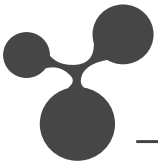
Technische Universität Dresden – Fakultät Informatik
Professur für Multimediatechnik, Privat-Dozentur für Angewandte Informatik

Prof. Dr.-Ing. Klaus Meißner
PD Dr.-Ing. habil. Martin Engelien
(Hrsg.)



GeNeMe '11

Gemeinschaften in Neuen Medien

an der
Fakultät Informatik der Technischen Universität Dresden

mit Unterstützung der

3m5. Media GmbH, Dresden
Communardo Software GmbH, Dresden
GI-Regionalgruppe, Dresden
FERCHAU Engineering GmbH, Dresden
IBM, Dresden
itsax.de | pludoni GmbH, Dresden
Kontext E GmbH, Dresden
objectFab GmbH, Dresden
queo GmbH, Dresden
Robotron Datenbank-Software GmbH, Dresden
SALT Solutions GmbH, Dresden
SAP AG, Resarch Center Dresden
Saxonia Systems AG, Dresden
T-Systems Multimedia Solutions GmbH, Dresden
Transinsight GmbH, Dresden
xima media GmbH, Dresden

am 07. und 08. September 2011 in Dresden

www.geneme.de
info@geneme.de

D.8 Die Rolle der Social Media im Information Security Management

Frederik Humpert-Vrielink
CETUS Consulting GmbH

1 Einleitung

Soziale Medien gewinnen in Unternehmen und Behörden sowie Institutionen der Forschung immer mehr an Bedeutung. Somit ist der Nutzung dieser Medien immanent, so dass sie bei klassischen Disziplinen eine zusätzliche Rolle übernehmen. Dieser Beitrag beleuchtet die Rolle der Sozialen Netzwerke mit Blick auf das unternehmens- und behördenweite Information Security Management. Dabei stellt der Beitrag heraus, dass diese neuen Medien sowohl Chancen wie auch Risiken bergen. Daher übernehmen die Plattformen unterschiedlicher Natur im Rahmen dieser unternehmerischen Management-Funktion auch unterschiedliche Rollen. Sie dienen zunächst als Analyseobjekt für die Betrachtung der Risiken, die in der Nutzung liegen. Gleichzeitig dienen diese neuen Gesellschaften aber auch der Recherche und der Beschleunigung, um zeitaufwändige und komplexe Analysen im Sicherheitsmanagement zu beschleunigen oder Projekte zu optimieren.
Wichtig bei der Betrachtung der Rollen ist jedoch, gleichzeitig auch die Aufgabe des Nutzers mit einzubeziehen. Ist er nun Sicherheitsmanager, der mit der Regulierung und Risikoanalyse beim Einsatz eines Medium befasst ist oder ist er Sicherheitsmanager, der selbst in der Rolle des Nutzers Informationen für seine Tätigkeit sammelt. Gleich wie die sozialen Medien genutzt werden, sie werden in jedem Fall die Aufgaben des Sicherheitsmanagers und seinen Arbeitsalltag verändern. Ob zum Positiven oder zum Negativen hängt von der konkreten Umsetzung der jeweiligen Person ab.

2 Aufgabenspektrum der Informationssicherheit

Management der Informationssicherheit in einem Unternehmen bedeutet, sowohl Überbringer schlechter Nachrichten als auch ständiger Mahner in Sachen Neuerungen zu sein. Das Bundesamt für Sicherheit in der Informationstechnik definiert die Aufgaben des Sicherheitsmanagers [BSI] als

- unabhängig und organisatorisch herausgehoben,
- Unterstützer der Leitungsebene bei der Wahrnehmung der Verantwortung,
- Koordinator und Berater in Projekte mit Sicherheitsbezug,
- Planer im Bereich der Notfallvorsorge

Klassisch umfasst das Aufgabenfeld noch zusätzliche Bereiche. Alle diese Aufgaben erfordern ständig aktuelles und am Stand der Technik orientiertes Wissen, dass teils sehr spezialisiert und technisch fokussiert sein muss.
Um diese Aufgaben korrekt zu erfüllen, ist es damit notwendig, die verantwortlichen

Personen mit Medien auszurüsten, die es ihnen ermöglichen, die Aufgabe korrekt und vollständig zu erfüllen. Das klassische Internet hilft hierbei nur bedingt, da viele Informationen, bis sie in einer Online-Form verfügbar sind, bereits veraltet oder nur noch bedingt aktuell sind. Genau diese Lücke schaffen soziale Medien auszufüllen.

