Leitfaden

IT-Sicherheitsmanagement in kleinen und mittleren Unternehmen

Grundvoraussetzungen, organisatorische und rechtliche Anforderungen

www.ecc-handel.de
www.ec-net.de

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Netzwerk Elektronischer
Geschäftsverkehr

Herausgeber
E-Commerce-Center Handel, Köln

Text und Redaktion
Sven Fehrmann & Andreas Gabriel
Universität Würzburg

Grafische Konzeption und Gestaltung
Sonja Rodenkirchen & Christian Bähr
E-Commerce-Center Handel, Köln

Bildquelle
www.fotolia.de

Stand
Januar 2011

Inhaltsverzeichnis

IT-Sicherheitsmanagement in kleinen und mittleren Unternehmen

1 Einleitung

Im beginnenden 21. Jahrhundert sind nahezu alle kleinen und mittleren Unternehmen auf die Nutzung von PC-Systemen angewiesen, um ihre Wettbewerbsfähigkeit langfristig zu sichern. Das Anbieten von Waren und Dienstleistungen oder die Vorstellung der eigenen Firma im Internet sind selbstverständlich geworden. Ein Großteil der Kommunikation mit Kunden und anderen Unternehmen findet inzwischen über E-Mail statt. Auch das digitale Anlegen, die Speicherung und Pflege von Kundendaten gehören zum alltäglichen Geschäftsleben. Insgesamt steigen daher die Anforderungen an das IT-Fachwissen der Mitarbeiter.[1]

In den meisten Fällen sind in kleinen und mittleren Unternehmen jedoch keine Mitarbeiter mit fachspezifischen IT-Kenntnissen oder gar IT-Fachleute angestellt. Das birgt die Gefahr, dass bei der alltäglichen Nutzung der IT-Systeme manche Sicherheitsgefahren nicht oder nur unzureichend erkannt werden.

Dieser Leitfaden gibt Auskunft über Grundanforderungen an die Basissicherheit in Unternehmen und welche organisatorischen sowie rechtlichen Anforderungen Unternehmen bewältigen müssen.

Die unternehmensspezifische Ausgestaltung der firmeneigenen Informationssicherheit ist von zahlreichen individuellen Gegebenheiten des Unternehmens abhängig und kann an dieser Stelle nicht pauschal beantwortet werden. In Abhängigkeit von der Branche, Größe und Ausrichtung Ihres Unternehmens müssen ggf. weiterführende Schutzmaßnahmen etabliert werden. Die Aspekte der Basissicherheit müssen in jedem Fall Berücksichtigung finden, um ein Mindestmaß an Sicherheit zu gewährleisten.

2 Basissicherheit

Entscheidender Faktor, um im unternehmerischen Alltag bestehen zu können, ist das Auseinandersetzen mit der IT. Zwar erleichtert der IT-Einsatz viele Arbeitsschritte und ist wichtig, um wettbewerbsfähig zu bleiben, jedoch darf die Verwendung nicht allzu sorglos erfolgen. Sie müssen sicherstellen, dass Sie Ihre Daten regelmäßig sichern, dass Sie sich um Virenschutzsoftware kümmern, Updatesregelmäßig einspielen und Ihr Netzwerk ausreichend absichern. Auf was Sie dabei im Einzelnen achten müssen, wird in den nächsten Kapiteln erläutert.

2.1 Datensicherung

Durch technisches Versagen, versehentliches Löschen oder Manipulation können gespeicherte Daten unbrauchbar werden bzw. verloren gehen. Um einem solchen Verlust vorzubeugen und den IT-Betrieb wieder kurzfristig aufnehmen zu können, muss der Datenbestand gesichert werden.

Jedes Unternehmen muss für die Sicherung seiner Daten ein Konzept entwerfen. Der erste Schritt ist der schriftliche Entwurf eines Datensicherungskonzepts. Die Dokumentation ist wichtig, um sich darüber klar zu werden, welche Daten regelmäßig gesichert werden müssen. Daten sind z. B.

- **Anwendungsdaten**
  Zu den Anwendungsdaten gehören alle Daten, die Sie bspw. in Word, Excel und PowerPoint oder anderen Programmen nutzen (Bsp.: Geschäftskontakte.xls).
- **Systemdaten**
  Hierbei handelt es sich um Daten, die Informationen über das System, wie bspw. diverse PC-Einstellungen enthalten. Diese Daten zu sichern, ist teilweise sehr aufwändig, lassen Sie sich hier von einer IT-versierten Fachperson unterstützen.
- **Software**
  Unter Software versteht man – vereinfacht gesagt – alle ausführbaren Programme auf Ihrem Computer und/oder den Servern, wie z. B. Acrobat Reader, Microsoft Word, Open-Office usw.

Der Speicherort der Daten ist wichtig. Befinden sich die Daten nur auf lokalen Rechnern (d. h. auf den PCs der Nutzer), müssen die Daten auf jeden Fall an einem anderen Ort gesichert werden. Falls Ihr Unternehmen einen Server betreibt, muss im Vorfeld geklärt werden, welche Daten auf dem Server und/oder auf den lokalen Rechnern gespeichert und inwieweit diese automatisch gesichert werden.

Nun muss sich das Unternehmen darüber klar werden, ob täglich der gesamte Datenbestand gesichert werden soll oder nur einen Teil davon. Falls die Entscheidung aus Zeit- und Speicherplatzgründen gegen eine Vollsicherung ausfällt, muss festgelegt und bestenfalls schriftlich dokumentiert werden, welcher Teil der Daten zu welchem Zeitpunkt gesichert werden soll. Dabei müssen bei den Überlegungen folgende Kriterien zum Tragen kommen:

- Wichtigkeit der Daten
- Änderungshäufigkeit der Daten

Dateien, die sehr wichtig sind und sich häufig ändern, sollten in jeden Sicherungslauf einbezogen werden. Wurden die relevanten Daten zur Sicherung identifiziert, müssen diese nun auf ein Speichermedium kopiert werden. Dabei muss unbedingt beachtet werden, dass nicht die letzte funktionierende Sicherung überschrieben wird, da bei Misslingen der Sicherung auch die letzte Sicherung zerstört werden würde. Verfolgen Sie bei der Sicherung Ihrer Daten das Prinzip:

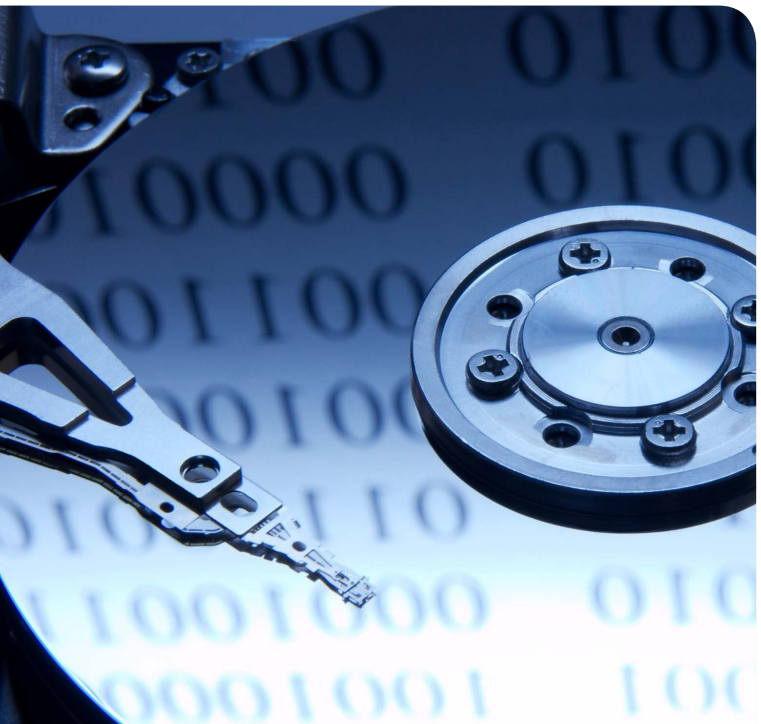
- Mindestens jede Woche alle wichtigen Daten sichern,
- Mindestens jeden Monat eine Vollsicherung durchführen, die frühestens nach einem Jahr überschrieben wird.

