FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

Dataminr®

Die Rolle von Social-Media-Analysen im Security Management

Adobestock

AUTORINNEN

Mag.ª Dr.in Beatrice Preßl


Ludwig Schedl

Mag.ª Dr.in Beatrice Preßl (*1984) ist seit 2016 als wissenschaftliche Mitarbeiterin für die methodische Betreuung der Abschlussarbeiten in den Forschungsbereichen Risikomanagement, Security Management sowie Cybersecurity und Wirtschaftsschutz tätig. Außerdem ist sie Modulverantwortliche und Lektorin für die Lehrveranstaltung Wissenschaftliches Arbeiten im Bachelorstudiengang Integriertes Sicherheitsmanagement. Nebenbei ist sie in die Forschungsarbeit am Fachbereich integriert. Mit Mai 2018 hat sie das Zertifikat als Senior Risk Managerin (SRM) nach EN ISO/IEC 17024 erlangt.
Preßl schloss ihr Diplomstudium der Geschichte 2008 ab; 2013 folgte die Promotion in Philosophie an der Universität Wien.

Mag.ª Dr.in Yvonne Prinzellner Bakk.


privat

Mag.ª Dr.in Yvonne Prinzellner Bakk. (*1984) ist seit Juni 2019 im Fachbereich Risiko- und Sicherheitsmanagement als wissenschaftliche Mitarbeiterin tätig. Neben ihrem Einsatz in der Lehre (vor allem Wissenschaftliches Arbeiten) und der Betreuung von Abschlussarbeiten arbeitet die Kommunikationswissenschafterin an Forschungsprojekten.
Prinzellner verfügt über Unterrichts- und Forschungserfahrung aus Lehraufträgen und Projektmitarbeit an der Universität Wien, der ARGE Bildungsmanagement sowie der TU Ilmenau. Nach ihrer Promotion an der TU Ilmenau war sie ab Herbst 2017 als wissenschaftliche Projektleiterin beim Kuratorium für Verkehrssicherheit in Wien tätig.

Das Projektteam

FH-Prof.in Mag.ª Claudia Körmer	Projektleitung
FH-Prof. DI Dr. Martin Langer	Fachbereichsleitung, Projektmitglied
Aldric Ludescher BSc MA	Lektor im Fachbereich, Experte für Security Management, Projektmitglied
Mag.ª Dr.in Beatrice Preßl	Projektleitung und -umsetzung
Mag.ª Dr.in Yvonne Prinzellner Bakk.	Projektmitglied und -umsetzung
Anna Rathmair BA MA	Projektmitglied und -umsetzung

IMPRESSUM

ISBN 978-3-902614-57-5
Medieninhaberin: FH Campus Wien – Verein zur Förderung des Fachhochschul-, Entwicklungs- und Forschungszentrums im Süden Wiens; ZVR-Zahl 625976320, Favoritenstraße 226, 1100 Wien.
Für den Inhalt verantwortlich: Mag.ª Dr.in Beatrice Preßl, Mag.ª Dr.in Yvonne Prinzellner Bakk.
Produktionsleitung: DI (FH) Mag. Thomas Goiser MBA MA; Lektorat: Mag.ª Verena Brinda.
Grafik: Doris Zemann, www.dggd.at; **Druck:** druck.at
Die Texte und Daten wurden sorgfältig ausgearbeitet; dennoch können wir keine Haftung für die Richtigkeit der Angaben übernehmen.
Kontakt für Feedback: riskmanagement@fh-campuswien.ac.at

Wien, März 2020

VORWORT

Gleichzeitig mit dem Megatrend Sicherheit erleben wir den „Gigatrend" Digitalisierung.
Wo sich diese beiden Trends treffen, wird es besonders spannend. Das betrifft einerseits Datenschutz sowie Datensicherheit in all ihren Aspekten, andererseits natürlich die rasante und tiefgreifende Veränderung unserer Wirtschaft und Kultur durch die vermehrte Mediennutzung.

Beide Themen haben große Relevanz für Security Manager*innen und somit für das Berufsbild unserer Absolvent*innen im Bachelorstudiengang Integriertes Sicherheitsmanagement.

Als die Idee zu diesem Forschungsprojekt das erste Mal diskutiert wurde, war sofort für uns klar, dass das Thema Social Media Intelligence hochinteressant und hochaktuell ist.

Dieses Forschungsprojekt liefert nun erstmals wissenschaftliche Erkenntnisse über die derzeitige Nutzung und Rolle von Social-Media-Analysen (z.B. mit einem Analysetool) im Bereich Security Management in der D-A-CH Region. Es ist uns als Fachbereich ein Anliegen, CSOs und CEOs über dieses bis dato noch wenig beleuchtete Thema zu informieren und somit Unterstützung in Entscheidungsprozessen zu bieten.

Ganz klar ist: Die rasche Verknüpfung von Informationen macht die angemessene Reaktion auf akute Bedrohungen leichter oder überhaupt erst möglich. Security Manager*innen brauchen dafür die entsprechende Einbindung in die Organisation, ausreichende Ressourcen sowie passende Prozesse und aktuelle Tools. Hier gibt es immer noch großen Handlungsbedarf.

Als Fachhochschule ist die Orientierung an aktuellen und praktischen Herausforderungen unsere Stärke. Angewandte Forschung mit Partnern – in diesem Fall mit dem Analysesoftware-Unternehmen Dataminr – hilft dabei, dass gesellschaftliche Problemstellungen benannt werden und der Dialog zwischen den Fachleuten intensiviert wird.

Ich wünsche Ihnen eine spannende Lektüre!

FH Campus Wien/Schedl

FH-Prof. DI Dr. Martin Langer
Leiter des Fachbereichs Risiko- und Sicherheitsmanagement der FH Campus Wien

ZUSAMMENFASSUNG

Das Hauptziel dieses im Zeitraum 01/2019–02/2020 durchgeführten Forschungsprojekts bestand darin, die Erstellung von Bedrohungsanalysen zu untersuchen, die von Security Manager*innen im deutschsprachigen Raum durchgeführt werden. Ein Schwerpunkt lag in der Analyse sozialer Medien als Informationsquelle und ihrer Einsatzgebiete innerhalb der Unternehmenssicherheit sowie deren Vor- und Nachteile.

Die Ergebnisse dieses Forschungsvorhabens zeigen Grundhaltungen von Security Manager*innen zu Social Media Intelligence (SOCMINT) auf: Beispielsweise stehen soziale Medien für Echtzeit-Informationen und sie kommen vorrangig als Sekundärquellen zum Einsatz. Zusätzlich zeigen sich Tendenzen in Bezug auf den Austausch zwischen einzelnen Geschäftsbereichen, gegenwärtige und zukünftige Herausforderungen der Unternehmenssicherheit, die Wichtigkeit von lokalen Netzwerken als Informationsquelle etc.

Methodisch bediente sich dieses Forschungsvorhaben eines Mixed-Methods-Designs. Zum einen wurden neun leitfadengestützte Expert*innen-Interviews mit Security Manager*innen von drei österreichischen, einem Schweizer und fünf deutschen Unternehmen von November 2018 bis März 2019 geführt, zum anderen eine quantitative Online-Befragung durchgeführt.

Die Ergebnisse der qualitativen Untersuchung wurden mittels qualitativer Inhaltsanalyse nach Kuckartz (2018) computerunterstützt (f4analyse-Programm) erhoben; der in LimeSurvey erstellte Fragebogen war im September 2019 und November 2019 online verfügbar. Der Datensatz wurde mittels der Statistiksoftware SPSS analysiert; insgesamt wurden 40 Fragebögen ausgewertet.

