IT-Sicherheit

IT-Sicherheitsrichtlinie

Version 1.1

Inhaltsverzeichnis:

1 Vorwort

Die vorliegende IT-Sicherheitsrichtlinie beinhaltet die Beschreibung grundlegender organisatorischer, personeller, infrastruktureller und technischer Standardsicherheitsmaßnahmen. Es stellt eine Ergänzung zu den bestehenden Regelungen und Vorschriften der jeweiligen Organisation dar.

2 Bauliche und infrastrukturelle Maßnahmen

2.1 Zutrittskontrolle

Der Zutritt zu schützenswerten Gebäudeteilen und sicherheitssensiblen Geräten (wie z. B. Serverräumen, Serverschränken, Servern, Firewalls, Viruswalls, usw.) ist zu überwachen. Es muss geregelt werden, welche Personen bzw. Personengruppen Zutritt zu welchen Bereichen erhalten. Dies sollte auch dokumentiert werden (Vergabe und Rücknahme von Zutrittsberechtigungen).

2.2 Zugriffsschutz und Raumsicherheit

- Räume sind, wo immer das möglich ist, beim Verlassen abzusperren.
- Schützenswerte Gebäudeteile (wie z. B. ein Serverraum) sollen bei Vorhandensein einer Schließanlage durch eine eigene Schließgruppe geschützt werden. Wenn dies aus räumlichen und organisatorischen Gründen nicht möglich ist muss sichergestellt werden, dass nur befugte Personen Zutritt zum betreffenden Gebäudeteil erhalten.
- Bildschirme sind nach Möglichkeit so aufzustellen, dass keine unbefugte Einsicht möglich ist.
- Datenträger und Ausdrucke sind vor Einsichtnahme zu schützen.
- Verbindungen (z. B. Internetverbindungen) sind zu trennen, sobald diese nicht mehr benötigt werden.

2.3 Verwaltung von Zutrittskontrollmedien

Für alle Schlüssel eines Gebäudes ist ein Schließplan zu erstellen. Die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln ist zentral zu regeln. Reserveschlüssel sind vorzuhalten und, ebenso wie nicht ausgegebene Schlüssel, gesichert und geschützt aufzubewahren.

Die Ausgabe der Schlüssel erfolgt gegen Quittung und ist zu dokumentieren. Es sind Vorkehrungen zu treffen, wie bei Verlust einzelner Schlüssel zu reagieren ist.

Bei Zuständigkeitsänderungen von Mitarbeitern sind deren Schließberechtigungen zu prüfen und die Schlüssel gegebenenfalls einzuziehen bzw. auszutauschen. Beim Ausscheiden von Mitarbeitern sind alle Schlüssel einzuziehen.

Diese Regelung gilt für andere Zutrittskontrollmedien (wie z. B. Chipkarten, usw.) sinngemäß.

2.4 Geeignete Aufstellung eines Arbeitsplatz-IT-Systems

Unter Arbeitsplatz-IT-Systeme sind z. B. PC’s, Notebooks, usw. zu verstehen. Bei der Aufstellung eines Arbeitsplatz-IT-Systems ist darauf zu achten, dass der Standort nach Möglichkeit so gewählt wird, dass nur dafür berechtigte Personen Zugang zu und Einsicht auf

die IT-Systeme haben.
Speziell bei der Abfrage von sensiblen Daten ist darauf zu achten, dass nur berechtigte Personen Einsicht auf den Bildschirm haben.

3 Personelle Maßnahmen

3.1 Administrator

Administratoren von IT-Systemen (und ihre Vertreter) müssen sorgfältig ausgewählt werden und absolut vertrauenswürdig sein. Sie haben auf den administrierten IT-Systemen oftmals allumfassende Rechte. Sie sind in der Lage, auf alle gespeicherten Daten zuzugreifen, sie gegebenenfalls zu verändern und Berechtigungen zu vergeben bzw. weiterzugeben. Aus diesem Grund muss bei der Auswahl des dafür eingesetzten Personals besonders sorgfältig vorgegangen werden.

