Daten gegen Diebstahl sichern

Die Schäden durch Angriffe im Internet zeigen, dass wir uns zurzeit nicht angemessen schützen.

Die Wirtschaftsleistung des deutschen Mittelstands ist enorm. Und gerade dort versuchen Angreifer im Internet immer häufiger, wichtige Daten abzugreifen – mit großen Schäden für die Betroffenen. Wie können auch kleinere Unternehmen ihre schutzwürdigen Daten nachhaltig sichern?

Die Exportnation Deutschland ist international für die Qualität ihrer Produkte “made in Germany“ bekannt. Das unternehmerische Wissen, dass hinter diesen Produkten und Abläufen steckt, wird - vom Großkonzern bis zu den Hidden Champions bei den kleinen und mittelständischen Betrieben - fast ausschließlich digital verwaltet. Nicht nur in Unternehmen, auch in der gesamten modernen Gesellschaft hat das Internet eine Relevanz bekommen, die noch weiter steigen wird. Parallel dazu wachsen gleichermaßen die Angriffsflächen der IT- und Internet-Technologie durch komplexere Software und kompliziertere Zusammenhänge zwischen Protokollen, Diensten und Infrastrukturen. Angriffe auf die immer größeren Werte auf den IT-Systemen werden schon heute öfter und auch raffinierter und professioneller ausgeführt, was Milliardenschäden verursacht. Die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesene professionelle Nachhaltigkeit.

Eine kritische Beurteilung der aktuellen IT-Sicherheitssituation zeigt, dass wir uns nicht angemessen schützen. Welches sind die deutlichsten Sicherheitsprobleme?

„Einfallstor Software“: Die Software stellt in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Wir nutzen Software in PCs, Notebooks, Smartphones, in sehr großen Rechnerzentren, aber auch immer mehr in Autos, in Industrieanlagen, im Haus und vielen weiteren Lebensbereichen. Ein großes Sicherheitsproblem ist, dass in der aktuell genutzten Software zu viele Schwachstellen vorhanden sind. Die Software-Qualität der Betriebssysteme und Anwendungen reicht bei der heutigen Bedrohungslage nicht mehr aus. So liegt die Fehlerdichte, also die Anzahl an Softwarefehlern pro 1.000 Zeilen Code, in qualitativ hochwertiger Software heute im Schnitt bei 0,3. Da gängige Betriebssysteme rund zehn Millionen Zeilen Code haben, sind danach durchschnittlich 3.000 Software-Fehler zu finden. Teile von diesen Softwarefehlern sind Ziele für erfolgreiche Angriffe. Bei den großen Betriebssystemen und Anwendungen ist in den nächsten zehn Jahren auch mit keiner sprunghaften Verbesserung der Software-Qualität zu rechnen und selbst wenn: Auch bei verbesserter Software-Qualität werden die Angreifer noch vorhandene Software-Schwachstellen professioneller ausnutzen. Die Hersteller von Software müssen ihre Softwareentwicklungsprozesse optimieren, um eine höhere Qualität zu erreichen und die Nutzer sollten pro-aktive Sicherheitssysteme verwenden, damit ihre IT-Systeme robuster und vertrauenswürdiger werden (s. auch „Mobile Geräte“).

“Schlechter Schutz vor Malware“: Malware ist der Oberbegriff für "Schadsoftware" wie Viren, Würmer, Trojanische Pferde und andere. Angreifer - wie kriminelle Organisationen, Spione oder Terroristen - nutzen Software-Schwachstellen aus, um

