Lars Behrens

WEKA

IT-Sicherheit

So schützen Sie Ihr Unternehmen vor Systemstörungen und Risiken

B BOOKS
BUSINESS BOOKS

Ein Problem? ***Kein Problem!***

CIP-Kurztitelaufnahme der deutschen Bibliothek

IT-Sicherheit

Autor: Lars Behrens

Projektleitung: Petra Schmutz

WEKA Business Media AG, Schweiz

WEKA Business Media AG
Hermetschloostrasse 77, CH-8048 Zürich
Telefon 044 434 88 88, Telefax 044 434 89 99
www.weka.ch

Zürich • Kissing • Paris • Amsterdam • Wien

ISBN 978-3-297-02063-0

1. Auflage 2013

Druck: Auble Druck GmbH, Layout: Dimitri Gabriel, Satz: Peter Jäggi

Inhaltsverzeichnis

Inhaltsverzeichnis

1. Grundlagen der IT-Sicherheit

1. Grundlagen der IT-Sicherheit

Dieses Kapitel beschäftigt sich mit den grundlegenden Bedrohungen der IT-Sicherheit, die sich aus organisatorischen, personellen und technischen Problemen zusammensetzen. Für die Bewertung der Gefahren, die von diesen Problemen ausgehen, sind eine Risikoabschätzung und gegebenenfalls eine Wirtschaftlichkeitsbetrachtung von Massnahmen zur IT-Sicherheit notwendig.

Sicherheit ist ein Prozess, der sich mit einer häufig ändernden Infrastruktur sowie mit täglich neuen Sicherheitslücken auseinandersetzt. Daraus ergeben sich bestimmte Anforderungen an die Einführung und Kontrolle der IT-Sicherheit selbst und an das Krisenmanagement im Notfall.

1.2 Bedrohung der IT-Sicherheit

Heutige IT-Strukturen sind meist recht komplexe Gebilde. Deshalb ergeben sich zahlreiche Möglichkeiten, Systeme oder Netzwerke zu stören, zu manipulieren oder unbefugt Daten zu lesen. Die IT-Sicherheit ist immer dann bedroht, wenn durch organisatorische, personelle oder technische Fehlleistungen Risiken entstehen und dadurch im ungünstigsten Fall Probleme auftreten.

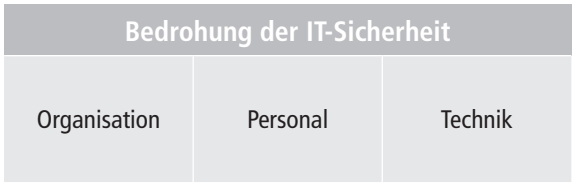

Abbildung 1: Bedrohung der IT-Sicherheit

Auf die Organisationsstruktur und die Auswahl des Personals hat ein Unternehmen einen entscheidenden Einfluss, während bei technischen Fehlern oft das Gefühl von Ohnmacht und Stochern im Nebel bleibt. Vielleicht ist das ein Grund dafür, dass zur Suche nach technischen Fehlern oft teure Security-Scanner angeschafft werden, dass aber offensichtliche personelle und organisatorische Probleme nur zögerlich angegangen werden.

> Die Erfahrung zeigt, dass die grössten Risiken im personellen oder organisatorischen Bereich liegen. Hier lohnt sich die Suche nach Sicherheitslücken also am meisten.

1.2.1 Bedrohungen durch organisatorische Fehler

Die Organisation der Arbeitsabläufe in einem Unternehmen oder einer Behörde ist oft über Jahrzehnte gewachsen. Da wird man manchmal betriebsblind gegenüber Mängeln.

BEISPIELE

Das Rechenzentrum ist durch eine teure Anlage vor unbefugtem Zutritt gesichert. Der Zugang durch die anliegende Druckerei ist leider nicht Bestandteil der Zutrittskontrolle.

Für die Zutrittskontrolle werden Chipkarten mit drei unterschiedlichen Berechtigungsstufen vergeben. Der Pförtner teilt die Karten an externe Personen nach der «Wichtigkeit» der Gäste aus und nicht nach deren Aufgaben.

Das Papierlager für die IT-Drucker befindet sich im selben Brandschutzabschnitt wie das Rechenzentrum.

