Internetsicherheit

1. Internetsicherheit

Betrachtet man Sicherheit als einen Zustand ohne Bedrohungen oder Gefahren, wird schnell klar, dass Internetsicherheit weit mehr ist als das, was im ersten Moment vermutet wird.

1.1 Wen betrifft Internetsicherheit?

Gerade Existenzgründer und Unternehmer müssen sich daher der möglichen Gefahren bewusst sein und analysieren, welche davon für die eigene Geschäftsidee relevant sind. Sicher im Netz der Netze unterwegs zu sein hat viele Seiten. Bereits bei den ersten Überlegungen, das Internet als Mittel zum Zweck oder als Gegenstand der Geschäftsidee zu nutzen, sollte dies berücksichtigt werden.

1.2 Was ist Internetsicherheit?

Drei Grundpfeiler der Internetsicherheit sind:

1. Verfügbarkeit,
2. Integrität und
3. Vertraulichkeit.

Hinzu kommt als 4. die Rechtssicherheit, d.h. das gesetzeskonforme Handeln (Compliance).

Nicht nur für Unternehmen ist also das Ziel, die genannten Kriterien für alle beteiligten Parteien zu sichern. Dies gilt für die Kommunikation mit Partnern, Kunden und Beschäftigten.

Jede der bekannten Bedrohungen hat Auswirkungen auf mindestens einen dieser Bereiche. Computerschädlinge könnten sich auf alle vier auswirken. Ein Stromausfall würde die Verfügbarkeit beeinträchtigen. Der Verstoß gegen Gesetze kann empfindliche Strafen nach sich ziehen. Der Weg zu mehr Internetsicherheit besteht also in der Sicherung der Verfügbarkeit, der Integrität, der Vertraulichkeit und der Gesetzeskonformität. Dies erfordert Maßnahmen in Bezug auf Organisation, Technik und Mensch.

1.3 Handlungsfelder

Besondere Bedeutung kommt einem planmäßigen und überlegten Handeln zu. Oft lässt sich mit wenig Aufwand viel erreichen. Dies können organisatorische oder technische Maßnahmen sein.

Ein besonders wichtiger Sicherheitsfaktor sind die Menschen im Unternehmen. Dies gilt ausnahmslos, also vom Geschäftsinhaber bis hin zum Praktikanten. Sind es doch die Menschen, die mit ihrer Intelligenz und dem Ziel, ihre Arbeit ordentlich zu erledigen, mühelos jede Sicherheitsmaßnahme umgehen oder außer Kraft setzen können. Hierbei gilt es verständlich zu machen, warum bestimmte Dinge zu tun oder zu lassen sind.

1.4. Absolut sicher?

Sicherheit ist relativ und nie zu 100% erreichbar. Es ist ein Prozess mit dem Ziel, ein Optimum zu erreichen. Ganz wichtig sind die ständige Auseinandersetzung mit den Themen der Internetsicherheit und die Aktualisierung des Wissensstandes. Wie aktuelle Zahlen belegen, steigt die Zahl der Fälle im Bereich der Internetkriminalität stetig an. Auch diese Bedrohungen gilt es zu beachten. Hilfreiche und aktuelle Informationen können als Newsletter zu verschiedenen Bereichen unter **www.buerger-cert.de/** abonniert werden. Konkrete Unterstützung bieten beispielsweise die Industrie und Handelskammern sowie Projekte zur Förderung des E-Business wie z.B. das mdc-ecomm. Vielfältige Informationen und Leitfäden finden sich unter **www.kmu-sicherheit.de.**

In Sachsen gibt es das besondere Präventionsangebot **„Sicheres Unternehmen"** der Polizei in Zusammenarbeit mit dem Sächsischen Verband für Sicherheit in der Wirtschaft e. V. (SVSW). Dieser kostenfreie Service beinhaltet einen Sicherheitscheck zum Objektschutz, zur Sicherheit in der Informations- und Kommunikationstechnik sowie zu organisatorischen Maßnahmen.

2. Organisation

Bereits mit organisatorischen Maßnahmen lässt sich die Sicherheit im Internet wesentlich erhöhen. Hierzu sind einige Überlegungen und Recherchen erforderlich. Im Fokus steht der Geschäftsgegenstand. An ihm orientieren sich alle Überlegungen, Regelungen und Maßnahmen. Für optimale Ergebnisse ist eine systematische Vorgehensweise oberstes Gebot. Die wesentlichen Phasen sind:

- Analyse/Planung,
- Umsetzung,
- Kontrolle und
- Anpassung

Es ist ein Kreislauf, der immer wieder durchlaufen wird. Dabei kann auch Vorhandenes effizient eingebracht werden. Internetsicherheit ist niemals finaler Zustand.

