Netzwerk Elektronischer Geschäftsverkehr

Fachhochschule Gelsenkirchen

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

IT-Sicherheitstipp: Beschäftigte für IT-Sicherheit sensibilisieren

Eine Kette ist nur so stark wie ihr schwächstes Glied **- eine alte Binsenweisheit und dennoch so aktuell wie nie zuvor. Obwohl die meisten Gefahrenquellen für Unternehmen mit IT-Anwendungen quantitativ gesehen außerhalb der betriebsinternen Netzwerkumgebung liegen, besteht eine weitaus größere Bedrohung der Informationssicherheit im Inneren Ihres Unternehmens: Die Beschäftigten. Laut der *RSA-Studie Gefahrenbarometer 2010 - Sicherheitsrisiken für den deutschen Mittelstand* glauben rund 58 Prozent der befragten Unternehmen, dass der leichtfertige Umgang von Mitarbeitern mit Sicherheitsstandards die größte Bedrohung für IT und Telekommunikation darstellt. Neben technischen Sicherheitsvorkehrungen der betrieblichen IT-Umgebung ist es für Unternehmer ebenso wichtig, ein gemeinsames Bewusstsein für IT-Sicherheit innerhalb der Belegschaft herzustellen. In diesem Sicherheitstipp erfahren Sie, wie Sie Ihre Beschäftigten für IT-Sicherheit sensibilisieren, um Sicherheitslücken Ihres Unternehmens schließen zu können.**

Kontrollieren Sie nicht - ermutigen Sie

Werden Unternehmen Opfer einer Phishing- oder Hacking-Attacke, beruht das selbstverständlich meist nicht auf den Absichten der eigenen Beschäftigten. Ganz im Gegenteil: Meist steht bei den eigenen Beschäftigten Hilfsbereitschaft, Gutgläubigkeit, Neugierde, Konfliktvermeidung und der Respekt vor Autoritäten im Vordergrund, wenn es einem Kriminellen gelingt an betriebsinterne Informationen zu kommen. Das Vorgehen der Datendiebe ähnelt sich dabei oft: Ein Beispiel ist das Auslegen eines präparierten USB-Sticks auf dem Firmenparkplatz. Schadprogramme, die sich auf dem Stick befinden, können nach dem Einstecken am Computer automatisch ausgeführt werden und dem Angreifer Zugriff auf die Daten und das gesamte Firmennetzwerk ermöglichen. Passwörter und Zugangscodes für das Unternehmensnetzwerk stellen die obersten Ziele der Datendiebe dar. Doch auch alle anderen – scheinbar unwichtigen – Daten können Hackern zum Zwecke der Wirtschaftskriminalität dienen.

Für alle sicherheitsrelevanten Maßnahmen der Geschäftsführung gilt: **Bilden Sie ein gemeinsames Bewusstsein für IT-Sicherheit**, denn jeder trägt mit seinem richtigen Handeln zur IT-Sicherheit bei.

Werden Sicherheitsregularien von Ihren Beschäftigten lediglich als autoritäre Kontrolle empfunden, so werden diese auch öfter missachtet. Ein Beispiel: Trotz der Tatsache, dass in Deutschland knapp die Hälfte der Unternehmen ihren Beschäftigten die Nutzung von Sozialen Medien (z.B. Erfahrungsaustausch mit anderen Unternehmen) während der Arbeitszeit verbietet, widersetzt sich jeder dritte Arbeitnehmer gegen diese Bestimmung. Ein Grund hierfür dürfte vor allem mangelndes Verständnis der Beschäftigten sein, da viele Chef-Etagen schlichtweg die Aufklärung über ihre Maßnahmen vernachlässigt haben. **Wecken Sie Verständnis für getroffene Sicherheitsmaßnahmen**, damit alle Beschäftigten verinnerlichen, dass die Einhaltung von sicherheitsrelevanten Maßnahmen wertvoll und notwendig sind, auch wenn sie manchmal Bequemlichkeit kosten.