Es wurden Fragen gestellt zu den Bereichen Corporate Security, Bedrohungsanalysen (v.a. Prozess, Quellen), Social-Media-Einsatz (v.a. Gründe, Einsatzgebiete, Methode). Meinungen über den Einsatz von Social-Media-Analysen im Security Management wurden qualitativ erfragt, ebenso wie Einstellungen zur Nicht-Nutzung von sozialen Medien. Weiteres Augenmerk wurde darauf gerichtet, inwiefern Fake News bzw. eine verminderte Zuverlässigkeit von Social-Media-Informationen den Einsatz von sozialen Medien in der Unternehmenssicherheit einschränken.

Hervorzuheben ist grundsätzlich die positive Haltung von Security Manager*innen hinsichtlich des Social-Media-Einsatzes für Sicherheitsbelange. Hierbei werden Vorteile wie Schnelligkeit der Quellenart, Datenvolumen, Verfügbarkeit vorgebracht. Primär werden soziale Medien als Informationsquellen für Bedrohungsanalysen zur raschen Erfassung von Situationen eingesetzt. Physische Sicherheit, Reisesicherheit, Veranstaltungssicherheit sowie Krisenmanagement sind hierbei als Anwendungsfelder anzuführen. Nachteile, die vorwiegend für eine eingeschränkte Nutzung von Social Media im Security Management sprechen, sind ethische, rechtliche und finanzielle Gründe sowie Nachteile der Quellenart wie z.B. begrenzte Zuverlässigkeit, eigene Sprache, unstrukturierte Informationen.

SUMMARY

The main objective of this research project (01/2019–02/2020) was to investigate the preparation of threat analyses carried out by security managers in German-speaking countries. One focus was on the analysis of social media as a source of information and its areas of application in the field of corporate security as well as its advantages and disadvantages.

The results of this research project present basic attitudes of security managers about social media intelligence (SOCMINT), e.g., social media stand for real-time information and act primarily as secondary sources. Additionally, trends in business division sharing as well as current and future enterprise security challenges, the importance of local networks as sources of information, etc., are demonstrated.

Methodically, this research project used a mixed methods design. Nine guide-based expert interviews with security managers of three Austrian, one Swiss and five German companies from November 2018 to March 2019 were conducted, and an online survey was conducted.

The interviews were analyzed by means of a qualitative content analysis according to Kuckartz (2018) using a computer-assisted program (f4analysis program). The questionnaire was distributed via LimeSurvey (available online in September 2019 and November 2019). The data was analyzed using the statistical software SPSS; a total of 40 questionnaires were evaluated.

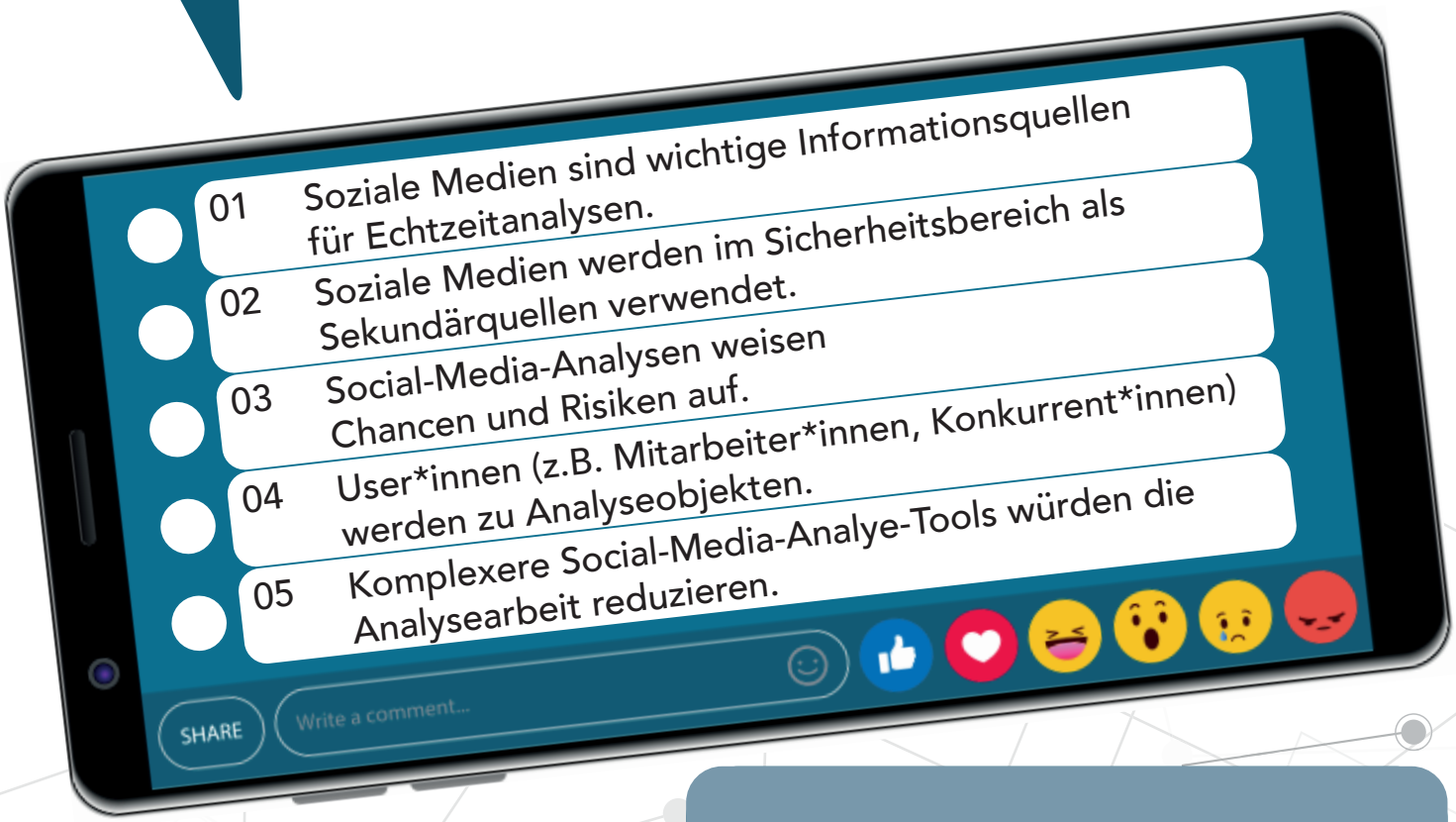
Questions were asked about corporate security, threat analysis (esp. process, sources) and social media use (esp. reasons, areas of application, method). Opinions on the use of social media analyses in security management as well as attitudes towards the non-use of social media were qualitatively analyzed. Further attention was paid to the extent to which fake news or a reduced reliability of social media information restrict the use of social media in corporate security.
The positive attitude of security managers with regard to the use of social media for security purposes should be emphasized. Advantages such as speed of source type, data volume, availability are presented. Social media are primarily used as a source of information for threat analysis, in order to understand situations quickly. Physical security, travel security, event security and crisis management are fields of application. Disadvantages that predominantly speak in favor of a restricted use of social media in security management are ethical, legal and financial reasons, as well as disadvantages of the source type such as limited reliability, a very specific language and unstructured information.