3.2 Benutzerkonten und Passwörter

3.2.1 Benutzerkonten

Die Anlage von Benutzerkonten erfolgt durch den Administrator. Es dürfen nur für berechtigte Personen Benutzerkonten angelegt werden. Die Benutzerkonten dürfen nur jene Rechte erhalten, welche sie zur Erfüllung der ihnen übertragenen Aufgaben benötigen. Eine Änderung in der Aufgabenzuordnung hat eine entsprechende Anpassung der Rechte nach sich zu ziehen.

Beim Einrichten des Benutzerkontos (Accounts) wird durch den Administrator ein zufälliges Passwort erstellt (die Regeln über die Vergabe sicherer Passwörter – siehe 3.2.2 - sind dabei einzuhalten), welches dem Benutzer nach Möglichkeit persönlich (mündlich) oder schriftlich übermittelt wird. Die Übermittlung mittels E-Mail sollte nur in Ausnahmefällen erfolgen.

Der Benutzer muss das durch den Administrator erstellte Passwort sofort ändern. Ein Benutzerkonto muss immer über ein Passwort verfügen. Benutzerkonten ohne Passwort sind nicht zulässig.

Gesperrte Benutzerkonten dürfen nur durch den Administrator reaktiviert werden. Die Passwortvergabe ist dabei analog zur Neuanlage durchzuführen.

Benutzerkonten sind immer personenbezogen! Nur der Eigentümer darf das jeweilige Benutzerkonto verwenden. Login und Passwort des Benutzerkontos dürfen unter keinen Umständen an andere Personen weitergegeben werden.

3.2.2 Passwörter

Ein Passwort soll aus mindestens 6 Zeichen bestehen und sollte nach 6 Monaten geändert werden. Das Passwort sollte aus Buchstaben und Zahlen (oder Sonderzeichen) bestehen. Wenn der Verdacht besteht, dass das Passwort anderen Personen bekannt ist, ist das Passwort sofort zu ändern.

Es ist darauf zu achten, dass die Eingabe des Passworts unbeobachtet erfolgt.

Die Verwendung von Trivial-Passwörtern ist unbedingt zu unterlassen. Trivial-Passwörter sind solche Passwörter, welche leicht von Außenstehenden erraten werden können, z. B. Namen,

Geburtsdaten, usw. Darunter fallen aber auch Standardausdrücke wie „Test“, „keines“, „abcdef“, „123456“, usw.

Passwörter dürfen nicht gespeichert, aufgeschrieben und an sichtbarer oder leicht zugänglicher Stelle aufbewahrt werden. Wenn ein Passwort schriftlich dokumentiert wird, muss es versiegelt an einem sicheren Ort (z. B. Safe, Schließfach, usw.) aufbewahrt werden.

Die Bestimmungen für Passwörter gelten gleichermaßen für Benutzerkonten in einem LAN, auf einem lokalen PC, in Anwendungen sowie PIN’s bei Chip- und Signaturkarten.

3.3 Signaturkarten

Für Signaturkarten gelten die gleichen Bestimmungen wie für Benutzerkonten und Passwörter. Sie sind immer personenbezogen und dürfen keinesfalls an Dritte weitergegeben werden. Dies gilt auch für die PIN’s der Signaturkarte.

3.4 Organisatorische Regelungen für Zugriffsmöglichkeiten in Vertretungs- bzw. Notfällen

Es sind Vorkehrungen zu treffen, die in dringenden Fällen bzw. Notfällen bei Abwesenheit eines Mitarbeiters (z. B. im Urlaubs- oder Krankheitsfall) seinem Vertreter Zugriff auf das IT-System bzw. die Daten ermöglichen.

Sollte es dabei notwendig sein, dass Passwort eines Benutzers zurückzusetzen, ist dieser sofort nach seiner Rückkehr über das Zurücksetzen bzw. die Weitergabe des Passworts in Kenntnis zu setzen und ein neues Passwort von ihm zu vergeben. Das Zurücksetzen eines Passworts und eine eventuelle Weitergabe sind zu dokumentieren.

Beim Einsatz von Chipkarten zur Authentisierung sind Vorkehrungen zu treffen, die es erlauben, bei momentaner Inoperabilität bzw. Nichtverfügbarkeit der Chipkarte einem Berechtigten den Zugang zum System zu ermöglichen.

