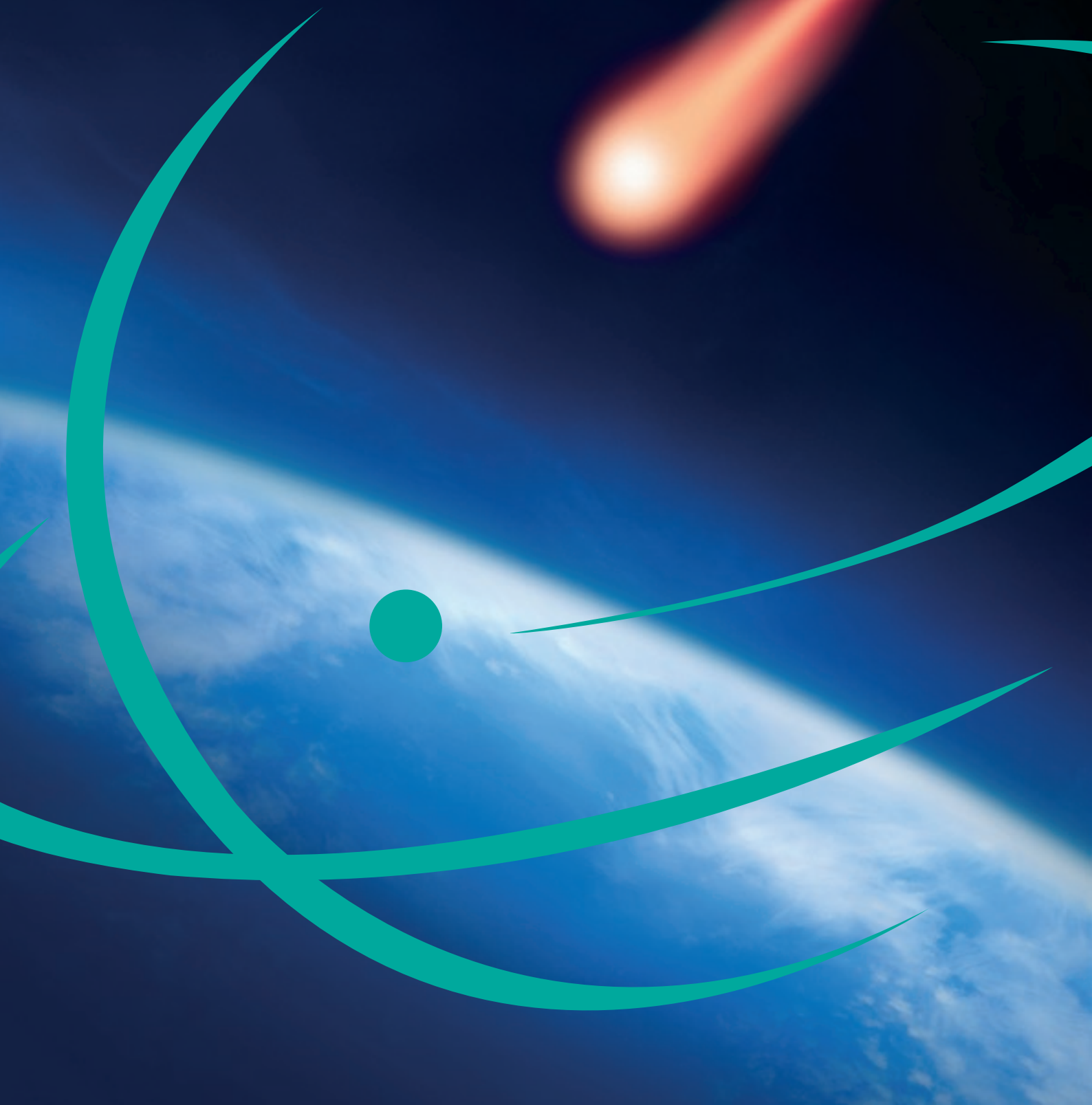


# SecurityRadar 2011

## Leseprobe Social Media & Reputationsrisiken

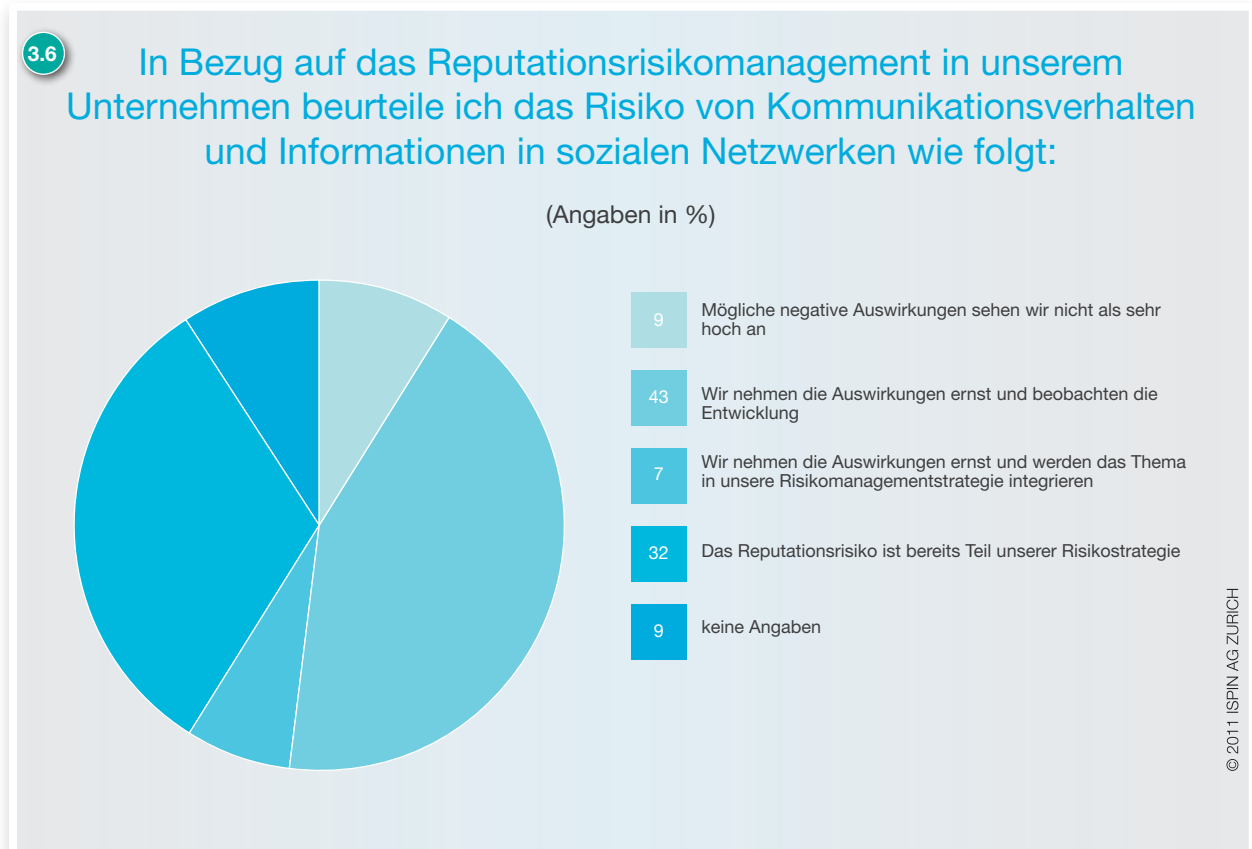


# IIIa Social Media (Reputationsrisiken)

**S**ocial Media als neuer und oft auch neuartiger Kommunikationskanal spielt beim Thema Reputationsrisiko eine wichtige Rolle, ist sogar der Treiber für das Thema Reputation in der Informationssicherheit. Auf technische Unterstützung kann bei der Eindämmung des mit Social Media einhergehenden Risikos nicht verzichtet werden. Gibt es im Bereich Print-Medien immer noch das Recht auf Berichtigung falsch dargestellter Tatsachen, herrscht im Web 2.0 dahingehend beinahe Anarchie. Nutzer berichtigen sich höchstens gegenseitig und nur bei besonders harten Fällen greift eine obere Instanz in Form eines Moderators oder des Plattformbetreibers ein. Einem jedem Unternehmen bleibt also nichts anderes übrig, als sich dem Thema aktiv zu stellen und produktiv die eigene Reputation mitzugestalten bzw. auf etwaige Vorkommnisse direkt zu reagieren. „Social Media wird Teil der klassischen Reputationsrisiken“, resümiert Marcus Beyer, Senior Architect Security Awareness bei der ISPIN AG ZÜRICH, „was früher der Chemieunfall war, kann heute bereits ein negativer Post auf Facebook oder Twitter sein.“