WICHTIGSTE ERKENNTNISSE:

EINSATZ VON SOCIAL MEDIA ANALYSIS IM SECURITY MANAGEMENT

Aus den Projektergebnissen lassen sich fünf zentrale Erkenntnisse ableiten:

„Das ist einfach eine neue, eine weitere Möglichkeit, Informationen in Echtzeit [...] zu generieren. Gerade jetzt im Vergleich zu, sage ich einmal, klassischen Medien, wo es dann erst in die Redaktion geht, dann ausgefiltert wird und dann weitergereicht wird. Da kann man natürlich wertvolle Minuten, Stunden [...] einfach sparen und zum anderen hat man natürlich viel, viel punktgenauere Informationen über Social Media." (Experte 7, Absatz 174)



„Aufgrund der starken Digitalisierung [hat man] […] eine immense Truhe an Daten zur Verfügung […], die für die Corporate Security und für das Sichern der Organisation in jedem Bereich extrem relevant sein können." (Experte 1, Absatz 7)

„Das, was sie über soziale Medien kriegen, das ist ja nicht immer sehr gut fundiert, sehr gut recherchiert, ist im Genauigkeits- und Detaillierungsgrad nicht das, was wir uns eigentlich wünschen." (Expertin 6, Absatz 112)

01 Soziale Medien sind wichtige Informationsquellen für Echtzeitanalysen.

Die Expert*innen schildern zwei Arten von Bedrohungsanalysen:

- **Ad-hoc-Analysen**
  Beispiel: Ein Bombenattentat passiert in der Stadt A. Security Manager*innen brauchen rasch Informationen, um Antworten zu Fragen wie „Was ist passiert?" und „Haben wir Mitarbeiter*innen in der Stadt A?" zu erhalten. Die Situation muss erfasst und verstanden werden, damit anschließend Entscheidungen für das Unternehmen und seine Mitarbeiter*innen getroffen und Maßnahmen gesetzt werden können.
- **Statische Analysen**
  Beispiel: Das Unternehmen möchte eine Veranstaltung im Land B durchführen und benötigt Vorab-Informationen über die soziale Lage, mögliche Bedrohungen etc.

Die befragten Expert*innen sind sich einig, dass soziale Medien vorrangig als Informationsquelle bei Ad-hoc-Analysen herangezogen werden, da hier der Faktor Zeit eine wesentliche Rolle spielt. Die Arbeitsweise zeigt sich incident-getrieben mit einer Affinität für „quick and dirty" – also rasche Ergebnisse ohne Anspruch auf Vollständigkeit. Mit der Verwendung von sozialen Medien verfolgen die Security Manager*innen das Ziel, ein Situationsbewusstsein in Echtzeit zu erlangen.

Um eine Situation zu erfassen, werden folgende drei Schritte vollzogen:

- Ansprechen: *Was ist passiert?*
- Beurteilen: *Was bedeutet das für mein Unternehmen?*
- Folgern: *Was muss ich tun?*

Informationen aus sozialen Medien können überwiegend für die Beantwortung der Frage „Was ist passiert?" herangezogen werden. Anhand dieser drei Analyseschritte werden die Stärken der sozialen Medien (z.B. Informationsfülle, Geschwindigkeit, Ortsungebundenheit), ihre Grenzen und das primäre Anwendungsfeld im Security Management (Einsatz bei Ad-hoc-Analysen) sichtbar.

02 Soziale Medien werden im Security Management als Sekundärquellen verwendet.

Die befragten Expert*innen bekräftigen die Quelleneinteilung in Primärquellen (z.B. Mitbewerber*innen, unternehmensinterne Quellen, direkt befasste Behörden) und Sekundärquellen (z.B. Medien, Datenbanken). Soziale Medien werden zu Hilfsmitteln – zu Sekundärquellen, die vor allem dann herangezogen werden, wenn Informationen schnell benötigt werden oder keine internen zuverlässigen Quellen verfügbar sind.

Insofern distanzieren sich die Expert*innen auch von einer Überbewertung dieser Quellenart und es wird die Empfehlung ausgesprochen, diese Quellenart dosiert einzusetzen.

Andererseits werden soziale Medien auch deshalb als Sekundärquellen ausgelegt, weil sie in erster Linie unstrukturierte Informationen liefern, die nach derzeitigem Stand eine zeitintensive – manuelle – Auswertung verlangen.

Soziale Medien zeigen sich demnach nicht als die „Haupt-OSINT-Quelle", sondern eine von vielen Quellen, die zur Informationsgewinnung teils manuell, teils automatisiert herangezogen werden, wobei davon ausgegangen werden kann, dass Daten aus dem Internet (v. a. aufgrund ihrer schnellen Verfügbarkeit) an Bedeutung gewinnen werden. Lokale Netzwerke, Nachrichtendienste, weitere Behörden, externe Dienstleister und Online-Quellen (exkl. Social Media) sind als sehr wichtige Informationsquellen anzuführen (siehe Grafik auf Seite 16 unten).

03 Social-Media-Analysen weisen Chancen und Risiken auf.

Aufgrund der eingeschränkten Zuverlässigkeit von sozialen Medien bzw. der fragwürdigen Richtigkeit frei verfügbarer Informationen sichern sich Security Manager*innen durch Cross-Checks (z.B. mit lokalen Kontaktpersonen, Behörden) ab.
Big Data zeigt sich zudem als Nachteil, da Unternehmen nur begrenzte Ressourcen zur Informationsverarbeitung durch Mitarbeiter*innen – mit oder ohne Softwaretools – besitzen. Die befragten Security Manager*innen sind sich sicher, dass in den nächsten Jahren die Automatisierung der Sammlung und Vorfilterung digitaler Informationen vorangetrieben wird, genauso wie die (Weiter-)Entwicklung von Softwaretools, um den derzeit hohen Arbeitsaufwand der Analyst*innen zu reduzieren.
Unternehmen sind aufgrund fehlender Ressourcen (z.B. Mitarbeiter*innen, Zeit, Analysetools) nicht in der Lage, weltweite Social-Media-Analysen durchzuführen. Social-Media-Analysen werden bereits als wichtiges Werkzeug verstanden, auf das sich Expert*innen derzeit aber nicht allein verlassen.

Die Expert*innen betonen einerseits Eigenschaften sozialer Medien, die für die Verwendung von Social Media als Informationsquellen für sicherheitsrelevante Belange sprechen:

- Big Data (Volumen)
- Geschwindigkeit
- Freie Verfügbarkeit der Informationen (eingeschränkt!)
- Orts-, raum- und zeitunabhängig

Andererseits werden folgende Eigenschaften kritisch gesehen:

- Nachteile der Quellenart (z.B. beschränkte Zuverlässigkeit, eigene Sprache, unstrukturierte Informationen)
- eingeschränkte Vertrauenswürdigkeit der Informationen (vgl. Fake News)

Unternehmen erkennen zunehmend, dass man durch soziale Medien nicht nur Informationen generieren (z.B. Vermarktung seiner eigenen Produkte, Veranstaltungsinformation), sondern auch für die eigene Unternehmenssicherheit gewinnen kann. Je nach Unternehmen (vgl. Rechtsform, Mitarbeiter*innen-Anzahl, Umsatz, Branche, Sitz, Risikoexposition, innovative vs. konservative Ausrichtung) variiert der Prozess der Bedrohungsanalysen und mit ihm die Durchführung von Social-Media-Analysen (z.B. nicht vorhanden, manuell, semi-manuell, automatisiert).