Risiken durch organisatorische Fehler können die Existenz einer Firma bedrohen, besonders in Kombination mit personellen Problemen.

Um organisatorische Risiken aufzuspüren, sind regelmässige Prüfungen aller Abläufe nötig, z.B. in Form eines Security Audits.

1.2.1.1 Verantwortlichkeiten

Vermutlich werden die meisten Fehler in der Organisation durch eine falsche Zuordnung von Verantwortungen zu den einzelnen Aspekten der IT-Sicherheit gemacht.

BEISPIELE

Der Administrator eines IT-Systems kontrolliert gleichzeitig die Log-Dateien.

Der Programmierer eines Programms ist auch gleichzeitig der Tester.

Vergib die Verantwortung nach dem Motto «Teile und herrsche», sodass sich das System selbst kontrolliert. Andernfalls entstehen immer Sicherheitslücken, die nur schwer aufzudecken sind.

PRAXISTIPP

Auf keinen Fall miteinander vereinbar sind folgende Funktionen:

- Rechteverwaltung und Revision
- Netzadministration und Revision
- Programmierung und Test bei selbst erstellter Software
- Datenerfassung und Zahlungsanordnungsbefugnis
- Revision und Zahlungsanordnungsbefugnis

1.2.1.2 Verwaltung der Betriebsmittel

Ein weiterer Punkt in der Organisation, wo besonders schnell Sicherheitslücken entstehen, ist die Verwaltung der Betriebsmittel. Dabei geht es weniger darum, ob ein Mitarbeiter eine Tintenpatrone oder ein paar Disketten «mitgehen» lässt, sondern vor allem um den Einsatz von Instrumenten zur Vergrösserung der Sicherheit der IT-Systeme wie:

- Firewalls
- Viren-Scanner
- Produkte zur Content-Security

Der praktische Einsatz dieser Hilfsmittel ist natürlich technischer Natur. Die Organisation hat jedoch für die Randbedingungen eines vollständigen und effektiven Gebrauchs zu sorgen, damit sich keine offenen Flanken zeigen.

1.2.1.3 Zutritt, Zugang und Zugriff

Diese Begriffe stehen für die Arbeit des Personals mit den IT-Ressourcen, die vielfältigen Einschränkungen unterliegen:

- Zutritt zu Räumlichkeiten
- Zugang zu IT-Systemen
- Zugriff auf Dateien, Drucker, E-Mail etc.

Die Organisation von Zutritt, Zugang und Zugriff fängt bei der Verwaltung von Schlüsseln an und hört bei der Vergabe von Dateirechten auf.

Wenn die organisatorischen Vorgaben hier kein lückenloses Gebilde ergeben, entstehen Risiken, bei denen Personen auf nicht zugelassene Ressourcen zugreifen können.

1.2.2 Bedrohungen durch das Personal

Grundsätzlich kommt jede Person als potenzieller Angreifer in Betracht, die Zugang zu einem IT-System hat oder sich diesen verschaffen kann:

- Berechtigte User können im Rahmen ihrer Autorisierungen zugreifen.
- Unberechtigte User sind interne oder externe Benutzer, die unter Ausnutzung von Sicherheitsmängeln IT-Systeme nutzen.
- Eigene oder externe Systemprogrammierer haben eine Vielzahl von Rechten auf den von ihnen betreuten IT-Systemen.
- Service-Technikern wird für die Zeit der Wartungstätigkeiten ebenfalls eine Vielzahl von Rechten eingeräumt.
- Operateure sorgen für den ordnungsgemässen Ablauf des Systems, fahren Backups usw. Sie arbeiten als Administratoren und haben daher alle Möglichkeiten, die ihnen das System bietet.

- Putzpersonal oder Handwerker können aufgrund ihrer Tätigkeiten in die Nähe von IT-Systemen gelangen und unter Ausnutzung von Sicherheitsmängeln zugreifen.
- Software-Hersteller haben die Möglichkeit, intelligente Manipulationen wie Trojaner, Computerviren usw. in ihre Software einzubauen.
- Hardware-Hersteller sind in der Lage, ihre Hardware so zu konzipieren, dass sie zu einem bestimmten Ereignis oder zu einer bestimmten Uhrzeit gezielt oder zerstörerisch Manipulationen im System vornimmt.