Malware auf IT-Endgeräten zu installieren. Hauptsächlich über E-Mail-Anhänge oder unsichere Webseiten mit Hilfe von sogenannten Drive-by Downloads wird Malware in IT-Endgeräte unbemerkt eingeschleust. Das Institut für Internet-Sicherheit geht zurzeit davon aus, dass auf jedem 25. IT-Endgerät in Deutschland ungewollte Malware vorhanden ist, die über ein Botnetz gesteuert wird. Ein Botnetz ist eine Gruppe von IT-Endgeräten, die unter zentraler Kontrolle eines Angreifers stehen und von ihm für Angriffe genutzt werden. Dadurch können Angreifer Informationen von IT-Endgeräten auslesen (Keylogger, Trojaner), IT-Endgeräte für die Spam-Verteilung und DDoS-Angriffe nutzen und zum Beispiel Daten verschlüsseln und Lösegeld für die Entschlüsselung verlangen. Bei Lösegeldforderungen verschlüsseln die Angreifer mit Hilfe der Malware wichtige Daten auf dem IT-Endgerät und verlangen vom Besitzer eine Summe für die Informationen, mit denen die Daten wieder entschlüsselt werden können.
Wir müssen kritisch feststellen, dass die Anti-Malware-Produkte heute mit 75 bis 95 Prozent eine zu schwache Erkennungsrate haben. Bei direkten Angriffen auf ein IT-System ist die Erkennungsrate im Schnitt sogar nur 27 Prozent. Advanced Persistent Threat (APT) ist die Begrifflichkeit, die sich für intelligente Malware wie Stuxnet und Flame international etabliert hat. APT wird in der Regel als ein gezielter Angriff mit komplexen Angriffstechnologien und -taktiken sowie aufwendigen Hintergrundinformationen eines Opfer-IT-Systems und dessen Umgebung verstanden. Dabei nimmt der Angreifer einen großen Aufwand auf sich (Advanced), um erfolgreich auf ein Opfer-IT-System zuzugreifen und dabei möglichst lange (Persistent) unentdeckt zu bleiben, um über einen längeren Zeitraum Informationen auszuspähen oder Schaden anzurichten.

„Keine internationalen Lösungen für Identifikation und Authentifikation“. Im Jahr 2013 werden immer noch Passworte für die Authentifikation im Internet genutzt. Die Probleme sind bekannt: Verwendet werden oft schlechte Passwörter, oder ein gutes Passwort für viele Anwendungen. Passworte werden zum Beispiel im Klartext in E-Mails durch das Internet übertragen. Durch die Nutzung dieser unsicheren Authentifikation-Technologien entstehen jährlich hohe Schäden von 1,9 Milliarden Euro (Verisign Fraud Barometer, 2009). Dabei sind sehr gute Identifikations- und Authentifikationslösungen vorhanden, wie zum Beispiel die ID-Funktion des neuen Personalausweises in Deutschland. Nur werden diese kaum angeboten oder genutzt und haben international wenig Bedeutung.

„Unsichere Webseiten im Internet“. Heute wird Malware hauptsächlich über unsichere Webseiten im Internet verteilt. Das Institut für Internet-Sicherheit misst im Projekt Internet-Kennzahlen-System, dass auf den deutschen gemessenen Webseiten zurzeit etwa 2,5 Prozent Malware direkt oder indirekt vorhanden sind, die dafür sorgen können, dass die Nutzer der Webseiten infiziert werden.
Unternehmen stellen Webseiten im Internet häufig zu sorglos zur Verfügung. Oft sind diese nicht sicher genug erstellt, so dass Angreifer die Webseiten mit Malware verseuchen können. Der Schwerpunkt in der eigenen Web-Darstellung liegt bei vielen Unternehmen und Behörden hauptsächlich auf der grafischen Darstellung, auf Benutzerführung und Farbgestaltung und nicht auf der IT-Sicherheit, die aber für die Nutzer der Webseite wichtig ist. Vergleichbar ist dies mit einem Logistikunternehmen, das seine LKWs ohne Bremsen im Straßenverkehr nutzt. Auch große Firmen wie Sony wurden schon mehrmals gehackt, weil sie sich und ihre Kunden nicht angemessen geschützt haben. Selbst Regierungsorganisationen lassen erkennen,

dass sie geheime Informationen oder datenschutzrelevante Bürgerinformationen nicht angemessen schützen.