Die interviewten Security Manager*innen der österreichischen Unternehmen sehen keine Notwendigkeit für (automatisierte) Social-Media-Analysen für österreichische KMUs oder Unternehmen mit einer geringen Risikoexposition. In den folgenden fünf Anwendungsfeldern werden Social-Media-Analysen bereits durchgeführt bzw. als wertvoll erachtet (siehe auch Grafik auf Seite 17):

- Personenschutz
- Reisesicherheit
- Veranstaltungssicherheit
- Public Relations und Branding
- Krisenmanagement

„Die Geschwindigkeit der Informationsarbeit hat sich hochskaliert. Früher war eine Krise eine Krise, die lokal eingedämmt werden konnte. Mittlerweile hat man in Sekunden Informationen über den Vorfall über alle Social Media verbreitet. Das erzeugt Druck und Handlungsgeschwindigkeit auch im Bereich Corporate Security." (Experte 3, Absatz 25)

04 User*innen (z.B. Mitarbeiter*innen, Konkurrent*innen) werden zu Analyse-objekten.

Security Manager*innen sehen sich nicht als Big Brother. „Die Leute geben [in Social-Media-Netzwerken] freiwillig Sachen preis, die sie einem niemals erzählen würden", erklärte einer der befragten Expert*innen im Interview und verwies auf die Gefahr der freien Verfügbarkeit von Millionen digitaler Daten. Die drei Internetgiganten Google, Facebook und Amazon besitzen unzählige Daten ihrer User*innen. Mit der Nutzung sozialer Medien agieren User*innen in einer öffentlichen Sphäre, sie können somit Teile von Analysen werden und die Grenze zwischen Analyse und Überwachung ist hierbei fließend.

Es gibt unterschiedliche Vorgehensweisen der Kontrolle/Beobachtung, aber jene Methoden werden von den befragten Security Manager*innen abgelehnt – es gehöre nicht zu ihrer Aufgabe, polizeiliche Ermittlungsarbeiten zu leisten.

Es bleibt festzuhalten, dass die Nutzung von SOCMINT-Quellen bei den Security Manager*innen je nach Quellenart (öffentlich oder privat) unterschiedlich gesehen werden – ein Experte erklärte dazu im Interview:

„Da weiß ich auch von anderen Kollegen, dass die das ganz anders sehen. Dass die sagen: Alles was [es] an öffentlichen Quellen gibt, kann ich auch explorieren. Ich sehe das anders und ich möchte mir auch nicht irgendwann mal in der Presse vorwerfen lassen, dass ich Leute ausgeguckt habe, nur weil die komische Bilder posten. Da muss man unterscheiden, was kann man mit Social Media machen und was sollte man vielleicht nicht mit Social Media machen. Nur weil wir Sicherheitsfunktionen sind, wir sind ja nicht die Polizei oder der Staat. Ich kann mir solche Rechte nicht selber geben. Es hat Grenzen. Es ist die Frage, was ist eine Bedrohung und was ist keine Bedrohung und was wollen wir überhaupt damit erreichen."
(Experte 3, Absatz 45)

05 Komplexere Social-Media-Analye-Tools würden die Analyse-arbeit reduzieren.

Social-Media-Analyse-Tools bedienen vorrangig eine Sparte (z.B. Branding, Security). Aufgrund dieser Einseitigkeit verwenden in erster Linie Großunternehmen mehrere Tools gleichzeitig, um relevante Daten für das Unternehmen zu erlangen.

Der Prozess der Informationsgewinnung und -verarbeitung (z.B. manuelle Social-Media-Analyse) variiert je nach Unternehmen, ein Faktor bleibt konstant: die Analystin bzw. der Analyst. Die Analyst*innen tragen – mit oder ohne Softwaretool – eine hohe Verantwortung.

Eingeschränkte Filter- und Analysefunktionen von Softwaretools werden als Schwachstelle gesehen. Selbst die Nutzung bestimmter Keywords liefern unstrukturierte Informationen und in diesem Sinne lassen sich keine Lagebilder auf der Grundlage automatisierter Social-Media-Analysen erstellen. Die Analyst*innen übernehmen weiterhin den zeitintensiven Analyseschritt.

Situation-Awareness-Tools liefern Echzeit-Informationen, die z.B. Security Manager*innen als Push-

Benachrichtigungen auf ihre Smartphones bekommen. Diese Programme filtern frei verfügbare Daten in Social-Media-Netzwerken nach voreingestellten Schlüsselbegriffen und bieten dazu weitere Funktionen wie etwa bestimmte Suchradien um Standorte oder ein Alarmsystem zur ersten Einstufung von Ereignissen.

Die befragten Security Manager*innen wünschen sich weitere Funktionen. Die Softwaretools von morgen sollen folgende vier Eigenschaften aufweisen, um dadurch den Arbeitsaufwand der Analyst*innen zu reduzieren:

- Verbesserung der Filterfunktion („filter signal from noise“)
- Vorsortierung nach Relevanz bzw. verbesserte Konfigurationsmöglichkeiten
- Trends erkennen und sichtbar machen
- Einfache Handhabung

Eine eingeschränkte Nutzung bzw. Nicht-Nutzung von Social-Media-Analysis-Tools argumentieren die Expert*innen vor allem finanziell, rechtlich, ethisch oder personell (als Generationenfrage bei den Beschäftigten im Bereich Security). Softwaregestützte Social-Media-Analysen finden vor allem in großen Unternehmen Anwendung. KMUs oder Unternehmen mit einer geringen Risikoexposition spricht man eine Notwendigkeit eher ab.

„Also ich meine, das ist eines der größten Probleme überhaupt, dass wir mit der Informationsflut im Grunde genommen nur schwer mithalten können, und da sehen wir eben auch, dass die Ausbildung und die Weiterbildung von Analysten hier extrem wichtig sind, weil ich nur durch Menschen intelligent am Schluss erkennen kann, inwieweit die Informationen, die geliefert werden – sei es durch Social Media oder durch externe Dienste – überhaupt nutzbar sind.“ (Experte 5, Absatz 114)

UMFRAGE UNTER SECURITY MANAGER*INNEN

Der Fragebogen war im September 2019 und November 2019 via LimeSurvey online verfügbar und richtete sich an Security Manager*innen. Insgesamt wurden 40 Fragebögen ausgewertet, meist kamen die Antworten von 38 Befragten. Der Datensatz wurde mittels der Statistiksoftware SPSS analysiert, bei den Prozentangaben in der Folge handelt es sich um gerundete Zahlen.

Wenn in der Folge von Open Source Online Information (OSOI) die Rede ist, kommt folgende Definition zur Anwendung: "Information collected from publicly available sources, including social media, blogs and sensory networks to be used by organizations to inform their business and corporate intelligence functions."

Zusammensetzung der Befragten

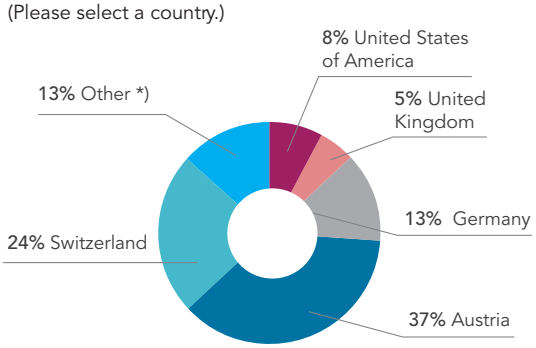
Nach Aufteilung des Herkunftslandes der Organisation zeigt sich folgende Verteilung: Die Mehrheit der Unternehmen, in welchen die Teilnehmer*innen tätig sind, kommt aus Österreich (37 %), gefolgt von der Schweiz (24 %), Deutschland (13 %), USA (8 %) und dem Vereinigten Königreich (5 %). Weitere Nennungen waren Australien, Liechtenstein und die Türkei (je eine Organisation).