Schließen Sie Sicherheitslücken in der externen Kommunikation

In der externen Kommunikation Ihrer Beschäftigten mit Geschäftspartnern, Kunden oder Interessierten liegt das größte Risiko für die Informationssicherheit Ihres Unternehmens. Beschäftigte wissen oft nicht, welche Informationen sie an welche Dialogpartner weitergeben dürfen. Um Irritationen in der Belegschaft zu vermeiden, sollten Sie einige **Richtlinien für die unterschiedlichen Kommunikationskanäle der externen Kommunikation festlegen.**

Untersuchen und dokumentieren Sie zunächst, welche Informationen für Ihren jeweiligen Geschäftspartner oder Kunden überhaupt relevant sind. Auf diese Weise erstellen Sie ein Raster für Ihre externe Unternehmenskommunikation, an dem sich Ihre Beschäftigten in Zukunft orientieren können. **Wichtig ist, dass für jeden externen Dialogpartner genau eine Kontaktperson festgelegt wird, mit der Ihre Beschäftigten in Zukunft kommunizieren sollen.** Es ist natürlich unumgänglich, dass Ihre Beschäftigten auch mit unbekannten Personen kommunizieren, wenn sie ein Anliegen an das Unternehmen herantragen. In diesen Fällen sollten Ihre Beschäftigten stets das Anliegen des Unbekannten hinterfragen und nur so viele Informationen preisgeben wie nötig. **Machen Sie Ihren Beschäftigten klar, dass keine Nachteile für Sie entstehen können, wenn sie einmal die Herausgabe von Betriebsinterna verweigern.**

Denn es gilt die Maxime: Sicherheit vor Höflichkeit. Die Annahme, dass Beschäftigte auf niedrigen Hierarchieebenen keine Angriffe durch soziale Manipulation, sogenanntes „Social Engineering“ (siehe: Informationsbroschüre mit Hintergrundinfos *„Gefahr durch Social Engineering“* [1]) wie Phishing E-Mails befürchten müssten, ist falsch. Ganz im Gegenteil: Zahlreiche Angriffe richten sich gegen Beschäftigte mit geringen Befugnissen, weil das Bewusstsein für IT-Sicherheit hier oft nicht besonders ausgeprägt ist. Ein einzelner Account kann dem Angreifenden dann schnell als Pforte für das gesamte Unternehmensnetzwerk dienen.

Sinnvollerweise sollten Sie für Ihre gesamte Unternehmenskommunikation bestimmte **Kommunikationskanäle (E-Mail, Telefon, Fax, Brief) für bestimmte Prozesse festlegen (beispielsweise für Terminabsprachen).** Definieren Sie hierzu **verschiedene Vertraulichkeitsstufen** für Ihre Daten.

Beschäftigte erkennen anhand der Einstufung, wie vertraulich betreffende Informationen sind und nutzen dann unter Berücksichtigung der Sicherheitsbestimmungen den hierfür vorgesehenen Kommunikationskanal: Vertragsangelegenheiten etwa könnten in Zukunft nur auf postalischem Wege geklärt werden. Auf diese Weise kann zum Beispiel die Herausgabe sensibler Unternehmensdaten via unverschlüsselter E-Mail verhindert werden.

Sorgen Sie für Sicherheit im Büroalltag

Innerbetriebliche Sicherheitsmaßnahmen für den Datenschutz werden oft vernachlässigt. Viele Beschäftigte unterschätzen die Gefahren, die während des Büroalltags entstehen können. So kann sich ein scheinbar harmloser Handwerker, der *nur eben schnell in Ihrem Büro etwas reparieren muss*, im Nachhinein als krimineller Datendieb entpuppen. **Wie auch in der externen Unternehmenskommunikation sollten Sie und Ihre Beschäftigten unbekannte Personen im Auge behalten und jedes Anliegen hinterfragen.** Kann sich ein Unbekannter nicht entsprechend als Handwerker ausweisen, so sollten ihre Beschäftigten im Zweifelsfall mit dem betreffenden Handwerksbetrieb Kontakt aufnehmen und dort mit dem Beauftragten Rücksprache halten. Es sollte stets vermieden werden, Fremden Zugang zu nicht besetzten Büroräumen zu gewähren. Auch sollte jeder Beschäftigte darauf achten, sein **Benutzerkonto zu *sperren***, sobald er seinen Arbeitsplatz verlässt (Für *Windows: Windows-Taste + L*). Natürlich sollten Ihre Beschäftigten im Vorfeld ein **sicheres Benutzerkennwort** erstellt haben (siehe: IT-Sicherheitstipp und Hintergrundinfos *Passwort sicher erstellen* [1]).

