unter einer falschen Benutzerkennung ins interne Netz einwählt (z.B. durch vorgängiges Herausfinden von Passwörtern auf dem Computersystem des berechtigten Benutzers mit Fernzugriff). Durch die Authentisierung mit mehreren Faktoren kann dieses Risiko verringert werden. Alternativ können Schulungen der Benutzer zum sicheren Umgang mit Passwörtern, verschlüsselte Kommunikationsverbindungen und sicher konfigurierte Client-Systeme das Risiko ebenfalls verringern.

## ★ M 5.21 – Sicherer Einsatz von telnet, ftp, tftp und rexec

Werden die weit verbreiteten Dienste "telnet" (Fernzugriff auf Konsole) und "ftp/tftp" (Datei-Transfer) ausschliesslich in verschlüsselter Form verwendet? ○ ja ○ nein

z.B. durch Einsatz des sicheren Kommunikationsprotokolls SSH (Secure Shell)

Der Einsatz von telnet, ftp und tftp ohne zusätzliche Sicherheitsmassnahmen erhöht das Risiko, dass die Kommunikation der betreffenden Systeme sehr einfach abgehört werden kann. Dadurch können unberechtigte Personen beispielsweise in den Besitz von Administrationspasswörtern gelangen, wodurch generell die Datensicherheit sämtlicher Systeme im lokalen Netz gefährdet wird.

## M 5.39 – Sicherer Einsatz der Protokolle und Dienste

Wird die Kommunikation verschlüsselt, wenn Administratoren mit dem Web-Browser die zentralen Netzwerkkomponenten administrieren? ○ ja ○ nein

Es sollten so genannte https-Verbindungen (SSL; Sicherheitsschloss im Browser angezeigt) für die Administration von Firewalls, Router, Switches etc. verwendet werden.

Wenn zentrale Netzwerkkomponenten über unverschlüsselte Verbindungen administriert werden, besteht das Risiko, dass die Passwörter der Administratoren abgehört werden. Dadurch können unberechtigte Personen die Netzwerk-Konfiguration ändern, wodurch die Sicherheit und Datenintegrität im lokalen Netz gefährdet ist. Um eine entsprechende Schwachstelle auszunutzen, ist ein gewisses Informatik-Wissen notwendig. Als alternative Massnahme zu verschlüsselten Verbindungen ist beispielsweise der Einsatz von Einmal-Passwörtern denkbar.

## M 1.63 – Geeignete Aufstellung von Access Points

Sind Wireless LAN Access Points im Gebäude derart aufgestellt, dass der unberechtigte Zugang erschwert ist? ○ ja ○ nein

z.B. in Doppelböden, in Metallgehäuse bei Wandhalterung etc.

Es besteht das Risiko, dass die Konfiguration des Wireless LAN Access Points unberechtigt geändert wird (z.B. mittels Reset-Knopf). Dadurch können Sicherheitsmechanismen ausgeschaltet werden, wie beispielsweise verschlüsselter Netzwerkverkehr oder Einschränkung der erlaubten Kommunikationspartner. Somit können Passwörter abgehört werden und die Nachvollziehbarkeit von Internet-Transaktionen ist nicht mehr gegeben (Surfen unter einer falschen IP-Adresse).

## ★ M 4.294 – Sichere Konfiguration der Access Points

Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des Access Points für drahtlose Netzwerke (WLAN) berücksichtigt worden? ○ ja ○ nein

Beispiele von wichtigen Sicherheitsmechanismen sind:
1) Aktivierung der Kommunikations-Verschlüsselung (es sollte mindestens das so genannte WPA Sicherheitsprotokoll verwendet werden; das WEP Protokoll bietet keine ausreichende Sicherheit);
2) Der Zugriff auf den Access Point bzw. die WLAN Kommunikation ist auf ausgewählte Computer eingeschränkt (Aktivierung des so genannten MAC-Filters und zusätzliche Authentisierung mittels Schlüssel/Passwörter)?
3) Die Passwörter/Schlüssel für den Zugriff auf den Access Point bzw. die WLAN Kommunikation sind nicht trivial (d.h. Mindestlänge von 8 Zeichen und kein Wort aus einem Wörterbuch);
4) Der Access Point wird abgeschaltet, wenn er längere Zeit nicht benötigt wird.

