# Die Gefahr aus dem Internet

E-Mails schreiben, Terminkalender pflegen, Informationen im Internet suchen, Bestellungen annehmen und verarbeiten - in den meisten Firmen geht nichts mehr ohne Computer. Die Mitarbeiter brauchen das Internet, um ihre Arbeit zu erledigen. Doch wissen die Mitarbeiter eigentlich darüber Bescheid, welche Gefahren im Internet und beim Datenschutz lauern, die der ganzen Firma gefährlich werden können?

Eine Umfrage des Branchenverbands BITKOM brachte zu Tage, dass jeder dritte Internet-Nutzer sich vor den Gefahren des weltweiten Netzes nicht schützt. Diese Nutzer verwenden keine Personal Firewall, keine Anti-Malware, gehen sorglos mit E-Mails und Links um, von der Preisgabe persönlicher Daten ganz zu schweigen. Eine aktuelle Studie der „Messaging Anti-Abuse Working Group“ ergab, dass 57 Prozent der Befragten schon einmal Spam-Mails geöffnet oder einen darin enthaltenen Link angeklickt haben. Hinter diesen Links verbirgt sich oft Schadware. Das ist nicht nur ein persönliches Problem der Mitarbeiter, sondern kann auch zur Gefahr für eine Firma werden. Ein Unternehmen braucht aufgeklärte Mitarbeiter, die die Gefahren kennen und sich und das Unternehmen dadurch schützen können.

Ein gut abgesichertes Firmennetzwerk ist der erste Schritt, aber nicht der einzige. Ein Vergleich mit dem Straßenverkehr ist hier sehr hilfreich. Ein Unternehmer würde niemanden mit einem Fahrzeug aus dem Fuhrpark fahren lassen, der keinen Führerschein hat und die Straßenverkehrsordnung nicht kennt. Eine solche 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.

**Sichere Passwörter und der Umgang damit**
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 hat ergeben, dass viele der Mitarbeiter das nicht richtig tun. Das bedeutet ein enorm erhöhtes Angriffspotenzial durch die Konkurrenz und kriminelle Organisationen. Doch selbst ein geändertes Passwort kann eine Firma nicht immer schützen. Denn viele Internet-Nutzer nutzen 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 Passwort muss heute aus mindestens zehn Stellen bestehen, aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen und keinen offensichtlichen Sinn ergeben. Erst dann ist es sicher! Eine weitere Herausforderung für den Mitarbeiter ist die Aufbewahrung von Passwörtern. Das ist umso schwerer, als das Passwort regelmäßig alle drei bis sechs Monate geändert werden sollte. Da viele Mitarbeiter

mehrere wichtige Passworte verwenden müssen, sollten ihnen Hilfestellungen, z.B. über Passwortverschlüsselungsprogramme, gegeben werden. In diesem Zusammenhang ist 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.

Doch woher weiß der Mitarbeiter über all diese Aspekte Bescheid?

**Der richtige Umgang mit dem Browser und das Verhalten beim Surfen**
Wir gehen heute davon aus, dass jeder 25. PC/Notebook eine Schadsoftware (Malware) über Software-Sicherheitslücken oder weitere Schwachstellen im Computer installiert hat, die von kriminellen Organisationen über Botnetze zentral gesteuert werden. Das bedeutet, dass die kriminellen Organisationen auf den infizierten PCs/Notebooks alles mitlesen können und unsere Computer für das Aussenden von Spam-Mails oder für verteilte Angriffe einfach nutzen können. Die Verteilung der Schadsoftware geschieht heute überwiegend über manipulierte oder falsche Webseiten. Für den Mitarbeiter, der im Internet arbeitet, bedeutet dies, dass er zusätzliche zum 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 Inhalte der Webseite, das Vorhandensein und der Umgang mit/von Werbung, ob es ein Impressum gibt, wer diese Webseite empfohlen hat, usw. Der Mitarbeiter sollte in der Regel nur auf vertrauenswürdigen Webseiten aktiven Inhalt über den Browser zugelassen. Dazu muss der Browser entsprechend eingestellt/konfiguriert sein. Der Mitarbeiter sollte wissen, dass, er wenn die Maus auf einen Link führt, 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-Angriff auf Kontodaten des EU-Emissionshandels“ hat gezeigt, dass Mitarbeiter auf solche Angriffe einfach reinfallen und damit hohe Schäden in Millionen-Höhe für Unternehmen verursachen können.

**Herausforderung Web 2.0 – Sozial Netzwerke**
Ein weiteres Beispiel sind Unternehmensdaten im Web 2.0. 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, was die Innovationsgeschwindigkeit im Unternehmen steigern kann. Dazu tragen natürlich auch 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. Auch sollte dem Mitarbeiter klar sein, dass die „Freundschaft“ im Internet, nicht die gleiche Vertrauenswürdigkeit hat, wie in der realen Welt.

**Risikofaktor E-Mail**

E-Mails sind ein weiterer großer Risikofaktor. Wir wissen von Untersuchungen und Befragungen, dass zurzeit weniger als 4 % alle E-Mail verschlüsselt werden.
Wir wissen aber auch, dass mindesten 43 % der E-Mails in Business-Prozessen verwendet werden. Aus diesem Grund sollten den Mitarbeitern im Unternehmen E-Mail-Verschlüsselungstechnologien zur Verfügung gestellt werden. Die Mitarbeiter müssen wissen, wie und - ganz wichtig - wann diese Verschlüsselungstechnologien für vertrauliche E-Mails verwendet werden sollen.

**Anforderungen des Datenschutzes**
Der Datenschutz wird zurzeit in vielen Unternehmen nicht sorgfältig umgesetzt. Die praktische Umsetzung von Maßnahmen für die Aufrechterhaltung des Datenschutzes ist durch mangelnde Vorgaben eher zufällig gut oder schlecht. Die Mitarbeiter kennen oft die Anforderungen des Datenschutzes nicht ausreichend und gehen daher mit den persönlichen Daten ihrer Kunden nicht angemessen um. Damit riskieren die Firmen einen großen Reputationsschaden.

**Der aufgeklärte Mitarbeiter**
Ein aufgeklärter Internetnutzer weiß die Vertrauenswürdigkeit von Webseiten einzuschätzen. Er geht sicher, dass die automatischen Updates des Computers eingeschaltet sind, dass der Virenscanner aktualisiert wird, die Personal Firewall aktiv ist, er weiß um die Gefahr von Phishing-Angriffen und kann diese erkennen, verschlüsselt sensible Mails und nutzt sichere Passwörter. Außerdem kennt der aufgeklärte Mitarbeiter die Datenschutzanforderungen und kann sie vertrauenswürdig umsetzen.

Dazu müssen die Mitarbeiter im Unternehmen für einen richtigen, bewussten Umgang mit Computern 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.

Weitere Hinweise:
Buch: Sicher im Internet: http://www.internet-sicherheit.de/buch-sicher-im-internet/
Der Marktplatz IT-Sicherheit: https://www.it-sicherheit.de/

Der Autor:
Prof. Dr. Norbert Pohlmann ist Geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen.
https://norbert-pohlmann.com/