Gefragt nach der Verteilung der geografischen Handlungsräume des Unternehmens zeigt sich, dass die überwiegende Mehrheit (66 % der Befragten) in Unternehmen arbeitet, welche in Westeuropa überwiegend aktiv sind, gefolgt von zentral- und osteuropäischen Ländern (CEEC; 53 %), dem Nahen Osten (47 %), USA und Kanada sowie Südostasien (je 45 %), Zentral- und Südamerika (40 %), Südasien (37 %), Ostasien sowie Nordafrika (je 34 %), Subsahara-Afrika sowie Ozeanien (je 32 %) und der Gemeinschaft Unabhängiger Staaten (CIS; 29 %). Weitere Angaben waren Österreich, D-A-CH, EU (je eine Nennung) und weltweit (je zwei Nennungen).

Mehr als die Hälfte der Teilnehmer*innen arbeitet in Großkonzernen mit mehr als 10.000 Beschäftigten (53 %).

Herkunftsländer der Organisationen

In which country is your organization based?
(Please select a country.)

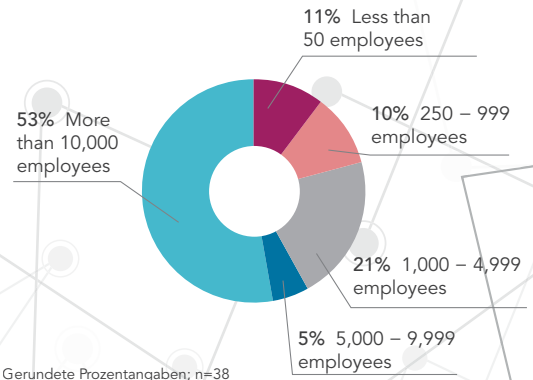


*) Other:
all countries and territories
Australia
in 40 countries
Liechtenstein
Turkey

Gerundete Prozentangaben; n=38

Größe der Organisationen (Anzahl Beschäftigte)

How many employees work at your organization?



Gerundete Prozentangaben; n=38

Die Befragten sind in den jeweiligen Unternehmen am häufigsten als Chief Security Officer (40 %), 8 % als Regional Security Manager tätig und jeweils 5 % nehmen die Funktion des Chief Information Security Officers, Country Security Managers oder Security Operations Center Managers ein.

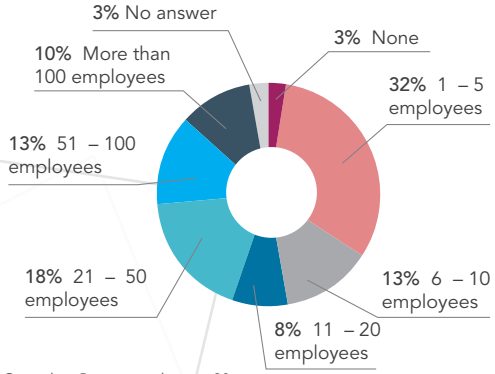
Die angegebenen Sicherheitsfunktionen, welche die Teilnehmer*innen (n=37) als Teil ihres Aufgabenportfolios in den entsprechenden Unternehmen einnehmen, gestalten sich sehr mannigfaltig. So sind sie vor allem in den Bereichen Security Strategy & Governance (92 %) sowie in Physical/ Site Security (87 %) und Crisis Management (82 %) tätig. Travel Security (79 %), Event Security (74 %), Executive Protection (66 %) und Business Continuity (50 %) wurden von über der Hälfte der Befragten als Aufgabenbereich angegeben.

Weitere Funktionen, die im Rahmen der Corporate Security abgedeckt werden, sind Investigation & Due Diligence (50 %), Information & Cyber Security (40 %), Disaster Recovery (34 %), Supply Chain Security (29 %), Data Protection & Privacy (26 %) und Product Security (21 %).

In den Unternehmen der Befragten entspricht die Größe des Corporate Security Teams in den häufigsten Fällen zwischen einem bis fünf Mitarbeiter*innen (32 %) und 21 bis 50 Mitarbeiter*innen (18 %).

Größe der Corporate Security Teams (Anzahl Beschäftigte)

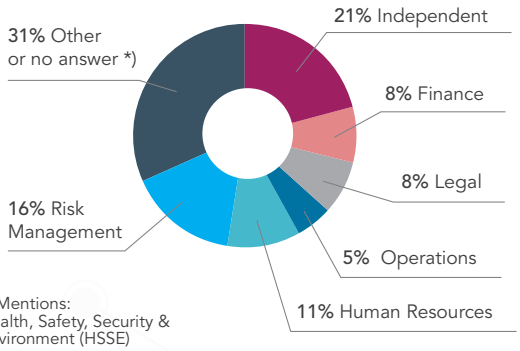
How many employees work in your Corporate Security Team (worldwide)?



Gerundete Prozentangaben; n=38

Organisatorische Eingliederung der Corporate Security

Under which department is Corporate Security located in your organization?



*) Mentions:
Health, Safety, Security & Environment (HSSE)
IT
Corporate Governance & Compliance
Sustainability

Gerundete Prozentangaben; n=38

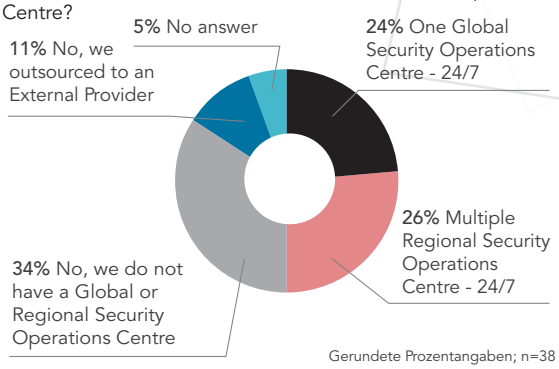
Von den 38 Befragten gaben 21 % an, dass die unternehmensinterne Corporate Security unabhängig von anderen Unternehmensbereichen agiert. 16 % geben an, dass der Bereich dem Risk Management zugeteilt ist. An dritter Stelle (11 %) wurde der Bereich Human Resources genannt, gefolgt von Finance und Legal (je 8 %) und Operations (5 %). 31 % der Teilnehmer*innen beschrieben Unternehmensbereiche wie Administration, Corporate Governance & Compliance, Executive, Health Safety, Security & Environment (HSSE), IT, Process & Data Management sowie Sustainability.

Ablauforganisation und Kommunikation

34 % der Teilnehmer*innen gaben an, dass das Unternehmen, in welchem sie tätig sind, über kein eigenständiges Security Operations Centre verfügt. 50 % der Befragten führen an, dass es in ihrem Unternehmen zumindest ein, wenn nicht mehrere Global bzw. Regional Security Operations Centre gibt. Und von den Befragten gaben 11 % an, dass sie diese Tätigkeiten an einen externen Anbieter ausgelagert haben; 5 % gaben keine Antwort.

