Informationsbroschüre

Informationsbroschüre für Einsteiger

IT-Sicherheit: Themenfokus Sicheres Mobiles Arbeiten

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

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Netzwerk Elektronischer
Geschäftsverkehr

Herausgeber
E-Commerce-Center Handel, Köln

E-Commerce-Center Handel

Text und Redaktion
Sonja Rodenkirchen,
ECC Handel –
E-Commere-Center Handel, Köln

Andreas Duscha,
ECC Handel, Köln

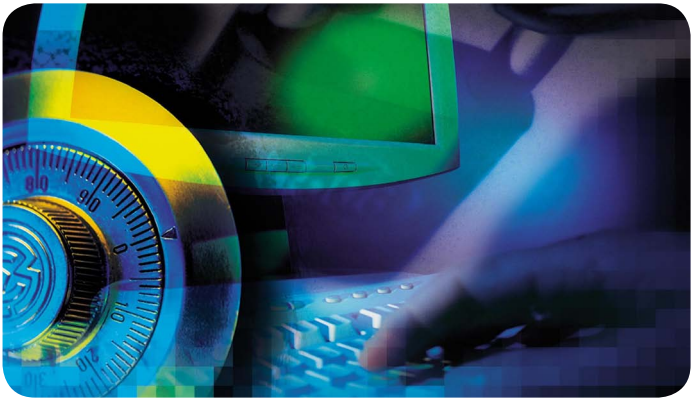
Judith Halbach,
ECC Handel, Köln

Grafische Konzeption und Gestaltung
Christian Bähr,
ECC Handel, Köln

Bildquelle
www.fotolia.de

Stand
April 2011

Inhalt



Die Relevanz von sicherem mobilen Arbeiten

Einleitung

Durch die Entwicklung neuer, kleiner und praktischer Notebooks, Smartphones und Wechseldatenträger sowie die flächendeckende Verfügbarkeit von drahtlosen Internetverbindungen, werden mobiles Arbeiten und komfortabler Datenaustausch immer leichter. Gleichzeitig wächst jedoch die Gefahr, dass Daten verloren gehen oder unbemerkt geklaut, überspielt oder manipuliert werden. Die Täter können dabei sowohl unternehmensexterne als auch -interne Personen sein. So können externe Täter beispielsweise Vertrauen zu Mitarbeitern aufbauen und sogenannte „Malware“ (von engl. „malicious software“ – schädliche Software) auf Computern platzieren oder Daten entwenden. Zur internen Täterschaft gehören sowohl Personen, die gezielt ihr Wissen einsetzen, um dem Unternehmen zu schaden, als auch Personen, die durch Unwissen oder Nachlässigkeit Gefahren erzeugen oder Daten sowie Datenträger verlieren. Diese Broschüre klärt Sie über die Gefahren des mobilen Arbeitens auf und gibt Ihnen nützliche Tipps an die Hand, um Risiken zu minimieren.

Wussten Sie schon, dass...

- ... 22 Millionen Deutsche bereits mindestens einmal Opfer eines Computervirus wurden und mehr als 15 Millionen Euro der erwartete Schaden durch Phishing und Betrug beim Online Banking sind?
- ... der Schaden, der der deutschen Wirtschaft pro Jahr durch Computerkriminalität entsteht, in den zweistelligen Milliardenbereich geht?
- ... sich die Höhe des verursachten Schadens bei KMU in drei Viertel der betroffenen Fälle auf weniger als 50.000 Euro beläuft – ein Betrag, der für Unternehmen dieser Größenordnung aber bereits schmerzhafte Verluste darstellt?
- ... Google kürzlich über 50 Apps für sein mobiles Betriebssystem Android, die Malware auf Smartphones bringen können, gelöscht hat?
- ... 70 Prozent der Unternehmen in erster Linie ehemalige Mitarbeiter oder Insider als Risikogruppe für den Datenklau nennen?

Notebooks und Netbooks

Der Einsatz von Notebooks oder Netbooks (die preiswertere und einfacher ausgestattete Variante eines Notebooks) ist ausgesprochen praktisch: Auch unterwegs oder auf Geschäftsreisen ist Arbeiten wie gewohnt möglich. Auf den Geräten befinden sich jedoch meistens sensible Daten, die nicht an die Öffentlichkeit beziehungsweise in falsche Hände gelangen dürfen. Dies könnte auf drei Arten geschehen: Durch den gezielten Diebstahl von einzelnen Daten, den Diebstahl des kompletten Geräts oder durch das Verlieren des Geräts. Es empfiehlt sich daher einige Sicherheitsmaßnahmen zu ergreifen.