Bei der Wahl des Speichermediums sollten Sie auf dessen Haltbarkeit sowie Funktionsumfang achten. DVDs eignen sich bspw. zur langfristigen Sicherung (Haltbarkeit bis zu 100 Jahre), Festplatten für eine Aufbewahrungsdauer von höchstens fünf Jahren (Haltbarkeit bis zu 10 Jahre).[2]

Enthält die Sicherung sensible Daten, die vor dem Zugriff unberechtigter Personen geschützt werden müssen, so ist eine Verschlüsselung der Daten sinnvoll (siehe 3.4 Datenträgerverschlüsslung).

Werden die Daten der Clients auf dem Server automatisch gesichert, so achten Sie darauf, dass dies im Idealfall in Echtzeit oder täglich nach Arbeitsende stattfindet und nach dem Prinzip einer redundanten Auslegung der Sicherung auf den Servern nach bspw. RAID erfolgt. Ein RAID-System ist vereinfacht gesagt die Speicherung der Daten auf unterschiedlichen Festplatten, so dass bei Ausfall einer der Festplatten trotzdem der gesamte gesicherte Datenbestand wiederhergestellt werden kann. Die am Sicherungsverbund beteiligten Festplatten sollten sich immer an unterschiedlichen Standorten befinden, um bspw. im Falle eines Brandes nicht den kompletten Datenbestand zu verlieren.[3]

Nach der Datensicherung ist es wichtig, dass Sie Ihre Sicherung überprüfen. Das bedeutet, dass Sie die Sicherung auf Vollständigkeit überprüfen. Der Prozess der Sicherung sollte dokumentiert werden, falls andere Personen die Sicherung erstellen oder alte Sicherungen nutzen wollen. Um einen einheitlichen, qualitativen hochwertigen Prozess zu gewährleisten, muss der Ablauf des Datensicherungsprozesses dokumentiert und allen Mitarbeiter mitgeteilt werden. Es ist ein dezidierter Arbeitsplan zu erstellen, welcher Mitarbeiter für die Durchführung bzw. Überwachung der Speichermedien verantwortlich ist, um im Schadensfall prüfen zu können, wer der verantwortliche Ansprechpartner ist.[4]



Checkliste | Datensicherung

- Einen verantwortlichen Mitarbeiter für die Durchführung der Sicherung bestimmen.
- Eine Vertreterregelung etablieren, um sicher zu stellen, dass dieser Prozess unterbrechungsfrei durchgeführt wird.
- Eine Liste der wichtigsten Daten erstellen sowie deren Speicherort ermitteln.
- Die Liste in regelmäßigen Abständen auf Aktualität überprüfen.
- Die wichtigsten Daten regelmäßig sichern.
- Die geheimen und/oder sensiblen Daten unbedingt verschlüsseln.
- Die Datensicherungen regelmäßig auf Funktion und Rückspielbarkeit überprüfen.
- Das Rückspielen stichprobenartig testen.
- Den Prozess der Datensicherung dokumentieren.
- Beim Arbeiten mit mobilen Datenträgern (Laptops) eine Regelung treffen, wie diese Daten gesichert werden.
- Eine sichere Aufbewahrung der Speichermedien gewährleisten (insbesondere als Schutz vor Diebstahl, unberechtigtem Zugriff und Schäden durch Feuer und Wasser).
- Im Störfall eine automatisierte Warnmeldung an den verantwortlichen Mitarbeiter versenden.

2.2 Virenschutz

Ein weiterer grundlegender Aspekt einer umfassenden Basissicherheit ist der Virenschutz. Dazu ist die Anschaffung, Installation und der Betrieb eines Virenschutzprogrammes auf ausnahmslos jeder IT-Komponente zwingend notwendig. Des Weiteren müssen Mitarbeiter über das Thema „Virenschutz“ aufgeklärt werden.

Um ein Unternehmen ausreichend vor einem Virenbefall zu schützen, müssen alle Systeme entsprechend geschützt werden. Dazu gehört die Installation von Virenschutzprogrammen auf allen lokalen Rechnern und – soweit vorhanden – auf allen Servern. Bei der Auswahl einer geeigneten Virenschutzsoftware ist die folgende Checkliste zu beachten.

Checkliste | Auswahl eines Virenschutzprogrammes

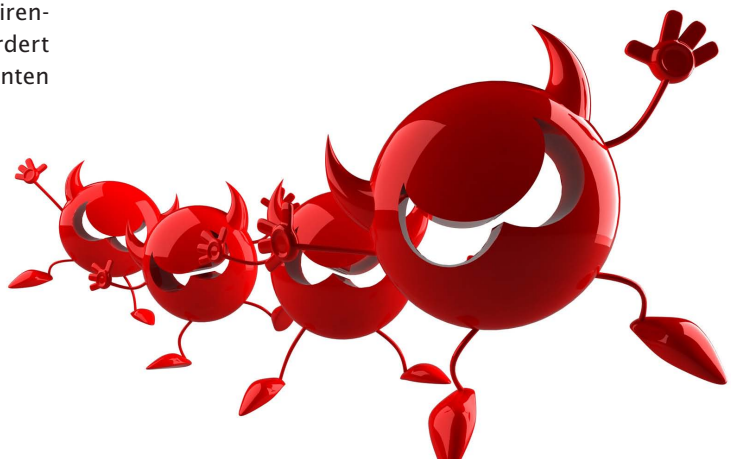
- Die Software sollte sich täglich mindestens einmal automatisch aktualisieren. Falls Sie sich über einer längeren Zeitraum nicht von selbst aktualisieren kann (weil bspw. keine Verbindung zum Internet hergestellt wird), muss das Antivirenprogramm eine Warnung ausgeben.
- Die Software muss für die Systemlandschaft geeignet sein, d. h. das verwendete System und die Formate müssen auch unterstützt werden (z. B. gibt es unterschiedliche Virenscanner für einen Windows-, Linux- oder Apple Macintosh-Rechner).
- Das Virenschutzprogramm sollte Schadprogramme in aktiven Inhalten erkennen.[5]

Sollten Sie sich bei der Auswahl eines geeigneten Virenprogrammes mit den genannten Aspekten überfordert fühlen, so fragen Sie die oben genannten relevanten Punkte beim Kauf ab.

Als nächstes klären Sie Ihre Mitarbeiter über allgemeine Gefahren auf. Mit ein paar wenigen Grundsätzen können die größten Gefahrenquellen ausgeschaltet werden:

- Niemals unbekannte E-Mail-Anhänge herunterladen oder gar öffnen,
- Keine Daten auf fragwürdigen Internetseiten herunterladen,
- Datenträger (wie USB-Sticks und CDs/DVDs) von externen Personen vor der Verwendung immer erst auf Viren überprüfen, bevor auf die Daten zugegriffen wird,
- Sperren diverser Funktionen, wie aktive Inhalte, Autostart-Funktion bei Einlegen eines Datenträgers, automatisches Herunterladen bei Downloads usw.[6]

Halten Sie sich an die genannten Punkte, so haben Sie die größten Gefahren gebannt. Weitere interessante und verständliche Informationen zum Virenschutz erhalten Sie beim Netzwerk Elektronischer Geschäftsverkehr (NEG, http://ec-net.de) und auf dem Internetportal des Bundesamtes für Sicherheit in der Informationstechnik (http://www.bsi.de).