Vollständige Überprüfung unmöglich
Besonders das Beispiel der Hersteller zeigt, dass eine Institution praktisch nicht in der Lage ist, alle am Arbeitsprozess beteiligten Personen zu überprüfen. Einzig der Teil des Personals, der sich in den eigenen Betriebsräumen aufhält, kann durch organisatorische Massnahmen daran gehindert werden, unberechtigt zuzugreifen.

1.2.2.1 Neue Mitarbeiter

Die Auswahl neuer Mitarbeiter ist unter dem Aspekt der IT-Sicherheit ein ganz kritischer Punkt. Dabei kann es allerdings nicht darum gehen, ein ungerechtfertigtes Misstrauen an den Tag zu legen. Doch sollte sich jeder Abteilungsleiter genau überlegen, wann er einem als Netzwerk-Administrator eingestellten Mitarbeiter den gesamten Satz an Schlüsseln und Passwörtern zur Verfügung stellt. Beim heutigen Mangel an Fachkräften ist es eher die Regel, dass neue Administratoren häufig sofort den vollen Zugang haben, ohne zunächst eine Vertrauensbasis zu schaffen.

Ähnliche Überlegungen gelten für die Einweisung bzw. Einarbeitung neuer Mitarbeiter. Sicherheitsprobleme entstehen nicht nur durch Böswilligkeit, sondern auch durch mangelndes Know-how und Erfahrung.

1.2.2.2 Alte Mitarbeiter und «vergessene» Accounts

Auch für ausscheidende Mitarbeiter müssen genaue Vorgaben existieren, was mit ihren Zugangsberechtigungen, Accounts und Daten zu geschehen hat.

WICHTIG

In der Hektik des Alltags wird gern vergessen, alte Accounts zu löschen und die dazugehörigen Daten an den Nachfolger bzw. die Kollegen zu verteilen. Das schafft Lücken, über die oft noch nach Jahren Zugriffe auf IT-Systeme möglich sind.

1.2.2.3 Schulungen und Sensibilisierungen

Besonders im recht komplexen IT-Bereich entstehen viele Sicherheitslücken durch Unkenntnis von Mitarbeitern. Das bedeutet für die Institution, eine meist beträchtliche Summe Geldes für Schulungsmassnahmen auszugeben.

Sicherheit geht alle an
Dabei ist es wichtig, dass nicht nur die Administratoren von IT-Systemen auf Schulungen zum Thema Sicherheit geschickt werden.

WICHTIG

Wenn nicht alle Mitarbeiter regelmässig auf die aktuellen Gefahren hingewiesen werden, entstehen durch Unkenntnis Löcher, durch die dann vielleicht trotz aller technischen Massnahmen ein Wurm oder Trojaner ins eigene Netz schlüpfen kann.

1.2.2.4 Checkliste: Private Nutzung und Überwachung von E-Mail und Internet

erfüllt	Massnahme
	Nutzungs- und Überwachungsreglement erstellen; Ziel: Klarheit und Sicherheit über die Rechte und Pflichten des Mitarbeiters im Umgang mit E-Mail und Internet sowie Klarheit über die Möglichkeit der Überwachung und Sanktionen
	Reglement den Nutzern zur Kenntnis bringen; den Erhalt des Reglements quittieren lassen
	Verbot der privaten E-Mail- und Internetnutzung am Arbeitsplatz theoretisch möglich; praktisch meist unverhältnismässig, daher massvolle Nutzung erlauben (allenfalls auf Randzeiten verlegen)
	Anonymisierte Überwachungen/Auswertungen vornehmen; personenbezogene Überwachungen und Auswertungen erst nach Feststellung des Missbrauchs durch Mitarbeiter durchführen
	Vor der Durchführung personenbezogene Überwachungen und Auswertungen den Mitarbeitern ankündigen
	Verzicht auf eine ständige personenbezogene Überwachung (eine solche Überwachung ist widerrechtlich)
	Überwachungen sind von übergeordneter Stelle anzuordnen und von spezialisiertem Personal vorzunehmen