3 Soziale Netzwerke als Risikotreiber und Nutzenbringer

3.1 Chancen und Nutzen aus verschiedenen Blickrichtungen

Bevor die Rollen sozialer Netzwerke konkreter beschrieben werden können, ist es notwendig, diese Medien in Bezug zu setzen zu Risiken und Chancen in Abhängigkeit von der jeweiligen Aufgabenstellung im Unternehmen und im Security Management. Denn je nach Anwendungs- und Einsatzspektrum umfasst ein soziales Medium entweder Chancen oder nicht zu unterschätzende Risiken. Chancen sind dabei als diejenigen Nutzungsergebnisse eines sozialen Mediums zu verstehen, die sich positiv auf den Erfolg oder die Produktivität eines Unternehmens auswirken. Dabei ist es jedoch unbedeutend, auf welcher Ebene ein soziales Medium eingesetzt wird. Demgegenüber stehen Risiken. Diese sind als diejenigen Nutzungsergebnisse definiert, die negative Auswirkungen auf den Erfolg oder die Produktivität eines Unternehmens haben können. Im Bereich eines Risikos ist es dabei wichtig, dieses nicht nur aus der Perspektive des nutzenden Unternehmens zu betrachten.
Abbildung 1 stellt ein beispielhaftes Chancen-Nutzen-Profil in Abhängigkeit der Art der Nutzung und der Nutzerart dar. Die unterschiedlichen Einstufungen ergeben sich gleichzeitig aus unterschiedlichen Aufgaben der jeweiligen Rollen im Betrieb.
Je nach Einsatzgebiet und Untersuchungsgegenstand beziehungsweise untersuchtem Unternehmen ergeben sich veränderte Einschätzungen. Der Autor steht bezüglich der empirischen Analyse der Einschätzungen von Chancen und Nutzen sozialer Medien im Rahmen der Informationssicherheit noch am Anfang seiner Untersuchungen. Somit sind die Einschätzungen in Abbildung 1 als beispielhaft anhand eines untersuchten Unternehmens aus der mittelständischen Industrie zu werten – nicht jedoch als allgemeine Einschätzungen oder Empfehlungen. Dies kann erst nach gründlicher empirischer Analyse festgelegt werden.

		Nutzerart			
		Forschung / Entwicklung	**Security Management**	**Geschäftsleitung**	**Mitarbeiter**
Art der Nutzung	**Recherche / Informationsbeschaffung**	hoher Nutzen hohes Risiko	hoher Nutzen mittleres Risiko	mittlere Chance hohes Risiko	mittlere Chance hohes Risiko
	Informationsverbreitung / Marketing	geringe Chancen hohes Risiko	keine Nutzung	sehr hoher Nutzen hohes Risiko	sehr hoher Nutzen hohes Risiko
	allgemeine Nutzung mit externem Bezug	geringe Chancen sehr hohes Risiko	geringe Chancen sehr hohes Risiko	geringe Chancen sehr hohes Risiko	geringe Chancen sehr hohes Risiko
	internes soziales Netzwerk	geringe Chancen geringe Risiken	hoher Nutzen geringe Risiken	geringe Chancen geringe Risiken	geringe Chancen geringe Risiken

Abbildung 1: Chancen und Nutzenprofil aus Sicht des Security Managements

Diese Abbildung ersetzt jedoch keine konkrete Risikoanalyse sowie konkrete Nutzenanalysen für die Informationssicherheit an sich. Jedoch lässt sich hieraus bereits ableiten, an welchen Punkten es notwendig ist, konkretere Untersuchungen beim Einsatz sozialer Medien vorzunehmen.
So ist dies insbesondere notwendig, wenn soziale Medien entweder mit externem Bezug eingesetzt werden oder zur Informationsverbreitung und -beschaffung.
Parallel hierzu ergibt sich gleichzeitig die Notwendigkeit einer konkreten Nutzenanalyse.

3.2 Nutzen sozialer Medien im Rahmen des modernen Security Management

Analog der Risiko-Chancen Matrix in Abbildung 1 lässt sich auch der konkrete Nutzen sowie die konkrete Rolle sozialer Medien im modernen Information Security Management auffächern. Dazu ist es notwendig, die oben beschriebene Matrix mit reinem Fokus auf die Nutzerart „Security Management“ und der Blickrichtung auf die konkrete Rolle zu beleuchten. Dabei ergeben sich vorrangig folgende Rollen sozialer Medien

- Informationsbeschaffung,
- Informationsverbreitung an Kunden,
- Informationsverbreitung an interne Nutzer,
- Krisenkommunikation,

Diese Rollen definieren gleichzeitig den konkreten Nutzen für den Sicherheitsmanager.