Risiken:
1) Wenn die Kommunikation über drahtlose Netzwerke nicht verschlüsselt wird, können vertrauliche Daten von Personen in der näheren Umgebung (ca. 200 m) abgehört werden. Anschliessend können beispielsweise die so erlangte Benutzerkennungen und Passwörter von der unberechtigten Person im Internet verwendet werden (Internetzugriff über eine fremde Benutzerkennung beim Provider; Webmail-Zugriff und E-Mail-Versand unter falscher Benutzerkennung etc.).
2 und 3) Wenn der Zugriff auf den Access Point und die WLAN Kommunikation nicht auf ausgewählte Computer eingeschränkt wird, besteht das erhöhte Risiko, dass unberechtigte Personen über das drahtlose Netz kommunizieren. Dadurch kann auf andere Computer des Netzwerks zugegriffen oder es kann unter einer fremden Benutzerkennung auf das Internet zugegriffen werden. Ein analoges Risiko besteht, wenn Passwörter und Schlüssel für die WLAN Kommunikation trivial gewählt werden.
4) Wenn der Access Point nicht benötigt und trotzdem nicht abgeschaltet wird, ist die WLAN Kommunikation unnötig gefährdet (durch beispielsweise Risiken wie oben genannt).

Weitere Informationen sind beim BSI zu finden unter M 4.293, M 5.139, M 5.141.

## M 4.295 – Sichere Konfiguration der WLAN-Clients

Sind wichtige Sicherheitsmassnahmen bei der Konfiguration des (Client-) Computers für drahtlose Netzwerke (WLAN) berücksichtigt worden? ○ ja ○ nein

Beispiele von wichtigen Sicherheitsmassnahmen sind:
1) Der Computer ist so konfiguriert, dass er selbst nicht WLAN Verbindungsanfragen von anderen WLAN Comutern direkt entgegen nimmt (d.h. der so genannte "Ad-hoc" Modus ist deaktiviert, so dass keine Client-Client Kommunikation stattfinden kann und der WLAN Verkehr stets über die Access Points führt).
2) Der Computer ist so konfiguriert, dass es nicht möglich ist, das WLAN zu nutzen, wenn der Computer gleichzeitig an ein "traditionelles" Kabelnetz angeschlossen ist.

Risiken:
1) Wenn Computer uneingeschränkt WLAN Verbindungsanfragen zulassen, besteht das Risiko, dass über diesen Weg unberechtigte Personen auf den lokalen Computer zugreifen. Alternativ können Verbindungsanfragen zugelassen werden, wenn zusätzliche Sicherheitsmassnahmen ergriffen

werden (insbesondere die Massnahmen "Restriktiver Zugriff auf Verzeichnisse und Dateien", "Sichere Access Point Konfiguration" und "Persönliche Firewalls" (BSI M 4.53, 4.294, 5.91)).
2) Wenn ein Computer gleichzeitig ans lokale (Kabel-) Netz und ans drahtlose Netz angeschlossen ist, besteht das Risiko, dass eine unberechtigte Person vom drahtlosen Netz über den lokalen Computer auf weitere Computersysteme im lokalen Netz zugreift. In diesem Szenario kann ein Angreifer über die drahtlose Verbindung auf das lokale Kabelnetz zugreifen und so die Kontrollen einer zentralen Firewall umgehen, welche eigentlich zum Schutz des lokalen (Kabel-) Netzes vorgesehen war.
Ohne wichtige Sicherheitsmassnahmen bei der Konfiguration des Client-Computers für drahtlose Netzwerke besteht somit das Risiko, dass über einen zusätzlichen Kanal auf den Client Computer zugegriffen werden kann (vorausgesetzt, es existieren keine kompensierenden Sicherheitsmassnahmen).

