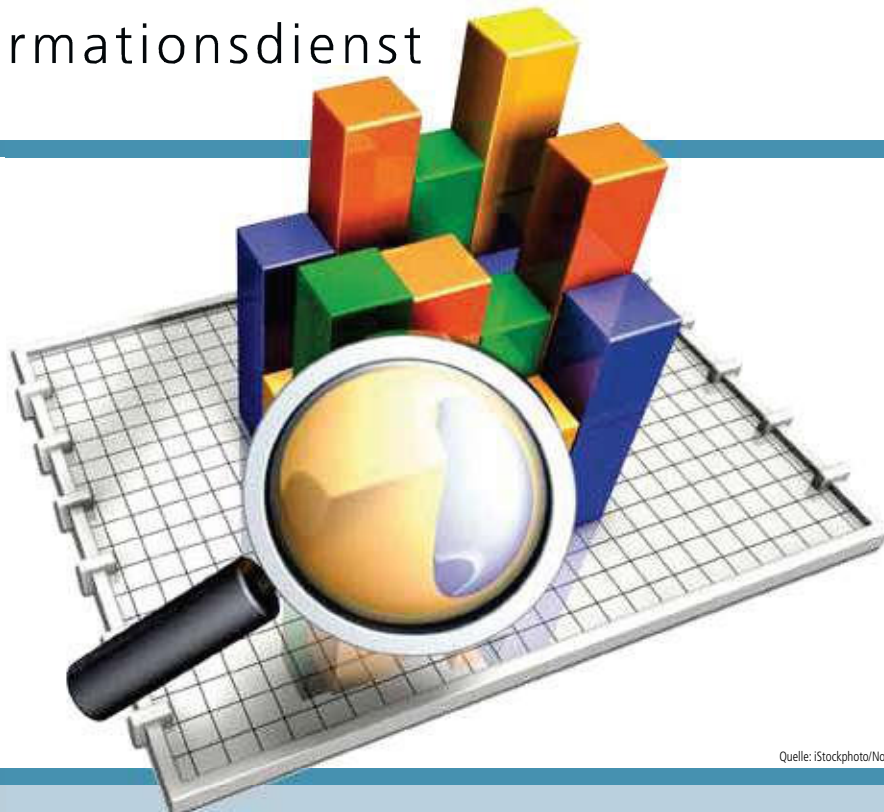


IT-Grundschutz

Informationsdienst



Quelle: iStockphoto/Norebbo

Studien und Analysen

Umfrage „IT-Sicherheitsstandards und IT-Compliance 2010“

Seite 3

NEWS

BSI stellt Eckpunktepapier zu Cloud Computing zur Diskussion Seite 2

Zahlreiche Fokus-Themen auf der it-sa 2010 Seite 2

Orientierung im Web 2.0 Seite 2

Rubriken

Editorial Seite 2

Impressum Seite 27

IT und Recht

Cloud Computing – aber sicher! Seite 17
Datenschutz beim Online-Marketing Seite 25

Studien und Analysen

Umfrage „IT-Sicherheitsstandards und IT-Compliance 2010“ Seite 3
Interview: Sicherheitsbedenken torpedieren Sicherheit Seite 21

Praxis und Anwendungen

Security-as-a-Service blockt Spam und Malware Seite 8
Empfehlungen zur Nutzung Sozialer Netzwerke Seite 14
Datenschutzverstöße sicher vermeiden Seite 28

Workshops

Airbag für Social Media Nutzung Seite 10
Transparente und sichere Datenauslagerung in der Cloud Seite 23



Der schnellste Weg zur IT-Sicherheit
it-sa Nürnberg
Die IT-Security Messe
19.-21.Okt. 2010

Kontrolliert zwitschern

Empfehlungen zur Nutzung Sozialer Netzwerke

Ralph Dombach, freier Autor und Sicherheitsadministrator, Secuteach.de

Social Networks sind eine der Kernkomponenten des Mitmach-Web 2.0. Jeder wird zum Gestalter und präsentiert sich und seine Themen im Web. Doch mit steigender Akzeptanz und Nutzung von Social Networks wächst auch deren Gefahrenpotenzial

