IT-Sicherheitstipp: Richtiger Umgang mit vertraulichen Daten

Vor ein paar Monaten erschuf der New Yorker IT-Experte Thomas Ryan ein gefälschtes Facebook-Profil einer jungen Internet-Schönheit. Drei Monate machte er sich ihre Online-Identität zu Eigen, um gezielt Kontakte zu hochkarätigen Persönlichkeiten aus Politik und Militär zu knüpfen. Hübsche Fotos und einige Chats reichten aus, um innerhalb kürzester Zeit in den Besitz hochsensibler Militärdaten zu kommen. Nachdem Ryan sein Vorhaben öffentlich machte, um das Fehlverhalten der Verantwortlichen aufzuzeigen, löste er einen innenpolitischen Skandal aus - zahlreiche Entlassungen waren die Folge. Dieses Beispiel zeigt die Gleichgültigkeit vieler Angestellter in Bezug auf die korrekte Handhabe vertraulicher Unternehmensdaten. Im Falle des Datenverlustes sollte die Schuld jedoch nicht nur beim Mitarbeiter gesucht werden. Häufig wird auf der Chefetage nicht festgelegt, wie sich etwa die Mitarbeiter in sozialen Netzwerken bewegen sollten. Studien ergaben, dass in 25 Prozent aller Fälle Mitarbeiter eines Unternehmens vertrauliche Daten unwissend weitergeben würden [1].

Auch die beste Sicherheitstechnik nützt nichts bei leichtfertigem Umgang mit vertraulichen Daten. Erfahren Sie in diesem IT-Sicherheitstipp, wie Sie die Sicherheit ihrer Daten durch kleine Verhaltenstipps deutlich erhöhen können.

Zunächst einmal soll geklärt werden, welche Daten in der Informationstechnologie überhaupt mit dem Attribut „vertraulich“ bezeichnet werden. Nach Meinung vieler Datenschützer sind **Sozialdaten (z.B. Renten- oder Krankenversicherungsnummer), Finanzdaten, Betriebs- und Geschäftsgeheimnisse sowie Personaldaten als besonders schützenswerte Informationen anzusehen.**

Je nach Verwendungszweck sollte diese Auflistung jedoch im Beruflichen und Privaten noch durch Positionen ergänzt werden.Viele Unternehmen legen beispielsweise fest, welche personenbezogenen Informationen nur auf dem Postwege an Kunden verschickt werden dürfen, sofern Sie nicht mittels verschlüsselter E-Mail-Kommunikation ausgetauscht werden können. Ein Beispiel für eine einheitliche Regelung geben Banken: Sie können sicher sein, dass Ihre

Zugangsdaten für das Online-Banking keinesfalls via E-Mail von ihrer Bank an Sie verschickt werden oder Ihre Bank Sie auffordert diese plötzlich einzugeben.

Falls noch nicht geschehen, **sollten Sie eine Klassifizierung aller betrieblichen Informationen vornehmen**. Überlegen Sie dazu, welchen Nutzen Dritte aus den jeweiligen Daten ziehen könnten und bewerten Sie danach die Schwere eines möglichen Verlusts. Daraus resultieren **Vertraulichkeitsstufen für Informationen**. Je nach Vertraulichkeitsstufe sollten dann verschieden sichere Kommunikationskanäle für den direkten Kontakt mit Kunden, Geschäftspartnern und unbekannten Personen gewählt werden. Falls Sie sich aus Kostengründen dazu entschließen, bestimmte sensible Daten via E-Mail auszutauschen, so sollten Sie hier stets nur verschlüsselte E-Mails versenden. Hinweise hierzu erhalten Sie im IT-Sicherheitstipp *„Sicherer Datenaustausch via E-Mail“* [1].

Bestenfalls sollten Sie im Betrieb zudem Kontaktpersonen für Ihre Kunden festlegen und sie besonders für das Thema Datensicherheit sensibilisieren.