3.5 Regelungen für Mitarbeiter

Neue Mitarbeiter müssen über interne Regelungen, Gepflogenheiten und Verfahrensweisen beim IT-Einsatz informiert werden.

Bei Abwesenheit sollte jeder Mitarbeiter seine vertraulichen Unterlagen verschließen. Es ist besonders darauf zu achten, dass keine unberechtigten Personen (Besucher, Reinigungspersonal, unbefugte Mitarbeiter usw.) Zugriff auf Schriftstücke und Datenträger mit sensiblen Inhalten haben.

Jeder Benutzer muss sich bei Verlassen des Arbeitsplatzes vom PC abmelden oder, bei kurzer Unterbrechung der Arbeit, eine Sperre (Bildschirmsperre) des PC vornehmen. Wenn es absehbar ist, dass es nur eine kurze Unterbrechung der Arbeit ist, kann an Stelle des Abmeldens auch eine nach einer gewissen Zeit automatisch aktivierte Bildschirmsperre (z. B. durch einen passwortgeschützten Bildschirmschoner) erfolgen. Die Wartezeit für die automatische Bildschirmsperre darf nicht länger als 5 Minuten sein.

Beim Ausscheiden von Mitarbeitern sind folgende grundlegende Punkte zu beachten:

- Sämtliche Unterlagen, ausgehändigte Schlüssel, Chip- oder Signaturkarten (sofern Karte und Signatur im Besitz der Organisation sind), zur Verfügung gestellte IT-Geräte

(z. B. tragbare Rechner, Speichermedien, Dokumentationen) sind zurückzufordern.
- Falls Signaturen mit Eigenschaften, welche auf die Organisation oder die Tätigkeit Bezug nehmen, auf private Chip- oder Signaturkarten aufgebracht werden, sind diese Signaturen zu widerrufen.
- Sämtliche Zugangsberechtigungen und Zugriffsrechte sind zu entziehen bzw. zu löschen. Dies betrifft auch externe Zugangsberechtigungen via Datenübertragungseinrichtungen. Wurde in Ausnahmefällen eine Zugangsberechtigung zwischen mehreren Personen geteilt, so ist nach Ausscheiden einer der Personen die Zugangsberechtigung zu ändern. Eine Neuvergabe der Benutzerkennung an einen anderen Mitarbeiter soll ausgeschlossen werden.

4 Virenschutz

Viren können, ebenso wie Trojaner, Würmer, Spyware und ähnliches, unkontrollierbare Schäden an Daten und Programmen anrichten bzw. geheime Informationen offen legen. Es sind daher vorbeugende Maßnahmen gegen derartige Attacken zu treffen.

- Einsatz eines marktgängigen und aktuellen Virenschutzprogramms.
- Regelmäßige Updates der Virendatenbank bzw. der Virensignaturen.
- Das Virenschutzprogramm muss auf allen Rechnern resident im Hintergrund laufen und aktiviert sein (zumindest für die Bereiche Dateisystem, Internet, E-Mail). Eine Deaktivierung des Virenschutzprogramms ist zu untersagen.
- Überprüfung aller ein und ausgehenden Datenträger.
- Die Mitarbeiter sind zu sensibilisieren, wie mit E-Mails mit Anlagen von unbekannten, aber auch vermeintlich bekannten oder vertrauenswürdigen Absendern umzugehen ist. Speziell betrifft dies das Öffnen, Doppelklicken oder Speichern der Anlagen eines E-Mails.
- Im Falle einer Vireninfektion ist unverzüglich die Internetverbindung zu trennen und der betroffenen Client bzw. Server herunterzufahren.
- Jedem Benutzer muss eine Ansprechperson bekannt sein, die sie in Notfällen verständigen kann, um weitere Maßnahmen einzuleiten und zu koordinieren.