„Nutzung mobiler Geräte“. Die Vorteile von mobilen Geräten wie Smartphones und Tablets sind bestechend. Über die vielfältigen Kommunikationsschnittstellen (wie UMTS/LTE, WLAN, Bluetooth, NFC) ist das Internet mit seinen Diensten stets und überall verfügbar. Mobile Geräte sind multifunktional: Handy, Navi, Musik/TV-Gerät, Medizin-/Gesundheitsgerät, Zugang zum Unternehmen, Internet-Dienste, universeller Computer mit Handy-Apps - alles ist in einem Gerät. Mit "Local Based Service” kommen nützliche und innovative Dienste vor Ort hinzu.
Mit diesen mobilen Geräten tauchen aber auch neue Angriffsvektoren auf, die weitere Risiken verursachen. Ständig wechselnde unsichere Umgebungen (Flughäfen, Bahnhöfe, Cafés) erhöhen die Wahrscheinlichkeit des unabsichtlichen Verlustes und des gezielten Diebstahls. Die Gefahr einer Bewegungsprofilbildung und die einfache Möglichkeit, in der Öffentlichkeit Einsicht zu nehmen, sind nicht zu unterschätzen. Die Nutzung von „bösen“ Apps, die unsere Daten auslesen, wird durch das Prinzip „Masse statt Klasse“ und nicht vertrauenswürdige App-Stores wahrscheinlicher. Aber auch die Nutzung von falschen oder manipulierten Hotspots wird durch ein „schnelles E-Mail-checken“ immer häufiger zum Angriffspunkt. Eine weitere Gefahrenquelle für Unternehmen ist die parallele Nutzung von mobilen Geräten für private und berufliche Zwecke. Ein großes Problem dabei ist, dass die meisten mobilen Geräte für den Verbraucher-Markt erstellt werden. Hier wird von den Anbietern die Strategie verfolgt: Die mobilen Geräte wie zum Beispiel das iPhone müssen für jeden Benutzer leicht verständlich erstellt werden. Erst mal funktioniert alles, wenn der Benutzer mehr Sicherheit möchte, muss er Einschränkungen vornehmen. Und das kann er meistens nicht.

Quote: Eine richtige Business-Strategie wäre: Es funktioniert erst mal gar nichts und der Benutzer muss Funktionen freischalten, die er unbedingt für die Erledigung seiner Aufgabenstellung braucht. Dadurch wird die Angriffsfläche auf mobile Geräte schon deutlich reduziert.

„Eine E-Mail ist offen wie eine Postkarte!“
Vom E-Mail-Dienst wird keine Vertraulichkeit garantiert! Passworte, Kreditkartennummern und weitere Bankdaten sowie vertrauliche Informationen werden im Klartext übertragen und stellen so ein großes Risiko dar. Denn die Möglichkeiten, eine E-Mail abzugreifen, sind sehr hoch. In einigen Ländern werden E-Mails analysiert, um zum Beispiel an das Know-how von Firmen aus anderen Ländern zu kommen. Damit sind E-Mails ein weiterer großer Risikofaktor. Wir wissen von Untersuchungen und Befragungen, dass heute weniger als vier Prozent aller E-Mails verschlüsselt werden.
Wir wissen aber auch, dass mindesten 43 Prozent der E-Mails in Business-Prozessen verwendet werden. Aus diesem Grund sollten den Mitarbeitern im Unternehmen E-Mail-Verschlüsselungstechnologien zur Verfügung gestellt werden. Typischerweise kommen in der Regel meist zwei verschiedene Standards zum Einsatz. Dies ist zum einen S/MIME, der vermehrt in größeren Unternehmen verwendet wird und zum anderen OpenPGP, der schnell und unabhängig ohne Unternehmensserver auf den IT-Endgeräten des Anwenders betrieben werden können. Außerdem müssen die Mitarbeiter wissen, wie und - ganz wichtig - wann diese Verschlüsselungstechnologien für vertrauliche E-Mails verwendet werden sollen.

„Internet-Nutzer haben zu wenig Internet-Kompetenz". Internet-Nutzer müssen die Gefahren des Internets kennen, sonst schaden sie sich und, über infizierte Malware, anderen. Laut einer BITKOM Umfrage von 2012 haben 30 Prozent der Internet-Nutzer keine Personal-Firewall und 28 Prozent keine Anti-Malware-Lösung auf ihrem IT-Endgerät und sind damit nicht angemessen geschützt.