Wichtigste Grundvoraussetzung: Sichere Passwörter

Wurden die meisten sensiblen Dokumente eines Unternehmens vor ein paar Jahrzehnten noch in großen, verschließbaren Wandschränken aufbewahrt, so lagern sie heutzutage meist in digitaler Form auf den Unternehmensservern. Passwörter zum Intranet ersetzen nun die zahlreichen Türschlüssel der Mitarbeiter. Aus diesem Grunde ist die **Erstellung sicherer Passwörter für alle sensiblen Daten eine unabdingbare Grundvoraussetzung im E-Business und auch im privaten Bereich.** Wie Sie sichere Passwörter erstellen und aufbewahren können, entnehmen Sie dem IT-Sicherheitstipp *„Passwort sicher erstellen“* und der „NEG-Awareness-TV“- Folge *„Wie erstelle ich ein sicheres Passwort?“* [1]. Neben dem Benutzerkonto und Netzwerkzugang sollten auch mobile Datenträger und Festplattenpartitionen mit sensiblem Inhalt einen besonderen Schutz erhalten. Nutzen Sie hierzu spezielle Software, um schützenswerte Inhalte zu verschlüsseln und mit einem Passwort zu versehen (siehe hierzu IT-Sicherheitstipp *„Sicherheitstipps für Ihr Notebook“* [1]).

Sensibilisieren Sie Ihre Beschäftigten für das Thema IT-Sicherheit

Auch wenn Sie nur für kurze Zeit Ihren Arbeitsplatz verlassen, sollten Sie stets Ihren PC sperren (bei *Windows*: *„Windows-Taste“* + *„L“*). Kriminellen genügen oft nur wenige Minuten Unachtsamkeit, um verheerenden Schaden anzurichten. In diesem Zusammenhang steht auch die Gefahr durch Social Engineering, die eine der größten Bedrohungen für die Sicherheit eines jeden Unternehmensnetzwerkes darstellt. Hier ein Beispiel aus der Broschüre *„Gefahr durch Social Engineering“*, herausgegeben vom *Netzwerk Elektronischer Geschäftsverkehr*:

„Ein Anrufer erhält von der hilfsbereiten Telefonistin in der Zentrale durch die Nennung eines Namens die Information, dass sich dieser Mitarbeiter noch mindestens zwei Stunden in einem

wichtigen Meeting befindet und nicht gestört werden möchte. Mit dieser Information meldet sich der Anrufer nun bei einem anderen Kollegen im Unternehmen und bezieht sich dabei auf ein erfundenes Telefonat mit dem Mitarbeiter aus dem Meeting, um bestimmte Informationen (z.B. den Marketingplan) zu erschleichen. Dabei gibt er an, dass er dies mit dem Mitarbeiter aus dem Meeting besprochen hat und bereits seit einer Stunde auf den Marketingplan wartet und diesen nun sehr dringend benötigt oder andernfalls die geplante Marketingkampagne abgesagt werden muss. Rückt der angerufene Mitarbeiter die Informationen zunächst nicht raus, droht ihm der Anrufer zumeist mit Ärger durch seinen Vorgesetzten. „Wollen Sie verantwortlich dafür sein, dass die Marketingkampagne für Ihr neues Produkt im nächsten Monat nicht startet?“. Der Mitarbeiter fühlt sich dabei bereits stark unter Druck gesetzt und gibt die gewünschte Information preis.“

Ähnliche Erfahrungsberichte von Social-Engineering-Opfern häufen sich. Daher sollten Sie Ihren Beschäftigten das Bewusstsein für IT-Security näher bringen. **Setzen Sie sich zum Ziel, den Leitspruch „Sicherheit vor Höflichkeit“ in Ihrem Betriebsalltag stets nachzukommen.** Wichtige Hinweise für den Schutz gegen das Ausspähen von Unternehmensdaten finden Sie im IT-Sicherheitstipp *„Mitarbeiter für das Thema IT-Sicherheit sensibilisieren“* und in der NEG-Awareness-TV-Folge *„Wie schütze ich mich vor Phishing?“* [1]. Beachten Sie auch die Praxistipps *„IT-Sicherheit – Faktor Mensch“* [2].

