



Risikomanagement

Sicherheitsrisiko Facebook, Twitter & Co.



Marcus Beyer,
Architect Security
Awareness,
ISPIN AG,
Bassersdorf
marcus.beyer@
ispin.ch
Twitter: @mbeyer

Die Zeiten, in denen Mitarbeiter nur passiv Informationen abgerufen haben, sind lange vorbei. Sie sind online aktiv und vernetzt, haben Profile in sog. Social Communities und Business-Netzwerken. Sie unterhalten sich in Fachforen und Blogs über ihre Arbeit und verwandte Themen. In ihrer Freizeit veröffentlichen sie online Bilder und Videos, bewerten Hotels, Restaurants, Produkte und nicht selten auch ihren Arbeitgeber. Die meisten dieser Inhalte sind über Suchmaschinen wie Google für jedermann auffindbar – zum Teil sogar noch, wenn sie auf der Ursprungsseite längst wieder gelöscht wurden. Denn das Internet vergisst nichts.

Blocken oder nutzen?

Gerade eben mit dem rasanten Wachstum von Facebook (1,5 Mio. Nutzer allein in der Schweiz innerhalb weniger Monate), Xing, LinkedIn & Co. oder dem Microbloggingdienst Twitter findet die Verbreitung (vielleicht auch ungewollter) Informationen immer schneller statt.

Allerdings: Wenn man sich den neuen Kommunikationswegen nicht stellt, verspielt man als Unternehmen sehr schnell wertvolle Chancen auf Dialoge mit seinen Kunden, Partnern und potenziellen Mitarbeitern sowie der gesamten

Öffentlichkeit – auch und gerade in klassischen Krisen- und Notfallsituationen.

Einige Schweizer Unternehmen blocken solche Netzwerke mit meiner Meinung nach oft fadenscheinigen Argumenten wie Netzlast oder dem Einschleusen von Viren und Trojanern (was ja mit einer funktionierenden IT-Sicherheitsinfrastruktur an sich kein Problem wäre) bzw. argumentieren mit Arbeitszeitverlust (machen wir doch dann parallel die unsägliche «Raucherpausen-Diskussion» auf – was ist gesünder?). Und seien wir doch ehrlich: Die Massnahmen des «Aussperrens» der Privatsphäre ist auf Dauer sicher keine effiziente Lösung. Sie hilft aber, uns mit dem Thema auseinanderzusetzen, zu lernen und zu verstehen. Das «Anger Management» (Wutmanagement) hat man eben nicht im Griff, denn dann agieren die Mitarbeiter einfach von zu Hause aus. Psychologisch gesehen ist die Hemmschwelle, am Arbeitsplatz negativ zu reden, wesentlich kleiner als in den eigenen privaten vier Wänden.

Eine 100%-ige Kontrolle der ausgehenden Informationen gibt es ab einer gewissen Unternehmensgrösse auch definitiv nicht mehr, und mit dem Mysterium einer «Privatsphäre im Internet» sollte man sehr schnell abschliessen. Soziale

Netzwerke bieten zusätzliche Einfallstore für Geheimnisverrat, Verbal Abuse, Social Engineering usw., die in diesem Kontext beobachtet werden sollten, um nicht die Gefahr von Reputations- und Ausspähungsschäden zu erhöhen.

Es herrscht in einigen Unternehmen eine latente Angst, immaterielle Assets wie Ruf und Reputation zu verlieren. Eine positive Reputation ist gekennzeichnet durch Eigenschaften wie Glaubwürdigkeit, Vertrauenswürdigkeit, Zuverlässigkeit und Verantwortung. Die Reputation muss also als schützenswertes Gut einer Unternehmung betrachtet werden. Somit besteht auch immer irgendwo die Gefahr, dass es geschädigt oder sogar vernichtet wird. Die Schädigung kann nun eine Konsequenz des eigenen Handelns, aber auch völlig ungerechtfertigt sein, z.B. bei einer ungerechtfertigten Verleumdungskampagne. Letzteres stellt ein allgegenwärtiges Risiko dar.

Das Reputationsrisiko ist Teil des unternehmerischen Risikos und sollte definitiv im Rahmen des Risikomanagements berücksichtigt werden. Und wenn hier nicht von vornherein genügend korrektive Massnahmen ergriffen werden, hat das jeweilige Unternehmen einen Risikofaktor mehr – ist das so? Wird das so gesehen?