Wie die Nutzer entdecken auch Cyberkriminelle und „kreative Verkäufer“ das Medium Social Networks als lohnendes Geschäftsfeld. Wie trickreich dabei die Methoden sind, belegen zahlreiche Fachartikel aus der jüngsten Vergangenheit¹. Fazit ist, wer heute Social Networks nutzen will, sollte sich vorab Gedanken zur Sicherheit machen. Dies gilt nicht nur für die private Nutzung, sondern auch für Unternehmen, die sich immer stärker mit der Anforderung konfrontiert sehen, einen Firmenzugang zu XING, Facebook, Twitter & Co. zu schaffen. Doch Regeländerungen an der Firewall oder dem URL-Blocker sind nur der kleinere Teil der anstehenden Aktivitäten. Wesentlich aufwendiger und vielschichtiger sind erforderliche organisatorische Änderungen, welche die Bereiche Anwender-Verantwortung, Informationstechnik, Datenschutz, Corporate Identity betreffen, um nur einige zu nennen. Vor allem die Information und Schulung der Anwender zu den vielfältigen Bedrohungen ist dabei der Schlüssel zum Erfolg. Twitter gilt aufgrund seiner hohen Reaktionsgeschwindigkeit und großen Verbreitung als besonders heißes Eisen im Firmenumfeld.

Twittern im Unternehmen

Unternehmen nutzen Twitter um Produktinformationen bereitzustellen, mit ihren Kunden zu kommunizieren und Marketing für die eigenen Produkte, die Unternehmensstrategie oder das Unternehmen selbst zu betreiben. Etablierte

Twitter-Kanäle gibt es beispielsweise von Daimler, der deutschen Bahn, Lufthansa und der Telekom. Üblicherweise wird das Management eines Twitter-Kanals im Unternehmen der Marketingabteilung oder der Unternehmenskommunikation zugeordnet. Wichtigster Punkt ist hierbei eine klare Regelung, wer das Sagen bei den veröffentlichten Beiträgen hat. Das Prinzip „Speaking to the Customer with One Voice“ hat hier höchste Priorität! Im Idealfall sind es mehrere Mitarbeiter, die sich gegenseitig vertreten und gegenüber dem Kunden die Kommunikation aufrecht halten. Ideal gelöst wurde diese Anforderung beispielsweise bei der Bahn, die die Kommunikationspartner direkt in den „Tweets“ benennt.

Ebenso nützlich ist es auch, einen Kanal-Namen zu verwenden, den der Kunde sofort mit dem Unternehmen in Verbindung bringt. Bei Twitter gilt „First Come, First Serve“ dies kann dazu führen, dass der gewünschte Name bereits vergeben ist. Analog zum „Domain-Grabbing“ geschieht dies oftmals mit der Absicht, den Namen später zu verkaufen. Allerdings geht diese Rechnung nicht immer auf, wie verwaiste Twitter-Kanäle zeigen. Die wichtigsten Empfehlungen, die man aus Unternehmenssicht beachten sollte sind:

- Einen sinnvollen, kurzen Twitter-Kanalnamen wählen
- Die Gruppe der Mitarbeiter vorab festlegen, die den Kanal mit Tweets füllt
- Gültigkeit von Warenzeichen und Copyright beachten

- Für regelmäßige Tweets sorgen
- Unternehmensspezifische Begriffe und Wortschöpfungen vor Verwendung auf Doppeldeutigkeit in Fremdsprachen überprüfen (religiöse Verstöße)
- Konsultation der hauseigenen Rechtsabteilung bezüglich der Impressumspflicht für Telemedien. Aktuell ist nicht eindeutig entschieden, ob Twitter-Kanäle ein Impressum benötigen. Siehe hierzu auch Impressumspflicht auf Twitter².
- Anpassen des Hintergrundbildes an das Corporate Design des Unternehmens
- Definieren einer Vorgehensweise zur Abarbeitung von Leser-Anfragen etc.
- Überwachen der Dinge, die in Twitter über das eigene Unternehmen gesagt werden. Dies geht über „search.twitter.com“ oder über Zusatzdienste wie Topsy und Wavematrix.