2.1 Analyse/Planung

Ausgangspunkt ist die Analyse aller möglichen Einflussfaktoren, die für die Internetsicherheit relevant sind. Dies sind im Wesentlichen rechtliche Anforderungen, die IT-Komponenten/Technik und natürlich der Mensch im Unternehmen. Für die Ermittlung der rechtlichen Aspekte sollte die Unterstützung von Spezialisten in Anspruch genommen werden.

Es folgt die Untersuchung, welche Themen für das Geschäft unbedingt erforderlich sind (Priorisierung: z. B. „sehr wichtig", „wichtig" und „weniger wichtig"). Anschließend wird analysiert, welche Einflüsse relevant sein könnten. Dies reicht von höherer Gewalt (z.B. Wasserschaden) über technische Defekte bis hin zu menschlicher Einwirkung (z.B. Fehlverhalten). Nach der Erfassung der potentiellen Bedrohungen folgt eine Bewertung ihrer Eintrittswahrscheinlichkeit (wie oft) und des damit verbundenen möglichen Schadens. Hierbei ist auch an Schäden zu denken, die nicht direkt materieller Natur sind, wie z.B. ein Imageverlust.

Mit den ermittelten Risiken kann unterschiedlich umgegangen werden. Im Wesentlichen sind das: die Verlagerung, die Akzeptanz und die Minimierung des Risikos. Bei der Minimierung kann entweder die Reduzierung der Eintrittswahrscheinlichkeit und/oder des damit verbundenen Schadens das Ziel sein.

Wertvolle Hinweise bietet z.B. das BSI (Bundesamt für Sicherheit in der Informationstechnologie) mit seinen Grundschutzkatalogen an: **www.bsi.bund.de**
Für die Auswahl der konkreten Aktivitäten kann die Inanspruchnahme von Spezialisten hilfreich sein. Vorrang haben Maßnahmen, bei denen mit wenig Aufwand (Zeit und Kosten) viel erreicht werden kann.

2.2 Umsetzung

Auch bei der Realisierung sollte in bestimmten Bereichen auf professionelle Unterstützung zurückgegriffen werden. Besondere Bedeutung kommt der Dokumentation der ergriffenen Maßnahmen zu. Sie ermöglicht es im Schadensfall, die Arbeitsfähigkeit schneller wieder herzustellen und gegenüber Dritten nachzuweisen, dass und welche Maßnahmen ergriffen wurden. Geeignete Dokumentationen können ein Notfallhandbuch oder ein IT-Sicherheitskonzept sein. In der Praxis hat es sich bewährt, derartige Dokumentationen als „lose Blattsammlung" anzulegen. Dies erleichtert die spätere Pflege und Aktualisierung. Wertvolle Tipps finden sich im **„Praxisbuch IT-Dokumentation"** von Manuela Reiss und Georg Reiss.

2.3 Kontrolle

Eine wesentliche Komponente des Sicherheitsprozesses ist die regelmäßige Überprüfung der getroffenen Maßnahmen. Alle Einflussfaktoren der Internetsicherheit unterliegen der Veränderung. Dies betrifft gesetzliche Regelungen, technische Neuerungen und ganz besonders das Internet selbst. Es ist daher sehr wahrscheinlich, dass einzelne Maßnahmen nicht mehr erforderlich sind, angepasst oder neu erstellt werden müssen.

2.4 Anpassung

Mit der Anpassung schließt sich der Kreis zum „Prozess Sicherheit". Ein gelebter Sicherheitsprozess ist die Garantie für ein hohes Niveau der Internetsicherheit.

3. Faktor Mensch

Der Mensch ist der Dreh- und Angelpunkt der Sicherheit im Internet, egal ob als Unternehmer, Mitarbeiter, Geschäftspartner oder Kunde. Ein Unternehmer, der die für sein Unternehmen relevanten Gesetze nicht kennt, ist ebenso ein Risiko wie ein Mitarbeiter, der leichtfertig Daten preis gibt.