Erklärungen zu den einzelnen Virenarten:
- Viren:
  Nicht selbständige, in andere Programme oder Dateien eingebettete Programmroutinen, die sich selbst reproduzieren und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen an anderen Programmen oder deren Umgebung vornehmen.
- Trojanische Pferde:
  Selbständige Programme mit verdeckter Schadensfunktion, ohne Selbstreproduktion. Trojanische Pferde dienen vor allem dazu, Computer auszuspionieren. Der Trojaner verdankt seinen Namen dem Umstand, dass die Schadensroutinen oft in vermeintlich gutartigen Programmen versteckt sind.
- Würmer:
  Selbständige, selbst reproduzierende Programme, die sich in einem System (vor allem in Netzen) ausbreiten. Zu diesem Zweck verwenden viele Würmer das Adressbuch des infizierten Rechners und versenden Mails mit gefälschten Absenderadressen. Das Öffnen solcher Mails kann bei einem ungeschützten System zu einer Infizierung führen.
- Spyware:
  Programme, die den User und/oder sein Surfverhalten ohne sein Wissen ausspionieren. Diese Daten werden an den Hersteller der Software oder auch an

Dritte, meist mit dem Zweck, personalisierte Werbung und Pop-ups einzublenden, weitergeleitet. Mittels Spyware können aber auch sensible persönliche Daten an Unbefugte übertragen werden.

- Spam:
  Mit Spam bezeichnet man unerwünschte Werbemails. Gefährlich ist Spam grundsätzlich nicht, allerdings geht beim Löschen von Werbe-Mails wertvolle Arbeitszeit verloren. Mittels eigener Spam-Filter können entweder bereits auf Provider-/Mail-Server-Ebene oder auch erst am lokalen Rechner unerwünschte Mails gefiltert und gelöscht werden.
- Phishing:
  Phishing ist ein Kunstwort aus den beiden Begriffen „Password“ und „Fishing“ und bezeichnet den Versuch, mittels gefälschter E-Mails an fremde Nutzerdaten (Login, Passwort, TAN etc.) zu gelangen. Normalerweise wird der Empfänger eines solchen Mails unter Vorspiegelung falscher Tatsachen (Userdaten gingen verloren, Neuidentifikation ist notwendig usw.) aufgefordert, die Webseite einer Bank (Internet-Banking, Kreditkarteninstitut, usw.) aufzusuchen und dort seine Nutzerdaten einzutippen. Diese Webseiten sind ebenfalls gefälscht und sehen den Originalen zum Verwechseln ähnlich. Die dort eingetippten Daten landen natürlich auf den Servern von Betrügern, die dann mit den Nutzerdaten Transaktionen zum Schaden des Users durchführen. Grundsätzlich fordert kein seriöses Unternehmen seine Kunden auf, seine Nutzerdaten über das Internet zu bestätigen. Es sind also alle diesbezüglichen Mails zu ignorieren. In Zweifelsfällen sollte man sich telefonisch mit dem (vermeintlichen) Absender in Verbindung setzen.
- Dialer:
  Diese Einwahl-Programme bauen, nachdem sie am Computer aktiviert wurden, eine Internetverbindung über eine Mehrwertnummer auf. Der User bleibt weiterhin online und bemerkt möglicherweise nicht den Wechsel der Internetverbindung. Die Aktivierung eines Dialers erfolgt in der Regel durch den User selbst, indem er dem Download oder der Installation eines Programms zustimmt. Die Kosten für eine Internetverbindung über einen Dialer betragen in der Regel mehrere Euro pro Minute. Betroffen davon sind allerdings „nur“ Nutzer von sog. Einwahl-Internetverbindungen mittels analoger und ISDN-Modems.

5 E-Mail

Bei den meisten E-Mail-Systemen werden die Informationen unverschlüsselt über offene Leitungen transportiert und können auf diversen Zwischenrechnern gespeichert werden, bis sie schließlich ihren Empfänger erreichen. Auf diesem Weg können Informationen eventuell manipuliert werden.

Aber auch der Versender einer E-Mail hat oft die Möglichkeit, seine Absenderadresse („From“) beliebig einzutragen. Viele Viren versenden sich selbst per E-Mail und fälschen dabei oft auch die Absenderadresse.

Man kann sich daher nur bedingt auf die Echtheit der Absenderadresse verlassen und sich nur nach Rückfrage oder bei Benutzung von digitalen Signaturen der Authentizität des Absenders sicher sein. In Zweifelsfällen sollte daher die Echtheit des Absenders durch Rückfrage oder durch den Einsatz von digitalen Signaturen überprüft werden.