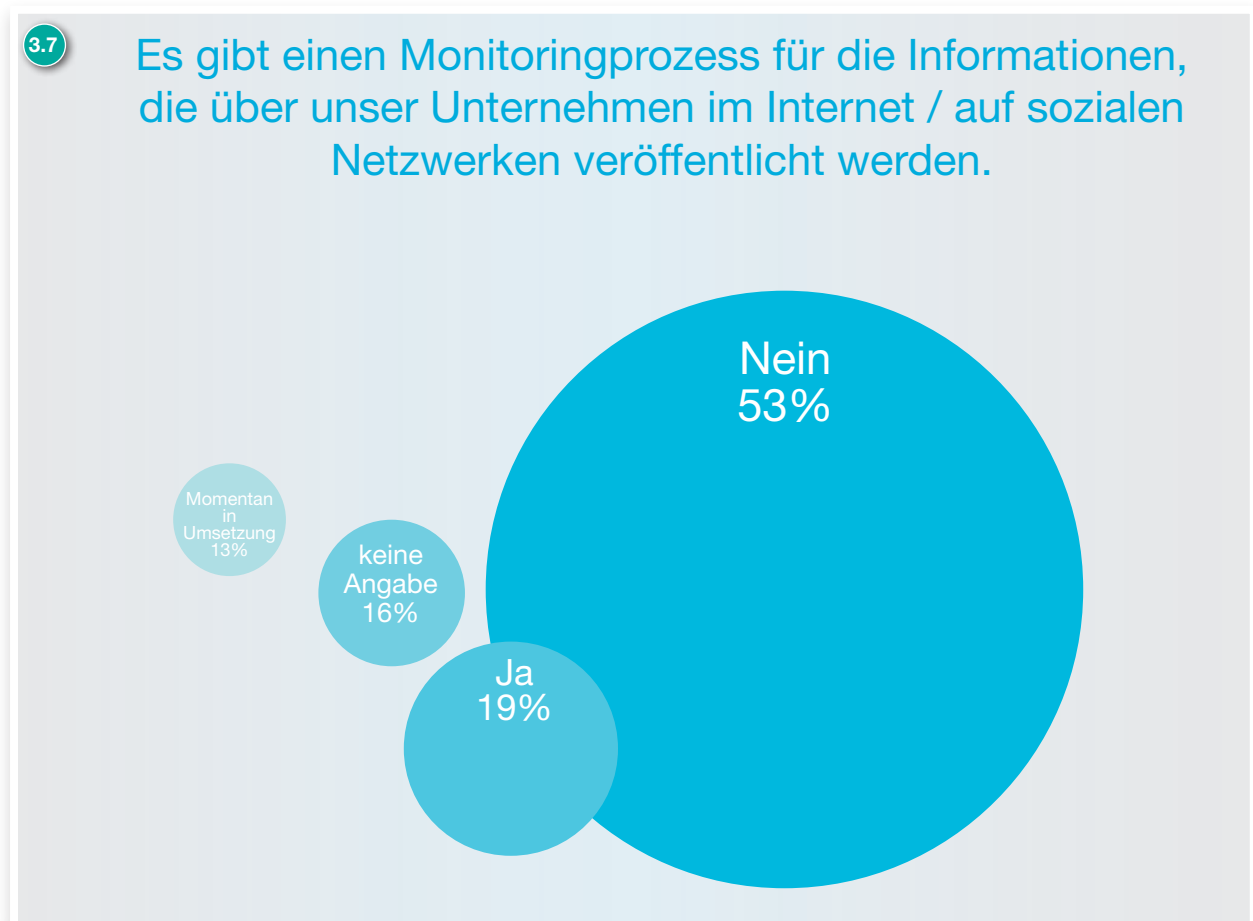
In Anbetracht dessen erstaunt es nicht, dass 43% der Befragten die Auswirkungen der sozialen Netzwerke auf das Reputationsmanagement in ihrem Unternehmen ernst nehmen und die Entwicklung beobachten. Bei 32% ist das Reputationsrisiko hinsichtlich Social Media sogar schon Teil der unternehmensinternen Risikostrategie (→Abb. 3.6).