Reputation im Risikomanagement

Ob gewollt oder ungewollt, die Finanzkrise zerrt das Risikomanagement ins Blickfeld der Unternehmen. Es gewinnt mehr und mehr an Bedeutung – und zwar auch in Unternehmen, die nicht im Finanzdienstleistungssektor tätig sind. Die Rezession schwemmt die Defizite im Risikomanagement an die Oberfläche. Neben den finanziellen Folgen haben viele Unternehmen äusserst schmerzhaft auch an Reputation eingebüsst. Gerade eben dieser Risikofaktor wurde bisher oftmals unterschätzt. Es lässt sich eine Fülle von Beispielen aufzeigen, in denen sich das Reputationsrisiko auf eine herausgehobene Person (Politiker, Sportler, Firmenchef) oder ein Unternehmen entfaltet. Diese hätten meist durchaus Steuerungs- und Kontrollmechanismen gehabt, haben die Risiken aber zu spät bemerkt oder die Mechanismen zu spät genutzt.

In der Regel kündigt sich das Reputationsrisiko bereits einige Zeit vorher einigen Insidern im Unternehmen an. Anschliessend kommt es scheinbar plötzlich zu einer Eskalation (Krise), die dann in eine Phase mündet, die als Kommunikationsphase bezeichnet wird. Wird diese signifikante Zeitspanne der Kommunikation überschritten und in dieser nur geschwiegen, besteht keine Möglichkeit der Abfederung mehr. Die Person bzw. das Unternehmen hat seine Chancen verspielt, das Geschehen zu ihren/seinen Gunsten zu beeinflussen.

Aus Sicht des Risiko-Controllings muss das Thema Reputation durchaus ernst genommen werden, insbesondere dann, wenn über eine Marke eine enge

Kundenbeziehung besteht, die durch Angriffe auf die Reputation des Unternehmens und der Marke ernsthaft geschädigt werden kann. Dann müssen über die Fachverantwortlichen Gegenmassnahmen eingeleitet werden, die letztendlich auch die Krisenorganisation berühren können und damit schnell zu einem BCM (Business Continuity Management)-Thema werden kann – auf interdisziplinärer Ebene.

Insbesondere bei OpRisk-Management-Projekten ist das Risikomanagement sogar oft eine der Triebfedern, sich des Themas anzunehmen – allerdings eher verstärkt aus der Informationssicherheitssicht, weniger aus BCM-Sicht. Bei der BCM-Sicht wird der Faktor «Aussenwirkung/Reputation» im Fall eines Notfalls bewertet, nicht jedoch die «heimliche» Kommunikation darüber.

Reputationsangst im Management

Das Management eint weltweit eine Sorge: 66% der befragten Manager fürchten aktuell eine Beschädigung der Reputation ihres Unternehmens. Neben der schwierigen wirtschaftlichen Situation mit steigendem Wettbewerbsdruck und schwer vorhersehbaren Geschäftsentwicklungen birgt das Internet zusätzliche latente Bedrohungen, beispielsweise die unkontrollierte Verbreitung vertraulicher Informationen. Trotzdem werden Reputationsrisiken im Netz noch immer unterschätzt. Zu diesen Ergebnissen kommt die Studie «Risky Business: Reputation Online», welche die internationale Kommunikationsagentur Weber Shandwick in Kooperation mit der Economist Intelligence Unit

durchgeführt hat. Die Themen «Negative Mitarbeiterkommunikation im Netz» und «Fehlgeleitete Nachrichten» stehen hier an oberster Stelle.

Viele Unternehmen sind sich der Risiken, aber auch der Chancen dieser neuen kommunikativen Online-Realitäten nicht bewusst. Oft wissen sie auch gar nicht, welche Möglichkeiten es gibt, die Online-Darstellung ihres Unternehmens durch ihre Mitarbeiter zu beeinflussen. Natürlich sind diese Möglichkeiten und Mittel von Unternehmen zu Unternehmen unterschiedlich. Im besten Fall sollten sie in ein massgeschneidertes strategisches Gesamtkonzept integriert sein, welches durch ein interdisziplinäres Team (Unternehmensstrategie, Kommunikation, HR, Compliance, Informationssicherheit) getragen und verantwortet wird.