Neben diesen rein organisatorischen Hinweisen gibt es zusätzliche Sicherheits-Empfehlungen, die die Anwender selbst bei Nutzung von Twitter beachten müssen, unabhängig davon, ob der Mitarbeiter privat oder für das Unternehmen twittert.

Empfehlungen für den Twitter-Anwender

Weltweit gibt es derzeit etwa 75 Millionen Twitter-Nutzer, die tagtäglich mehr als 1,3 Millionen Tweets veröffentlichen. Allein wegen der schiereren Menge sollte man der Qualität und dem Wahrheitsgehalt

der Nachrichten mit einer gesunden Skepsis gegenüber stehen. Vermeintliche spektakuläre Neuigkeiten werden häufig dazu benutzt, um Schadsoftware zu verbreiten. Mit der Nachricht vom überraschenden Unfalltod eines Prominenten wird Aufmerksamkeit erregt, der beigefügte Link führt zu einer Webseite, die Schadsoftware beinhaltet. Twitter prüft zwar verlinkte Webseiten vorab auf Ihre Reputation³, dies aber ist kein absoluter Schutz. Abgesehen davon sollte es selbstverständlich sein, dass man sich nur mit einer Security-Software im Internet bewegt.

Ebenso wichtig ist es, sich über die Informationen Gedanken zu machen, die man Twitter oder einem anderen Social Network anvertraut. Ein Paradebeispiel für das negative Potenzial, zeigte die Mashup-Seite „Please-Rob-Me (übersetzt etwa: Bitte raub mich aus), die verschiedene öffentliche Datenquellen kombinierte. So wurden Aufenthalts- bzw. Abwesenheits-Meldungen (Fliege heute um 14:20h nach Berlin) mit der Anschrift des Autors kombiniert. Fertig war die Einbrecher-Liste von Wohnungen, deren Bewohner nicht zuhause ist.

Twitter erlaubt zwar das nachträgliche Löschen von irrtümlich veröffentlichten Tweets, aber diese Option gilt nur für Twitter selbst. Die Vielzahl von Diensten, die Tweets lesen und archivieren bleibt davon unberührt. Auch hier gilt wieder die Tatsache, dass man dem Internet nur sehr schwer Informationen wieder entreißen kann. Die wichtigsten Empfehlungen, die man als Twitter-Anwender beachten sollte sind:

- Trennen Sie strikt berufliche und private Nutzung / Kommunikation.
- Nachträglich gelöschte Tweets sind weiterhin bei anderen Diensten archiviert.
- Geben Sie so wenig private Daten als möglich über sich bekannt.
- Verwenden Sie Ihr Twitter-Passwort nicht zusätzlich bei andere Diensten.

- Befolgen Sie die bekannten Passwort-Regeln und wählen Sie ein sicheres Passwort.
- Zusatzprodukte, die eine erweiterte Twitter-Funktionalität bieten, benötigen Ihr Twitter-Passwort. Beschränken Sie daher die Anzahl dieser Tools auf die notwendige Anzahl. Twitter wird demnächst OAuth zur Autorisierung verwenden, die unsichere Passwortweitergabe damit hinfällig.
- Lesen Sie vor Nutzung von Zusatzprodukten, ob diese auch von anderen Anwendern oder Blogs empfohlen werden. So vermeiden Sie irrtümlich Crime- und Ransomware einzusetzen.
- Wenn Sie einen ReTweet machen, also die Weiterempfehlung von Tweets, kontrollieren Sie, welche Informationen die ggf. vorhandene URL enthält, damit Sie nicht unabsichtlich auf verbotene oder schädliche Seiten verweisen.
- Nutzen Sie immer eine Sicherheits-Software auf Ihrem Computer-System.
- Melden Sie Accounts mit reinen Spam-Nachrichten an Twitter.
- Wenn Sie URL-Verkürzungsdienste verwenden, nutzen Sie solche, die eine Preview-Funktion anbieten. Demnächst wird Twitter seinen eigenen Verkürzungsdienst anbieten. Eine Alternative stellt auch der neue Verkürzungsdienst von McAfee⁴ dar, der die Reputation der Ziel-Webseite überprüft.
- Reagieren Sie auf private Nachrichten, die man ihnen schreibt.
- Überprüfen Sie periodisch, ob Ihre Twitter-Einstellungen noch den Vorgaben entsprechen.
- Achten Sie auf Security-Hinweise von Twitter und befolgen sie diese.
- Kontrollieren Sie, welche Zusatzprodukte auf Ihren Account zugreifen dürfen.
- Wählen Sie keinen Kanal-Namen, der unter den Markenschutz fällt oder anderweitig geschützt ist.
- Klicken Sie keine Links, die