Im Vergleich zu der im DACH-Raum durchgeführten Studie „Social Media und Reputationsrisiken“ von RiskNET und PRGS ist das ein bemerkenswertes Ergebnis. Auf die gleiche Frage geben hier nur 7% an, dass der Aspekt des Reputationsrisikos in der vorherrschenden Risikostrategie berücksichtigt wird. Zwar wird in dieser Studie der Punkt ‚keine Angaben/weiss nicht‘ nicht einbezogen, rechnet man die uns für die Schweiz vorliegenden Werte dementsprechenden um, stehen den 7% aus dem DACH-Raum sogar 35% gegenüber.



Das Risiko ‚Soziale Netzwerke‘ in Zusammenhang mit mobilen Plattformen ist auch in dem Annual Security Report 2010 von Cisco ein grosses Thema. Hier wird besonders auf Social Engineering – oder wie es wörtlich heisst – „exploitation of trust“ (S. 3) verwiesen. Die Geschichte um ‚Robin Sage‘ wird als Beispiel für die Gefahren, die in den sozialen Netzwerken lauern, aufgeführt. Zusammen mit der Tatsache, dass – wegen der immer grösseren Verbreitung von mobilen Plattformen – auch immer zahlreichere Exploits speziell für die mobilen Plattformen entwickelt werden, besteht hier also ein Risikopotential, das noch lang nicht seinen Höhepunkt erreicht hat. Jedoch sind natürlich gerade neue Technologien wichtig für die Weiterentwicklung von Organisationen oder sogar der ganzen Branche. So betont auch Cisco in der oben genannten Studie, dass diesem Vorteil mit veränderten und erweiterten Policies begegnet werden muss. Es geht um eine Öffnung zu den neuen Technologien, „to support these new ways of working“ (ebd. S. 35).

Obwohl nun fast die Hälfte der Befragten angibt, hinsichtlich Reputationsrisiken die sozialen Netzwerke zu beobachten, haben nur 19% der Unternehmen einen Monitoringprozess für die Informationen, die im Internet bzw. auf sozialen Netzwerken über ihr eigenes Unternehmen veröffentlicht werden – bei 10% ist die Integration solch eines Vorgangs gerade in der Umsetzung (→ Abb. 3.7). Das heisst also, dass über die Hälfte der hier befragten Unternehmen ein Monitoring dieser Art weder vorgesehen noch umgesetzt hat. Ein manuelles Durchsuchen oder Kontrollieren der entsprechenden Bereiche im Internet ist allerdings mühsam, häufig unzureichend und stellt immer nur eine subjektive Momentaufnahme dar.



<sup>2</sup> Robin Sage ist eine fiktive Person, die auf ihrem Facebook-Profil angibt, 25 Jahre alt zu sein und als Cyber Threat Analyst bei der Naval Network Warfare Command zu arbeiten. Sie wurde im Dezember 2009 von Thomas Ryan erfunden, um aufzuzeigen, wie gefährlich die Freigabe persönlicher Daten sein kann bzw. wie schnell und unreflektiert User den Angaben im Netz vertrauen. Zwischen Dezember 2009 und Januar 2010 befreundete sich Thomas Ryan alias Robin Sage mit Männern und Frauen jeden Alters, die fast alle für das Militär, die Regierung oder Unternehmen der United States arbeiteten. Ryan erhielt letztendlich Zugriff auf Email-Adressen, sensible Daten und Informationen, Bankkonten oder Standpunkte von Militärstützpunkten.