Weitere aktuelle Herausforderungen ergeben sich auch durch die Veränderungen der Rahmenbedingungen. Das Internet geht über alle Grenzen und Kulturen hinaus. Die Auffassungen darüber, was richtig und was falsch ist, sind unterschiedlich. Auch die Unsicherheiten bei verschiedenen Rechtssystemen müssen berücksichtigt werden. In vielen Ländern ist noch keine Strafverfolgung bei Missbrauch möglich. Außerdem erleben wir gerade eine radikale Entwicklung und Veränderung in der IT und im Internet sowohl durch Soziale Netzte wie Facebook und Twitter wie auch durch Cloud Computing und den Betrieb von kritischen Infrastrukturen per Internet. Wir haben durch neue Betriebssysteme, neue IT-Konzepte, neue Angriffsstrategien und neue Player im IT-Markt veränderte Bedingungen, auf die wir uns sehr schnell einstellen müssen. Der Atomausstieg sorgt zum Beispiel für mehr Risiko in der Energieversorgung, da jetzt die Stromnetze und deren Komponenten vernetzt werden, um intelligenter, also effizienter zu werden. Dadurch steigen unter den heutigen Voraussetzungen das Risiko einer Unterbrechung der Stromversorgung und damit die Funktionsfähigkeit unserer Gesellschaft durch Internet-Angriffe erheblich.
Die grundsätzlich unsichere und schlecht umgesetzte Technologie, kombiniert mit einer ungenügenden Internet-Kompetenz der Nutzer, macht einen Paradigmenwechsel dringend notwendig. Nur dann können wir zukünftig die moderneren Internet-Technologien und -Dienste mit weniger Risiko nutzen.

Wichtige IT-Sicherheitsaspekte
Was sollten Unternehmen mindestens tun, um sich angemessen zu schützen? Zunächst sollten sie definieren, welche Daten im Unternehmen überhaupt schützenswert sind und wo diese Daten gespeichert sind. Nach Untersuchungen sind im Schnitt nur rund fünf Prozent aller vorhandenen Unternehmensdaten besonders schützenswert. Für das Aufspüren und Klassifizieren dieser schützenswerten Daten werden auf dem Markt Sicherheitslösungen angeboten, die diesen Prozess unterstützen.

Ein gut abgesichertes Firmennetzwerk mit Hilfe von Firewall- und VPN-Systemen ist ein wichtiger Schritt, aber nicht der einzige. Zum praktischen Vergleich: Ein Unternehmer würde nie jemanden mit einem Fahrzeug aus dem Fuhrpark fahren lassen, der keinen Führerschein hat und die Straßenverkehrsordnung nicht kennt. Eine geregelte Kompetenz wie im Straßenverkehr müssen Mitarbeiter auch für das Internet entwickeln, bevor sie die Firmencomputer und das Internet aus dem Unternehmen heraus nutzen dürfen.
Die notwendigen Kompetenzen sind sehr vielfältig und durch den raschen Wandel in der IT und im Internet auch sehr schnelllebig. Unternehmen können hier zum Beispiel die vielfältigen Angebote nutzen, die das Bundeswirtschaftsministerium über Projekte fördert (siehe Linkliste IT-Sicherheit).

Umgang mit sicheren Passwörtern
Das Firmennetzwerk und Dienste im Internet bergen eine große Gefahr. Mitarbeiter bekommen Nutzer-Accounts für den Zugang zu unterschiedlichen IT-Systemen und Diensten, die aus Benutzernamen und Passwörtern bestehen. Das erste Passwort muss direkt geändert werden, um Angriffe zu verhindern – doch Versuche des Instituts für Internet-Sicherheit haben ergeben, dass viele der Mitarbeiter das nicht richtig tun. Das bedeutet ein enorm erhöhtes Angriffspotenzial von der Konkurrenz und kriminellen Organisationen. Doch selbst ein geändertes Passwort kann eine Firma nicht immer schützen. Denn viele Internet-Nutzer nehmen unsichere Passwörter. Das Passwort „geheim“ ist eben nicht geheim!
Sehr viele Mitarbeiter nutzen heute immer noch den Firmennamen in Kombination mit fortlaufenden Zahlen als Passwort.
Ein sicheres und gutes Passwort muss heute aus mindestens zehn Stellen bestehen, aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen und keinen offensichtlichen Sinn ergeben, zum Beispiel Jh1mN!9loP. Erst dann ist es sicher. Eine weitere Herausforderung für den Mitarbeiter ist die Aufbewahrung von Passwörtern. Das ist umso schwerer, wenn das Passwort regelmäßig alle drei bis sechs Monate geändert werden sollte. Da viele Mitarbeiter mehrere wichtige Passworte verwenden müssen, sollte ihnen Hilfestellungen über Passwortverschlüsselungsprogramme gegeben werden, wie zum Beispiel Keepass.
Dabei ist es auch wichtig, dass Nutzer-Accounts von Mitarbeitern, die das Unternehmen verlassen, gelöscht werden, so dass die ehemaligen Mitarbeiter keinen Zugriff mehr auf das IT-System haben. Zudem muss ein Arbeitgeber stets auf den Nutzer-Account zugreifen können. Denn wenn der ausgeschiedene Mitarbeiter noch Daten gespeichert hat, die vom Arbeitgeber benötigt werden, braucht dieser den Zugriff auf das Material.