Vorhandensein eines Security Operations Centers in der Organisation

Does your organization have a dedicated Security Operations Centre?



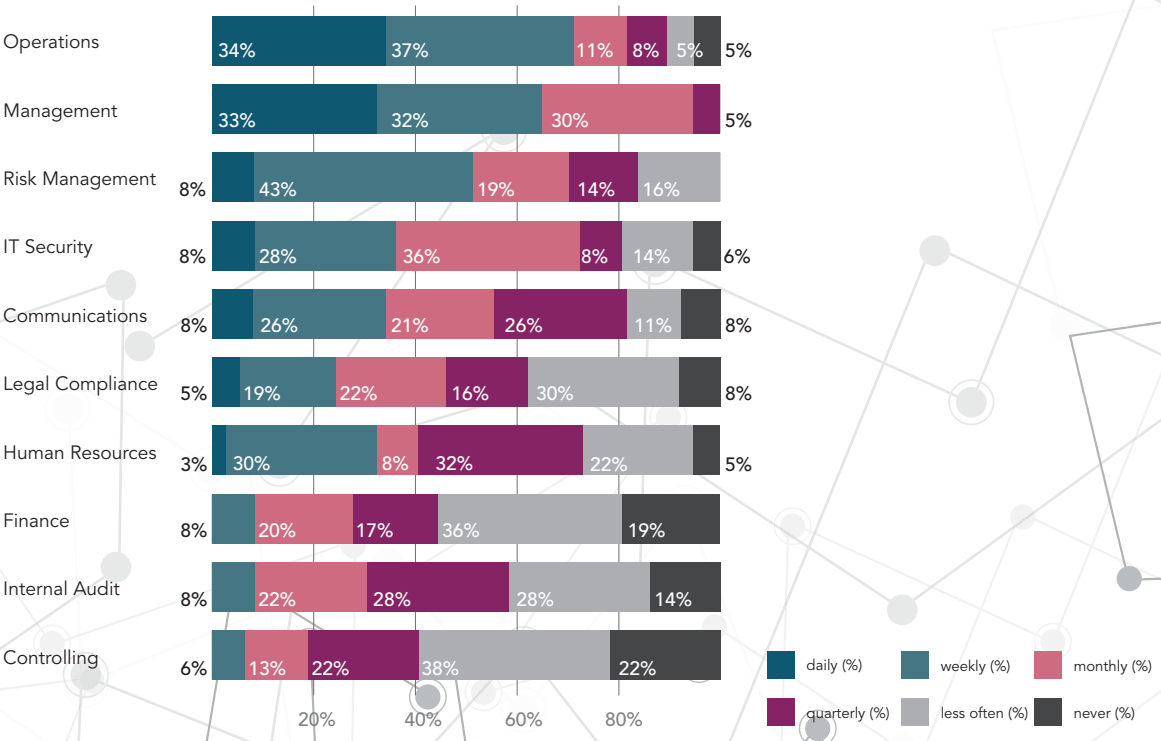
Gerundete Prozentangaben; n=38

Je 40 % der Befragten gaben an, dass in ihrem Unternehmen kein*e eigenständige*r Security Analyst*in bzw. nur ein*e bis fünf Mitarbeiter*innen mit dieser Funktion betraut sind. 8 % der Teilnehmer*innen gaben eine Anzahl von sechs bis zehn Mitarbeiter*innen an. Eine höhere Anzahl von Security Analyst*innen (elf bis 50 Mitarbeiter*innen) wurde nur von 6 % angegeben; drei Befragte haben keine Angaben zu dieser Frage gemacht.

34 % der Befragten kommunizieren täglich mit der Abteilung Operations und 33 % mit dem Management. Wöchentlich wird vor allem mit der Abteilung Risk Management (43 %) kommuniziert und monatlich erfolgt ein regelmäßiger Austausch mit der IT-Security-Abteilung (36 %). Zumindest einmal im Quartal wird von den Befragten am häufigsten mit Human Resources (32 %) kommuniziert. Unter jenen Abteilungen, mit welchen sich weniger oft bzw. nie ausgetauscht wird, ist das Controlling (38 % bzw. 22 %).

Frequenz der Kommunikation mit anderen Business Units

Please indicate to which extent you communicate to the following business units on a regular basis.

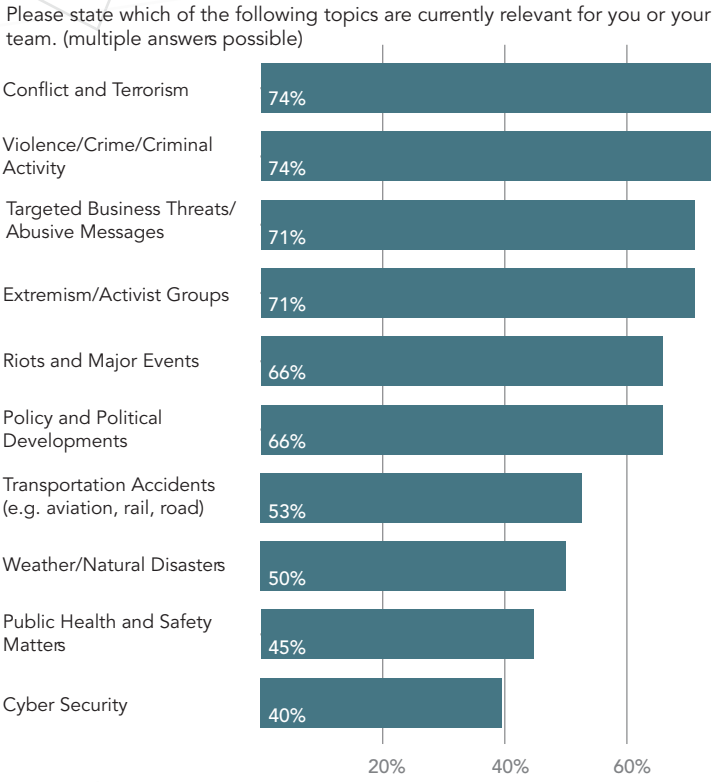


Gerundete Prozentangaben; n=38

Relevante Sicherheitsthemen und Herausforderungen

74 % der Befragten nennen Conflict & Terrorism und Violence/Crime/Criminal Activity als relevantes Thema für Security Teams. Es folgen mit jeweils 71 % Extremism/Activist Groups und Targeted Business Threats/Abusive Messages.

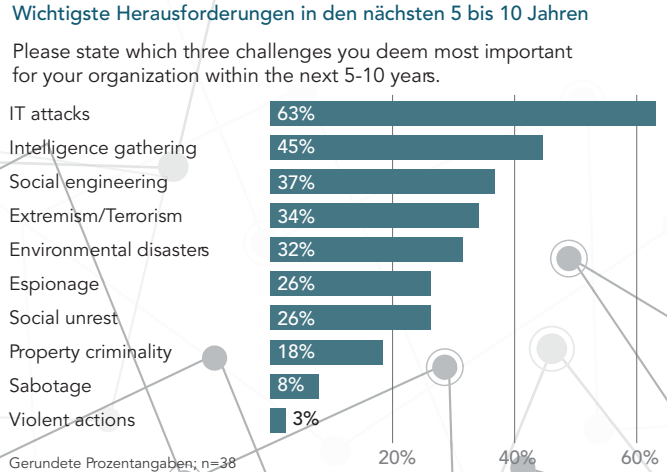
Einschätzung relevanter Sicherheitsthemen



Gerundete Prozentangaben; n=38

Die drei größten Herausforderungen für Unternehmen in den nächsten fünf bis zehn Jahren sind: IT Attacks (63 % der Teilnehmer*innen), Intelligence Gathering (45 %) und Social Engineering (37 %).