Wenn Nachrichten verschlüsselt werden ist allerdings zu beachten, dass diese im Allgemeinen nicht zentral auf Viren überprüft werden können (dazu wäre die zentrale Hinterlegung der notwendigen Schlüssel erforderlich). Es ist daher festzulegen, ob

verschlüsselte Nachrichten zugelassen sind und wie damit zu verfahren ist. Wenn verschlüsselte Nachrichten nicht zugelassen sind, können diese etwa durch eine Poststelle geblockt werden.

Die Benutzer müssen vor dem Einsatz von Kommunikationsdiensten wie z. B. E-Mail geschult werden, um Fehlbedienungen zu vermeiden und die Einhaltung der organisationsinternen Richtlinien zu gewährleisten. Insbesondere müssen sie hinsichtlich möglicher Gefährdungen und einzuhaltender Sicherheitsmaßnahmen beim Versenden bzw. Empfangen von E-Mails sensibilisiert werden.

Zur Vermeidung von Überlastung durch E-Mail sind die Mitarbeiter über potentielles Fehlverhalten zu belehren. Sie sollten dabei ebenso vor der Teilnahme an E-Mail-Kettenbriefen, vor Spams, der unnötigen Weiterverbreitung von Virenwarnungen sowie vor der Abonnierung umfangreicher Mailinglisten gewarnt werden.

Benutzer müssen darüber informiert werden, dass Dateien, deren Inhalt Anstoß erregen könnte, weder verschickt noch nachgefragt werden dürfen.

6 WWW-Browser

Eine Gefährdung der lokalen Daten geht beispielsweise von Programmen aus, die aus dem Internet geladen werden und ohne Nachfrage auf dem lokalen Rechner ausgeführt werden (z. B. ActiveX-Programme). Auch innerhalb von Dokumenten oder Bildern können Befehle enthalten sein, die automatisch beim Betrachten ausgeführt werden und zu Schäden führen können (z. B. Makro-Viren in Winword- oder Excel-Dokumenten).

Die Benutzer dürfen sich nie darauf verlassen, dass die geladenen Dateien oder Programme aus vertrauenswürdigen Quellen stammen. Alle Benutzer müssen darauf hingewiesen werden, dass sie selber dafür verantwortlich sind, beim Dateiladen alle entsprechenden Vorsichtsmaßnahmen zu ergreifen. Selbst wenn über die Firewall automatisch die geladenen Informationen auf Viren überprüft werden, bleiben die Benutzer verantwortlich für die Schadensfreiheit von geladenen Dateien oder Programmen.

Grundsätzlich müssen bei der Installation von Programmen natürlich die organisationsinternen Sicherheitsregeln beachtet werden.

7 Netzwerke und Internetzugang

Netzwerke, die zeitweise oder dauernd mit dem Internet verbunden sind, müssen über ausreichende Sicherheitseinrichtungen geschützt werden. Solche Sicherheitseinrichtungen werden als „Firewalls“ bezeichnet.

7.1 Firewall

- Jede Kommunikation zwischen dem Netzwerk (= LAN, WLAN, usw.) und Internet muss ausnahmslos über eine Firewall geführt werden. Wenn der zentrale Einsatz einer Firewall nicht möglich ist (z. B. in kleinen Organisationen), muss am Client eine Firewall eingesetzt werden. Dies kann auch eine Firewall sein, welche vom Betriebssystem bereitgestellt wird. Wenn der Zugriff aus einem VPN heraus erfolgt (die Verwaltung greift aus einem VPN heraus auf das Stammportal zu), kann der Einsatz einer Firewall entfallen, wenngleich er trotzdem empfohlen wird.

- Die Firewall muss korrekt installiert und administriert werden.
- Die Konfiguration und Administration der Firewall darf nur durch befugte Personen über einen gesicherten Weg möglich sein. Es darf nicht möglich sein, die Konfiguration der Firewall über das Internet auszulesen oder zu verändern.
- Wenn das eingesetzte Betriebssystem eine Firewall beinhaltet, sollte diese ebenfalls zusätzlich aktiviert werden.