2.3 Updates

Wie schon im Kapitel Virenschutz erläutert, ist eine regelmäßige Aktualisierung aller Anwendungsprogramme (Einspielen sog. Updates) sehr wichtig, um Sicherheitslücken zu beseitigen. Bei vielen Betriebssystemen von Microsoft und Apple erfolgt das Einspielen der Updates automatisch. Um zu überprüfen, ob auch alle Geräte immer auf dem aktuellen Stand sind, müssen Sie sich erst einen Überblick verschaffen, welche Programme von Ihnen aktuell eingesetzt werden. Dazu gehören das Betriebssystem, der Browser, die Office-Software, das Virenschutzprogramm, alle branchenspezifischen Anwendungsprogramme usw.

Notieren Sie sich, welche Programme sich automatisch aktualisieren und welche Sie selbst aktuell halten müssen. Informieren Sie sich über die Updatemöglichkeit Ihrer Softwareprodukte und achten Sie darauf, ob es noch einen Support (Unterstützung, u. a. auch das Herausbringen von Updates) zu Ihrer Software gibt. Falls der Support für Ihr Softwareprodukt schon ausgelaufen ist (es besteht die Gefahr, dass Sicherheitslücken nicht geschlossen werden), informieren Sie sich über Upgrade-Möglichkeiten (Update der Software auf eine neue Version) oder ein alternatives Produkt.

Achtung:

Das Einspielen der Updates für Ihr Betriebssystem kann unter Umständen zu Störungen bei weiteren Anwendungsprogrammen führen. Um zu vermeiden, dass branchenspezifische Programme nach der Durchführung des Updates nicht mehr oder nur eingeschränkt zur Verfügung stehen, sollten Sie

- entweder einen Testlauf auf lediglich einem Rechner Ihres Unternehmens durchführen oder
- eine gewisse Zeit warten, bevor Sie das Update durchführen, um dieses Problem zu vermeiden.

Im Endeffekt kommt es hier zu einer Abwägung zwischen einer tagesaktuellen Sicherheit durch das sofortige Einspielen der neuen Programmbausteine oder aber dem Inkaufnehmen einer gewissen Verzögerung zu Testzwecken, um auf diesem Weg zu erreichen, dass alle Programme störungsfrei betrieben werden können.

Checkliste | Updates

- ✓ Liste aller genutzten Programme erstellen.
- ✓ Jedes gelistete Programm auf die Möglichkeit von Updates prüfen (z. B. das Programm starten und dort in der Hilfefunktion das Suchwort „Update“ eingeben).
- ✓ Liste der genutzten Programme neu strukturieren:
  - Updates verfügbar:
    - Automatisches Update des Programms ist eingestellt,
    - Automatisches Updaten ist nicht eingestellt, aber möglich,
    - Das Einspielen von Updates ist nur manuell möglich.
  - Keine Updates mehr verfügbar (unabhängig davon, ob die Programme sich automatisch updaten können oder nicht).
- ✓ Regelmäßiges Updaten aller Programme, die nur manuell aktualisierbar sind (spätestens jeden Monat). Hierfür sollten Sie sich entsprechende Termine eintragen, damit diese Maßnahme im Arbeitsalltag nicht in Vergessenheit gerät.
- ✓ Regelmäßige Überprüfung aller Programme auf Aktualität, die sich automatisch updaten (mindestens einmal im Quartal).
- ✓ Upgrade auf neuere Versionen oder Ersatzbeschaffung für alle Programme, für die es keine Updates und/oder Support mehr gibt.[6]

2.4 Netzwerk

Unabhängig davon, ob es in Ihrem Unternehmen ein Firmennetzwerk gibt oder nur einzelne Clients an das Internet angebunden werden, benötigen Sie eine Firewall. Diese dient dazu, den Datenverkehr zu überwachen und nicht erlaubte Zugriffe zu unterbinden. Der Betrieb einer Firewall ist wichtig, um im Falle einzelner – an das Internet angebundener – Clients vor unberechtigten Zugriffen zu schützen. Es existieren Hard- und Software-Firewalls am Markt, hier reicht in der Regel eine Softwarelösung aus.[7]

Falls ein Firmennetzwerk existiert, sollte – neben einer Softwarefirewall auf jedem Rechner – zusätzlich eine Netzwerk- bzw. Hardwarefirewall betrieben werden. Eine Netzwerk- bzw. Hardwarefirewall ist ein Schutzsystem, das auf einem zusätzlichen Gerät betrieben wird. Die meisten Switch- und Router-Hersteller (Switch und Router sind Netzwerkkomponenten, mit denen der Datenaustausch zwischen den Rechnern eines Netzwerks und dem Internet ermöglicht wird) bieten solche Geräte in Kombination mit einer Firewall an.[8] Lassen Sie sich im Falle einer Anschaffung von einem Fachmann beraten.

Betreiben Sie ein WLAN-Funknetz in Ihrem Unternehmen, so müssen Sie auch dieses absichern. Die Über-tragung muss unbedingt verschlüsselt werden. Achten Sie bei der Einstellung Ihrer Geräte (in der Regel Router) auf die Aktivierung der WPA2-Verschlüsselung. Steht Ihnen diese Verschlüsselungsart nicht zur Verfügung, dann kann in der Regel die WPA oder WEP-Verschlüsselung aktiviert werden. Beherrscht Ihr Gerät nur WEP-Verschlüsselung, so sollte mittelfristig ein Gerät angeschafft werden, dass die WPA2-Verschlüsselung beherrscht, da WEP aus heutiger Sicht nicht mehr ausreichende Sicherheit bietet. Alle Geräte, die Sie über WLAN einbinden, müssen eine eigene Firewall-Software besitzen.[9]

Der Betrieb des WLANs sollte sich ausschließlich auf die Firmenzeiten beschränken, um sich vor Missbrauch durch Dritte zu schützen.[10]

3 Organisatorische Anforderungen

Im unternehmerischen Alltag gibt es zahlreiche organisatorische Herausforderungen. Aus Sicht der IT-Sicherheit sind das insbesondere der richtige Umgang mit Mitarbeitern sowie deren Unterweisung in Ihren Arbeitsplatz und in die Anforderungen im Unternehmen. Weitere Aspekte in diesem Umfeld sind die Etablierung einer rechtssicheren und bindenden Sicherheitsrichtlinie und den dazugehörigen Sicherheitskonzepten, der Entwurf eines Berechtigungskonzept, die Pflicht zur Datenverschlüsselung und die Analyse potenzieller Risiken im Unternehmen.

3.1 Mitarbeiterunterweisung

Entscheidender Faktor für den sicheren Betrieb von Rechnern, Servern und der Telekommunikationsinfrastruktur ist die regelmäßige Unterweisung der Mitarbeiter in die IT sowie die Hinführung zum Thema „Sicherheit".

Die Unterweisung der Mitarbeiter ist wichtig, um ihnen einen Einblick in die Prozesse und Abläufe und die damit verbundenen Bedrohungen zu geben. Bei der Einweisung eines neuen Mitarbeiters in eine Maschine (wie z. B. einer Drehbank) ist das selbstverständlich. Genauso selbstverständlich sollte auch eine Unterweisung in den Umgang mit der IT des Unternehmens sein. Werden dort elementare Fehler begangen, kann dies den kompletten Geschäftsbetrieb unterbrechen. Daher im Folgenden einige Grundsätze bei der Unterweisung der Mitarbeiter:

- Unterrichten Sie die Mitarbeiter über ihre IT-Nutzungsrechte und –pflichten,
- Zeigen Sie neuen Mitarbeitern, wo sich die jeweils relevanten Programme auf dem Rechner befinden und erläutern Sie die maßgeblichen Funktionen,
- Unterrichten Sie über zentrale Vorgaben, wie z. B. Speicherung von Daten, Benennung von Dateien oder Klassifikation von Informationen (welche Inhalte dürfen nach außen weitergegeben werden und welche nicht).