Erstellen Sie ein Systemkennwort – das erschwert Unbefugten den Zugang. Sie erreichen den Menüpunkt zumeist über „Start > Systemsteuerung > Benutzerkonten“. Den Passwortschutz können Sie darüber hinaus über einen integrierten oder nachträglich angebrachten Fingerabdruckscanner erhöhen. Wenn Sie das Gerät dann einmal für einen Moment unbeaufsichtigt lassen, sperren Sie es durch gleichzeitiges Drücken der Windows-Taste und der L-Taste. Simpel, aber effektiv gegen Diebstahl schützt ein Notebookschloss, mit dem das Gerät an unbeweglichen Gegenständen im Raum angeschlossen werden kann.

Sollte das Gerät trotz aller Vorsicht dennoch gestohlen werden, ist es gut, wenn Sie die sensiblen Daten zuvor verschlüsselt haben. Dies ist möglich mit kostenlosen Programmen wie TrueCrypt oder DiskCryptor. Sie sind benutzerfreundlich und verwenden zur Verschlüsselung den derzeit als sehr sicher geltenden Verschlüsselungsstandard AES. Dieser wird in den USA sogar für staatliche Dokumente mit höchster Geheimhaltungsstufe verwendet. Darüber hinaus befähigen Sie regelmäßige Sicherheitskopien dazu, die Daten nach einem Verlust zu rekonstruieren. Weiterführende Informationen zur sicheren Nutzung eines Notebooks finden Sie in den „IT-Sicherheitstipps: Notebook“ des Netzwerk Elektronischer Geschäftsverkehr (NEG).

Wechseldatenträger

Wechseldatenträger sind aus dem Arbeitsalltag sowie aus dem Privatleben nicht mehr wegzudenken. Damit gemeint sind austauschbare und tragbare Datenträger, die neben der Festplatte im Computer zur zusätzlichen Speicherung von Daten dienen. Dazu zählen USB-Sticks sowie optische Datenspeicher wie CD-ROM und DVD. Mit ihnen können Daten leicht transportiert und getauscht oder auch Sicherheitskopien anfertigt werden. Sie bergen allerdings auch Gefahren. Da sie so klein sind, können sie leicht verloren gehen oder gestohlen werden. Sie werden außerdem ihrem Ruf als „Virenschleudern“ gerecht (das trifft vor allem für USB-Sticks zu), da sie schnell infiziert werden können und die Malware dann an alle Computer weiter verbreiten, an die sie angeschlossen werden.

Wenn Sie jedoch einige Sicherheitsrichtlinien einhalten, können Sie die Risiken, die von Wechseldatenträgern ausgehen, deutlich minimieren. Zunächst sollten die auf dem Wechseldatenträger befindlichen Informationen verschlüsselt werden. Manche USB-Sticks sind hierfür von Werk aus mit speziellen Bauteilen ausgestattet, bei anderen kann man dafür eine Software verwenden. Hierbei gibt es sowohl kommerzielle Angebote, als auch kostenlose Software, wie beispielsweise TrueCrypt oder DiskCryptor. Außerdem sollten Sie für Ihren USB-Stick ein sicheres Passwort erstellen (Weiterführende Informationen zur sicheren Passwortwahl finden Sie in den „IT-Sicherheitstipps: Sicherer Umgang mit Wechseldatenträgern“ des NEG). Weiterhin sollten Sie darauf achten, dass die Sicherheitssoftware Ihres Computers auf dem neusten Stand ist. Häufig wird Malware verteilt, die auf neue Sicherheitslecks abzielt und sich anschließend über das gesamte Unternehmensnetzwerk ausbreitet. Um dies zu verhindern, sollte Ihr Virenscanner ständig aktualisiert werden. Die Vergabe beschränkter Nutzerrechte ist darüber hinaus hilfreich, da sich Malware dadurch auch nur beschränkt ausbreiten kann. Schließlich sollten Sie die mobilen Datenträger sowohl beim Eingang (wenn Sie die CD-ROM einlegen oder den USB-Stick anschließen), als auch beim Ausgang auf Malware überprüfen.

Darüber hinaus ist es wichtig, dass Sie Ihre Wechseldatenträger richtig behandeln, damit die darauf befindlichen Daten nicht zerstört werden. Dazu gehört die richtige Lagerung (trocken, keine starken Temperaturunterschiede, keine direkte Sonneneinstrahlung), die Beschriftung nur mit speziellen Stiften (da sonst Kratzer oder Lösungsmittel die Reflexionsschicht beschädigen können und die Daten nicht mehr lesbar sind)

sowie das Fernhalten von magnetischen Wechselmedien (wie externe Festplatten) von anderen magnetischen Komponenten (wie Lautsprecher). Sollten Sie die Daten willentlich entfernen wollen, reicht es nicht aus, sie einfach zu löschen. Dies käme lediglich dem Löschen eines Inhaltsverzeichnisses gleich. Stattdessen sollten Sie spezielle Software nutzen, wie beispielsweise die kostenlosen Angebote von Eraser, CBL Daten-Shredder, Secure Eraser und Darik's Boot and Nuke (DBAN). Zuletzt sollten Sie auf dem Wechseldatenträgern immer nur Kopien speichern, damit die Daten im Falle des Verlusts des Wechseldatenträgers immer noch vorhanden sind.

