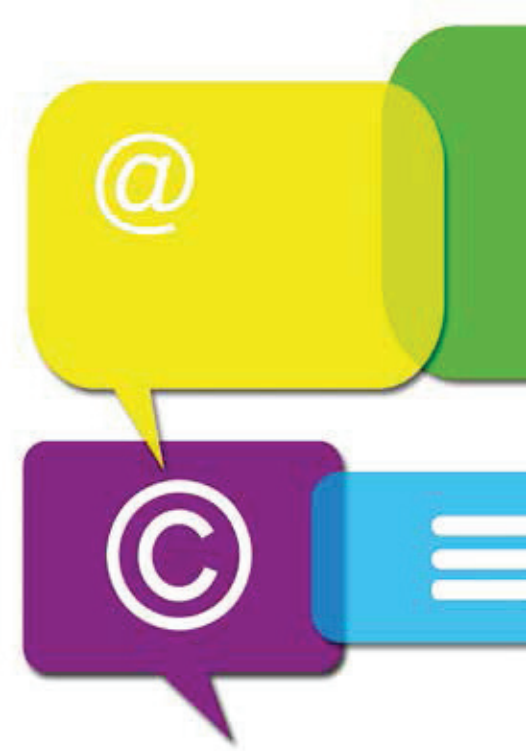
Social Media in der Unternehmenssicherheit

Einsatz, der sich auszahlt

Marcus Nebel



Soziale Medien haben die Kommunikation, aber auch die Verbreitung und Verfügbarkeit von Informationen und nicht zuletzt den Umgang mit persönlichen Daten in unserer Gesellschaft maßgeblich verändert. Während die sozialen Netzwerken der ersten Generation längst vom Markt verschwunden sind, entwickelt sich die aktuelle Social Media-Landschaft rund um Facebook, Twitter & Co. täglich weiter. Diese kann einen wesentlichen Beitrag zur Unternehmenssicherheit leisten.

Wer soziale Netzwerke für die Unternehmenssicherheit nutzen möchte, kommt nicht umhin, sich intensiv mit den Spezifika, Möglichkeiten und den Nutzergruppen sowie deren Verhalten intensiv zu beschäftigen und die Erkenntnisse in die Entwicklung eines strukturierten Social Media Risk Assessment, aber auch in die Entscheidung, welche Medien aktiv genutzt werden sollen, einzubeziehen.

Am Anfang war der Shitstorm …

Im Kontext betrieblicher Sicherheit ist das Thema Social Media bereits vor längerer Zeit angekommen: Nachdem die verschiedenen Social Webs als Marketinginstrumente für Produkte und Dienstleistungen entdeckt und in der Folge intensiv genutzt wurden, nutzten auch die User, zum Beispiel Kunden, die Möglichkeit der Interaktion. So entstand – insbesondere in Negativfällen – eine Community, die einer ungeschickten Öffentlichkeitsarbeit in den sozialen Medien Gesichter gab und den Verursacher an den Pranger stellte. Der Shitstorm als Social Media Bedrohungsszenario war geboren. Bis heute zeigen zahlreiche Beispiele, wie jüngst beim Waffenhersteller Heckler & Koch, bei American Airlines oder der Modekette H&M, welche Risikopotenziale soziale Medien für das Image von Unternehmen besitzen.

In der Folge reagierten Unternehmen mit dem Aufbau spezialisierter (Krisen-)Onlinekommunikation und - da auch potenziell jeder eigene Mitarbeiter als Kommunikator in Erscheinung treten kann - mit der Entwicklung von Social Media Security Policies und Guidelines, die sowohl die Nutzung im Unternehmensalltag regeln als auch konkrete Richtlinien der Kommunikation in sozialen Netzen definieren.

Sicherheitsabteilungen fokussierten in diesem Kontext zunächst fast ausschließlich auf die Gefährdungspotenziale und agierten reglementierend beziehungsweise kontrollierend.

Fragt man aktuell nach der Nutzung sozialer Medien im Bereich der Unternehmenssicherheit, so zeigt sich eine Tendenz zur Fokussierung auf die Informationsgewinnung und Risikoidentifizierung durch gezieltes Monitoring und Screening: Wie lassen sich Incidents frühzeitig erkennen? Wie lassen sich „Influencer“ mit großer Reichweite in den einzelnen Netzen identifizieren? Das Ziel: Krisenpotenziale und Beteiligte bereits in der Entstehung erkennen und im Sinne der eigenen Handlungsoptionen „vor der Lage bleiben“.

Wo finde ich was?

Unterschieden werden hier das Horizontmonitoring, welches dazu dient, definierte Risikothemen beziehungsweise Ereignisarten (Stromausfall, Überschwemmung), zu betrachten, und das Incident Monitoring, welches im Krisenfall ein konkretes Ereignis durch kontinuierliche (Live-)Datenanalyse begleitet.

Es gibt zahlreiche Tools und Methoden, welche ein strategisches Open Information Monitoring unterstützen: Vom einfachen Google-Alert bis hin zu teils plattformübergreifenden beziehungsweise kostenpflichtigen Analysetools, wie zum Beispiel Talkwalker, Hootsuit oder Twazz-up. Allen Ansätzen und Tools gemein ist, dass klar definierte und strukturierte Abfragen (Queries) zu definieren sind, um innerhalb der Medienlandschaft die relevanten Daten auch aussagekräftig herausgefiltert zu bekommen.