Weitere Informationen sind beim BSI zu finden unter M 4.297.

# Modem / ISDN

*Modul: Modem / ISDN*

## M 2.61 – Regelung des Modem-Einsatzes

Existieren angemessene Regelungen für den Einsatz von Modems? ○ ja ○ nein

Beispiele von Regelungen: Festlegung der berechtigten Benutzer, Protokollierung der Modem-Nutzung, Einschränkungen beim Versand von sehr vertraulichen Daten etc.

Es besteht das Risiko, dass Modemleitungen abgehört werden oder dass über Modems unberechtigt auf dahinter liegende Systeme zugegriffen wird.

## M 3.17 – Einweisung des Personals in die Modem-Benutzung

Werden Mitarbeiter über mögliche Gefährdungen, einzuhaltende Sicherheitsmassnahmen und Regelungen beim Betrieb eines Modems unterrichtet? ○ ja ○ nein

Es besteht das Risiko, dass Mitarbeiter durch unsachgemässe Handhabung der Modem-Nutzung einem Unberechtigten den Zugang zu Daten aktiv oder passiv verschaffen.

## ★ M 5.30 – Aktivierung einer vorhandenen Callback-Option

Ist das Modem an lokalen Computern derart konfiguriert, dass eingehende Telefonanrufe / Verbindungsanfragen standardmässig nicht beantwortet werden (d.h. die so genannte „Auto-Answer Funktion ist deaktiviert)? ○ ja ○ nein

Wenn das Modem eingehende Telefonanrufe / Verbindungsanfragen automatisch entgegen nimmt, besteht das Risiko, dass sich unberechtigte Personen über diese Verbindung Zugang zu dahinter liegenden Systemen verschaffen.

Ist bei eingehenden Telefonanrufen, welche durch das Modem automatisch abgenommen werden, die Rückruf-Funktion aktiviert? ○ ja ○ nein

Beispiel: Die Einwahl ins Firmennetz über ein Modem ist nur von ausgewählten Rufnummern möglich. Deshalb trennt das Modem eingehende Verbindungsanfragen umgehend und ruft automatisch zurück, wenn die Rufnummer in der Liste der autorisierten Anrufer ist.

Ohne die Aktivierung der Rückruf-Funktion bei Modems besteht das Risiko, dass eine unberechtigte Person von einem beliebigen Telefonanschluss über das Modem auf das dahinter liegende Computersystem (Einzelplatz-Rechner oder lokales Netz) zugreift. Mit der Aktivierung der Rückruf-Funktion kann das Risiko reduziert werden, da nur noch von ausgewählten Rufnummern über das Modem auf das Computersystem zugegriffen werden kann. Auf die Aktivierung der Rückruf-Funktion kann verzichtet werden, wenn alternativ andere Massnahmen zur Authentisierung eingesetzt werden, üblicherweise mit Benutzerkennung, Passwort UND Streichlisten/Nummerngeneratoren (Einmal-Passwörter) (d.h. Authentisierung mit etwas, was man weiss, und zusätzlich mit etwas, was man hat/ist).

Weitere Informationen sind beim BSI zu finden unter M 5.31.

# Datenbank / Anwendungsprogramm



## ★ M 2.221 – Änderungsmanagement

Wird im Rahmen von Änderungen an Datenbanken und Anwendungsprogrammen systematisch überprüft, ob sich dadurch neue oder geänderte Anforderungen für die Sicherheit ergeben?

○ ja ○ nein

Wenn die systematische Überprüfung der Sicherheitsanforderungen nicht erfolgt, besteht das Risiko, dass die getroffenen Massnahmen nicht mehr wirksam sind. Es besteht das erhöhte Risiko, dass man sich in einer falschen Sicherheit wähnt.

Weitere Informationen sind beim BSI zu finden unter M 2.62.