Wichtigste Herausforderungen in den nächsten 5 bis 10 Jahren



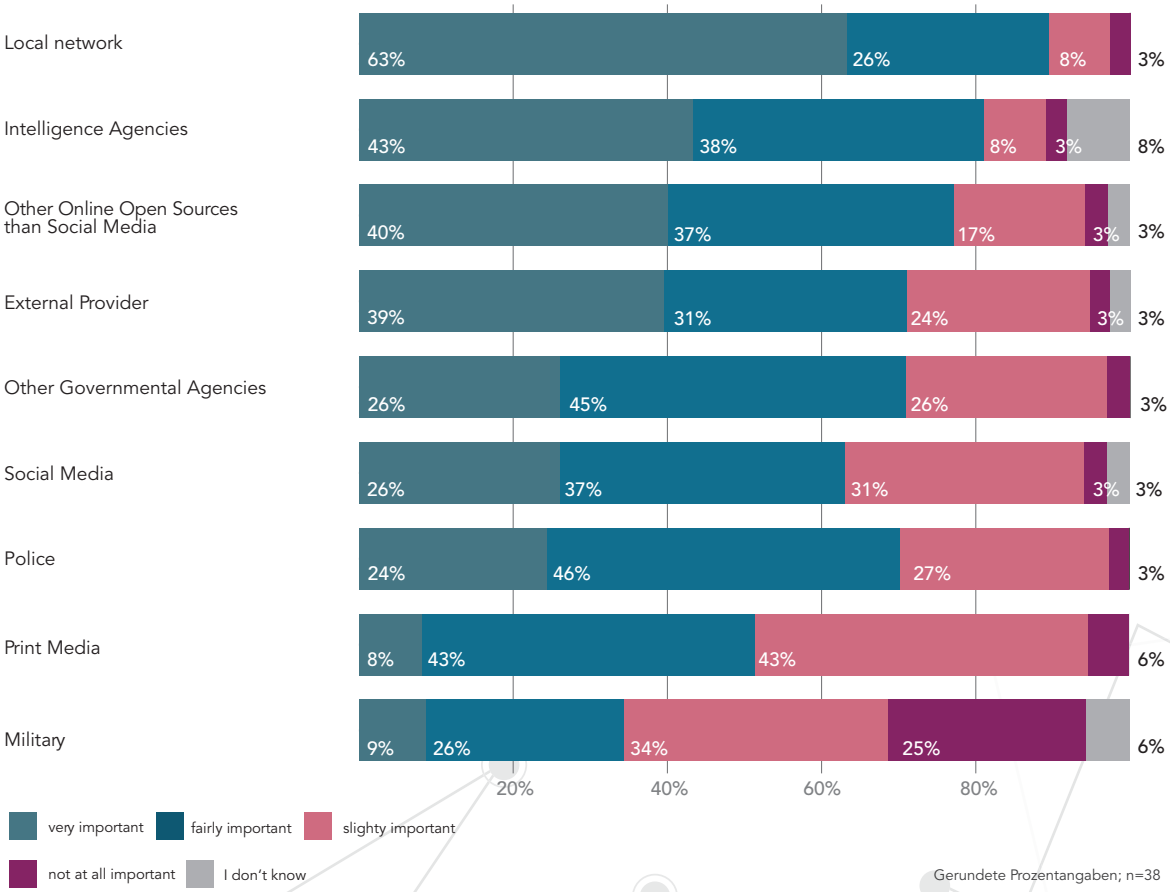
Gerundete Prozentangaben; n=38

Bedeutung von Informationsquellen und Arbeit damit

63 % der Befragten benennen das lokale Netzwerk als sehr wichtige Informationsquelle, 26 % als ziemlich wichtig, 8 % als wenig wichtig und 3 % als überhaupt nicht wichtig. Weitere bedeutende Informationsquellen sind nachrichtendienstliche Behörden (43 %), externe Dienstleister (39 %) sowie andere Online-Quellen als soziale Medien (40 %). Soziale Medien werden von 26 % der Befragten als sehr wichtige, 37 % als ziemlich wichtige, 31 % als wenig wichtige und 3 % als überhaupt nicht wichtige Informationsquelle bei der Erstellung des Information Collection Plans genannt.

Quellen für die Erstellung des Information Collection Plans

Please indicate to which extent the following sources are important for the creation of the Information Collection Plan.

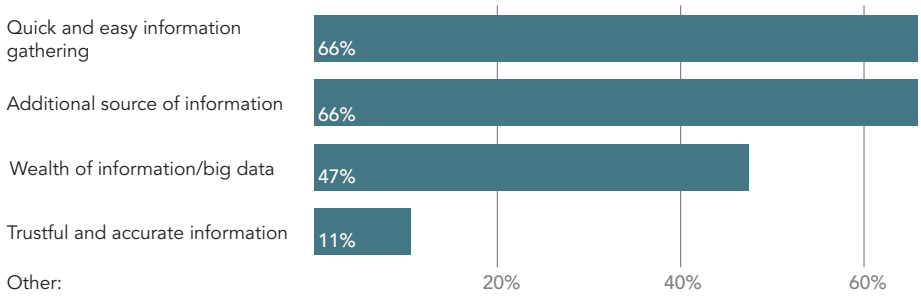


Gerundete Prozentangaben; n=38

Nach der Frage, ob die Befragten Open Source Online Information für die Zusammenstellung ihres Information Collection Plan nutzen, bejahten dies 89 % (n=36). Die Gründe für die Nutzung von Open Source Online Information sind vor allem "quick and easy information gathering" (66 %), "additional source of information" (66 %) sowie "wealth of information & big data" (47 %). Deutlich seltener wird als Motiv "trustful and accurate information" (11 %) genannt.

Gründe für Nutzung von Open Source Online Information

Why do you use Open Source Online Information for your Information Collection Plan? (multiple answers possible)

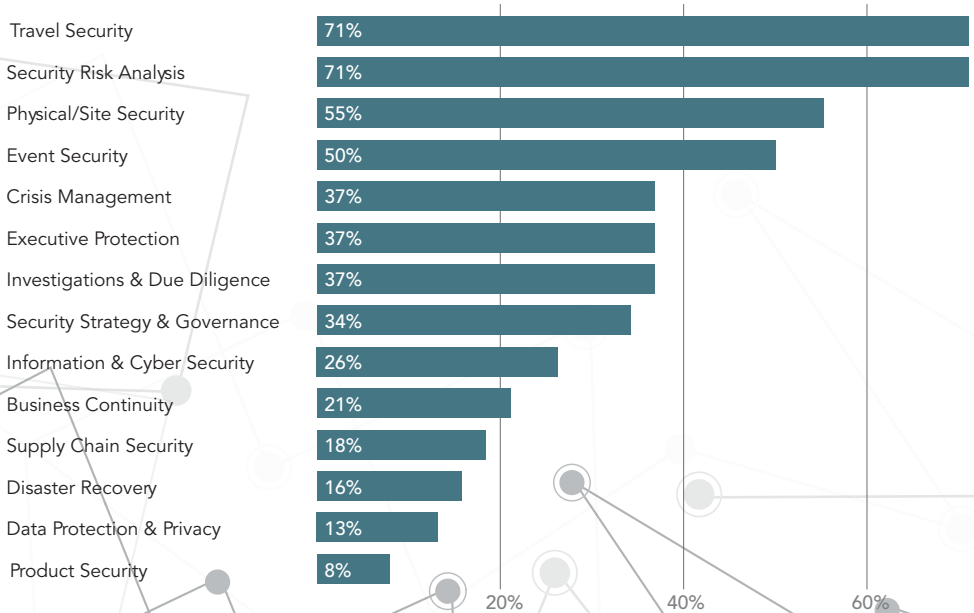


Gerundete Prozentangaben; n=38

Open Source Online Information werden laut den Befragten vor allem in den Bereichen Travel Security und Security Risk Analysis (je 71 %) angewendet. Seltener kommt es in den Bereichen Data Protection & Privacy (13 %) sowie bei Product Security (8 %) zum Einsatz.