Handys und Smartphones

Auch auf Handys und insbesondere auf Smartphones werden wichtige und sensible Daten gespeichert und diese können, ebenso wie Notebooks und Wechseldatenträger, manipuliert und infiziert werden. Im Falle des Verlusts der Daten, drohen hohe wirtschaftliche Schäden (durch den Verlust von Kontakten und Informationen) sowie finanzielle Schäden (möglicherweise wird ein infiziertes Gerät für Telefonate oder zum Ausführen kostenpflichtiger Programme benutzt). Unseriöse Apps (kurz für Applikationen; damit sind kleine Programme für Smartphones gemeint) können darüber hinaus Funktionen aktivieren oder Daten speichern, die für die Nutzung der Dienste eigentlich nicht notwendig sind.

Echte Handy-Viren sind zwar selten und die Gefahren für herkömmliche Handys sind eher gering, denn für SMS oder MMS gibt es eindeutige Protokolle und abweichende Nachrichten werden von den Netzbetreibern rausgefiltert. Sehr gefährdet sind jedoch Smartphones. Sie besitzen diverse Kommunikationsschnittstellen wie Bluetooth, E-Mail,

Speicherkarten und mobiles Internet. Dadurch sind sie den gleichen Risiken ausgesetzt wie die oben beschriebenen Geräte und sollten auch mit der gleichen Sorgfalt behandelt werden. So sollten Sie nur vertrauenswürdige Software oder Apps installieren. Informieren können Sie sich hierüber zum Beispiel durch Erfahrungsberichte im Internet. Des Weiteren sollten Sie einen Virenscanner auch auf Ihrem Smartphone installieren. Diese werden von den bekannten Herstellern für PC-Virenscanner wie beispielsweise Avira oder McAfee auch für Smartphones angeboten. Sie müssen, wie auch die Firmware (also das Betriebssystem) regelmäßig aktualisiert werden, um Sicherheitslücken zu vermeiden. Fremde Speicherkarten sollten Sie nicht ohne vorherige Malware-Prüfung einlegen.

Darüber hinaus sollten Sie die Verbindungsmöglichkeiten des Smartphones kontrollieren und Bluetooth, UMTS, WLAN etc. nur einschalten, wenn sie benötigt werden. Es ist ebenfalls unerlässlich, dass Sie die Sicherheitseinstellungen aktivieren, wie beispielsweise den Kennwortschutz. Bei besonders sensiblen Daten sollten Sie eine Verschlüsselung in Betracht ziehen, auch hierfür gibt es, wie oben angeführt, spezielle Programme.

Das Internet

Über ein WLAN (Wireless Local Area Network) hat man mit mobilen Endgeräten wie Smartphones oder Notebooks immer bequemen Zugang zum Internet. Ein kritischer Aspekt ist dabei jedoch die Sicherung und Verschlüsselung des mobilen Netzwerks. Jeder, der ein WLAN betreibt, ist dafür verantwortlich, dass dieses vor dem unberechtigten Zugriff Dritter geschützt ist. Sonst drohen empfindliche Strafen, wenn andere das Netzwerk für illegale Zwecke nutzen, etwa um Musik herunter zu laden. Weiterhin

sollten Sie sich darüber bewusst sein, dass Ihre Aktionen einfach „mitgelesen“ werden können, wenn Sie sich in das ungeschützte Netzwerk eines anderen einwählen. Ein WLAN sollte daher idealerweise mit einer WPA2-Verschlüsselung, zumindest aber mit einer WPA-Verschlüsselung geschützt werden. Eine WEP-Verschlüsselung ist nicht zu empfehlen, da diese mittlerweile binnen einer Minute zu knacken ist. Möglicherweise ist für die Verwendung einer WPA2-Verschlüsselung die Aktualisierung Ihres Betriebssystems notwendig. Informationen zur Verwendung einer WPA2-Verschlüsselung mit älteren Geräten finden Sie auf den Internetseiten der Hersteller. Darüber hinaus sollten Sie für die Verschlüsselung ein starkes Kennwort verwenden (mindestens 13 Stellen lang, sinnfrei zusammengesetzt und aus Zahlen, Zeichen und Sonderzeichen wie „!“ oder „$“ bestehend), um sich vor Missbrauch zu schützen. Wenn Sie schließlich sensible Daten (beispielsweise mit Kunden) über das Internet austauschen, sollten Sie dafür eine verschlüsselte Methode verwenden, wie beispielsweise VPN oder SSL. Weiterführende Informationen zur sicheren Nutzung des Internets finden Sie in den „IT-Sicherheitstipps: Sicherer Umgang mit dem Internet“ des NEG.