Richtiger Umgang mit dem Browser und beim Surfen
Für den Mitarbeiter, der im Internet arbeitet, bedeutet dies, dass er zusätzlich zum bereits erwähnten Basisschutz (Anti-Malware-Software, Personal-Firewall, Aktivierung der automatischen Updates) auch mit seinem Browser sicher umgehen können muss. Dazu gehört auch die Einschätzung, wie vertrauenswürdig eine Webseite ist. Das lässt sich vielfach schon an einfachen Merkmalen einschätzen: der Aufbau und der Inhalt der Webseite, vorhandene Werbung und dessen Auftritt. ein Impressum, oder Empfehlungen auf diese Website. Der Mitarbeiter sollte in der Regel nur auf vertrauenswürdigen Webseiten aktiven Inhalt über den Browser zulassen. Dazu muss der Browser entsprechend eingestellt sein. Informationen, wie das funktioniert, gibt es unter folgendem. Der Mitarbeiter sollte wissen, dass bei einem Mausklick auf einem Link in der Statuszeile zu sehen ist, wo der Link wirklich hinführt. Mit diesem Wissen können die Mitarbeiter Phishing-Angriffe verhindern. Das gilt auch für Links in E-Mails. Der Fall von Phishing-Angriffen auf Kontodaten des EU-Emissionshandels hat gezeigt, dass Mitarbeiter auf solche Angriffe leicht hereinfallen und damit hohe Schäden für Unternehmen verursachen können.

Informationen in sozialen Netzwerken
Das Web 2.0 kann auch für Unternehmen interessant sein. Mitarbeiter können sich über Web-2.0-Anwendungen sehr schnell neues Wissen aneignen und Informationen beschaffen, Das steigert auch die Innovationsgeschwindigkeit im Unternehmen. Dazu tragen Diskussionen unter den Mitarbeitern über neue Ideen bei. Doch wer sich an Diskussionen in den Web-2.0-Anwendungen beteiligt, sollte immer bedenken, dass er der Konkurrenz damit unter Umständen wertvolle Informationen in die Hände

spielt. Daher gilt: Vertrauliche Unternehmensinformationen sollten generell nicht im Internet besprochen werden!

Basisschutz in Unternehmen

Die Unternehmen müssen dafür sorgen, dass die schützenswerten Daten identifiziert werden und die notwendigen IT-Sicherheitsmechanismen wie Firewall-Systeme, Anti-Mailware-Produkte, E-Mail-Verschlüsselungsmöglichkeiten sowie Management-Systems für Smartphones und andere mobile Geräte vorhanden sind. Sie müssen auch für eine stetige qualitative Softwareentwicklung und sichere Webseiten sorgen. Die Mitarbeiter sollten die Vertrauenswürdigkeit von Webseiten einschätzen können, sie sollten sicherstellen, dass die automatischen Updates der IT-Endgeräte eingeschaltet sind, dass der Virenscanner aktualisiert wird und die Personal Firewall in Betrieb ist. Auch sollten sie darüber aufgeklärt werden wie man Phishing-Angriffe erkennt, wie sensible Mails verschlüsselt werden und sie sollten sichere Passwörter nutzen.

Dazu müssen die Mitarbeiter im Unternehmen für einen richtigen, bewussten Umgang mit IT-Endgeräten und dem Internet geschult werden, das heißt, sie müssen die Regeln und richtigen Verhaltensweisen verinnerlichen, um die Risiken und Gefahren erkennen und abschätzen zu können. Nur dann ist ein Unternehmen in der vernetzten Informations- und Wissensgesellschaft angemessen geschützt. Das Thema IT-Sicherheit ist sehr komplex, es gibt aber viele gute Webseiten, auf denen hilfreiche Informationen zum Thema IT-Sicherheit zu finden sind.