(Spärliches) Reputationsbewusstsein

Vielen Mitarbeitern ist nur selten bewusst, dass sie immer auch ein Stück weit Botschafter ihres Unternehmens sind, sobald sie, wie z.B. im online Business-Netzwerk Xing, mit Klarnamen oder ihrem Arbeitgeber identifizierbar sind. Durch ihr Auftreten und ihre Interaktionen gestalten sie die Online-Reputation ihres Unternehmens entscheidend mit. Besonders in Krisenzeiten wird der Mitarbeiter im Social Web schnell zum

Kurz & bündig

Soziale Netzwerke sind bereits heute ein wichtiger Kommunikationskanal – für Unternehmen wie auch deren Mitarbeiter. Man kann sie aus Angst vor Reputationsverlust blocken oder sich aktiv mit ihnen auseinandersetzen. Aus dem Fokus der Kommunikation und des Risikomanagements verbannen kann man sie aber definitiv nicht mehr.

Ansprechpartner und für diverse Stakeholder zur Informationsquelle aus erster Hand. Das Gespräch am Messestand, abends an der Bar oder in der Bahn nach Hause ist virtuell geworden – und Journalisten, Kunden, Konkurrenten, potenzielle Mitarbeiter und alle sonstigen Stakeholder können zuhören.

Selbst «privat» verfasste Äusserungen ohne direkten Geschäftsbezug können das Erscheinungsbild eines Unternehmens beeinflussen, da die Zugehörigkeit eines Mitarbeiters zu einem Unternehmen i.d.R. gerade über soziale Netzwerke und den gängigen Suchtechnologien leicht zu recherchieren ist.

Mitarbeiter jeden Levels haben das Potenzial, die Reputation ihres Unternehmens online zu schädigen, sagt die Weber-Shandwick-Studie. 87% der befragten Führungskräfte geben zu, irrtümlich mindestens eine fehlgeleitete elektronische Nachricht (via E-Mail, SMS oder Twitter) versandt oder erhalten zu haben. Und auch die Chefetage ist dagegen nicht immun: 80% der CEOs/Vorstände haben versehentlich persönliche Nachrichten falsch gesendet oder empfangen.

Daher ist es umso wichtiger, die Mitarbeiter für die Aussenwirkung ihrer Social-Media-Aktivitäten zu sensibilisieren und ihnen entsprechende Leitlinien in die Hand zu geben. Ein Ergebnis, zu dem wir in mehreren Projekten kamen, ist daher auch die Entwicklung und Implementierung von Social Media Guidelines oder Policies – also die Schaffung eines Bewusstseins (Awareness) für

einen verantwortungsbewussten Umgang mit diesen Kanälen.

Zusammenfassung und Fazit

Eine gute und solide Reputation aufzubauen, ist ein langwieriger und mühsamer Prozess, dessen Ergebnis in wenigen Minuten zerstört sein kann. Hier sind Methoden des Business Continuity prädestiniert. Es müsste – in Anlehnung an einen Business Continuity Plan (BCP) – einen Reputation Continuity Plan (RCP) für die Kommunikation im Fall eines eingetretenen Reputationsrisikos entworfen werden, um das eingetretene Reputationsrisiko abzumildern. Bei strukturierten Risiko-Assessments muss aus meiner Sicht die Reputation als mögliche Auswirkungsdimension (neben finanziellen, rechtlichen und operativen Auswirkungen) auf jeden Fall jetzt und zukünftig betrachtet werden.

Bei allen Entscheidungen ist zu schauen, welchen Einfluss diese auf die Reputation des Unternehmens haben könnten. Sie sollten sich immer die Fragen stellen: Darf man jetzt auf bestimmte Aussagen in Sozialen Netzwerken reagieren oder es einfach so «dahinplätschern» lassen? Wer macht das – ein eingekaufter Blogger, der externe PR-Profi oder ein interner Mitarbeiter wegen der Authentizität? Welche Attraktivität verliert mein Unternehmen, wenn ich soziale Netzwerke oder gar die gesamte Internetnutzung sperre? Ist Employer Branding (Aufbau einer positiven Reputation für zukünftige Fach- und Führungskräfte) tatsächlich ein

zukunftsorientiertes HR- und Kommunikationsthema oder eine moderne Marketingblase? Sie sehen – das Thema ist komplexer als gedacht.