E-Mail

erfüllt	Massnahme
	Uneingeschränkter Schutz privater E-Mails, wenn als solche erkennbar (idealerweise als solche kennzeichnen bzw. in Ordner ablegen)
	Kontrolle von geschäftlichen E-Mails erlaubt (Leistungs- und Geschäftskontrolle)
	Bei Verdacht einer strafrechtlichen Handlung via E-Mail: Beweissicherung erlaubt (Abspeichern des E-Mails). Einsicht in das E-Mail ist nicht erlaubt und hat durch die Strafverfolgungsbehörden zu erfolgen
	Stellvertretungsregelungen für Abwesenheiten aufstellen
	Regelung bei Austritt aus dem Unternehmen vorsehen

1.2.2.5 Beispiel: Weisung zum Gebrauch von Informatikinstrumenten und zur Benutzung von elektronischen Kommunikationseinrichtungen (technische Betriebsmittel)

Präambel

Das Unternehmen stellt den Mitarbeitern zur Erbringung ihrer Arbeitsleistung Informatikinstrumente (insb. PC) und elektronische Kommunikationseinrichtungen (E-Mail, Internet) zur Verfügung. Nebst den vielen Vorteilen (rasche Kommunikation, einfache Informationsbeschaffung usw.) bietet die Nutzung von Computer, E-Mail und Internet während der Arbeit auch wesentliche Gefahren und Nachteile für das Unternehmen und den einzelnen Mitarbeiter: die übermässige private Nutzung von Internet und E-Mail, Ausbleiben der erwarteten Arbeitsleistung, Sicherheitsrisiken für die Informatik des Unternehmens, Internetsucht usw.

Diese Weisung soll Klarheit bezüglich der Rechte und Pflichten der Mitarbeiter im Umgang mit den zur Verfügung stehenden Informatikinstrumenten und elektronischen Kommunikationseinrichtungen liefern und aufzeigen, wie und wann das Unternehmen Kontrollen zur Einhaltung der Weisung vornimmt.

Die Vereinbarung ist in 4 Bereiche aufgeteilt:

- **Allgemeines,** insb. Grundsatz, Regelung des persönlichen Geltungsbereichs und der Verbindlichkeit (Ziff. 1).
- **Informatikinstrumente und Sicherheit im eigenen Netzwerk,** insb. die Beschaffung von Hard- und Software und der Einsatz von privaten Informatikinstrumenten, Vorgaben für das An- und Abmelden am Informatiksystem, Umgang mit Passwörtern und der Einsatz des Virenschutzes (Ziff. 2).
- **Nutzung von elektronischen Kommunikationseinrichtungen (E-Mail und Internet),** insb. die private Nutzung sowie die Kontrolle und Überwachung des Nutzerverhaltens unter bestimmten Voraussetzungen (Ziff. 3).
- Die Sanktionierung von Verstössen (Ziff. 4).

1. Allgemeines

1.1 Grundsatz

Die Benutzung der Informatikinstrumente und elektronischen Kommunikationsmittel hat in direktem Zusammenhang mit der Tätigkeit des Arbeitgebers zu stehen. Sie soll dazu dienen, die unternehmerischen Ziele werkzeuggestützt und effizient zu erreichen.

Eine massvolle, gelegentliche private Benutzung dieser Betriebsmittel ist unter bestimmten, im Folgenden ausgeführten Voraussetzungen erlaubt.

1.2 Geltungsbereich

Der persönliche Geltungsbereich dieser Weisung umfasst alle Arbeitnehmer des Unternehmens, auch Praktikanten, Temporär- und Aushilfspersonal.

1.3 Verbindlichkeit

Diese Weisung ist für alle betroffenen Personen verbindlich. Sie räumt den Mitarbeitern Rechte und Pflichten ein, deren nicht Beachtung sanktioniert werden können.

2. Informatikinstrumente und Sicherheit im Unternehmensnetzwerk

2.1 Informatikinstrumente des Unternehmens

Beschaffung

Die Beschaffung von Informatikinstrumenten erfolgt zentral durch den internen Informatikdienst («IT-Abteilung»). Beschaffungen für das Unternehmen durch den Mitarbeiter sind nicht gestattet. Die Informatikinstrumente sind Eigentum des Unternehmens.

Hardware

Der jeweilige Benutzer ist für die sorgfältige Benutzung von PCs, Notebooks, Bildschirmen, Arbeitsplatzdrucker und andere Peripheriegeräten verantwortlich.