Prof. Dr. Norbert Pohlmann

Informationen zur IT-Sicherheit:

- http://ratgeber.it-sicherheit.de – IT-Sicherheitstipps und Hintergrundinfos
- www.sicher-im-internet.de – Buch „Sicher im Internet“ als Download
- https://www.internet-sicherheit.de – Sicherheitstipps
- https://www.bsi-fuer-buerger.de – Sicherheitstipps
- https://www.sicher-im-netz.de/ – Sicherheitscheck
- http://www.it-sicherheit-in-der-wirtschaft.de/ – IT-Sicherheitsnavigator
- https://norbert-pohlmann.com/

Der Autor:

Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen.

securityNews App
App informiert über aktuelle Sicherheit

Cyber-Kriminelle suchen heutzutage gezielt nach Schwachstellen in Software-Produkten mit hohem Verbreitungsgrad. Findet sich beispielsweise eine Sicherheitslücke im Adobe Flash Player, der laut Herstellerangaben auf 99 Prozent aller internetfähigen PCs installiert ist, setzen Angreifer alles daran, die Lücke für ihre Zwecke auszunutzen. Schaffen sie dies, bieten sie ihren Schädlingen einen potenziellen Nährboden von hunderttausenden Systemen. Die Hersteller betroffener Software-Produkte versuchen im Gegenzug, Sicherheitslecks durch ein Software-update zu versiegeln. Nur häufig spielen die Software-Anwender das als nervig empfundene Update spät oder womöglich gar nicht auf. Damit schenken sieden Angreifern Zeit, um die Rechner mit Viren, Würmern und Trojanern zu infizieren. Der kostenlose Sicherheitsservice securityNews hilft dabei, den Überblick zu behalten. Dank aktueller Sicherheitshinweise für Smartphone, Tablet, PC und Mac kann die Angriffsfläche für Kriminelle minimiert werden. Die Experten vom Institut für Internet-Sicherheit wählen täglich die wichtigsten Meldungen aus und informieren in verständlicher Sprache über dringende Sicherheitsmaßnahmen, wie Sicherheitsupdates. securityNews gibt es in der mobilen Variante als App für Smartphone und Tablet (verfügbar für iPhone, iPad und alle Android-Geräte), als E-Mail-Dienst und als Web-App zum Einbetten in Websites.
Informationen und App kostenlos unter: https://www.it-sicherheit.de/securitynews/was_ist_securitynews/

Bildunterschrift: Newsbereich des securityNews-App

Beispiel: Checkliste
Smartphone vor Dritten schützen

√ Sorgen Sie für einen angemessenen Basisschutz:
- vorhandene Sicherheitseinstellungen eingeschalten
- automatische Softwareupdates aktivieren, damit Sicherheitsupdates nach dem Erscheinen unmittelbar eingespielt werden
- egelmäßig Updates für Betriebssystem und die installierten Programme herunterladen
- Virenschutz einrichten und regelmäßig auf Schädlinge prüfen

√ Nutzen Sie Schnittstellen nur bei Bedarf:
- drahtlose Schnittstellen wie WLAN, Bluetooth und Infrarot nur bei Bedarf ein- und nach Benutzung wieder ausschalten
- WLAN-Verbindung mittels WPA2 verschlüsseln. Alte Standards wie WEP sind unsicher!
- anonyme Gerätekennung ein stellen für die Benutzung von Bluetooth

√ Schützen Sie Ihre Daten vor Dritten:
- Smartphone niemals unbeobachtet lassen oder verleihen nur notwendige Apps und nur aus vertrauenswürdigen Quellen installieren
- kontrollieren, ob eine App nur Daten erfasst, die für die Benutzung notwendig sind. Apps können persönliche Daten ausspähen und versenden
- sensible Daten, wie Geschäftsdaten, vertrauliche E-Mails und Passwörter mit einer speziellen Software veschlüsseln

√ Sichern Sie Ihre Daten regelmäßig:
- regelmäßig wichtige Daten des Smartphones sichern
- die Datensicherung an einem sicheren Ort aufbewahren

Weitere Checklisten und Tipps unter: http://ratgeber.it-sicherheit.de

- Sicherheit für Ihr Notebook
- Sicherer Dokumentenaustausch via E-Mail
- Der richtige Umgang mit dem Browser und verhalten beim Surfen
- Webseiten sicher betreiben
- Sicheres Speichern und Löschen Ihrer Daten