3.1 Datenschutz

Der Schutz von personenbezogenen Daten (z. B. Namen, Geburtsdatum, Anschrift, Bankverbindung u. v. m.) gilt für alle Individuen, also auch Mitarbeiter, Geschäftspartner und Kunden. Wesentliche Anforderungen regelt z.B. das Bundesdatenschutzgesetz (BDSG).

Jeder Unternehmer sollte prüfen, welche Anforderungen für sein Unternehmen relevant sind und wie sie in der Praxis umgesetzt werden können. Oft lässt sich dies mit Unterstützung einer fachkundigen Person mit wenig Aufwand klären. Die Anforderungen des Datenschutzes lassen sich oft mit technischen und organisatorischen Maßnahmen umsetzen. Besonders sei darauf hingewiesen, dass bei der Veröffentlichung von Mitarbeiter- und Kundendaten (wie z. B. Fotos von einer Firmenveranstaltung) besondere Regeln einzuhalten sind. Eine Nichtbeachtung kann erhebliche Konsequenzen haben.

3.2 Social Engineering

Der Begriff Social Engineering oder auch Social Hacking beschreibt ein Vorgehen, bei dem speziell ausgebildete Personen versuchen, mit „normalen" Mitteln Informationen von anderen Menschen zu erlangen. Hierbei werden alle Wege zwischenmenschlicher Beziehungen und Methoden des Ausspähens in Kombination eingesetzt. Eine so angegriffene Person bemerkt dies oft nicht einmal.

Zur Beschaffung weiterer Informationen werden auch öffentlich zugängliche Quellen wie z. B. Webseiten, Informationen aus sozialen Netzwerken, Veröffentlichungen usw. eingesetzt. Es sollte daher unbedingt geprüft werden, welche Informationen wo öffentlich gemacht werden.

3.3 Wissen und Awareness als Schlüssel

Leicht lässt sich erkennen, dass alle bisher genannten Aspekte etwas mit Wissen zu tun haben.
Doch Wissen allein genügt nicht – die einzelnen

Informationen müssen im Zusammenhang betrachtet werden. Für ein hohes Niveau der Internetsicherheit ist Wissen eine notwendige Voraussetzung, aber allein nicht ausreichend. Besonders wichtig ist die Art der Wissensvermittlung. Sie muss so gewählt werden, dass die betroffenen Personen Zusammenhänge erkennen können. Jeder einzelne Beschäftigte im Unternehmen soll erkennen, was genau in seiner Position für mehr Internetsicherheit getan werden kann.

Oft helfen Parallelen und Vergleiche zwischen dem privaten Bereich und der Situation im Unternehmen. Privat erwartet jeder, dass seine Bankdaten vertraulich bleiben – warum sollte das in der Firma anders sein? Reale Beispiele erhöhen die Praxisbezogenheit und wecken Interesse.

Nicht jede mögliche Sicherheitsbedrohung lässt sich vorhersehen. Somit scheidet auch eine Übung für einen derartigen Notfall aus! Die Herausforderung besteht darin, alle im Unternehmen in die Lage zu versetzen, mögliche Risiken frühzeitig zu erkennen und ein Gespür dafür zu entwickeln, wann eine Situation ungewöhnlich ist. Frei nach dem Motto „Gefahr erkannt – Gefahr gebannt" kann die Reaktion auf neue Situationen trainiert werden.

Eine wichtige Erkenntnis ist, dass einmalige Maßnahmen nicht ausreichen. Ziel ist eine ständige Anpassung und Aktualisierung des Wissens und des Sicherheitsbewusstseins.

Gut informierte Menschen verstehen, was von ihnen erwartet wird. Diese Einsicht führt dazu, dass sich Verhaltensweisen ändern und auch die Motivation steigt. Besonders positiv wirkt sich ehrliche Anerkennung für bewusstes Handeln aus. Eine weitere Quelle für mehr Internetsicherheit sind die Ideen und Vorschläge der Beschäftigten. Einmal erschlossen, fördert das eine gemeinschaftliche Atmosphäre des Sicherheitsbewusstseins (Awareness).

4. Infrastruktur

Die IT-Infrastruktur ist das Rückgrat vieler Unternehmen. Zur IT-Infrastruktur gehören die Hardware - Computer, Netzwerkkomponenten, (Mobil-)Telefone, Kopierer - sowie die darauf laufende Software. In den meisten Fällen wird die eigene IT mit externen Anbietern kombiniert. Die Gewährleistung von Verfügbarkeit, Vertraulichkeit und Integrität der damit verarbeiteten Daten ist essentiell.