Im Vergleich dazu zeichnet sich im DACH-Raum ein anderes Bild. Laut der genannten Studie von RiskNET und PRSG betreiben 36% der Befragten ein Monitoring für die Informationen, die über das jeweilige Unternehmen im Internet oder auf sozialen Netzwerken veröffentlicht werden. Bei 24% ist es gerade in der Umsetzung. Das heisst, knapp die Minderheit verneint, einen solchen Prozess im eigenen Unternehmen zu benutzen. (Allerdings sei hier kurz angemerkt, dass die Teilnehmergruppen beider Studien sehr unterschiedlich sind. Die RepRisk-Studie von RiskNET und PRSG befragte Risikomanager und Kommunikationsverantwortliche, die z.B. auch ohne Absprache mit der IT ein Web-Monitoringtool zu Marketingzwecken o.ä. einsetzen könnten.)

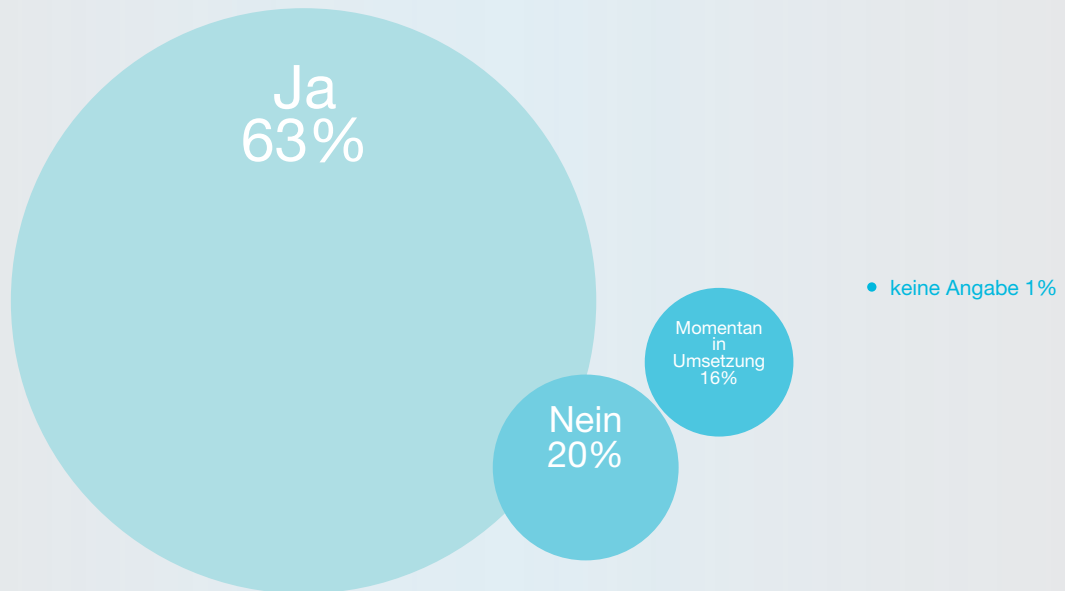
Immerhin geben aber 63% der Befragten an, dass in ihrem Unternehmen Richtlinien zur Internetnutzung oder Social Media Guidelines existieren (→Abb. 3.8). Deutlich wird, wie aktuell die Frage nach dem Umgang mit Social Media in der Schweiz ist. Für die Reputation des Unternehmens ist es Segen und Fluch zu gleich. Also, öffnet oder verschliesst man sich diesem neuen Kommunikationskanal? Wenn öffnen, bis zu welchem Grad? Eine Entscheidung hängt stark mit der jeweiligen Unternehmenskultur zusammen. „Die Tendenz zu einer Beschäftigung mit dem Thema ist aber eindeutig zu erkennen“, berichtet Marcus Beyer, Senior Architect Security Awareness bei der ISPIN AG ZÜRICH. Das unterstreichen auch weitere Ergebnisse der vorliegenden Studie. So geben knapp 22% der Befragten an, dass Social Media Policies auf der Roadmap stehen (→Abb. 8.1). Auf den ersten Blick scheint das nicht viel, betrachtet man aber dieses Ergebnis im Ranking aller hier gemachten Angaben, belegt der Punkt Social Media Policies Platz eins der geplanten Massnahmen. Ziehen wir hier auch wieder die RepRisk-Studie zu einem Vergleich heran, können wir interessante Aussagen treffen. Nur 31% der im DACH-Raum befragten Unternehmen geben an, interne Richtlinien zur Nutzung von Internet und sozialen Netzwerken eingeführt zu haben. Schweizweit ist der Prozentsatz mit 63% doppelt so hoch! Die auf den ersten Blick naheliegende Vermutung, dass Schweizer Unternehmen also mehr Wert auf Offenheit und Verantwortungsbewusstsein ihrer Mitarbeitenden legen als auf schlichte Kontrolle, ist vielleicht etwas vorschnell. Immerhin ist nicht ersichtlich, in wie vielen dieser Richtlinien zur Internetnutzung bzw. Social Media Guidelines die Benutzung einschlägiger Websites überhaupt gestattet, also nicht einfach schön umschrieben aber verboten ist.