Aber: Welche Daten sind in welcher Validität verfügbar und für die Unternehmenssicherheit überhaupt interessant? Hierzu lohnt es sich Parameter wie Echtzeit, Repräsentativität, Lokalität (Geoinformationen), Häufungen innerhalb der verschiedenen Webs zu kennen und hinsichtlich möglicher Verknüpfungen zu bewerten und auch die Application Programming Interfaces (API)

zum INHALT

Bild: JMG/Pixelio

Die sozialen Medien können zur Unternehmenssicherheit beitragen

BdSI-Lehrgang

Fundiertes Wissen zu Einsatzmöglichkeiten von Social Webs in der Unternehmenssicherheit vermittelt der neue dreitägige Zertifikatslehrgang zum „Social Media Security Expert, BdSI" des Bundesverbandes deutscher Sicherheitsberater und -Ingenieure (BdSI) und der Simedia Akademie: Live-Training direkt am Rechner – Die aktuell wichtigsten Webs und Tools für Monitoring, zielgerichtete Analysen und Einsatzsteuerung.

Alle Informationen unter
www.social-media-security-expert.de

der Netzwerke in Hinblick auf die Auslieferung und Verknüpfung von Daten zu untersuchen.

Neue Einsatzpotenziale integrieren

Das Social Media Monitoring findet bereits vielfach Anwendung, so zum Beispiel im Zuge der Lagebewertung und Einsatzplanung während des G20-Gipfels in Hamburg, wo neben diversen Online-Newsquellen, Live-Verkehrsdaten des ÖPNV und der Straßensituationen sowie Wetterdaten auch die Online-Aktivitäten verschiedener Gruppierungen und Einzelpersonen in großen Social Webs, aber auch kleinen thematischen Blogs analysiert wurden.

Möglichkeiten der Personenanalyse werden oft im Sinne des Pre-Employment-Screenings diskutiert, bieten aus Sicht der Unternehmenssicherheit aber auch Potenziale, um zum Beispiel Personenschutzmaßnahmen zu ergänzen beziehungsweise zu optimieren oder im Sinne eines Penetrationstests die Gefährdung für Social Engineering Angriffe auf sicherheitskritische Mitarbeiter (zum Beispiel auf Vorstandsebene) abzuschätzen. Der proaktive, nach außen gerichtete Einsatz sozialer Medien, zum Beispiel im Sinne der Information und Handlungsanleitung im Ereignisfall an die Öffentlichkeit oder eine interne Zielgruppe (Expatriates, Geschäftsreisende) bietet weitere gewinnbringende Chancen für die Unternehmenssicherheit.

In jedem Fall ist eine tiefgehende Beschäftigung mit den rechtlichen Fragestellungen notwendig: Was bedeuten die Allgemeinen Geschäftsbedingungen von Facebook, Twitter, Instagram und Co. für Nutzer und Nutzung? In welchen Fällen sind Betriebsvereinbarungen ein Muss? Wie sind die Datenerhebung und Datenanalyse sowie einzelne Tools juristisch zu bewerten? Welche datenschutzrechtlichen Aspekte sind relevant? Um nicht in juristische Fallen zu tappen, sind vor jedem neuen Schritt zahlreiche Fragen zu beantworten und Regelungen zu treffen. Hier bedarf es unbedingt einer Unterstützung durch fachkundige Experten.

Kein Ein-Mann-Job!

Auch wenn zahlreiche Tools das Social Media Monitoring unterstützen und Daten bereits gefiltert aufbereiten, so ist das Thema als „One-Man-Show" nicht geeignet. Führungsstäbe aus dem behördlichen Bereich, wie zum Beispiel des THWs oder großer Berufsfeuerwehren, setzen mittlerweile auf „Virtual Operation Support Teams" (VOST), die die „klassische" Einsatzsteuerung durch Sammlung, Auswertung und zielgerichtete Weitergabe zusätzlicher Informationen aus den sozialen Medien beziehungsweise aktive Kommunikation über verschiedene Social Media Kanäle unterstützen. Aber auch innovative Sicherheitsorganisationen in Unternehmen setzen auf agile Teamstrukturen, so dass im Ereignisfall erfahrene „Netzwerker" aus unterschiedlichen Bereichen auf Basis einer klar definierten Herangehensweise dem Lagemanagement beziehungsweise dem Krisenstab zuarbeiten.

Die eigenen Kompetenzen weiterentwickeln

Wer erst im Ereignisfall auf die Idee kommt, einen Twitter-Account anzulegen, dem ist nach den obenstehenden Ausführungen nicht mehr zu helfen. Vorbereitung und Training sind auch hier alles! Das Spektrum sozialer Medien ist breit, die Möglichkeiten der Nutzung für die Unternehmenssicherheit sind vielfältig, dementsprechend braucht es Zeit, Fachwissen und Übung, um Webs und Tools im Alltag der Sicherheitsorganisation wirksam und effizient einzusetzen.

Um sich mit der eigenen Abteilung auf den Weg zu machen, empfiehlt sich zunächst, die fähigsten „Netzwerker" im Team zu identifizieren. Affinität im Umgang mit Twitter, Facebook und Co. sind Grundvoraussetzung, reflektierter Umgang mit zur Verfügung stehenden Tools, Kommunikationsgeschick und Kreativität ebenfalls unverzichtbar.

Aber Anwenderwissen allein reicht nicht aus: Ein Mix aus externer fachlicher Schulung zur Entwicklung passgenauer Such- und Monitoring-Algorithmen, Hintergrundwissen zur Verfügbarkeit von Daten, deren Analyse und Interpretation, ein kontinuierlich aktualisierter Überblick über die „Medienlandschaft" und themenspezifisches Networking sind als wesentliche Erfolgsgaranten zu nennen.

Der Einsatz sozialer Medien in der Unternehmenssicherheit ist gewinnbringend und arbeitsintensiv – in jedem Fall aber perspektivisch unverzichtbar!

Marcus Nebel, Experte für Weiterbildungskozepte der SIMEDIA Akademie GmbH, www.simedia.de