Einsatzbereiche für Open Source Online Information

In which of the following areas do you use Open Source Online Information at the moment? (multiple answers possible)



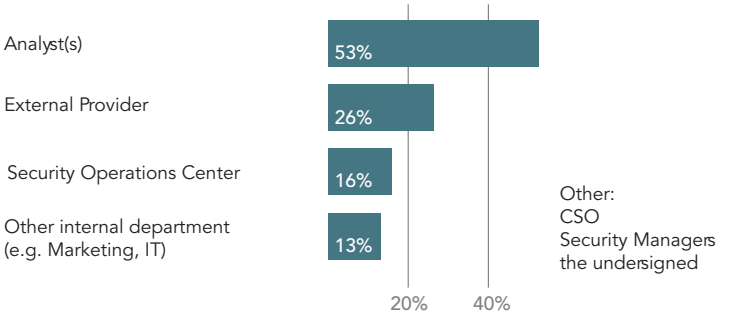
Gerundete Prozentangaben; n=38

Zuständigkeiten und Werkzeuge der Informationssammlung, -analyse und -aufbereitung

In den jeweiligen Unternehmen sind vor allem Analyst*innen (53 %) für die Sammlung, Analyse und Aufbereitung von Open Source Online Information für Corporate Security Anliegen zuständig. Seltener beschäftigen sich externe Dienstleister (26 %), Security Operations Center (16 %) oder ein anderer Unternehmensbereich (13 %) mit entsprechenden Anliegen.

Zuständigkeit für die Sammlung, Analyse und Aufbereitung von Open Source Online Information

Who is primarly responsible for the collection and processing of Open Source Online Information for Corporate Security purposes? (multiple answers possible)

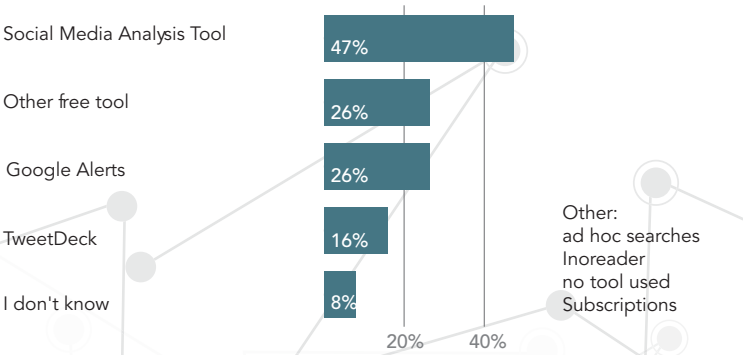


Gerundete Prozentangaben; n=38

Open Source Online Information werden am häufigsten über Social Media Analysis Tools (47 %) gesammelt. Google Alerts und andere frei verfügbare Tools kommen mit je 26 % sowie TweetDeck mit 16 % hierfür zum Einsatz. Als andere Datenbeschaffungsmaßnahmen wurden ad-hoc searches, Inoreader und Subscriptions genannt.

Verbreitung bestimmter Suchmethoden

How do you collect Open Source Online Information? (multiple answers possible)



Gerundete Prozentangaben; n=38

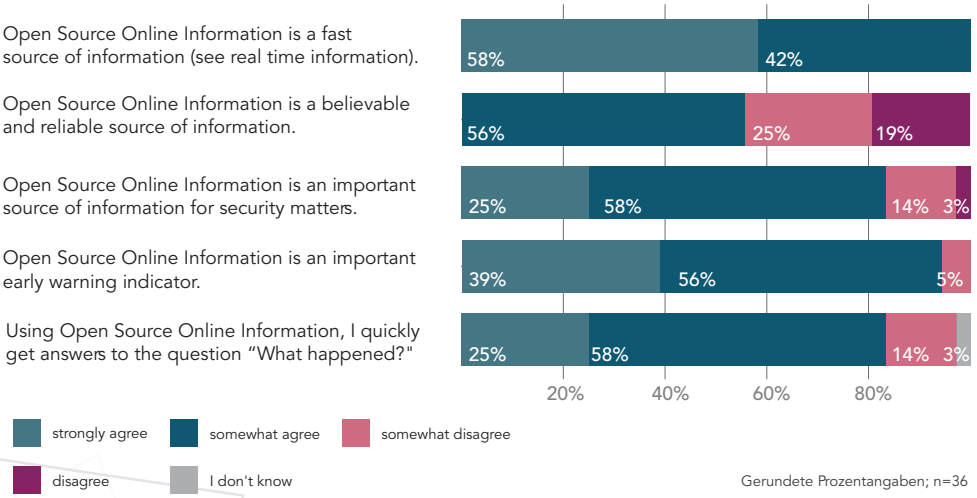
Beurteilung von Open Source Online Information

58 % der Befragten stimmen stark und 42 % stimmen eher der Aussage zu, dass Open Source Online Information schnell verfügbare Informationsquellen im Sinne von Echtzeitinformationen sind. 56 % der Teilnehmer*innen stimmen der Aussage – Open Source Online Information sind glaubwürdige und zuverlässige Quellen – eher zu, 25 % sind mit dieser Aussage nicht ganz einverstanden und 19 % stimmen nicht zu. Wobei insgesamt 83 % den Aussagen (eher bzw. stark) zustimmen, dass Open Source Online Information wichtige Quellen in Sicherheitsfragen darstellen und Antworten auf die Frage „Was ist passiert?" geben können.

95 % der Befragten bewerten Open Source Online Information als einen wichtigen Frühwarnindikator (39 % stimmen dieser Aussage stark zu, 56 % stimmen eher zu und 5 % stimmen eher nicht zu).

Allgemeine Einschätzungen

Please indicate to which extent you agree to the following statements about the features of Open Source Online Information.



Gerundete Prozentangaben; n=36

Fast die Hälfte der Teilnehmer*innen (47 %) vertritt die Meinung, dass Open Source Online Information in den derzeitigen Corporate Security Standards, Normen und Branchenrichtlinien verankert sein sollte (39 % stimmen dieser Aussage eher zu und 14 % stimmen eher nicht zu).

Über die Hälfte (63 %) der Befragten ist davon überzeugt, dass Open Source Online Information auch für andere Departments (z.B. Communications) in ihren jeweiligen Unternehmen relevant sein könnte. 50 % der Befragten stimmen stark mit der Aussage überein, dass die Bedeutung für Open Source Online Informationen für Corporate Security in den nächsten fünf bis zehn Jahren stark steigen wird (42 % stimmen dieser Aussage eher zu).