## ★ M 4.42 – Implementierung von Sicherheitsfunktionalitäten in der IT-Anwendung

Sind zusätzliche Sicherheitsfunktionalitäten in kritischen IT-Anwendungen und Datenbanksystemen implementiert?

○ ja ○ nein

Beispielsweise können bei IT-Anwendungen mit wichtigen Daten folgende Zusatz-Massnahmen ergriffen werden:
1) Vergabe von angemessen abgestuften Zugriffsrechten innerhalb des Anwendungsprogramms
2) Protokollierung der Transaktionen von Benutzer und Administratoren

Wenn Benutzer innerhalb des Anwendungsprogramms Zugriff auf sämtliche Daten haben, besteht das Risiko, dass auf vertrauliche Daten zugegriffen wird. Zudem kann bei fehlender Protokollierung und grossem Benutzerkreis nicht mehr nachvollzogen werden, wer welche Transaktionen durchgeführt hat.
Ohne Protokollierung ist nicht nachvollziehbar, wer welche Transaktionen durchgeführt hat (ausser ein einziger Benutzer besitzt die entsprechenden Zugriffsrechte).

Weitere Informationen sind beim BSI zu finden unter M 2.129, M 2.132.

## ★ M 4.72 – Datenbank-Verschlüsselung

Werden Daten aus Datenbanksystemen und kritischen IT-Anwendungsprogrammen verschlüsselt abgelegt?

○ ja ○ nein

Die in Datenbanken und Anwendungsprogrammen bearbeiteten Daten werden in Form von Dateien vom Betriebssystem gespeichert. Wenn diese Dateien unverschlüsselt abgespeichert werden, besteht das Risiko, dass Benutzer direkt vom Betriebssystem auf die Dateien zugreifen und die Daten abändern. In einem solchen Szenario ist nicht mehr nachvollziehbar, welcher Benutzer die Daten eingegeben bzw. geändert hat. Die Zugriffskontrollen der Anwendungsprogramme und Datenbanksysteme sind in einem solchen Fall wirkungslos und werden umgangen.

## M 4.133 – Geeignete Auswahl von Authentikations-Mechanismen

Werden bei der Anmeldung an sehr kritische Systeme / Anwendungs-programme neben Benutzerkennung und Passwort weitere Elemente zur Authentisierung benötigt?

○ ja ○ nein

Beispielsweise werden bei der Anmeldung zusätzlich benötigt: Eingabe eines Einmal-Passworts aus einer Liste, Biometrische Eingabe mittels Scan des Fingerabdrucks, Eingabe eines Pins aus einem Nummern-Generator etc.

Es besteht das Risiko, dass eine Benutzeranmeldung am System unter einer falschen Benutzerkennung erfolgen kann. Bei absoluter Verlässlichkeit auf kompensierende Sicherheitsmechanismen (Verschlüsselung, sicherer Passwortumgang etc.) kann auf zusätzliche Elemente zur Authentisierung verzichtet werden. Aufgrund der generellen Fehleranfälligkeit besteht insbesondere bei kritischen Systemen das Risiko, dass der Schutz ohne diese zusätzlichen Authentikations-Mechanismen nicht angemessen ist.

## 1.5 Glossar

Einige der Begriffe stammen aus www.wikipedia.de; eine weitere hilfreiche Quelle ist www.whatis.com.