4.1 Computersicherheit

Die Sicherheit der einzelnen Rechner - ob Desktop-PC, Laptop oder Server - hängt von der Auswahl der Geräte, deren ordnungsgemäßer Administration und dem Nutzerverhalten ab. Unternehmen sollten in Hardware investieren, die für den Businesseinsatz vorgesehen ist und Sicherheitsfeatures wie z.B. Smartcard-Leser u. a. besitzt.
Die Hardware muss regelmäßig gewartet und die Daten gesichert werden. Sinnvolle Ergänzungen, wie z. B. Unterbrechungsfreie Stromversorgungen (USV) erhöhen die Verfügbarkeit.

4.2 Netzwerksicherheit

Das Netzwerk muss den Datenverkehr nach Sicherheitsvorgaben regeln können (z. B. Firewall). Es wird festgelegt, welche Geräte wie kommunizieren dürfen. Die ständige Überwachung der Aktivitäten und Protokoll-Dateien hilft Probleme rechtzeitig zu erkennen. Besonderes Augenmerk erhalten natürlich Komponenten und Dienste, die Daten sowohl aus dem internen als auch dem Internet verarbeiten. Das Netzwerk sollte von Anfang an gut geplant und in verschiedene logische Segmente aufgeteilt werden. Regelmäßige Audits oder Penetrationstest helfen den Verantwortlichen, Schwachstellen aufzudecken und Aktivitäten für einen sicheren Betrieb zu dokumentieren.

4.3 Softwaremanagement

Mit Software wird meistens zu arglos umgegangen. Lizenzmanagement und Vorgaben zur Validierung der Software-Herkunft helfen Schäden durch Strafen oder Malware zu vermeiden. Ein absolutes Muss für alle Rechner ist ein aktuelles Virenschutzprogramm - besser noch eine Security-Suite. Homogene, standardisierte Software spart nicht nur Wartungskosten, sondern fördert auch die Sicherheit, da die Angriffsmöglichkeiten minimiert werden und die Administration Maßnahmen für große Teile der eingesetzten Geräte gleichzeitig durchführen kann. Der Einsatz der Software muss auch durch Vorgaben geregelt und durchgesetzt werden z.B. E-Mail-Nutzung, Verwendung von Browserplugins oder die Installation von Programmen durch den Nutzer.

4.4 Sicheres Cloud Computing

Gerade kleine und mittelständische Unternehmen sind auf Angebote von IT Dienstleistern angewiesen. Der Wechsel von Investitionen in Personal und Hardware hin zu flexiblen Betriebskosten machen manche Unternehmung erst möglich. Heutzutage kann fast alles extern eingekauft werden, vom Hosting von Webseiten und E-Mail über Datenspeicher in der Cloud bis zur Lohnbuchhaltung online. Doch Vorsicht, die Auswahl der Anbieter und Dienste, die Gestaltung der Service Level Agreements (Verfügbarkeits- und Performance Regelungen) bergen einige Fallstricke, insbesondere bei ausländischen Anbietern. Wichtig sind die Strategie und das Risikomanagement bei der Auslagerung von IT-Komponenten. Es ist zu prüfen, ob die Auslagerung das Kerngeschäft betrifft, ob sie mit gesetzlichen Vorgaben wie dem Datenschutz vereinbar ist und ob bei Problemen alternative Anbieter verfügbar sind. Externe Ressourcen werden nach Abstraktionslevel eingeteilt:

- IaaS (Infrastructure as a Service) externe Hardwareressourcen
- PaaS (Platform as a Service) externe Softwareplattformen zur Entwicklung
- SaaS (Software as a Service) externe Softwarelösungen

und sind entsprechend der internen Regeln zu behandeln. Die Unternehmen sind verpflichtet, die Einhaltung der Sicherheitsstandards durch die Anbieter zu prüfen.

4.5 Weiterführendes

Das BSI und der Branchenverband BITKOM bieten Leitfäden und konkrete Anforderungen an eine sichere IT-Infrastruktur unter:
www.bsi.bund.de/IT-Grundschutz.html
www.bitkom.org

5. Handel und Finanzen

Aspekte der Internetsicherheit spielen in den Bereichen Handel und Finanzen eine besonders wichtige Rolle. Ein wesentlicher Schwerpunkt liegt dabei beim Internetrecht und den möglichen Maßnahmen, ihm zu entsprechen.