Alle Beschäftigter sollten **sorgsam mit mobilen Datenträgern** wie CDs, USB-Sticks oder externen Festplatten umgehen und **niemals unbekannte Geräte an ihren Arbeits-PC anschließen,** da sie eventuell Schadsoftware enthalten können. Alle **vertraulichen Dokumente**, die nicht mehr benötigt werden, **sollten nicht im Papierkorb landen, sondern in dem Aktenschredder vernichtet werden.**

Generell ist es wichtig, sich in einer sicheren Arbeitsumgebung zu bewegen. Dies gilt für den Online- als auch für den Offline-Bereich. **Appellieren Sie an Ihre Beschäftigten, dass sie niemals wichtige Dokumente offen auf Ihrem Schreibtisch liegen lassen sollen, sondern diese bestenfalls verschlossen aufbewahren.**

Nutzen Sie den Einfluss von Sozialen Medien für Ihr Image

Die Präsentation Ihrer Beschäftigten in der Öffentlichkeit prägt das Bild Ihres Unternehmens. Auch die beste Unternehmenskommunikation kann durch das Fehlverhalten Ihrer Beschäftigten mit der Öffentlichkeit zunichte gemacht werden. Gerade im Bereich der Sozialen Medien scheint es, als würden viele Beschäftigten recht freizügig über ihren Büroalltag berichten, so dass das Image der betreffenden Unternehmen beschädigt wird. Auch Betriebsinterna gelangen auf diese Weise häufig an die Öffentlichkeit. Die Konsequenz hieraus muss jedoch nicht unbedingt ein Verbot der Nutzung sozialer Netzwerke sein, da der Bereich der Sozialen Medien durchaus auch Vorteile für Unternehmen bietet. Sie als Unternehmer sollten versuchen, gemeinsam mit Ihren Beschäftigten einen **Leitfaden zu entwickeln, inwieweit Informationen, die das Unternehmen betreffen, bedenkenlos publiziert werden können**. Möglich erscheint auch eine Trennung von geschäftlicher und privater Nutzung von sozialen Netzwerken durch verschiedene Benutzerprofile oder veränderte Privatsphäre-Einstellungen. **Schaffen Sie ein gemeinsames Interesse für eine gelungene Außenwirkung** Ihres Unternehmens, das in der Rückwirkung wieder positiv auf die Beschäftigten zurückfällt.

Auch bei Terminen im Außendienst oder bei Messeveranstaltungen sollten sich die **Beschäftigten an Datensicherheitsbestimmungen orientieren können**, damit keine Betriebsinterna unbeabsichtigt an Wettbewerbskonkurrenten weitergegeben werden.

Falls Sie oder Ihre Beschäftigten mit einem Laptop von unterwegs aus arbeiten, **sollten Sie auf einen geeigneten Sichtschutzfilter achten**, um das Ausspähen Ihrer Daten durch Unbefugte zu verhindern (siehe: IT-Sicherheitstipp und Hintergrundinfos *Sicherheit für Ihr Notebook [1]*).

Konfrontieren Sie Ihre Beschäftigten regelmäßig mit dem Thema *IT-Sicherheit* mithilfe von Schulungen, Flyern, Broschüren und Sicherheitstipps. Nur wer aktuelle Sicherheitstrends berücksichtigt, kann langfristig dafür sorgen, dass erst gar keine Sicherheitslücken entstehen. Ein gemeinsames Bewusstsein für Informationssicherheit stärkt das Teamgefühl und ist der Schlüssel zu einem sicheren Unternehmensnetzwerk.

Autoren:

Malte G. Schmidt, FH Gelsenkirchen, Institut für Internet-Sicherheit

Dipl.-Inform.(FH) Sebastian Spooren, FH Gelsenkirchen, Institut für Internet-Sicherheit

B.Sc. Deborah Busch, FH Gelsenkirchen, Institut für Internet-Sicherheit

Prof. Dr. (TU NN) Norbert Pohlmann, FH Gelsenkirchen, Institut für Internet-Sicherheit

Weiterführende Informationen:

[1] http://ratgeber.it-sicherheit.de

http://www.ec-net.de

https://www.it-sicherheit.de

http://www.kmu-sicherheit.de

http://www.bsi.bund.de

Bildquelle: © pressmaster – Fotolia.com

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 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. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Fachhochschule Gelsenkirchen, Institut für Internet-Sicherheit - if(is)

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Dr. (TU NN) Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: http://www.internet-sicherheit.de

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt 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. Alle Details finden Sie unter: http://www.kmu-sicherheit.de