Viele Weiterbildungs- und Schulungsangebote werden nur wahrgenommen, wenn diese verpflichtend sind. Daher empfiehlt es sich, die Mitarbeiter zur Schulung in einem Mindestportfolio an Themengebieten zu verpflichten. Dazu gehört natürlich auch eine Schulung zum Thema „IT-Sicherheit". Sind Sie selbst nicht im Stande, Schulungen zum Thema „IT-Sicherheit" anzubieten, dann besuchen Sie entweder Schulungen von Fremdanbietern (HWK, IHK usw.) oder nehmen Sie externe Trainer in Anspruch, die für Ihr Unternehmen maßgeschneiderte Lösungen anbieten. Der Inhalt einer Schulung zur IT-Sicherheit sollte alle genannten Aspekte dieses Ratgebers enthalten und die IT-Landschaft Ihres Unternehmens abdecken. Als Erfahrungswert hat sich herausgebildet, dass bei der Fortbildung von Einzelpersonen eines Unternehmens Schulungen von Kammern oder vergleichbaren Anbietern sinnvoll sind, bei Gruppen ab ca. fünf Personen (aus einem Unternehmen) sich eine maßgeschneiderte Schulung empfiehlt. Das liegt zum einem an dem angepassten Schwierigkeitsgrad an die Personengruppe sowie dem Behandeln der für das Unternehmen bzw. Branche relevanten Themengebiete.[11]

Checkliste | Mitarbeiterunterweisung

- ✓ Neue Mitarbeiter am ersten Tag begleiten und unterstützen.
- ✓ Alle Mitarbeiter über Spezifika bei der Nutzung der IT aufklären.
- ✓ Schulungen für alle Mitarbeiter regelmäßig und verpflichtend anbieten.
- ✓ Nach kurzer Zeit sollte eine Auffrischung der Schulung erfolgen.
- ✓ Durch das Aufzeigen von potenziellen Schadensszenarien wird den neuen Mitarbeitern ein grundsätzliches Verständnis dafür vermittelt, warum die vorgestellten Vorgaben existieren.

3.2 Sicherheitsrichtlinie und -konzept

Das vorangegangene Kapitel macht klar, dass Mitarbeiter eindeutige, schriftlich fixierte Regeln benötigen. In diesem Zusammenhang ist die Erstellung einer Sicherheitsrichtlinie sowie eines Konzepts notwendig. Eine Sicherheitsrichtlinie ist für ein Unternehmen wichtig, da dort folgende Punkte geregelt werden:

- Benennung der Sicherheitsziele und Beschreibung der Sicherheitsstrategie,
- Sanktionierung von Verstößen gegen die Richtlinie,
- Regelmäßige Überprüfung von Sicherheitsmaßnahmen,
- Verpflichtende Schulungs- und Weiterbildungsmaßnahmen,
- Benennung des Verantwortlichen für die IT-Sicherheit und dessen genaue Funktion.

Wichtig ist zudem, dass die Sicherheitsrichtlinie durch den Geschäftsführer bzw. die Geschäftsleitung unterstützt wird, von diesen Personen offiziell verabschiedet wurde und dadurch nachweislich eine hohe Bedeutung für das Unternehmen hat.

Die Sicherheitsrichtlinie beinhaltet mehrheitlich Sachverhalte, die sich mittelfristig nicht ändern. Neben der Richtlinie muss noch ein Sicherheitskonzept entworfen werden, in dem für die IT relevante Themen behandelt werden, die sich kurzfristig ändern können. Dazu gehören Hinweise beim Umgang mit der IT (Bsp.: Nur Outdoor-Handys in den Maschinenhallen benutzen) sowie allgemeine Handlungsanweisungen (Bsp.: Der Schrank mit den Datensicherungen muss immer verschlossen sein). Weitere Punkte, die in einem Sicherheitskonzept festgehalten wird, sind:

- Fixierung eindeutiger Regeln für den Umgang mit der betriebseigenen Hardware (PC und Telefon),
- Passwortwahl und -umgang,
- Datensicherungskonzept,
- Virenschutzkonzept.

Zentraler Punkt ist, dass die Inhalte der Richtlinie und des Sicherheitskonzepts den Mitarbeitern bekannt sind, alle Beteiligten den Inhalt verstehen und die Einhaltung der Vorgaben schriftlich bestätigen. Daher sind regelmäßige Informationsveranstaltungen Pflicht, um neue Mitarbeiter einzuweisen und den bestehenden Mitarbeitern Veränderungen und Neuerungen mitzuteilen. Darüber hinaus müssen die Verantwortlichen in regelmäßigen Abständen prüfen, ob die Regelungen auch befolgt werden. Denn nur dann kommen die Mitglieder der Geschäftsleitung ihrem Kontrollanspruch nach.[12]

3.3 Benutzerkonzept

In einem Benutzerkonzept wird der Zugang zu einzelnen Informationen des Unternehmens geregelt. Im schlimmsten Fall hat jeder Benutzer des Firmennetzwerkes uneingeschränkten Zugriff auf interne Informationen. Im Idealfall sind die Zugriffsrechte innerhalb des Unternehmens für jeden Angestellten entsprechend seiner Position und Funktion klar geregelt. Wichtig ist, dass die Verantwortlichen für die Freigabe eindeutig benannt wurden und es ein Freigabeverfahren gibt, das allen Mitarbeitern bekannt ist.[13]

Achtung: Die wichtigsten Punkte beim Aufbau eines Benutzerkonzepts:

- Entwerfen Sie ein Benutzerkonzept, in dem festgelegt wird, welche Daten für alle Mitarbeiter zugänglich sein dürfen/müssen.
- Benennen Sie einen Verantwortlichen für die Zuweisung der Nutzerrechte und teilen Sie die verantwortliche Person allen Mitarbeitern mit.
- Legen Sie einen klaren Ablauf fest, wie die Erteilung/Veränderung und Löschung der Nutzerrechte zu erfolgen hat.

Die eindeutige Definition von Benutzerrechten wird übrigens auch vom Bundesdatenschutzgesetzt (BDSG) gefordert. Daher sollten Sie den Aufbau eines derartigen Konzepts nicht auf die leichte Schulter nehmen.

3.4 Datenträgerverschlüsselung

Mit einer Datenträgerverschlüsselung schützen Sie Ihr Unternehmen davor, dass sich unberechtigte Personen Zugang zu Ihren Informationen/Betriebsgeheimnissen (wie z. B. Konstruktionszeichnungen neuer Produkte) verschaffen. Das typische Beispiel ist ein in der Hektik vergessener Laptop am Flughafen. Sind Ihre Daten auf dem Rechner unverschlüsselt, können die Daten von jeder-mann kopiert und lukrativ an die Konkurrenz verkauft werden. Das beschriebene Szenario wirkt absichtlich sehr angsteinflößend, soll aber den Aufwand einer Datenträgerverschlüsselung im Vergleich zum Verlust von Informationen verdeutlichen.

Ein Datenträger ist jedes Medium, auf dem Daten gespeichert werden. Dazu gehören CDs, DVDs, USB-Sticks, tragbare Festplatten, Laptops usw. Benutzen Sie den Datenträger nur im eigenen Büro, so ist in den meisten Fällen keine Verschlüsslung notwendig. Haben Sie jedoch Daten mit sensiblen Informationen auf Außeneinsätzen, Dienstreisen oder im Urlaub dabei, so sollten Sie die Daten auf jeden Fall verschlüsseln. Auf dem Softwaremarkt gibt es eine große Auswahl an kommerziellen und Open-Source-Verschlüsselungsprogrammen. Bei der Auswahl einer Software müssen Sie darauf achten, dass die Software einfach zu bedienen ist und eine Verschlüsselungsrate von 128 Bit oder mehr hat.[9] Sind Sie sich über den Begriff der Verschlüsslungsrate unsicher, so geben Sie beim Kauf das Kriterium der Anforderung von 128 Bit oder mehr an.