| | |
|---|---|
| Access Point | Bezeichnung für eine aktive Verbindung zum Internet bzw. zu einem Online-Dienst. Ein Wireless Access Point ist ein elektronisches Gerät, das als Schnittstelle zwischen einem Funknetz und einem kabelgebundenen Rechnernetz fungiert. |
| ActiveX | ActiveX ist eine Entwicklung von Microsoft, welche die Freigabe von Informationen zwischen Anwendungen erleichtert und die Einbettung beliebiger Objekte (Video, Sound,...) in fremden Dokumenten wie z.B. Web-Seiten erlaubt. Damit lassen sich also "aktive Inhalte" in Web-Seiten realisieren: Programme werden vom Server auf den Rechner des "Surfers" übertragen und dort ausgeführt. |
| Administrator | Als Administrator wird der Systemverwalter zum Beispiel eines Netzwerks, eines Computers oder eines ganzen Computer-Systems bezeichnet. Er besitzt weit reichende Zugriffsrechte, kann oft zahlreiche oder alle Einstellungen am System vornehmen, Benutzernamen und Kennwörter verwalten und ist für die Aufrechterhaltung des IT-Systems zuständig. |
| Authentisierung | Die Begriffe Authentisierung und Authentifizierung werden hier synonym verwendet für den Vorgang des Nachweises der eigenen Identität bzw. den Vorgang der Überprüfung (Verifikation) der behaupteten Identität eines Gegenübers, beispielsweise einer Person oder eines Computersystems. |
| Backup | Unter Backup (auch Datensicherung genannt) versteht man das Kopieren der in einem Computersystem vorhandenen Daten auf ein alternatives (häufig transportables) Speichermedium. Dort werden diese mit dem Ziel aufbewahrt, den Datenverlust bei Systemausfällen zu begrenzen. |
| Betriebssystem | Ein Betriebssystem ist die Software, welche die Verwendung (den Betrieb) eines Computers ermöglicht. Es verwaltet Betriebsmittel wie Speicher, Ein- und Ausgabegeräte und steuert die Ausführung von Programmen. |
| BIOS | Basic Input Output System: BIOS ist der hardwaregebundene Kern eines Betriebssystems, der beim Ausschalten nicht gelöscht wird. Dieser Chip wird einmalig mit Daten beschrieben, die vom Computer nur gelesen und nachträglich lediglich mit Hilfe von Spezialprogrammen verändert werden können. Nach jedem Einschalten des Rechners führt das BIOS zunächst einen Selbsttest durch. Dann benutzt der Computer das BIOS, um das Betriebssystem zu starten und die Daten zwischen der Festplatte, Grafik-Karte, Keyboard, Maus und Drucker zu kontrollieren, bis ihm diese Aufgabe von einem anderen System - z.B. dem Betriebssystem - abgenommen wird. |
| BSI | Bundesamtes für Sicherheit in der Informationstechnik (Deutschland) |

| | |
|---|---|
| Callback-Option | Rückruf-Funktion |
| Client | Programm oder ein Computer, der in direkter Verbindung mit einem Server Informationen abruft. |
| Datenbank | Die Datenbank gleicht einem elektronischen Karteikasten. Hier findet man eine Sammlung von Daten, die miteinander in Beziehung stehen und stets aktualisiert werden. Übersichtliches Suchen, Korrigieren, Sortieren und Bearbeiten von vielen unterschiedlichen Daten wird hier ermöglicht. |
| DHCP | Dynamic Host Configuration Protocol: Das DHCP weist den angeschlossenen Clients aus einem festgelegten Bereich von IP-Adressen automatisch eine IP-Adresse zu und spart so viel Konfigurationsarbeit bei grösseren Netzen. |
| Email | Elektronische Post. Einer der wichtigsten Internet-Dienste, der das schnelle Übermitteln von Nachrichten ermöglicht. Im Anhang (Attachment) von E-Mails können auch Bild- und Textdateien sowie Softwareprogramme mit verschickt werden. |
| Exchange | Der Exchange Server ist ein Groupware- und Messaging-System der Firma Microsoft. Er kann für umfangreiche und vielfältige Aufgaben in von Microsoft-Produkten geprägten Infrastrukturen eingesetzt werden und eignet sich sowohl für kleine als auch grosse Netzwerke: so können beispielsweise E-Mails verwaltet und gefiltert, Zeitpläne erstellt, Termine vereinbart und Diskussionen geführt werden. |
| Firewall | Eine Firewall auch Sicherheitsgateway, Netzwerk-, oder Hardware-Firewall genannt, ist eine Netzwerk-Sicherheitskomponente in der Computertechnik, die Netzwerkverkehr anhand eines definierten Firewall-Regelwerks erlaubt oder verbietet. Das Ziel einer Firewall ist, den Datenverkehr zwischen Netzwerksegmenten mit verschiedenen Vertrauens-Stufen abzusichern. Ein typischer Einsatzzweck ist es, den Übergang zwischen einem lokalen Netzwerk (LAN) (hohes Vertrauen) und dem Internet (kein Vertrauen) zu kontrollieren. |
| FTP | File Transfer Protocol: wichtiger Dienst, der es ermöglicht, Dateien von externen Servern auf den eigenen Computer herunterzuladen (Download) und lokal erstellte Dateien (z.B. Aktualisierungen der eigenen Webseite) auf den Server zu kopieren. |
| Gateway | Computer/Gerät am Übergang zwischen zwei Netzwerken |
| Hacker | Ein IT-Spezialist, der mit seinem Fachwissen Sicherheitslücken sucht und ausnutzt. |
| HTTPS | HTTPS steht für Hyper Text Transfer Protocol Secure. Das Protokoll dient zur Verschlüsselung und zur Authentisierung der Kommunikation zwischen Webserver und Browser im World Wide Web. |
| Internet | Weltweiter Verbund von Computernetzwerken auf der Grundlage des einheitlichen Übertragungsprotokolls TCP/IP, in dem Kommunikation und Datenaustausch mit Hilfe verschiedener Internet-Dienste möglich |