Gehen wir in unseren Überlegungen noch einmal zurück: Natürlich gibt es auch die Möglichkeit, Social Media schlichtweg zu ignorieren, d.h. Soziale Netzwerke zu sperren und deren Benutzung zu untersagen. So hat der Connected World Report von Cisco gezeigt, dass einer von drei CISOs davon überzeugt ist, dass Mitarbeitende während der Arbeitszeit mit den firmeneigenen Devices keinen Zugriff auf Social Media haben sollten. Das ist der einfachere Weg. „Man will oft nicht noch eine Baustelle aufreissen, also wird in vielen Unternehmen einfach der Zugang zu sozialen Netzwerken gesperrt“, sagt Marcus Beyer. Jedoch erkennen immer mehr Unternehmen, dass die reflexartige Entscheidung zur Verdrängung der vermeintlichen Gefahr im Nachhinein nicht unbedingt sinnvoll war. Liegt doch auch unheimliches Potenzial in der Nutzung der Sozialen Netzwerke! Das Unternehmen kann sich kostengünstig einer breiten Masse präsentieren, man liegt im Trend und kann sein (Kunden-)Netzwerk simpel erweitern und pflegen. Doch was nun? „Öffnet man nur für bestimmte Bereiche den Zugang zu den sozialen Netzwerken, fühlen sich die anderen Mitarbeitenden benachteiligt und wenden sich frustriert an die IT, die ja letztendlich dafür verantwortlich ist“, erläutert Marcus Beyer, „die IT ihrerseits befindet sich dann in einem argen Kommunikationsdilemma.“ Wie Awareness ist auch die Nutzung der Social Media ein Querschnittsthema. Um gegebene Risiken zu minimieren und gleichzeitig das Potenzial auszuschöpfen, muss interdisziplinär zusammengearbeitet werden. Leider gestaltet sich das in der Praxis oft sehr schwierig. ■

<sup>3</sup> schon auf die genannte Weise zur besseren Vergleichbarkeit umgerechnet

3.8

In unserem Unternehmen gibt es interne Richtlinien für die Nutzung von Internet und sozialen Netzwerken (SocialMedia-Guidelines).



# Bestellung

Der ausführliche Studienband enthält alle Fragen sowie die kommentierten Ergebnisse des ISPIN Security Radar 2011 und ist für CHF 470,00 über [securityreport@ispin.ch](mailto:securityreport@ispin.ch) bestellbar.

Alternativ können Sie auch das nachfolgende Faxformular ausfüllen, ausschneiden oder kopieren und mit Ihrer Bestellung an folgende Nummer faxen: [+41 44 838 31 12](tel:+41448383112)

Mitglieder der Fachverbände ISSA, ISACA, Infosurance, ASIS, SwissICT, ISSS und BCM.net/BCI sowie Hochschulangehörige und Lehrpersonal erhalten einen Rabatt von 15% auf den Studienpreis. Bitte Fachverband oder Organisation bei der Bestellung angeben.

## Faxformular



ISPIN AG ZURICH | Grindelstrasse 15 | CH-8303 Bassersdorf | Switzerland | Fax: +41 44 838 31 12

### ABSENDER:

Firma.....  
Name.....  
Vorname.....  
Funktion.....  
Strasse.....  
PLZ/Ort.....  
E-Mail.....  
Tel.....  
Mobil.....  
Fachverband/Organisation.....