Datei- und Datenbankserver, Netzwerkkommunikationsgeräte und Netzwerk- sowie Sicherheitseinrichtungen dürfen nur von Mitarbeitern der IT-Abteilung oder von bezeichneten Dritten (externe Berater und Fachkräfte) bedient werden.

2.1.1 Software

Es gelangen nur Programme zum Einsatz, die von der IT-Abteilung getestet und freigegeben wurden und für welche das Unternehmen die entsprechenden Lizenzen erworben hat.

2.1.2 Installationen

Sowohl Hardware- wie auch Software-Installationen werden durch Mitarbeiter der IT-Abteilung vorgenommen. Dies gilt auch im Falle von Bürowechseln. Ohne Rücksprache mit der IT-Abteilung ist das Installieren von peripheren Geräten wie z.B. Drucker, Scanner, Modems untersagt.

Das Installieren und Benutzen von Fremdsoftware durch den Mitarbeiter ist untersagt.

2.2 Private Informatikinstrumente

Private Informatikinstrumente wie Scanner, Notebooks etc. dürfen grundsätzlich nicht im Firmennetz eingesetzt werden. Ausnahmen werden durch die IT-Abteilung bewilligt. Es besteht kein Anspruch auf finanzielle Vergütung. Auch die Versicherung solcher Geräte ist Sache des Eigentümers.

2.3 Private Daten auf dem Dienstcomputer

Mit im Unternehmen vorhandenen Programmen erstellte private Dateien sind ausschliesslich auf dem zu privaten Zwecken vorgesehenen Laufwerk H des Dienstcomputers zu speichern. Das Laufwerk H ist auf eine Speicherkapazität von 100 MB beschränkt.

Stösst das Unternehmen bei legitimen Kontrollen auf dem Dienstcomputer des Mitarbeiters (ausserhalb des Laufwerks H) auf Dateien, die möglicherweise privaten Charakter haben, so wird der Mitarbeiter über die Natur des Dokuments befragt. Deklariert der Arbeitnehmer die Daten sodann als privat, so hat dieser die Daten ins Laufwerk H zu verschieben. Stattdessen kann das Unternehmen diese Daten auch löschen (lassen).

2.4 An- und Abmelden am Informatik-System

2.4.1 Benutzerauthentisierung

Die Anmeldung erfolgt über eine benutzerspezifische Authentisierung. Über diese Authentisierung werden die Zugriffsberechtigungen auf die einzelnen Bereiche des Netzwerks sowie der Programme geregelt. Die Verantwortung für die dem Benutzer zugewiesenen Authentisierungsmittel (Benutzername und Passwort) trägt jeder Benutzer selbst. Sie sind persönlich, nicht übertragbar und dürfen anderen (Dritten oder Mitarbeiter) nicht zugänglich gemacht werden.

2.4.2 Abmeldung vom System

Wird der Arbeitsplatz für mehr als 5 Minuten verlassen, muss die Arbeitsstation vor unberechtigtem Zugriff gesichert werden. Die Dienstcomputer inkl. Bildschirme und lokale Arbeitsplatzdrucker müssen bei längerer Abwesenheit, vor allem über Nacht und am Wochenende, abgeschaltet werden.

2.5 Passwort

2.5.1 Passwortwechsel und Kreieren von Benutzerpasswörtern

Ein Passwortwechsel wird vom System alle 6 Monate verlangt. Während 4 Passwortwechseln kann dasselbe Passwort nicht erneut verwendet werden.

Passwörter dürfen nie in unmittelbarem Zusammenhang mit dem Benutzer stehen (z.B. Name des Kindes oder Partners, Geburtsdatum, Telefonnummer, Autokennzeichen). Grundsätzlich gilt, je komplexer ein Passwort ist, desto sicherer ist es.

2.5.2 Passwort-Sperre

Aus Sicherheitsgründen wird das Benutzer-Konto nach sechsmaliger Fehleingabe des Passworts automatisch gesperrt. Das Entsperren des Kontos wird durch die IT-Abteilung vorgenommen.