| | |
|---|---|
| | sind. Zugang zum Internet verschaffen ISP (Internet Service Provider) und Online-Dienste. |
| Internetprovider | Zugangsvermittler zum Internet. |
| Intranet | Firmeninternes Netzwerk auf Grundlage der Internet-Dienste und Technologien (TCP/IP). Über ein Intranet kann (muss aber nicht) ein Zugang zum Internet und Extranet hergestellt werden. |
| IP-Adresse | Adresse eines einzelnen Computers im Internet. Die IP-Adresse besteht aus vier Zahlen von 0 bis 255, jeweils durch Punkte getrennt (Beispiel: 193.7.250.19). |
| ISDN | ISDN steht für "integrated services digital network". Die Leitidee des ISDN ist die Integration verschiedener Informationsformen (Sprache, Text, Bild, Daten), für die früher aufgrund ihrer unterschiedlichen physikalischen Struktur auch unterschiedliche Kommunikationsnetze bereitgestellt werden mussten. |
| Java-Skripts | Scriptsprache von Netscape, die im lokalen Browser interpretiert und ausgeführt wird, ohne dass dabei der Webserver involviert ist. |
| Konfiguration | Mit einer Konfiguration bezeichnet man eine bestimmte Einstellung von Programmen oder Hardwarebestandteilen eines Computers. |
| Konsole | Fenster, in dem Befehle per Kommandozeile eingegeben werden können. |
| LAN | Lokales Netzwerk, das Arbeitsplatzrechner (Clients) untereinander und (zumeist) mit einem oder mehreren Servern verbindet. Grundvoraussetzung für den internen Datenaustausch und die Realisierung eines Intranets. |
| MAC-Adresse | Media Access Control: Ein Zugangsverfahren zum eigentlichen Medium (Kabel) eines Netzes, das im Netzwerkcontroller implementiert ist - also beispielsweise in der Netzwerkkarte. Diese verfügt über eine so genannte MAC-Adresse (oder Hardware-Adresse), durch die eine Station eindeutig im Netz identifiziert ist. Es handelt sich sozusagen um die unverwechselbare Seriennummer eines Netzwerkgerätes. |
| Mailprovider | Zugangsvermittler zum Mail. |
| Modem | Modem ist ein Gerät zur Datenfernübertragung, welches eine Verbindung zu einer Gegenstation aufbaut, Signale, die vom Computer kommen, in Töne umsetzt und diese zur Gegenstation sendet und - auf der anderen Seite der Leitung eingesetzt - die empfangenen Töne wieder in maschinenverständliche Signale zurückübersetzt (moduliert). |
| Netzwerk | Verbund von Rechnern, die untereinander Daten austauschen. Netzwerk-Rechner können als Host beziehungsweise Server Daten zur Verfügung stellen oder als Client auf diese zugreifen. In manchen Netzwerken üben die verbundenen Rechner auch beide Funktionen gleichzeitig aus. |