Alternativ zur Verschlüsselung mit einer Software gibt es die Möglichkeit, Daten hardwareseitig zu verschlüsseln. Dazu müssen Sie Verschlüsselungshardware beschaffen, die Ihre Daten in Echtzeit ver- und entschlüsseln. Mit einem zusätzlichen Gerät (oftmals wie ein USB-Stick aussehend), können Sie die Daten wieder entschlüsseln. Lassen Sie sich bei der Anschaffung einer Hardwareverschlüsselung von einem IT-Fachmann beraten.[14]

Bitte achten Sie unbedingt darauf, dass der Prozess der Datenver- und -entschlüsselung den Arbeitsablauf auf keinen Fall beeinträchtigen darf. Die vernünftige Umsetzung einer Verschlüsselungslösung wird vom Anwender – im Idealfall – nicht bemerkt, da lediglich ein zusätzliches Passwort beim Login eingegeben werden muss. Nur wenn dieser Prozess als problemlos eingestuft wird, findet er vollumfassend bei allen Geschäftsprozessen Anwendung.

3.5 Risikoanalyse

Ein Aspekt, der oftmals erst in großen Unternehmen zum Tragen kommt, ist das Risikomanagement. Um IT-Risiken zu identifizieren und anschließend entgegenwirken zu können, müssen diese im Vorfeld analysiert werden. Ein unentdecktes Risiko kann insbesondere in komplexen Geschäftsprozessen oder einem aufwändigen Aufbau der IT sowie aktuellen Angriffsarten, wie z. B. einem neuen Computerschädling, liegen.

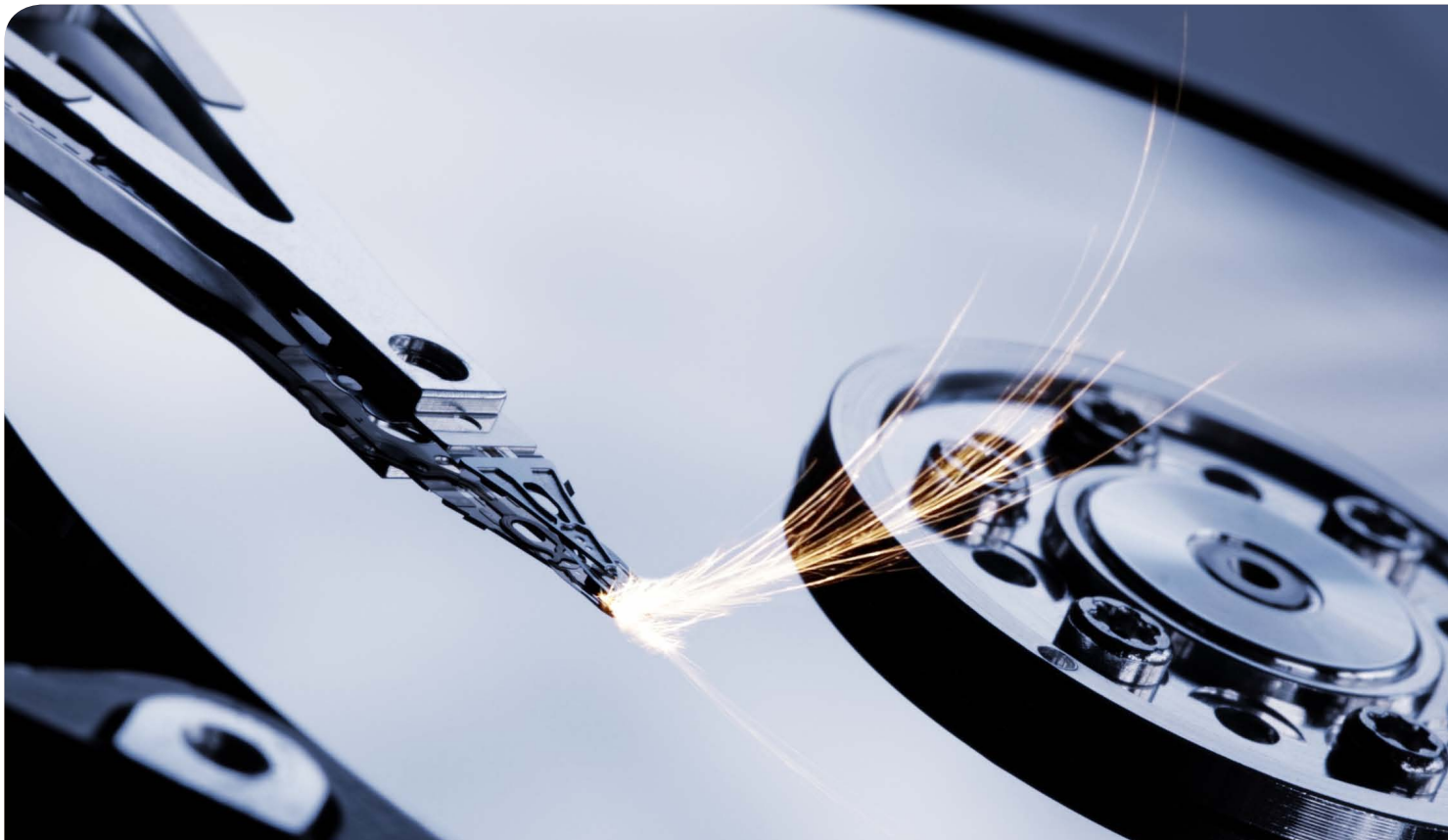
An die Erkennung von Risiken muss man sich systematisch heranarbeiten. Eine Risikoanalyse setzt sich aus den folgenden Teilschritten zusammen:

- Identifikation der möglichen Risiken,
- Bewertung aller identifizierten Risiken hinsichtlich deren Relevanz und Schadenspotential,

Ein Risiko tritt i. d. R. immer dann ein, wenn das Unternehmen mit einer externen oder internen Bedrohung konfrontiert wird. Diese entwickelt sich dann zu einer Gefahr, wenn das Unternehmen durch eine offene Schwachstelle eine entsprechende Angriffsfläche bietet. Nur durch angemessene Schutzmaßnahmen können eigene Schwachstellen geschlossen werden, um zu vermeiden, dass eine Bedrohung Realität wird.

Viele kleinere Risiken sind mit einem Gespür für das eigene Unternehmen bzw. die Abteilung erkennbar und bereits mit einem geringen Mitteleinsatz verringerbar. Andere Risiken sind akzeptabel, falls sie weder eine hohe Eintrittswahrscheinlichkeit noch eine empfindliche Schadenshöhe besitzen.[15]

Mit einer Risikoanalyse sollen gerade die häufig auftretenden und besonders kostspieligen Schadensfälle schon im Vorfeld entdeckt und im Idealfall ausgeschlossen werden. Jedoch besteht gerade bei der Identifikation der möglichen Risiken die Gefahr des Übersehens. Die besten Erfahrungen haben Unternehmen gemacht, die in enger Zusammenarbeit zwischen Mitarbeitern und externen Beratern erfolgreich ihre unternehmensspezifischen Risiken identifiziert haben.