2.6 Virenschutz

Auf den Servern der IT-Abteilung sind alle Benutzer durch den Virenschutz des Unternehmens geschützt. Die im Netzwerk des Unternehmens gespeicherten Dokumente werden laufend geprüft. Des Weiteren befindet sich auf jeder Arbeitsstation ein lokales Virenschutzprogramm, welches automatisch und periodisch mit den neusten Virensignaturen versorgt wird. Das Virenschutzprogramm darf nie ausgeschaltet werden. Mobile Geräte, welche sporadisch ins Unternehmensnetzwerk angeschlossen werden, müssen zwingend mit einem Virenschutzprogramm mit aktualisierten Virensignaturen versehen sein.

3. Nutzung von elektronischen Kommunikationseinrichtungen

3.1 E-Mail

3.1.1 Generelles

Das elektronische Mail-System des Unternehmens dient dem geschäftlichen Informations- und Datenaustausch mit internen und externen Geschäftspartnern. Die angemessene, private Benutzung ist unter den folgenden Voraussetzungen erlaubt.

3.1.2 Private Benutzung

Die massvolle, gelegentliche Nutzung der E-Mail vorname.nachname@firma.ch (Mitarbeiter-E-Mail) zu privaten Zwecken während der Arbeitszeit ist erlaubt, sofern dadurch die Arbeitsleistung und die technischen Ressourcen der IT-Abteilung nicht beeinträchtigt werden. Nicht zu privaten Zwecken benützt werden dürfen Team-E-Mail-Adressen (z.B. einkauf@firma.ch, info@firma.ch). Die Kommunikation über diese E-Mails kann von allen Mitarbeitern des jeweiligen Teams eingesehen werden.

Private E-Mails sind im Betreff als solches zu kennzeichnen (Betreff: Privat) und in einem privaten Ordnern (Ordner «private Korrespondenz») abzulegen oder zu löschen.

Von allen Mailboxen auf dem Server werden nächtliche Backups erstellt. Der Benutzer hat private Mails auf einen anderen Datenträger zu speichern, wenn er diese Sicherung der privaten E-Mails nicht wünscht.

3.1.3 Generell nicht erlaubt sind

- das Verwenden der geschäftlichen E-Mail-Adresse zur Registrierung für private Dienstleistungen
- das Versenden von privaten E-Mails an den internen Mailverteiler (und damit Zustellung an alle Mitarbeiter des Unternehmens)
- das Versenden von privaten E-Mails, die grösser als 2 MB sind
- das Öffnen, Versenden und Weiterleiten von Mail-Beilagen wie z.B. ausführbare Programme (z.B. Dateierweiterungen .exe oder .vbs), Spiele, Kettenbriefe etc.
- das Versenden und Weiterleiten von Witzen, Comics, Fun-Videos und dergleichen
- das Versenden und Weiterleiten von unsittlichen und strafrechtlich relevanten Inhalten
- die Belästigung anderer Personen und Mobbing per E-Mail
- das Antworten auf Spam- oder Phishing-Mails (als Spam- oder Phishing-Mail erkennbare E-Mails sind ungeöffnet zu löschen)
- das Versenden von Geschäftsgeheimnissen an Unberechtigte

3.1.4 Maximale Grösse von E-Mails inkl. Anhänge

Die Grösse von E-Mails inklusive allfälliger Anhänge ist auf 6 MB beschränkt. Grosse Dateien sind über das Programm WinZip zu komprimieren.

3.1.5 Mailarchivierung

Gesetzliche Auflagen verpflichten das Unternehmen, geschäftsrelevante ein- und ausgehende E-Mails inkl. Anhängen während 10 Jahren aufzubewahren. Das eingesetzte Mailarchivierungs-Tool macht keinen Unterschied zwischen geschäftlichen und privaten E-Mails, d.h. es wird alles archiviert. Der Mitarbeiter erklärt sich mit dieser Archivierung einverstanden. Für das Öffnen privater E-Mails, die im Mailarchiv gespeichert sind, gilt die Regelung in Ziff. 3.3.4 und 3.3.5.

3.1.6 E-Mail-Account des Mitarbeiters, der das Unternehmen verlässt

Der Mitarbeiter muss alle privaten Elemente aus seinem Postfach löschen. Die geschäftlichen E-Mails, die weiterhin benötigt werden oder noch in Bearbeitung sind, hat er an seinen Stellvertreter, zuständigen Vorgesetzten oder Nachfolger weiterzuleiten oder entsprechend abzulegen. Nach dem letzten Arbeitstag des betreffenden Angestellten wird sein E-Mail-Postfach von der IT-Abteilung blockiert.