Informationsbeschaffung

Insbesondere für die Beschaffung von Informationen werden soziale Netzwerke durch Sicherheitsmanager bereits genutzt. Den Nachweis hierzu führt eine Suche beim Business Netzwerk XING. Eine Suche in den auf dieser Plattform verzeichneten Gruppen nach dem Stichwort „IT-Sicherheit“ liefert 1.190 Gruppen, die sich in Forenbeiträgen oder im Volltext mit der Thematik befassen [XING]. Viele der Nutzer dieser Foren nutzen dabei XING, um sich Informationen über

- die Anwendung von Normen,
- technische Sicherheitsinformationen oder
- allgemeine Sicherheitsinformationen

zu besorgen.

Krisenkommunikation

Sofern die Aufgabe eines Sicherheitsmanagers auch das Krisenmanagement oder Business Continuity Management umfasst, können soziale Medien und soziale Netzwerke eine wichtige Rolle in der Krisenkommunikation spielen. Hierbei spielen Plattformen wie XING, LinkedIn, Facebook, Twitter und andere einen großen Vorteil

der Konzeption aus. Die schnelle und zeitgleiche Verbreitung von Informationen. Somit könnten gezielt eingesetzte und gut gepflegte Social Media-Kampagnen in Business Continuity-Plänen einen wichtigen Platz einnehmen. Gleichzeitig fordert dies jedoch die Kooperation zwischen Security Management und Social-Media Management.

Informationsverbreitung
Unabhängig von notwendiger Vorbereitung und Nutzung im Rahmen der Krisenkommunikation ist es auch sinnvoll, soziale Netzwerke bereits bei der allgemeinen Verbreitung von Informationen anzuwenden. Dies allerdings mit der gebotenen Sorgfalt. So ist es sicherlich kontraproduktiv, Informationen über konkret getroffene Sicherheitsmaßnahmen zu verbreiten. Die allgemeine Kommunikation, das Thema Security zum Ziel des Unternehmens zu erklären und auch unterschiedliche Arten angewendeter Sicherheit, die keinen Rückschluss auf Lücken zulassen, sind hier jedoch sinnvoll.
Auch in der internen Anwendung großer Konzerne ist es sinnvoll, soziale Medien für die Verbreitung von Informationen einzusetzen.

3.3 Risiken sozialer Medien

Die sich weiter verbreitende Nutzung sozialer Medien in Unternehmen birgt auch Risiken, die im Rahmen des Security Management zu adressieren sind. Hierzu ist es jedoch notwendig, die Risiken zu klassifizieren. Im Wesentlichen gibt es hier zwei Risikoarten, diese sind

- technische Risiken aus der technischen Anwendung sozialer Plattformen und
- diffuse Risiken aus der Nutzung sozialer Plattformen.

Zu den Risiken erster Kategorie zählen zum Beispiel sogenannte „Drive-by“ Attacken durch präparierte Nachrichten in einem sozialen Medium oder das Ausnutzen offener Ports durch Applikationen sozialer Medien. Diese Risiken sind durch die verantwortlichen Sicherheitsmanager konkret zu analysieren. Bei der Erarbeitung adäquater Gegenmaßnahmen ist Wert darauf zu legen, dass diese die technische Realisierung der Plattformen ausreichend berücksichtigen. Zumeist ist mit klassischen Mitteln der IT-Sicherheit, zum Beispiel Firewall-Systeme, Applikationsfilter oder ähnlichem nicht ausreichend Abhilfe zu schaffen.
Die diffusen Risiken der zweiten Kategorie umfassen mehr Risiken, die aus der „Sicherheitslücke Mensch“ als Nutzer eines sozialen Medium entstehen. Konkret zählen hierzu die Bereiche

- Social Engineering,
- unreglementierte und offene Nutzung und
- vorsätzlicher Informationsabfluss.

Die oben stehende Liste ist selbstverständlich nicht abschließend. Es sind generell weitere Risiken aus der Nutzung sozialer Medien denkbar. Eine komplette Risikoanalyse ist jedoch anhand konkreter Nutzungsszenarien mit unterschiedlichen Geltungsbereichen durchzuführen und würde den Rahmen dieses Beitrages sprengen. Bei der Bewertung aller im Rahmen der Risikoanalyse ermittelten Risiken gilt wie bei allen Risikoanalysen auch: Die Geschäftsleitung oder Behördenleitung ist verantwortlich für den korrekten Umgang und die korrekte Adressierung dieser Risiken.