4 Rechtliche Anforderungen

Viele einschlägige Rechtsvorschriften im Bereich der IT-Sicherheit sind nicht in einem einzelnen Gesetz zusammengeführt, sodass ihre Zusammenhänge oftmals unterschätzt werden. Eine Zuwiderhandlung kann nicht nur haftungsbedingt zivilrechtlichen Schadensersatz zur Folge haben, sondern auch eine Ordnungswidrigkeit oder gar Strafe bedeuten. Daher sind die Geschäfts-führer bzw. Vorstände sowie alle Mitarbeiter gut beraten, wenn sie die rechtlichen Anforderungen zur IT-Sicherheit beachten. Klassische Herausforderungen im Rahmen der IT-Sicherheit sind der Datenschutz, unterschiedliche unternehmensspezifische Gesetze und Herausforderungen an die Gestaltung eines Vertrags im Falle des Outsourcings von IT-Dienstleistungen.

4.1 Umsetzung der Vorgaben des Datenschutzes

Beim Umgang mit personenbezogenen Daten (z. B. Geburtsdatum, Familienstand usw.) müssen die gesetzlichen Bestimmungen eingehalten werden. Die Vorschriften zum Datenschutz für Unternehmen sind im BDSG niedergeschrieben. Die Aufgabe des Datenschutzes ist es nach § 1 BDSG, „...den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“. Hinzu kommen bereichsspezifische Regelungen, die Vorrang vor dem BDSG haben, wie z. B. das Sozialgesetzbuch oder die Polizeigesetze. Um den Überblick in Sachen Datenschutz zu behalten, empfiehlt es sich, dass ein eigener Datenschutzbeauftragter im eigenen Unternehmen berufen und entsprechend ausgebildet wird oder die Dienste eines externen Datenschutzbeauftragten in Anspruch genommen werden.

Falls zehn oder mehr Mitarbeiterinnen und Mitarbeiter Zugriff auf personenbezogene Daten Ihrer Angestellten, Kunden oder Lieferanten haben, ist die Bestellung eines Datenschutzbeauftragten gesetzlich vorgeschrieben. Im Sinne des § 3(9) BDSG sind personenbezogene Daten insbesondere Informationen über „rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“. Diesen Informationen müssen die Verantwortlichen ein besonders hohes Augenmerk zukommen lassen, da ein zu sorgloser Umgang mit diesen Daten schnell zu juristischen Folgen führen kann.

Um den Anforderungen an den Datenschutz gerecht zu werden, muss sich im Unternehmen eine fachkundige Person befinden. Das ist auch empfehlenswert, falls der Zugriff auf die personenbezogenen Daten bei weniger als zehn Mitarbeitern liegt und somit ein Datenschutzbeauftragter nicht mehr gesetzlich verpflichtend ist.[16]

Die Ausbildung zum Datenschutzbeauftragten wird von unterschiedlichen Bildungsträgern angeboten, ein selbständiges Einarbeiten in das Thema ist meistens mühsam und weniger erfolgreich. Um sich in dem Themenfeld zügig und erfolgreich weiterbilden zu können, ist fachliches Vorwissen im IT-Bereich nahezu unerlässlich.

Eine zweite Variante ist die Bestellung eines externen Datenschutzbeauftragten. Je nach Unternehmenssituation kann der Aufbau eines eigenen Datenschutzbeauftragten sinnvoll sein oder das Abschließen eines (evtl. kostengünstigeren) Vertrags mit einem externen Dienstleister. Falls Sie sich zu einem externen Datenschutzbeauftragten entschließen, so beachten Sie auch den Punkt 4.3 Outsourcing.[17]

4.2 Gesetze

Jedes Unternehmen tangiert Gesetze und Vorschriften. Da sich manche Gesetze und Vorschriften hin und wiederändern,müssenSiesichübergesetzlicheÄnderungen informieren. Die jeweiligen Kammern (IHK oder HWK) bieten gute Informationen, können aber – allein schon aus Zeitgründen – nicht immer alle für Ihr Unternehmen relevanten Gesetzesänderungen sofort erfassen und kommunizieren. Nehmen Sie hier die Beratung durch einen fachkundigen Rechtsanwalt in Anspruch. Alternativ können Sie auch auf einen Steuerberater zurückgreifen. Wägen Sie jedoch ab, ob dieser für die Beratung in Ihrer Branche das notwendige Wissen über Ihr Unternehmen und die dazugehörige Gesetzeslage mitbringt.

In jedem Fall ist es wichtig, dass Gesetzesänderungen zeitnah und proaktiv an Sie kommuniziert werden. Denn nur so können Sie sicherstellen, dass alle Geschäftsprozesse vollumfänglich gesetzeskonform abgewickelt werden. Um zu gewährleisten, dass ein schneller Informationstransfer erfolgt, ist auch die Vereinbarung eines Honorars in Erwägung zu ziehen.

4.3 Outsourcing (Verträge mit Dienstleistern)

In vielen Unternehmen werden IT-Leistungen ausgelagert und an andere Firmen weitergegeben. Haben Sie bspw. den Internetauftritt oder die Wartung Ihrer IT-Systeme an ein anderes Unternehmen übertragen, so müssen Sie zahl-reiche Aspekte berücksichtigen. Die größten Fehler werden bei der Vertragsgestaltung gemacht. Im schlimmsten Fall werden nur mündliche Vereinbarungen getroffen, im Idealfall erfolgt eine vollumfängliche vertragliche Fixierung. Gerade wenn die Leistungsbeschreibung des Unternehmens und die Leistungserbringung des Anbieters stark auseinandergehen, ist ein ordentlich erstellter, rechtssicherer Vertrag von Vorteil. Um einer – im schlimmsten Fall – gerichtlichen Auseinandersetzung standzuhalten, muss im Vertrag geregelt sein, welche organisatorischen und technischen Maßnahmen in welchen Zeitabständen durch den Partner erfüllt werden müssen. Des Weiteren sollten insbesondere größere Verträge von einem Juristen erstellt bzw. kleinere Verträge vom Juristen zumindest qualitätsgesichert werden.

Die folgenden Punkte sollten Berücksichtigung finden:

- Der Leistungsumfang des Dienstleistungsvertrag sollte detailliert geregelt werden.
- Es ist eindeutig zu fixieren, welche Aufgaben und Pflichten der Dienstleister zu erbringen hat. Hierfür muss ein Timing verankert werden.
- Die Eigentumsverhältnisse sind juristisch einwandfrei zu regeln (z. B. Besitz der Internetadresse bei der Vergabe des Betriebs der eigenen Homepage).
- Wenn zeitkritische Aspekte zu berücksichtigen sind, müssen Themen wie „Verfügbarkeit“ und „Reaktion bei Störfällen“ eindeutig festgeschrieben werden, da ein Ausfall des Dienstleistungsgegenstands (z. B. ein Online-Shop) schnell zu einem erheblichen Verdienstausfall führen kann. In einem solchen Fall müssen Haftungsfragen juristisch geregelt werden.
- Die Abnahme der eigenen Homepage durch einen erfahrenen Anwalt mit dem Schwerpunkt „Online-Recht“ kann vor unangenehmen Abmahnungen o. Ä. schützen und sollte daher in jedem Fall in Erwägung gezogen werden.

5 Schlussbetrachtung

Der Aufbau und die Aufrechterhaltung eines hohen Maßes an IT-Sicherheit stellen KMU vor eine große Herausforderung, bieten jedoch auch zahlreiche Chancen.

Neben dem umfassenden Schutz der IT verbessern viele Sicherheitsmaßnahmen die Abläufe im Geschäftsverkehr. Zum Beispiel gibt eine Sicherheitsrichtlinie Mitarbeitern eine klare Regelung an die Hand, wie sie mit unterschiedlichen Vorkommnissen umzugehen haben. Anstatt der Suche nach den für diesen Bereich Verantwortlichen und der – im schlimmsten Fall – Nennung unterschiedlichster Herangehensweisen, kann in der Sicherheitsrichtlinie der betreffende Punkt nachgeschlagen werden.