Fazit

Mobiles Arbeiten mit Notebooks, Smartphones und portablen Speichermedien ist seit einigen Jahren auf dem Vormarsch. Nicht immer sind jedoch die damit verknüpften Risiken bekannt und die notwendigen Sicherheitsmaßnahmen werden nicht eingehalten. Daher müssen Mitarbeiter aufgeklärt und geschult werden, es müssen Richtlinien geschaffen und eingehalten werden. Die wichtigsten Stichpunkte in diesem Zusammenhang sind:

- Starker Passwortschutz für alle Geräte und Netzwerke,
- Verschlüsselung sensibler Daten,
- Ständig aktualisierte Malware-Schutzsoftware/Virenscanner,
- Erhöhte Aufmerksamkeit zur Vermeidung des Verlierens von Datenträgern,
- Prüfung von Wechseldatenträgern bei Eingang und Ausgang.

Quellen

- Netzwerk Elektronischer Geschäftsverkehr (NEG): IT-Sicherheitsratgeber: Passwörter,
- NEG: IT- Sicherheitstipps: Notebook,
- NEG: IT-Sicherheitstipps: Sicherer Umgang mit Wechseldatenträgern,
- NEG: IT- Sicherheitstipps: Sicherer Umgang mit dem Internet,
- NEG: Informationsbroschüre für Einsteiger: Praxisleitfaden mobile Datenträger,
- NEG: Informationsbroschüre: Sicherheit mobile Einzelarbeitsplätze,
- NEG: Informationsbroschüre: Sicherer elektronischer Geschäftsverkehr,
- NEG: Elektronischer Geschäftsverkehr in Mittelstand und Handwerk 2010,
- KPMG: e-Crime-Studie 2010 Computerkriminalität in der deutschen Wirtschaft.

Weiterführende Informationen

- http://www.kmu-sicherheit.de, Aktuelle Informationen und alle Materialien des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“
- http://www.ec-net.de/sicherheit. Online-Portal des Netzwerks Elektronischer Geschäftsverkehr

Das Verbundprojekt „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. Das Gesamtprojekt setzt sich neben dieser und zwei weiteren Einsteigerbroschüren insbesondere aus den nachfolgenden Tätigkeiten zusammen:

- Unter der Überschrift „Stammtische IT-Sicherheit" wird eine Reihe regionaler „Unternehmerstammtische" bundesweit etabliert Die kostenfreien Stammtische sind ein Forum für Dialog und Information und bilden eine Plattform für den Austausch von Unternehmern untereinander
- Die jährlich veröffentlichte Studie „Netz- und Informationssicherheit in Unternehmen" zeigt auf, wie es um die Informationssicherheit in Unternehmen bestellt ist und wie leicht unternehmensfremde Personen an Geschäftsdaten kommen können. Die kompletten Berichtsbände finden Sie zum kostenlosen Download unter: **http://www.kmu-sicherheit.de**
- Kostenfreie IT-Sicherheitsratgeber bieten insbesondere KMU neutrale und praxisnahe Hinweise und Tipps, wo Sicherheitslücken bestehen und wie mit ihnen umgegangen werden sollte. Themenschwerpunkte sind u. a. „Basisschutz für den PC", „Sicheres Speichern und Löschen von Daten", uvm. Download unter: **http://www.kmu-sicherheit.de**
- Aktuelle und neutrale Informationen zur Informationssicherheit werden Ihnen im Internet auf der Informationsplattform des NEG unter der Rubrik „Netz- und Informationssicherheit" angeboten: **http://www.ec-net.de/sicherheit**

Fachhochschule Gelsenkirchen

Sebastian Spooren

ECC E-Commerce-Center Handel

Andreas Duscha

m/e/c/k Sicherheit im Internet

Andreas Gabriel

TeleTrusT Pioneers in IT security.

Ekkehard Diedrich

SAGeG Kompetenzzentrum Elektronischer Geschäftsverkehr

Dagmar Lange (Konsortialführung)

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 Ansprechpart nern 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.

Netzwerk Elektronischer Geschäftsverkehr

ECC E-Commerce-Center Handel