### LIEFERANSCHRIFT (falls vom Absender abweichend):

Firma.....  
Name.....  
Vorname.....  
Funktion.....  
Strasse.....  
PLZ/Ort.....  
E-Mail.....  
Tel.....  
Mobil.....

### BESTELLUNG

Anzahl Studien  \* bei 3 oder mehr Ex. erhalten Sie 15% Rabatt

\_\_\_\_\_  
Datum, Ort/Unterschrift

**ISPIN AG ZURICH**  
**swiss made security.®**

# Herausgeber und Kontakt

## Herausgeber

ISPIN AG ZÜRICH . Grindelstrasse 15 . CH-8303 Bassersdorf . Switzerland  
Tel.: +41 44 838 31 11 . Fax: +41 44 838 31 12 . <http://www.ispin.ch>

## © ISPIN AG ZÜRICH 2011

Die Inhalte der Studie dürfen ausschliesslich auszugsweise und unter Nennung der ISPIN AG ZÜRICH zitiert werden.

## An der Studie haben mitgewirkt

Marco MARCHESI, CEO der ISPIN AG ZÜRICH.

Marcus BEYER, Senior Architect Security Awareness bei der ISPIN AG ZÜRICH

Daniel STÄDELI, Senior Information Risk und Security Consultant bei der ISPIN AG ZÜRICH

Ivan ALLEMANN, Head Business Security und Compliance bei der ISPIN AG ZÜRICH

Zrinka MASLIC, Chief Technology Officer bei der ISPIN AG ZÜRICH

Thomas MÜLLER, Security Consultant bei der ISPIN AG ZÜRICH

Katja DÖRLEMANN, Assistenz Business Security bei der ISPIN AG ZÜRICH

## Produktion

Carina LINNEMANN (Infografiken), Dietmar POKOYSKI (Fachlektorat, Layout) / known\_sense (Köln)



Katja Dörlemann



Marcus Beyer

## Kontakt

Katja Dörlemann/Marcus Beyer, Studienteam SecurityRadar 2011  
[securityradar@ispin.ch](mailto:securityradar@ispin.ch)

**ISPIN AG ZÜRICH**  
**swiss made security.®**

# Themenübersicht des SecurityRadar 2011 – das erwartet Sie in diesem Studienband:

- ⊞ Informationssicherheit in Schweizer Unternehmen
- ⊞ Risiken erkennen und managen (inkl. Schwerpunktthema I: Social Media)
- ⊞ Der Faktor Mensch und (Security) Awareness
- ⊞ Compliance, Governance & Datenschutz
- ⊞ Schwerpunktthema II: Business Continuity Management und Notfallvorsorge
- ⊞ Normen und ISMS
- ⊞ Security-Projekte: Planung, To-Do und Umsetzungsstrategien
- ⊞ Ressourcen und Budget
- ⊞ Studiengrundlage/Demografische Daten
- ⊞ Sicherheit auf und in allen Kanälen



NETBREEZE

Qualitativ erweitert wird der SecurityRadar in diesem Jahr mit einer Online-Trendanalyse „Sicherheit“, welche wir mit unserem Online-Monitoringpartner NETBREEZE AG erstellen. Rapportiert wird über Sicherheitsthemen und Dienstleister aus diesem Bereich. Somit bekommen Sie eine Gesamtschau darüber, welche Sicherheitsthemen in der Fachwelt via Online-Newsportalen, Twitter, Facebook oder Foren gerade im letzten Jahr aktiv diskutiert wurden. Der hier eingesetzte ComMonitor der NETBREEZE AG unterstützt uns auch in der Realisierung unseres Reputation Management Service. Wenn Sie hierzu Fragen haben, setzen Sie sich einfach direkt mit uns in Verbindung.

**ISPIN AG ZÜRICH**  
**swiss made security.®**

[www.ispin.ch](http://www.ispin.ch)

#### **Kontakt und Anfragen zum SecurityRadar 2011**

Marcus Beyer und Katja Dörlemann  
Studienteam des SecurityRadar 2011  
mail: [securityradar@ispin.ch](mailto:securityradar@ispin.ch)

#### **ISPIN AG ZÜRICH**

Grindelstrasse 15  
CH-8303 Bassersdorf  
Tel.: +41 44 838 31 11