In Zukunft wird der Einsatz von IT-Komponenten und Systemen immer stärker zunehmen. Dabei darf die Sicherheit nicht vernachlässigt werden. Je nachdem in welcher Branche Ihr Unternehmen tätig ist, kann IT-Sicherheit in Zukunft eine zentrale Rolle einnehmen. Viele Automobilhersteller fordern schon jetzt von den Zulieferunternehmen eine Zertifizierung nach dem Qualitätsmanagement (ISO 9001). Mit der steigenden Vernetzung von Unternehmen wird in Zukunft neben der ISO 9001 auch immer öfter eine Zertifizierung nach IT-Sicherheitsverfahren der ISO 27001 gefordert werden.

Setzt Ihr Unternehmen die im Ratgeber angesprochenen Themen gut um, so profitieren Sie von verbesserten Abläufen, klaren Regeln für Mitarbeiter sowie der Möglichkeit sich verändernden Anforderungen – wie bspw. die Forderung eines Auftraggebers, zwecks Zusammenarbeit die eigene IT-Sicherheit zertifizieren zu lassen – schneller stellen zu können.

Die in diesem Leitfaden zusammengestellten Informationen und Handlungsempfehlungen sollen für kleine und mittlere Unternehmen eine Hilfestellung zur Verbesserung ihrer IT-Sicherheit darstellen. Die enthaltenen Checklisten unterstützen Sie dabei, herauszufinden, ob Sie die organisatorischen und rechtlichen Anforderungen bereits erfüllen oder ob noch Handlungspotenziale offen sind.

6 Projektpartner

ECC Handel

Das ECC Handel wurde 1999 als Forschungs- und Beratungsinitiative unter der Leitung des Instituts für Handelsforschung an der Universität zu Köln ins Leben gerufen. Das Ziel ist es, insbesondere kleine und mittlere Handelsunternehmen zum Thema E-Commerce zu informieren. Zahlreiche Aspekte des E-Commerce im Handel hat das ECC Handel in eigenen Studien untersucht. Es wird vom BMWi gefördert und ist in das NEG als Branchenkompetenzzentrum mit Themenfokus Handel eingebunden.

ECC
E-Commerce-Center Handel

Kontakt

ECC Handel am Institut für Handelsforschung
Dürener Str. 401 b
50858 Köln

Tel.: +49 221 943607-70

E-Mail: info@ecc-handel.de
Internet: www.ecc-handel.de

Universität Würzburg

Der Lehrstuhl für Betriebswirtschaftslehre und Wirtschaftsinformatik wurde im Jahr 1985 an der wirtschaftswissenschaftlichen Fakultät der Universität Würzburg neu eingerichtet. Das Ziel war von vornherein, mit nur einem derart ausgerichteten Lehrstuhl das gesamte Spektrum der Wirtschaftsinformatik in der Lehre anzubieten, damit die Studierenden der Betriebs- und Volkswirtschaftslehre eine attraktive und praxisbezogene Wahl- bzw. Kombinationsmöglichkeit für ihren Studienaufbau erhalten. In der Forschung werden die wesentlichen Entwicklungen verfolgt und, wo möglich, durch eigene Beiträge ergänzt. Der Lehrstuhl unterstützt zahlreiche Unternehmen und staatliche Institutionen bei der Umsetzung unterschiedlicher Projekte aus verschiedenen Themengebieten, wie bspw. der Implementierung betriebswirtschaftlicher Standardanwendungssoftware, dem Entwurf von eGovernment Lösungen, der Beratung im Bereich der IT-Sicherheit und vielem mehr.

Lehrstuhl Prof. Thome

Kontakt

Universität Würzburg
Lehrstuhl für Betriebswirtschaftslehre
und Wirtschaftsinformatik
Neubaustraße 66
97070 Würzburg

Tel.: +49 931 35012-53

E-Mail: sfehrmann@wiinf.uni-wuerzburg.de
agabriel@wiinf.uni-wuerzburg.de
Internet: www.wiinf.uni-wuerzburg.de

IT-Akademie Mainz

Die IT-Akademie Mainz ist eine Projekt- und Bildungseinrichtung, die auf eine langjährige Erfahrung sowohl im Bereich von eBusiness Projekten als auch in der IT-Qualifizierung zurückschauen kann. Ziel der Akademie ist es, durch Projekt- und Bildungsarbeiten eine marktgerechte Verbesserung der Qualifikation von IT-Fachkräften zu erreichen. Die IT-Akademie Mainz sieht sich als Dienstleister und steht im kontinuierlichen Austausch mit Unternehmen, Unternehmerverbänden, Kammern (z. B. IHK, HWK), Arbeitsverwaltungen, Fachverbänden und anderen kompetenten Institutionen. Außerdem ist sie Mitglied der Mittelstandsoffensive coNNect des rheinland-pfälzischen Wirtschaftsministeriums und berät als aktiver Partner im landesweiten Netzwerk mittelständische Unternehmen zu den Themen IT-Qualifikation und eBusiness.

Kontakt

IT-Akademie Mainz GmbH
Wilhelm-Theodor-Römheld-Str. 34
55130 Mainz

Tel.: +49 6131 972363-2

E-Mail: office@ita-mainz.de
Internet: www.ita-mainz.de

Kompetenzzentrum Elektronischer Geschäftsverkehr Rheinland-Pfalz KLICK

Das Kompetenzzentrum Elektronischer Geschäftsverkehr Rheinland-Pfalz KLICK ist eines von bundesweit 28 regionalen Kompetenzzentren, die auf Initiative des Bundesministeriums für Wirtschaft und Technologie (BMWi) im Mai 1998 ins Leben gerufen wurden. Die Geschäftsstelle Pfalz wird getragen von der IHK Zetis GmbH - dem Zentrum für Technologie- und Innovationsberatung Südwest. Zetis ist die Projekt-Tochtergesellschaft der IHK Pfalz mit Geschäftsstellen in Ludwigshafen und Kaiserslautern. In eng vernetzten Strukturen agierend, ist die IHK Zetis GmbH der zentrale Ansprechpartner für kleine und mittelständische Unternehmen und Existenzgründer zu allen Fragen rund um IT / Internet und Innovation. Das Themenspektrum reicht im Event -und Beratungsbereich von der Innovations- und Patentförderung über E-Business-Lösungen bis hin zu Kooperations- sowie Personal- und Bildungsfragen. Die IHK Zetis GmbH ist im Projekt "coNNect - Mittelstand vernetzen" IT-Beratungspartner der Landesregierung und für die Bundesregierung Kompetenzzentrum für den elektronischen Geschäftsverkehr sowie SIGNO-Innovationspartner für Rheinland-Pfalz.

klick
Kompetenzzentrum elektronischer Geschäftsverkehr Rheinland-Pfalz

Kontakt

Klick RLP - Geschäftsstelle Pfalz
c/o IHK Zetis GmbH
Dipl.-Ing. Bernd Heß
Europaallee 10
67657 Kaiserslautern

Tel.: +49 631 303-1230
Fax: +49 631 303-1249

E-Mail: hess@zetis.de
Internet: www.klick-rlp.de und www.zetis.de

Netzwerk Elektronischer Geschäftsverkehr (NEG)

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in derzeit 28 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert.

Auf dem zentralen Auftritt des Netzwerks im Internet www.ec-net.de finden Sie weitere Informationen des Netzwerks sowie Studien, Leitfäden und andere Publikationen zum kostenlosen Download. Die Arbeit des Netzwerks Elektronischer Geschäftsverkehr wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Netzwerk Elektronischer Geschäftsverkehr

Kontakt

Bundesministerium für Wirtschaft und Technologie
Referat Öffentlichkeitsarbeit
Scharnhorststraße 34-37
10115 Berlin

E-Mail: info@bmwi.de
Internet: ec-net.de

Sichere E-Geschäftsprozesse in KMU und Handwerk

Das Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert.