| | |
|---|---|
| Patch | Kleines Programm, das Fehler in Anwendungsprogrammen oder Betriebssystemen behebt. |
| PC | Personal Computer |
| PDA | Persönlicher Digitaler Assistent: Ein PDA ist ein Computer im Westentaschenformat. Die Geräte verfügen über Büro-Funktionen wie Kalender, Adress- oder Notizbuch und erlauben die digitale Kommunikation (z.B. für E-Mail per Handy-Modem). |
| PDF | PDF steht für Portable Document Format und ist ein plattformunabhängiges weit verbreitetes Dateiformat. PDF-Dokumente können zwischen Rechnern unterschiedlicher Betriebssysteme ausgetauscht und auch in Browsern mit dem entsprechenden PlugIn (PDF-Viewer) dargestellt werden. |
| Pin | Verfahren zur Authentisierung. Hierbei sind für den Zugang zum Konto neben der Konto- oder Kundennummer die geheime PIN (Personal Identification Number) anzugeben. |
| Plug-In | Hilfsprogramm, das sich in ein anderes Programm "einklinkt" und dessen Funktionalitäten erweitert. |
| Protokollierung | Dokumentieren in Protokollen (oder Protokolldateien, Log-Files), welche Transaktionen ausgeführt wurden oder welche Fehler aufgetreten sind. |
| Rexec | Um Befehle auf einem Nicht-Windows-Remotecomputer auszuführen, können von Computern unter Betriebssystemen der Windows Server 2003-Produktfamilie, Windows XP und Windows 2000 mit dem Tool Rexec eine Verbindung zu Nicht-Windows-Computern hergestellt werden. Der Befehl rexec authentisiert den Benutzernamen auf dem Remotecomputer, bevor der angegebene Befehl ausgeführt wird. |
| Router | Ein Router ist eine Netzwerkkomponente, die mehrere Rechnernetze koppelt. |
| RAS | Remote Access Service: Online-Anwendung, mit dessen Hilfe sich externe Nutzer (z.B. Aussendienstmitarbeiter) über Telekommunikationsleitungen in ein internes Firmennetz (LAN, Intranet) einwählen können und Zugriff auf alle dort verfügbaren Programme und Dateien haben. |
| Server | Computer, der im Dauerbetrieb arbeitet, Programme und Dateien (Datenbanken, Textdateien) zentral speichert und diese zum Abruf durch Client-Rechner bereithält. Server sind einerseits Knotenpunkte in firmeninternen Netzen (LAN, Intranet) und halten dort gemeinsam genutzte Programme und Dateien vor. Mailserver dienen zur Verwaltung und Weiterleitung von E-Mails. Webserver speichern Webseiten und machen sie im Internet verfügbar. |
| SSH | Secure Shell: Programm und Netzwerkprotokoll gleichen Namens, um sich übers Internet auf einen entfernten Computer einzuloggen und Daten auszutauschen oder dort Programme auszuführen. Im Gegen- |