(angeblich) zur Twitter-Login-Seite führen! Verwenden Sie nur Ihre gespeicherten Bookmarks oder tippen Sie die korrekte URL selbst ein.

Behalten Sie die Twitter-Szene im Auge. In Blogs, Foren und Twitter-Kanälen werden Sicherheits-Hinweise sehr schnell veröffentlicht!

Stolpersteine

Peter Ustinov sagte einmal „Jeder Mensch macht Fehler. Das Kunststück liegt darin, sie dann zu machen, wenn keiner zuschaut“. Dieser gute Ratschlag ist im Web schwer umzusetzen, weil fast immer jemand zusieht. Daher sollte man, gerade wenn es Unternehmen betrifft, vorab häufig auftretende Situationen mit Gefahrenpotenzial durchplanen. Einige davon sind nachfolgend genannt:

- E-Mail-Adressen: Mitunter ist es erforderlich, einen E-Mail-Kontakt zwischen Autor und Leser herzustellen, beispielsweise um spezifische Fragen zu erörtern. Welche E-Mail-Adresse soll man verwenden? Die personalisierte E-Mail-Adresse, die allgemein für Kommunikation verwendet wird? Oder ist es besser eine (neutrale) „Marketing-Adresse“ zu verwenden? Was geschieht, wenn die Adresse für Spam missbraucht wird oder bei einer persönlichen Adresse der Mitarbeiter das Unternehmen verlässt oder andere Aufgaben übernimmt?
- Design: Twitter hat eine überarbeitete GUI angekündigt. Diese GUI führt dazu, dass Informationen, die bisher im Background-Image abgebildet wurden, nicht mehr sichtbar sind. Eine häufig genutzte Informations- und Werbefläche entfällt damit. Wie geht man damit um – und wo platziert man nun diese Informationen?
- Arbeitsfreie Zeit: Wer kümmert sich um Twitter in der arbeitsfreien Zeit, an Wochenenden

oder während der Betriebsferien? Gibt es eine Follow-The-Sun-Regelung oder wird Twitter zum Arbeitszeitende „stillgelegt“? Für den Verbraucher kann dies zum entscheidenden Faktor werden, sie nutzen Twitter zwischen 16h bis 23h häufiger als sonst.

- Authentizität: Will man den eigenen Kanal verifizieren lassen⁵? Wie geht man mit Falschmeldungen um und wie reagiert man auf negative Publicity?
- Globaler Ansatz: Twittert man in Deutsch, in Englisch oder in mehreren Landessprachen? Gibt es verschiedene Kanäle und lokale Ausprägungen? Spricht man überall die gleichen Themen an, oder sind diese regional unterschiedlich? Wer koordiniert dies und wer verantwortet den globalen Auftritt?

Dies sind nur einige Themen, die man vorab überdenken sollte. Erfahrungsgemäß ist es billiger und besser sich vorab Gedanken

zu machen, als erst dann zu reagieren, wenn das virtuelle Kind in den Brunnen gefallen ist.

Handlungsbedarf

Wer Social Networks nutzt, muss Regeln erlassen und Arbeitsabläufe definieren. Dies gilt für Twitter ebenso, wie für alle anderen Dienste. Nach einer aktuellen Studie von McAfee⁶ verfügen ein Drittel der Befragten über keine Social-Media-Richtlinien. Eine häufige Reaktion ist daher das Sperren der entsprechenden Dienste (URL-Blocking). Aber mit einer Blockade von Web 2.0 Services verpassen Firmen das positive Potenzial von Social Networks. Beachten Sie daher folgendes:

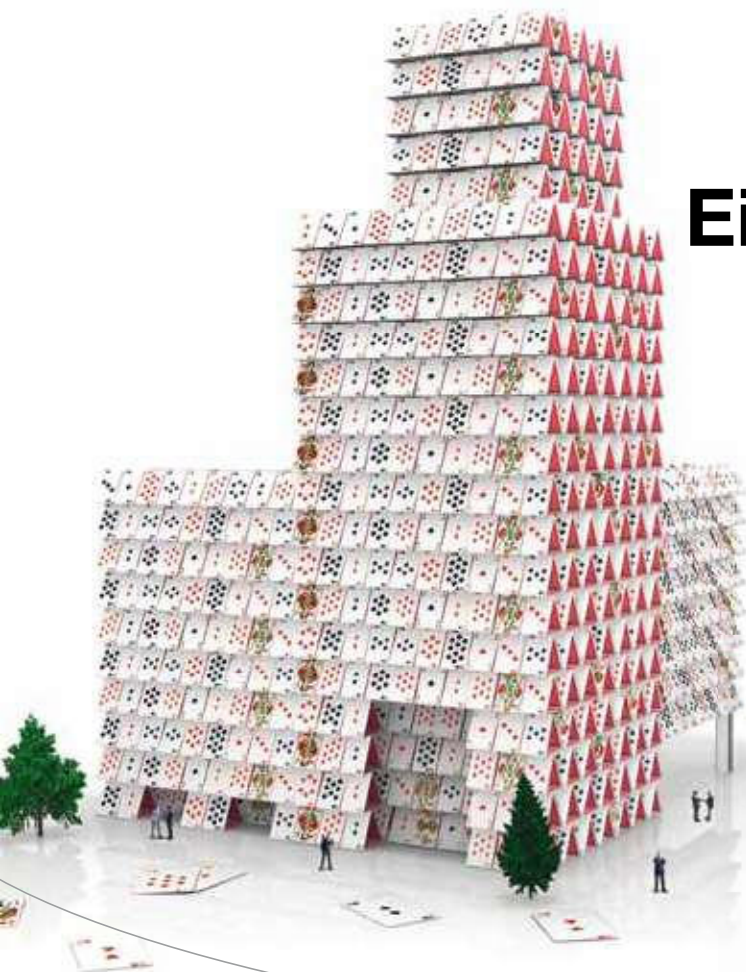
- Klären Sie die Ausrichtung und den Umfang, in dem Sie Twitter nutzen wollen.
- Definieren Sie ein Regelwerk, welches den Mitarbeitern einen Rahmen für das Konsumieren

aber auch für das Publizieren im Web 2.0 vorgibt.

- Wenn Sie selbst aktiv twittern, stellen Sie technische und persönliche Ressourcen bereit und stimmen Sie die Aktivitäten global ab, wenn vorhanden auch mit dem Datenschutzbeauftragten und dem Betriebsrat.
- Informieren Sie Ihre Mitarbeiter über die Chancen aber auch über die Risiken von Twitter.
- Berücksichtigen Sie das Know-how Ihrer eigenen Security-Experten.

Quellen

- 1 <http://www.viruslist.com/de/analysis?pubid=200883692>
- 2 <http://www.impressum-recht.de/meldung/items/impressumspflicht-auf-twitter.html>
- 3 <http://www.computerbild.de/artikel/cb-News-Internet-Twitter-mehr-Schutz-vor-Spam-und-Malware-5132240.html>
- 4 <http://www.mcaf.ee/>
- 5 <http://twitter.com/help/verified>
- 6 <http://newsroom.mcafee.com/images/10039/Web2report.pdf>



Einstu

Passgenaue IT-Sicherheit macht Ihren Erfolg stabil.

Schützen Sie Ihre wichtigsten Werte. IT-Sicherheit ist der Wegbereiter für eine intakte IT-Infrastruktur und alle Prozesse. Setzen Sie mit secunet auf die richtige Karte: Wir unterstützen Sie mit Expertise und Weitblick bei der Realisierung anspruchsvoller IT-Sicherheitslösungen.

secunet

www.secunet.com

IT-Sicherheitspartner der
Bundesrepublik Deutschland