Schützen Sie Ihren mobilen Arbeitsplatz

Die Absatzzahlen für mobile Endgeräte wie Smartphone und Tablet-PC wachsen nahezu exponentiell: In Deutschland werden 2011 laut *Bitkom* [3] 40 Prozent mehr Smartphones verkauft als noch im Vorjahr. Auch die Verkaufszahlen der Tablet-PCs scheinen zu explodieren. *Bitkom* prognostiziert, dass sich die Verkäufe in diesem Jahr mehr als verdreifachen – der Trend hin zum mobilen Arbeitsplatz ist deutlich zu erkennen. Von immer mehr Beschäftigten wird eine ständige Erreichbarkeit erwartet. So sollen beispielsweise E-Mails auch von unterwegs aus umgehend beantwortet werden. Unter steigendem Arbeitsdruck leidet dann nicht selten die Anwendung festgelegter Sicherheitsregeln: Vertrauliche Daten werden unverschlüsselt verschickt, drahtlose Schnittstellen wie Bluetooth, Infrarot und WLAN werden nach der Benutzung nicht deaktiviert.

In Zukunft wird das Thema „Mobile Security“ daher immer bedeutsamer. Bedenken Sie stets, dass der Entwicklungsstand von Technik und Sicherheitssoftware der Smartphones noch nicht das Niveau der großen Desktop-PCs erreicht hat. Daher sollten Sie mit Bedacht vorgehen, wenn Sie mit vertraulichen Daten via Smartphone interagieren. **Lassen Sie Ihr Smartphone niemals unbeobachtet und verleihen Sie es nicht. Drahtlose Schnittstellen wie WLAN, Bluetooth und Infrarot sollten nur bei Bedarf eingeschaltet werden und nach der Benutzung stets deaktiviert werden.** Mehr Informationen zu diesem Thema finden Sie im IT-Sicherheitstipp *„Sicherheit bei mobilen Geräten“* und im NEG-Awareness-TV-Video *„Wie schütze ich mein Smartphone vor digitalen Bedrohungen?“* [1]. Weitere wichtige Hinweise erhalten Sie in der Informationsbroschüre

„*Themenfokus M-Business*“ und der Praxisbroschüre „*Mobile Sicherheit in der Praxis*“ [2].

Der Speicherort als Risikoquelle

Sicherheitslücken im Unternehmensnetzwerk entstehen manchmal schon durch die falsche Wahl des Daten-Speicherorts. Speichern Sie niemals besonders vertrauliche Daten auf einem zentralen Ablageort im Intranet – je mehr Kollegen auf Daten zugreifen können, desto größer ist die Gefahr des Datenverlusts durch Social Engineering. **Es ist sinnvoll, wenn Sie einige Verzeichnisse zusätzlich verschlüsseln und durch automatischen Backups absichern.**

Sofern Sie externe Hard- und Softwareressourcen in einem Online-Netzwerk, sprich in einer Cloud, nutzen, sollten Sie dort keinesfalls vertrauliche Daten speichern. Denn die Serversicherheit ist hier sehr stark abhängig vom jeweiligen Anbieter. **Informieren Sie sich im Vorfeld genau über Nutzungsbedingungen und Datensicherheit, bevor Sie Ihre Daten hochladen.** Auch hier gilt: Verschlüsseln Sie nach Möglichkeit Ihre Daten mit einer speziellen Verschlüsselungssoftware, bevor Sie sie in der Cloud ablegen. Detaillierte Handlungsempfehlungen zum Thema Cloud Computing finden Sie im IT-Sicherheitstipp „*Cloud-Dienste sicher nutzen*“ [1].

Autoren

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

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

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

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

Weiterführende Informationen:

[2] http://www.kmu-sicherheit.de

http://www.ec-net.de

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

[3] http://www.bitkom.org

https://www.internet-sicherheit.de

http://www.bsi-fuer-buerger.de

http://www.sicher-im-netz.de

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.

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

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