3.2 Internet

3.2.1 Nutzungsbestimmung

Das Internet dient der geschäftlichen Informationsbeschaffung für den Mitarbeiter. Die massvolle, gelegentliche Nutzung zu privaten Zwecken während der Arbeitszeit ist erlaubt, sofern dadurch die Arbeitsleistung sowie die technischen Ressourcen der IT-Abteilung nicht beeinträchtigt und die folgenden Regeln beachtet werden.

3.2.2 Generell nicht erlaubt sind:

- das Herunterladen und Installieren von Browser Plug-Ins und Programmen
- die Verwendung von Online-Spielen
- das Erstellen oder Verbreiten von schädlichen Programmcodes (z.B. Viren, Trojaner, Würmer)
- der Zugriff auf rassistische, pornographische, extremistische oder (andere) widerrechtliche und unsittliche Inhalte

3.2.3 Nicht erlaubt, falls dies nicht in geschäftlichem Auftrag erfolgt, sind:

- die Teilnahme an Börsenforen und das Online-Handeln (z.B. Aktien, Fonds, Wertpapiere, Güter) und E-Banking
- das Verschieben von Dateien über das FTP-Protokoll (File Transfer Protocol)
- die Teilnahme an Online-Auktionen und Versteigerungen (z.B. ebay)
- die Benutzung von Internet-Radiostationen oder Internet-Fernsehen
- die Benutzung von sozialen Internetplattformen, wie facebook.com, xing.com
- die Teilnahme an Newsgroups (Diskussionsforen), Blogs, Twitter

3.3 Aufzeichnungen und Kontrolle

3.3.1 Aufzeichnung des Internetverkehrs

Aus Sicherheitsgründen wird der Internetverkehr laufend von den Firewall-Servern des Unternehmen aufgezeichnet und protokolliert (Log-Files). Die Protokollierungen werden nach 7 Tagen automatisiert gelöscht. Im Rahmen der personenbezogenen Überwachung oder Strafverfolgungen werden die Protokollierungen bis zur Beendigung der Verfahren aufbewahrt.

Heruntergeladene Webseiten verbleiben im Zwischenspeicher des Browsers und des unternehmensinternen Proxy-Servers. Die Inhalte sämtlicher Zwischenspeicher werden nach 30 Tagen automatisch gelöscht. Der Mitarbeiter kann den Browserverlauf über die entsprechenden Funktionen des verwendeten Browsers jederzeit selber löschen.

3.3.2 Überprüfung der Log-Files

Bei Störungen und Ausfällen prüft die IT-Abteilung die nach Ziff. 3.3.1 angefallenen Daten. Die Log-Files werden dabei nicht mit einem bestimmten Computer (IP-Adresse) oder einer bestimmten User-ID (Passwort) eines Mitarbeiters verknüpft.

Besteht aufgrund der getätigten Überprüfung der Verdacht auf Missbrauch der elektronischen Kommunikationseinrichtungen, informiert die Geschäftsleitung die Informatik-Anwender, dass Missbräuche vorgekommen sind und dass die IT-Abteilung mit einer zeitlich befristeten, personenbezogenen Auswertung des Internetverhaltens der Mitarbeiter ab dem Folgetag der Information beauftragt wird.

Der Leiter der IT-Abteilung übergibt die Auswertungsresultate der Geschäftsleitung. Bei fehlbaren Mitarbeitenden sperrt die IT-Abteilung auf Anordnung der Geschäftsleitung den Zugang vorsorglich. Zudem werden verdächtige Informationen zur späteren Auswertung durch die Anwaltschaft oder den Richter sichergestellt.

3.3.3 Aufzeichnung des E-Mail-Verkehrs

Von den Mailboxen auf dem Server werden Backups erstellt (vgl. Ziff. 3.1.2). Zudem werden E-Mails (vgl. Ziff. 3.1.5) archiviert. Versandte E-Mails werden zusätzlich in der Ausgangsbox des Benutzers gespeichert.

3.3.4 Überprüfung von E-Mails

Das Unternehmen kann die Nutzung von Team-E-Mails (info@...ch; sales@...ch; usw.) jederzeit kontrollieren.