5.1 Handel im Internet

Der Handel im Internet ist ein besonders komplexer Vorgang. Normalerweise, z. B. in einem Ladengeschäft, sind die Vertragspartner anwesend. Entweder wechselt eine Ware den Besitzer oder eine Dienstleistung wird angeboten und bezahlt. Oft kennen sich die Vertragspartner nicht einmal. Beim Handel im Internet ist das alles anders, da die Vertragspartner nicht körperlich anwesend sind, wird hierbei von Fernabsatz gesprochen. Letztlich geht es darum, ein rechtlich einwandfreies Vertragsverhältnis herzustellen. Insbesondere die Rechte der Verbraucher führen zu hohen Anforderungen an die Unternehmer.

Auf Grund der hohen Komplexität des Themas empfiehlt es sich, professionelle Hilfe in Anspruch zu nehmen. Dies gilt besonders im Fall einer Abmahnung. Speziell in dieser unschönen Situation gilt es zügig, aber nicht voreilig zu handeln.

5.2. Finanztransaktionen

Egal, ob es sich um einen Online-Shop, die Bezahlung einer Lieferung oder die Gehaltszahlungen handelt – es wird Geld transferiert. Besonders hier werden Kriminelle angelockt. Neben der Erfüllung der rechtlichen Anforderungen kommt der Abwehr von Angriffen aus dem Netz eine hohe Bedeutung zu. Dies kann mit technischen und organisatorischen Maßnahmen sowie der nötigen Awareness, also dem erforderlichen Sicherheitsbewusstsein, erreicht werden. Der Nutzer sollte ein Gefühl dafür entwickeln, was z. B. in der elektronischen Kommunikation mit Banken wahrscheinlich ist.

Eine Bank wird wichtige Sachverhalte niemals per E-Mail klären oder gar nach vertraulichen Informationen (z. B. PIN/TAN) fragen.

Besonders wichtig ist es zu erkennen, ob es sich tatsächlich um die Webseite der Bank handelt. Der Weg dorthin sollte niemals über einen Link führen! Der sicherste Weg ist die direkte Eingabe der Internetadresse (URL). Eine Betrachtung der Internetadresse liefert weitere Informationen. Hier sollte als Übertragungsprotokoll **„https"** und nicht nur **„http"** angezeigt werden. Auch weitere Adressbestandteile liefern wichtige Informationen.

Bei einem einzelnen Online-Banking Vorgang werden nie mehrere TANs abfragt.

Für Online-Banking ist die Nutzung der HBCI-Technologie empfehlenswert. Wird auf einem alten PC/Notebook ein kostenfreies Linux-System installiert, entsteht auf diesem Weg ein relativ sicherer Online-Banking PC, wenn er nur dafür genutzt wird.

5.3 Elektronische Identitäten

Ein zentrales Thema bei der Kommunikation im Internet ist die Identität der Beteiligten. Wie kann ermittelt werden, ob die Person wirklich die ist, für die sie sich ausgibt? Eine E-Mail-Adresse ist keine Garantie – sie ist mit wenig Aufwand zu fälschen. Eine herkömmliche Unterschrift kann durch eine elektronische Signatur ersetzt werden. Nicht gemeint ist dabei die Text-Signatur in einer E-Mail – sondern geeignetes elektronisches Schlüsselmaterial. Ein Beispiel ist der neue Personalausweis.

Es ist zu beachten, dass nur bestimmte Signaturen ein vollwertiger Ersatz für eine Unterschrift sind. Die Einsatzmöglichkeiten sind vielfältig. So lässt sich z. B. auch mit einer einfachen elektronischen Signatur nachweisen, dass eine E-Mail tatsächlich vom angegebenen Absender stammt. Mit relativ wenig Aufwand ist dann auch eine Verschlüsselung möglich. Ab einer bestimmten Qualität der Signatur lassen sich Dokumente elektronisch signieren, also rechtskräftig unterschreiben.

Für einen sicheren Austausch von Dokumenten bieten verschiedene Anbieter Lösungen, bei denen Dokumente verschlüsselt auf einem Server hinterlegt und von dort von berechtigten Personen verschlüsselt abgeholt werden können.

6. Social Media

Social Media wird auch bei Unternehmen immer beliebter. Plattformen wie Facebook, Twitter und Xing haben sich längst als zusätzliches Kommunikationsinstrument für Gewerbetreibende aller Branchen und Unternehmensformen etabliert.