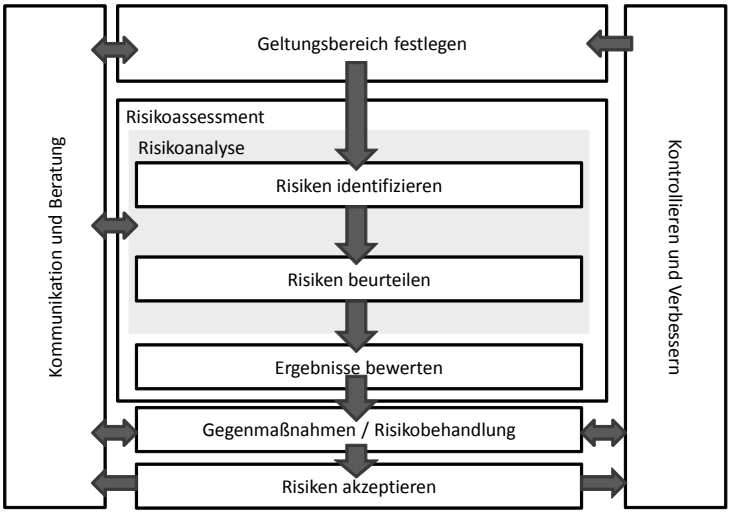


Abbildung 2: Methodik zur Risikoanalyse nach ISO 27005

Schwierigkeiten in der Risikobewertung

Die tatsächliche Schwierigkeit bei der Risikobewertung offenbart sich, wenn wir einen Blick in die Vorgehenweise der Risikobewertung wagen. Im Rahmen einer jeden Risikoanalyse ist eine Vorgehenweise wie in Abbildung 2 Stand der Technik.
Sowohl bei der Vorgehensweise zur Risikoidentifikation wie auch zur Risikobeurteilung ist es noch einfach, soziale Medien zu analysieren. Kompliziert wird dies jedoch, wenn die Frage der korrekten Risikobewertung gestellt wird. Hierfür wird allgemein eine sogenannte Risikopotenzialzahl ermittelt. Diese ergibt sich aus Schadenshöhe und Schadenswahrscheinlichkeit. Beide Werte werden zunächst aus Vergangenheitsbetrachtungen herangezogen. Nun sind soziale Medien jedoch ein

verhältnismäßig neuer Risikofaktor der Informationssicherheit. Im Gegensatz zu Bedrohungen für die Infrastruktur und die Anwendungsebenen sowíe Systeme aus klassischen Gefährdungen gibt es für Soziale Medien keine hinreichenden Daten über Schadenshöhen und Schadenswahrscheinlichkeiten. Dies liegt vermutlich darin begründet, dass sowohl die tatsächlich bekannt gewordenen Schäden durch Risiken wie auch die Schadenshöhen nicht bezifferbar sind.

4 Fazit

Soziale Medien und die Weiterentwicklung des „alten" Internet zum Web 2.0 sind ein großer Nutzenstifter für das moderne Information Security Management. Sie beseitigen sowohl Informationsasymmetrien als auch die bisher vorherrschenden großen Investitionen an Zeit und Personal für die Durchführung notwendiger Risikoanalysen. Zusätzlich ergänzen soziale Netzwerke und Gemeinschaften in neuen Medien auch die Krisenkommunikationskanäle und übernehmen eine wichtige Rolle im Business Continuity Management.

Gleichzeitig bergen diese neuen Netzwerke jedoch auch Risiken. Diese Risiken zu adressieren ist eine große Herausforderung für das Security Management und fordert eine starke Verzahnung und eine hohe Social Media Kompetenz. Somit wird die Tätigkeit der Sicherheitsmanager in Unternehmen immer stärker weg von der Technik hin zur Managementaufgabe migrieren.

Substanziell befinden sich die Forschungen zur Rolle der neuen Medien und sozialen Netzwerke im Security Management noch am Anfang. Dennoch zeichnet sich bereits jetzt ab, dass die Plattformen eine breite Rolle spielen werden.

Literatur

[BSI] Muster für die Bestellung eines IT-Sicherheitsbeauftragten, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/hilfmi/muster/muster.html, abgerufen am 01.05.2011

[XING] https://www.xing.com/app/search?op=combined&section=groups&keywords=it+sicherheit&sorting=default#history:op=combined&section=groups&keywords=it%20sicherheit, abgerufen am 02.05.2011