Und es geht um viele verschiedene Spielwiesen, die man zu einem gesamten Ganzen zusammenfügen muss. Das Marketing will kommunizieren, die Stakeholder erreichen; das HR braucht motivierte und qualifizierte Mitarbeiter – und die haben (glücklicherweise) auch eigene persönliche Ansprüche; Compliance/Legal ist um die Einhaltung besorgt, und die Informationssicherheit mit dem Schutz von Daten und Informationen durch technische (Viren, Trojaner etc.) und menschliche Risiken (Fehlverhalten, Unwissenheit, Absicht, Social Engineering) beschäftigt. Hier ist eine Moderation des Prozesses (am besten von aussen) strategisch wichtig und auch als nachhaltig einzuschätzen.

Erfolgreiches Reputationsmanagement

Aktives Web- und Social-Media-Monitoring

Ausschnittsdienste in PR-Abteilungen berichten nur eins: Wo wurde über mich, mein Unternehmen und unsere Produkte berichtet? Klassische Medien lassen aber nun mal nur eine äusserst beschränkte Feedback-Möglichkeit zu. Die Diskussion finden meist im Dialog online statt – und hierüber wissen die meisten Unternehmen einfach zu wenig. Kennen Sie die Protestgruppe zu Ihrem Unternehmen bei Facebook? Sollten Sie mal nachschauen.

Richtlinien/Guidelines und «Awareness»

Viele Unternehmen entdecken die sozialen Netzwerke und andere Web-2.0-Dienste langsam, aber sicher auch als Kommunikations-, Marketing- und Vertriebskanal. Die Sicht ist dabei auf die Stakeholder

Literatur, weiterführende Links

- <http://www.reputationmanagement.ch/>.
- <http://klauseck.typepad.com/prblogger/krisenpr/>.
- [#reputation bzw. #reputationsmanagement](http://www.twitter.com)
- <http://www.reputation-management-blog.de/>.
- «Reputationsrisiko Social Media» wird in einem Vortrag auf dem ISPIN-WakeUp am 25.3.2010 thematisiert; Infos dazu unter <http://www.ispin.ch/>.

gerichtet. Intern wird geblockt – warum? Derartige Richtlinien sollten die Mitarbeiter in ihren Online-Aktivitäten in erster Linie nicht massregeln, sondern vielmehr ein Bewusstsein für die Möglichkeiten, Risiken und Fallstricke der Online-Kommunikation schaffen.

Verantwortlichkeiten klären

Jemand muss den Hut aufhaben, den Lead erfolgreich führen und begleiten. Ob es ein Social-Media-Beauftragter ist oder ob gar – in vielen internationalen Unternehmen mittlerweile üblich – ein Chief So-

cial Media Officer (CSMO) aufgestellt wird oder ob das Thema über ein interdisziplinäres Team geführt wird – jemand muss sich verantwortungsvoll der Sache annehmen und die rasanten Entwicklungen in der Online-Kommunikation im Blick haben. ■

agenda

Swiss IT Academy @Community36

Unabhängige Schweizer IT-Konferenz
6./7. Mai 2010, Zürich
<http://www.swissitacademy.ch>

Eurocrypt 2010

International Association for Cryptologic Research (IACR)
30. Mai–3. Juni 2010, Nizza/F
<http://crypto.rd.francetelecom.com/events/eurocrypt2010/>

Orbit-iEX 2010

4.–7. Mai 2010, Zürich

Sommerakademie 2010

«Codex digitalis – Grundrechtsschutz durch künftige Normen und Techniken»
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
30. August 2010, Kiel/D
<http://www.datenschutzzentrum.de/sommerakademie/>

15. Symposium on Privacy and Security

Stiftung für Datenschutz in Informationssicherheit
31. August 2010, ETH Zürich
<http://www.privacy-security.ch/>

D-A-CH Security 2010

Gemeinsame Arbeitskonferenz von GI, OCG, BITKOM, SI, Teletrust und TU Wien
21./22. September 2010, Wien/A
<http://www.syssec.at/dachsecurity2010>

Sicherheit 2010

5. Konferenz «Sicherheit, Schutz und Zuverlässigkeit» von ISSS und GI
5.–7. Oktober 2010, Berlin/D
<http://www.sicherheit2010.de>

13. ISSS Berner Tagung für Informationssicherheit

25. November 2010, Bern
<http://www.iss.ch/veranstaltungen/2010/13-berner-tagung/>

Nächste Nummer

Die nächste Ausgabe von *digma* erscheint im Juni 2010 und widmet sich schwerpunktmässig dem Thema «**Soziale Netzwerke**»