Längst haben auch Betrüger Social Media für sich entdeckt, daher sollte man Kontaktanfragen und Nachrichten mit Anhängen oder Links von Unbekannten kritisch prüfen.

Was auf Xing eher selten ist, ist bei Facebook oder Twitter an der Tagesordnung. Sogenannte Scams gaukeln Ihnen z. B. vor, wie man auf Facebook das Profillayout ändern oder zeigen kann, wer Ihr Profil besucht hat. Das ist bei Facebook jedoch derzeit gar nicht möglich. Es handelt sich um Betrugsmaschen mit dem Ziel, an Ihre Daten zu kommen oder Ihr Profil als Werbeplattform zu nutzen. Wichtig ist es zu verstehen, dass neben neuen auch „alte" Betrugsmaschen in sozialen Netzwerken eingesetzt werden.

6.1 Was ist Scam?

Scam (engl. Betrug) ist eine Sonderform von Spam, von der erhöhte Gefahr ausgeht. Zwar infiziert man sich nicht gleich zwangsläufig mit einem Virus oder Trojaner, dennoch landet man oft auf Webseiten von Kriminellen. Der größte Teil der im Umlauf befindlichen Scams ist in englischer Sprache verfasst, jedoch finden sich gerade auf Facebook immer häufiger deutschsprachige Scams, meist schlecht übersetzt und relativ leicht zu enttarnen. Scams zielen auf die Neugierde des Empfängers ab, um ihn über den Klick auf Links auf andere Webseiten und interessante Inhalte zu locken. Vorsicht ist bei vermeintlichen Bild- oder Videoinhalten geboten.

6.2 Phishing im Web 2.0

Unter Phishing werden Versuche verstanden, über gefälschte Webseiten, Log-in Fenster, E-Mail oder Kurznachrichten an Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Auch über Facebook werden solche Attacken ausgeführt.

Aufforderungen wie **"Sieh, wer besonders oft dein Profil ansieht"** sollen sofortiges Handeln provozieren. Der Klick auf "Zulassen", wenn eine solche App nach einer Genehmigung fragt oder Sie zu einer Umfrage führt, ist schnell ausgeführt. Und schon findet sich ein fremder Post oder Werbung im eigenen Profil, ohne dass man weiß, woher. Die möglichen Folgen sind Kennwort-Diebstahl, Daten-Klau, Spam-Attacken oder sogar die Integration des Rechners in ein Bot-Netz (Netz gekaperter und fernkontrollierter Rechner), meist ohne dass der Benutzer es merkt.

Auch Nutzer von Twitter können davon betroffen sein. Es werden s. g. Direct Messages verschickt, die den Nutzer auf eine gefälschte Twitterseite leiten sollen, um sich dort einzuloggen. Wer das befolgt, verschickt über seinen Account bald ebenfalls massenhaft Spam-DMs.

6.3 Die andere Bedrohung: Abmahnungen

Eine ganz andere Art von Bedrohungen stellen Abmahnungen für gewerblich genutzte Social Media Auftritte dar, denn für Facebook Fanpages, Firmen Tweets und Co. sind gesetzliche Vorgaben zu beachten, z.B. das Datenschutz-, Marken- und Urheberrecht. „Findige Abmahner" suchen systematisch nach fehlerhaften Websites und Social Media Auftritten von Firmen. Die Abmahnkosten können beträchtlich sein.

Auch für gewerbliche Social Media Auftritte ist eine Beratung durch geeignete Spezialisten erforderlich. So ist z.B. ein vorschriftsmäßiges Impressum auch für Social Media Auftritte Pflicht.

Auch wenn die Social Media Auftritte meist etwas lockerer als die eigene Webseite aufgemacht und betrieben werden, so sind auch hier Betriebs- und Geschäftsgeheimnisse zu wahren und geschäftsschädigende Äußerungen zu unterlassen.

7. Mobilität

Mobile Endgeräte wie Smartphones und Tablet Computer sind auch aus dem Geschäftsalltag nicht mehr wegzudenken. Vor Kurzem galten mobile Endgeräte, deren Betriebssysteme (z. B. iOS oder Android) sowie Applikationen (Programme oder kurz: Apps) noch als relativ sicher. Durch ihre rasante Verbreitung wurden sie jedoch zum attraktiven Ziel für Kriminelle. Bedingt durch einen starken Wettbewerb steigt gleichzeitig die Zahl der Sicherheitslücken in Betriebssystemen und Applikationen.