Weitere Details finden sich auf www.ec-net.de/sicherheit.

Kontakt

SAGeG - Kompetenzzentrum Elektronischer Geschäftsverkehr
c/o Industrie- und Handelskammer Chemnitz
Dagmar Lange
Strasse der Nationen 25
09111 Chemnitz

Telefon: +49 371 6900 1211
Fax: +49 371 6900 191211

E-Mail: langed@chemnitz.ihk.de
Internet: www.sageg.de

7 Quellen

[1] Netzwerk elektronischer Geschäftsverkehr: Elektronischer Geschäftsverkehr in Mittelstand und Handwerk 2010 – Zusammenfassung der Studie. Unter: http://www.ec-net.de/EC-Net/Redaktion/Pdf/neg-umfrage-2010-zusammenfassung,property=pdf,bereich=ec_net,sprache=de,rwb=true.pdf

[2] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Speichermedien – Diese Speichermedien gibt es. Unter: https://www.bsi.bund.de/BSIFB/DE/ITSicherheit/Datensicherung/Speichermedien/speichermedien_node.html

[3] ZDNet.de (Hrsg.): RAID-Level im Überblick. Unter: http://www.zdnet.de/zentrale_speicherung_und_rechenleistung_storage_server_in_unternehmen_raid_level_im_ueberblick_story-20000003-39119381-1.htm

[4] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge - 11. Ergänzungslieferung. Unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge_2009_EL11_de.pdf?__blob=publicationFile, S. 71f., S. 3.821-3.845

[5] Hansen, H.; Neumann, G. (2001): Wirtschaftsinformatik I, S. 242-245

[6] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge - 11.Ergänzungslieferung. Unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge_2009_EL11_de.pdf?__blob=publicationFile , S. 86, S. 1.096-1.100

[7] Internationale Organisation für Normung (Hrsg.): ISO 27001 – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen. ISO/IEC 27001:2005

[8] Netzwerk elektronischer Geschäftsverkehr. Unter: http://www.ec-net.de/EC-Net/Navigation/Themen/netz-informationssicherheit,did=261330.html

[9] Ertel, W. (2001): Angewandte Kryptographie, S. 24f.

[10] Eckert, C. (2004): IT-Sicherheit: Konzepte – Verfahren – Protokolle, S. 43-67

[11] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge - 11. Ergänzungslieferung. Unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge_2009_EL11_de.pdf?__blob=publicationFile , S. 65-67, S. 2.264-2.270

[12] Datenschutz-Praxis. Unter: http://www.datenschutz-praxis.de/fachwissen/fachartikel/so-sollte-eine-sicherheitsrichtlinie-aussehen/

[13] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge - 11. Ergänzungslieferung. Unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/it-grundschutz-kataloge_2009_EL11_de.pdf?__blob=publicationFile , S. 1.896

[14] Pohlmann, R. (2003): Firewall-Systeme, S. 185-211

[15] Cottin, C.; Döhler, S. (2009): Risikoanalyse – Modellierung, Beurteilung und Management von Risiken mit Praxisbeispielen, S. 13-24

[16] Bundesministerium der Justiz (letzte Änderung 2009): Bundesdatenschutzgesetz, diverse Paragraphen

[17] Witt, C. (2010): Datenschutz kompakt und verständlich – Eine praxisorientierte Einführung, S. 2-9

8 Weiterführende Literatur

IT-Grundschutzkataloge

herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (2009)

Der IT-Sicherheitsleitfaden: Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen (Key-Competence)

von Norbert Pohlmann, Hartmut Blumberg, mitp Verlag (2006)

Das IT-Gesetz: Compliance in der IT-Sicherheit: Leitfaden für ein Regelwerk zur IT-Sicherheit im Unternehmen

von Ralf-T. Grünendahl, Andreas F. Steinbacher und Peter H. L. Will, Vieweg+Teubner Verlag (2009)

Praxisbuch IT-Dokumentation: Betriebshandbuch, Projektdokumentation und Notfallhandbuch im Griff.

von Georg Reiss und Manuela Reiss, Addison-Wesley Verlag (2010)

Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung und Online-Service

von Bernhard Carsten Witt, Vieweg+Teubner Verlag (2010)

Wie sichere ich meine Daten – 10 Tipps zur Datensicherung

herausgegeben vom Netzwerk Elektronischer Geschäftsverkehr. Unter: http://www2.ec-kom.de/ec-net/20100804_Flyer_10_Praxistipps_Sicherheit.pdf

Sicherheitstipp: "Basisschutz für Ihren PC"

herausgegeben vom Netzwerk Elektronischer Geschäftsverkehr. Unter: http://www2.ec-kom.de/ec-net/20100728_IT-Sicherheitstipp-Basisschutz.pdf

Sicherheitstipp: "Sicheres Speichern und Löschen Ihrer Daten"

herausgegeben vom Netzwerk Elektronischer Geschäftsverkehr. Unter: http://www2.ec-kom.de/ec-net/20100728_Sicheres_Speichern_und_Loeschen_IT-Sicherheitstipp.pdf

Sicherheitstipp: „Wie schütze ich mein WLAN vor Dritten?“

herausgegeben vom Netzwerk Elektronischer Geschäftsverkehr. Unter: http://www2.ec-kom.de/ec-net/20100728_WLAN-Sicherheit.pdf

Sicherheitstipp: „Sicherheitstipps für Ihr Notebook“

Unter: http://www.internet-sicherheit.de/fileadmin/docs/publikationen/spooren/Sicherheitstipps-Notebook.pdf

- Regionales Kompetenzzentrum
- Branchen-Kompetenzzentrum
- Externer Netzwerkpartner

Das Netzwerk Elektronischer Geschäftsverkehr

E-Business für Mittelstand und Handwerk

Das Netzwerk Elektronischer Geschäftsverkehr (NEG) ist eine Förderinitiative des Bundesministeriums für Wirtschaft und Technologie. Seit 1998 unterstützt es kleine und mittlere Unternehmen bei der Einführung und Nutzung von E-Business-Lösungen.

Beratung vor Ort

Mit seinen 29 bundesweit verteilten Kompetenzzentren informiert das NEG kostenlos, neutral und praxisorientiert – auch vor Ort im Unternehmen. Es unterstützt Mittelstand und Handwerk durch Beratungen, Informationsveranstaltungen und Publikationen für die Praxis.

Das Netzwerk bietet vertiefende Informationen zu Kundenbeziehung und Marketing, Netz- und Informationssicherheit, Kaufmännischer Software und RFID sowie E-Billing. Das Projekt Femme digitale fördert zudem die IT-Kompetenz von Frauen im Handwerk. Der NEG Website Award zeichnet jedes Jahr herausragende Internetauftritte von kleinen und mittleren Unternehmen aus. Informationen zu Nutzung und Interesse an E-Business-Lösungen in Mittelstand und Handwerk bietet die jährliche Studie „Elektronischer Geschäftsverkehr in Mittelstand und Handwerk".

Das Netzwerk im Internet

Auf www.ec-net.de können Unternehmen neben Veranstaltungsterminen und den Ansprechpartnern in Ihrer Region auch alle Publikationen des NEG einsehen: Handlungsleitfäden, Checklisten, Studien und Praxisbeispiele geben Hilfen für die eigene Umsetzung von E-Business-Lösungen.

Fragen zum Netzwerk und dessen Angeboten beantwortet Markus Ermert, Projektträger im DLR unter 0228/3821-713 oder per E-Mail: markus.ermert@dlr.de.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Netzwerk Elektronischer
Geschäftsverkehr

www.ec-net.de

IT-Akademie Mainz GmbH

Lehrstuhl Prof. Thome

klick
Kompetenzzentrum elektronischer
Geschäftsverkehr Rheinland-Pfalz

ECC
E-Commerce-Center Handel