| | |
|---|---|
| | satz zu z.B. TELNET geschieht die Kommunikation über ein ungesichertes Netzwerk, aber verschlüsselt und mit Authentisierung. |
| SSL | Secure Socket Layer: Möglichkeit zur Verschlüsselung der Datenübertragung. SSL ist zwar grundsätzlich für verschiedene Anwendungen nutzbar, wird aber relativ häufig bei Web-Zugriffen im Bereich des E-Commerce, Online-Banking oder E-Governments eingesetzt. |
| Switch | Ein Switch (engl. Schalter, auch Weiche) ist eine Netzwerk-Komponente zur Verbindung mehrerer Computer beziehungsweise Netz-Segmente in einem lokalen Netz (LAN). |
| TELNET | Dienst im Internet, der es erlaubt sich auf entfernten Rechnern einzuloggen und zu arbeiten. |
| TFTP | Das Trivial File Transfer Protocol (TFTP) ist ein sehr einfaches Dateiübertragungsprotokoll. TFTP unterstützt lediglich das Lesen oder Schreiben von Dateien. |
| Tools | Dienstprogramm, das für den Benutzer beziehungsweise Systemverwalter eines Computers allgemeine, oft systemnahe Aufgaben ausführt. Üblicherweise gehört eine Reihe von Dienstprogrammen zum Lieferumfang eines Betriebssystems, wobei jedes Dienstprogramm meistens auf eine ganz bestimmte Aufgabe spezialisiert ist. |
| Trojanisches Pferd | Programm, das neben einer offiziellen Funktion eine zweite Funktion (in der Regel eine Schadfunktion) hat. Sinn eines Trojanischen Pferds kann es beispielsweise sein, Zugangskennungen mitzuprotokollieren. |
| Update | Eine Aktualisierung, oft auch als (engl.) Update bezeichnet, beschreibt den Vorgang, etwas bereits Vorhandenes auf den neuesten Stand zu bringen. Eine Aktualisierung beziehungsweise ein Update kann also nur durchgeführt werden, wenn eine bestehende Version existiert. |
| Verschlüsselung | Übersetzung von sinnvollen Daten in scheinbar sinnlose Daten mit Hilfe eines (elektronischen) Schlüssels. Eine Rückübersetzung ist nur mit Hilfe eines geeigneten Schlüssels möglich. Sind die Schlüssel für Ver- und Entschlüsselung identisch, handelt es sich um symmetrische Verschlüsselung. Wird zum Entschlüsseln ein anderer (privater) Schlüssel als zum Verschlüsseln (öffentlicher) benötigt, spricht man von asymmetrischer Verschlüsselung. |
| VPN | VPN steht für Virtual Privat Network. Mit VPN lässt sich der Zugriff auf einen Rechner oder ein Firmennetzwerk über das Internet aufbauen. |
| Webmail | Nach Überprüfung der Zugangsberechtigung stellt dieses Interface dem Benutzer die Funktionalität eines E-Mail-Clients über das Internet zur Verfügung. E-Mails können so online über die Web-Oberfläche gelesen oder verschickt werden. |
| WEP | Wired Equivalent Privacy: Bezeichnet ein Verschlüsselungsverfahren, das für Wireless LANs verwendetet wird. |

| | |
|---|---|
| WLAN | Wireless-LAN, auch W-LAN genannt, bezeichnet ein Netzwerk, das nicht wie bekannt über Kabel, erstellt ist, sondern kabellos (Englisch: wireless) funktioniert. |
| WPA | WPA steht für Wi-Fi Protected Access: Nachdem sich die WLAN-Verschlüsselung WEP als unsicher erwiesen hat, wurde der WPA-Standard zur Absicherung von Funknetzen entwickelt. Er bietet zusätzlichen Schutz durch dynamische Schlüssel. |
| WWW | Das World Wide Web (kurz Web, WWW oder deutsch: Weltweites Netzwerk; wörtlich: web „Gewebe, Netz“) ist ein über das Internet abrufbares Hypertext-System. Hierzu benötigt man einen Webbrowser, um die Daten vom Webserver zu holen und z.B. auf dem Bildschirm anzuzeigen. |
| WWW-Browser | Programm zum Abruf und zur Anzeige von Dokumenten im World Wide Web; notwendige Voraussetzung zur Informationssuche im Netz und zum Besuch von Webseiten. Die am weitesten verbreiteten Browser sind Netscape Navigator und Microsoft Internet Explorer. |