7.2 WLAN

- Drahtlose Netzwerke (WLAN) müssen verschlüsselt arbeiten. Mindestanforderung ist dabei eine Verschlüsselung mit WEP 128 Bit. Es wird aber empfohlen, auf aktuelle bzw. verbesserte Sichrheitsmechanismen (wie z. B. WPA, 802.11i, …) zurück zu greifen.
- Beim WLAN ist das Senden der Service Set ID (SSID) zu deaktivieren. Wenn dies aus Kompatibilitätsgründen nicht möglich ist, ist die Default-SSID zu ändern. Der dabei neu vergebene Name soll nicht auf die Verwaltung, Abteilunge oder ähnliches schließen lassen.

7.3 RAS/RDP-Zugang

Sollte das LAN über RAS (Remote Access Service) bzw. RDP (Remote Desktop Protocol) zugänglich sein, sind die für das LAN geltenden Richtlinien analog anzuwenden. Speziell ist dabei auf

- Zugangssicherheit: Der entfernte Benutzer muss durch das System eindeutig identifiziert werden können. Die Identität des Benutzers muss durch einen Authentisierungsmechanismus bei jedem Verbindungsaufbau zum lokalen Netz sichergestellt werden.
- Zugriffskontrolle: Ist der entfernte Benutzer authentisiert, so muss das System in der Lage sein, die Remote-Zugriffe des Benutzers auch zu kontrollieren. Dazu müssen die Berechtigungen und Einschränkungen, die für lokale Netzressourcen durch befugte Administratoren festgelegt wurden, auch für den entfernten Benutzer durchgesetzt werden.
- Wenn der RAS- bzw. RDP-Zugriff über das Internet erfolgt, sollte dazu aus Sicherheitsgründen ein VPN (Virtual Private Network) aufgebaut werden.

zu achten.

7.4 Installation

- Die Installation, Administration und Betreuung sämtlicher IT-relevanten Komponenten und Systeme darf nur durch ausgebildetes Personal oder berechtigte Dienstleister erfolgen.

7.5 Handhabung des Internets

- Alle Benutzer sind in der Handhabung von Internet-Browsern und Internet-Diensten zu unterweisen. Die Benutzer müssen darauf hingewiesen werden, dass sie selbst dafür verantwortlich sind, beim Umgang mit dem Browser und vor allem beim Öffnen oder dem Download von Dateien entsprechende Vorsichtsmaßnahmen zu treffen.

8 Änderung und Aktualisierung der IT-Sicherheitsrichtlinie

Um die Aktualität der beschriebenen Maßnahmen sicherzustellen, wird die IT-Sicherheitsrichtlinie bei Bedarf überarbeitet und aktualisiert.

Das aktualisierte Dokument wird an die zugriffsberechtigte Stelle (die unterzeichnende Behörde) übermittelt und gilt als angenommen, wenn nicht binnen 14 Tagen Einspruch erhoben wird. Im Falle des Einspruchs durch die zugriffsberechtigte Stelle müssen für diese die Zugriffsrechte für sämtliche zugeordneten Portalverbundsapplikationen deaktiviert werden.

9 Kontrolle über die Einhaltung der IT-Sicherheitsrichtlinie

Die zugriffsberechtigte Stelle (die unterzeichnende Behörde) verpflichtet sich, dem Servicepartner bzw. einer von diesem dazu beauftragten Person eine Überprüfung der Einhaltung der IT-Sicherheitsrichtlinie zu gestatten.

Der Servicepartner ist jene Firma, mit welcher die zugriffsberechtigte Stelle (die unterzeichnende Behörde) die Portalverbund-Vereinbarung über die Zugriffsrechte abgeschlossen hat (Dokument „PV-Zugriff… .DOC“).

Die Nichteinhaltung der IT-Sicherheitsrichtlinie kann den Verlust der Zugriffsrechte auf die Portalverbunds-Applikationen nach sich ziehen.

10 Verpflichtungserklärung

Die zugriffsberechtigte Stelle (die unterzeichnende Behörde) verpflichtet sich und Ihre Mitarbeiter sowie alle Personen, die in ihrem Auftrag tätig werden, diese Bestimmungen bei allen Tätigkeiten, die mit dem Betrieb von Anwendungen im Portalverbundsystem zusammenhängen oder diese beeinflussen könnten, einzuhalten.

Für die zugriffsberechtigte Stelle:

_____

Datum, Unterschrift