7.1 Nie unbeaufsichtigt

Mobile Endgeräte sollten niemals unbeaufsichtigt zurückgelassen oder verliehen werden. Nehmen Sie ihre mobilen Geräte nicht zu Besprechungen mit sensiblem Inhalt mit, da sie sowohl hard- als auch softwareseitig als „Wanze" umfunktioniert werden können. Wer nicht darauf verzichten kann: den Akku während der Zeit entfernen.

7.2 Drahtlos, nicht verantwortungslos

Drahtlose Verbindungen wie Bluetooth, WLAN (Wireless LAN) oder Infrarot sollten generell nur dann aktiviert werden, wenn sie auch zum Einsatz kommen. Eine WLAN-Verbindung muss den aktuellen Empfehlungen entsprechen, also ausreichend verschlüsselt sein. In der Bluetooth-Konfiguration des Gerätes ist die Benutzerkennung generell auf **"verbergen/verstecken"** umzustellen. Die Benutzerkennung bei Bluetooth sollte nur dann kurz aktiviert werden, wenn erstmalig die Kommunikation mit neuen Geräten der Umgebung aufgebaut wird. Die Benutzerkennung darf keinen Rückschluss auf den Gerätetyp beinhalten, da ein Angreifer mit dieser Information gezielter nach Sicherheitslücken suchen kann. Der Gerätename ist meist voreingestellt und muss geändert werden. Gleiches gilt im Übrigen auch für WLAN Router selbst.

Eine regelmäßige Datensicherung ist auch bei mobilen Geräten wichtig, um bei einem Systemabsturz oder Ausfall nicht alle Daten zu verlieren. Auch der Internetzugang sollte nur dann aktiviert werden, wenn er auch genutzt wird.

7.3 Apps aus sicheren Quellen

Die Anzahl nützlicher Apps wächst sehr schnell. Als Quelle sollten nur vertrauenswürdige App-Stores genutzt werden. Es ist aber zu bedenken, dass sich auch hier vermehrt Schadprogramme einschleichen können, auch wenn die Anbieter Gegenmaßnahmen ergriffen haben. Vor dem Herunterladen der Apps sollte man sich genau ansehen, auf welche Funktionen die Apps zugreifen. Häufig sind Standortabfrage und Zugriff auf das Adressbuch automatisch eingestellt. Foren und Testberichte im Internet liefern weitere Informationen.

7.4 Gefahr bei Verlust

In einem verschlüsselten WLAN Netzwerk wird ein gemeinsamer „Pre-Shared Key" (vorher vereinbarter Schlüssel) genutzt, um die Vertraulichkeit der Kommunikation zu gewährleisten. Geht ein mobiles Endgerät aus diesem Netzwerk verloren, so kann auch der Schlüssel in falsche Hände geraten. Das wiederum kann einen unbefugten Zugriff auf das Firmennetzwerk zur Folge haben.

7.5 Sensibilisierung als wichtigster Faktor

Neben allen technischen und organisatorischen Vorkehrungen sollte man die Mitarbeiter für einen sicherheitsorientierten Umgang mit Unternehmensdaten sensibilisieren. Die Einführung von Sicherheitsrichtlinien für mobile Geräte ist hier das Ziel.

Darauf ist beim Einsatz mobiler Endgeräte zu achten:

- Sichere Konfiguration, Nutzung der vorhandenen Sicherheitsfunktionen
- Verschlüsselung sensibler Daten
- Verwendung komplexer Passwörter
- Sperren bei Inaktivität
- Löschen bei Verlust
- automatische Update-Funktion nutzen
- Sensibilisierung für Umgang mit Geräten und Daten
- Mögliche Gefahren müssen kommuniziert werden
- entsprechende Abwehrmaßnahmen sind einzusetzen

Autoren: Helmuth Hilse, Lars Nöcker und Thomas Reiche, MGID Mitteldeutsche Gesellschaft für Informationssicherheit und Datenschutz mbH (Version V 1.0, August 2012)

Ansprechpartner

Industrie und Handelskammer zu Leipzig
Goerdelerring 5 | 04109 Leipzig
Geschäftsbereich Dienstleistungen
Abteilung Unternehmensförderung
Jenny Krick
Telefon 0341 1267-1176
Telefax 0341 1267-1420
E-Mail krick@leipzig.ihk.de