Bei der individualisierten Geschäfts-E-Mail (vorname.nachname@firma.ch) kann das Unternehmen (bzw. der Vorgesetzte) die geschäftlichen E-Mails des Mitarbeiters einsehen. Die Einsichtnahme dient einerseits der Geschäftskontrolle, andererseits, um bei Abwesenheiten des Mitarbeiters auf geschäftsrelevante E-Mails zugreifen zu können.

Auf als «Privat» gekennzeichnete E-Mails bzw. E-Mails, die im separaten Ordner «private Korrespondenz» abgelegt sind, darf das Unternehmen nur im Einzelfall mit vorgängiger, ausdrücklicher Zustimmung des Mitarbeiters für diesen Einzelfall zugreifen. Dasselbe gilt für E-Mails, die noch nicht im privaten Ordner abgespeichert sind, jedoch anhand des Betreffs als privat erkennbar sind.

3.3.5 Beweissicherung, Einsicht bei begründetem Verdacht

Falls konkrete Anhaltspunkte für eine Straftat unter Verwendung von E-Mails bestehen, hat das Unternehmen das Recht, entsprechendes Beweismaterial zu sichern. Die Geschäftsleitung beauftragt die IT-Abteilung zur Beweissicherung.

Die Geschäftsleitung kann die privaten E-Mails des Mitarbeiters einsehen, falls dies zwingend notwendig ist, um den Verdacht besser zu begründen oder zu zerstreuen. Dazu braucht das Unternehmen jedoch die vorgängige schriftliche Einwilligung des Arbeitnehmers ins Öffnen der privaten E-Mails. Für die Beweisaufnahme werden die entsprechenden staatlichen Untersuchungsbehörden beigezogen.

4. Sanktionen

Eine weisungswidrige Benutzung der Informatikinstrumente und elektronischen Kommunikationseinrichtungen können arbeitsrechtliche Sanktionen bis hin zur fristlosen Entlassung sowie strafrechtliche Untersuchungen zur Folge haben.

Die Geschäftsleitung kann insbesondere folgende Sanktionen erheben:

- Verwarnung gegen die fehlbaren Personen
- Schadenersatzforderungen
- Einreichung einer Strafanzeige
- (fristlose) Kündigung oder Freistellung

Die fristlose Kündigung kann ausgesprochen werden, wenn dem Arbeitgeber nach Treu und Glauben die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden kann. Das ist z.B. bei schwerwiegenden Fällen, wie bei wiederholtem Missbrauch trotz Verwarnung oder bei verhärtetem Verdacht auf Begehen einer Straftat der Fall.

5. Verpflichtung/Unterschrift

Der Mitarbeiter bestätigt per Unterschrift den Erhalt dieser Weisung, anerkennt die darin enthaltenen Bestimmungen und verpflichtet sich zu deren Einhaltung. Der Mitarbeiter akzeptiert er ausdrücklich, dass alle (auch privaten) E-Mails archiviert werden.

[Ort], Datum

Name, Vorname (Blockschrift)

Unterschrift

1.2.3 Bedrohungen durch technische Mängel

Die durch den technischen Zustand von Hard- und Software entstehenden Risiken lassen sich in mehrere Kategorien einteilen. Bei der Hardware hängt es oft vom Alter der Systeme und den regelmässigen Wartungsintervallen ab, ob Probleme entstehen können oder nicht. Schlechter in den Griff zu bekommen sind Bedrohungen, auf die das Unternehmen bzw. die Behörde gar keinen Einfluss hat:

- Die eingesetzte Software enthält Programmierfehler in Form von Sicherheitslücken, über die ein gezielter Angriff möglich ist. Die dazugehörigen Angriffsprogramme werden auch als «Exploit» bezeichnet.
- Von aussen kommt Software in das eigene Netzwerk, die den Angriff enthält. Viren, Würmer und Trojanische Pferde gehören zu dieser Kategorie, die oft vereinfachend als «Malware» bezeichnet wird.

Eine Sicherheitslücke wird im täglichen Gebrauch oft auch als «Vulnerability» bezeichnet.

1.2.3.1 Sicherheitslücken und Exploits

Die vielen bisher bekannt gewordenen Angriffe unter Ausnutzung von Sicherheitslücken können wie folgt eingeteilt werden: