Deloitte.

Fraunhofer SIT

Cyber-Security
Die Perspektive des Informationsaustausches

Cyber Security
Die Perspektive des Informationsaustausches

Inhaltsverzeichnis

Einleitung

Am 7. Februar 2013 veröffentlichte die Europäische Kommission die Cyber Security Strategy der Europäischen Union mit dem Untertitel „An Open, Safe and Secure Cyberspace“. Die Strategie definiert fünf kurz-und langfristige Ziele und Maßnahmen, die die EU-Institutionen, die Mitgliedsstaaten und die Industrie betreffen:

1. Erreichung von Cyber Resilience
2. Drastische Reduzierung von Cyber-Kriminalität
3. Entwicklung von Cyber-Defense-Richtlinien und -Kapazitäten
4. Entwicklung industrieller und technologischer Ressourcen für Cyber-Sicherheit
5. Schaffung einer kohärenten, internationalen Cyberspace-Richtlinie für die Europäische Union

Ein Aspekt, der in nahezu jedem Ziel und jeder Maßnahme auftaucht, ist der Austausch von Cyber-Security-Informationen innerhalb und zwischen den privaten Sektoren, nationalen Einrichtungen, Mitgliedsstaaten und EU-Institutionen wie ENISA, Europol/EC3 und EDA.

Im April und Mai 2013 hat Deloitte in einer Online-Umfrage private europäische Organisationen aus der Forbes-Global-2000-Liste und ausgewählte öffentliche europäische Organisationen und Forschungsinstitute der ENSA Who-is-Who-Liste befragt.

Die Durchführung der Umfrage und die Auswertung der Ergebnisse erfolgten in Zusammenarbeit mit dem Deutschen Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

Ziele

Ziel der Umfrage war die Identifizierung des aktuellen Standes zum Cyber-Security-Informationsaustausch innerhalb der EU-Mitgliedsstaaten unter Einbeziehung folgender Themen:

- Reaktionsfähigkeit auf Cyber-Vorfälle und Eskalationsverhalten
- Bedeutung des Informationsaustausches für Cyber Security
- Vorhandensein und Auswirkungen aktueller nationaler Cyber-Richtlinien oder -Verordnungen
- Häufigkeit und Quellen für Cyber-Security-Informationseinholung
- Bereitschaft und tatsächliche Umsetzung des Informationsaustausches zu Cyber Security
- Kenntnis der EU Cyber Security Strategy und erwartete Auswirkungen

Ansatz

Die Teilnehmer wurden per E-Mail eingeladen, den Online-Fragebogen auszufüllen. Alle Antworten wurden anonym gesammelt, sodass Antworten keinem bestimmten Teilnehmer zugeordnet werden können. Die Ergebnisse der Umfrage sind dementsprechend ebenfalls anonym.

Cyber-Security-Informationsaustausch ist bereits ein europäisches Schwerpunktthema

Cyber-Sicherheit – neues Buzzword oder eine echte Herausforderung für Unternehmen und Behörden?

Mechthild Stöwer
Security Management
Fraunhofer SIT
Tel: +49 (0)2241 14 3123
mechthild.stoewer@
sit.fraunhofer.de

Peter Wirnsperger
Partner Cyber Security
Deloitte
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Eine absolute Cyber-Sicherheit gibt es nicht. Die Frage ist also nicht, ob ein Angriff auf das eigene IT-System erfolgt, sondern nur wann. Forschung, Wirtschaft und die öffentliche Hand sind gefordert, im Sinne einer „Collective Intelligence" gemeinsam gegen aktuelle und künftige Bedrohungen vorzugehen. Deloitte und das Fraunhofer SIT pflegen eine enge Kooperation und geben Antworten auf Fragen rund um Cyber-Sicherheit.

Was verbirgt sich hinter Cyber Security?

Deloitte
Cyber Security ist die logische Weiterentwicklung dessen, was man früher Informationssicherheit nannte. Heute geht es aber nicht mehr darum, spezielle Daten vor Einzeltätern zu schützen, sondern sich innerhalb eines komplexen Bedrohungsumfelds gegen die vielfältigen Formen von Angriffen zu wehren. Entsprechend deckt ein wirksamer Schutz die ganze Bandbreite verfügbarer Tools und Techniken aus den Bereichen Information Security, Operational Technology Security und IT Security ab. Wer also meint, mit aktueller Qualitätssoftware, implementierten Sicherheitsrichtlinien und -standards sei er auf der sicheren Seite, denkt zu kurz. Unternehmen müssen zugleich kontinuierlich ihre Infrastrukturen und Applikationen auf Sicherheitslücken kontrollieren und für den Fall einer Cyber-Attacke über Intrusion-Detection-Systeme sowie Notfallpläne verfügen.

Fraunhofer SIT
Der Begriff Cyber Security macht deutlich, dass alle mit dem Internet und vergleichbaren Netzen verbundenen Informations- und Kommunikationssysteme aus dem privaten, öffentlichen oder wirtschaftlichen Umfeld Angriffen aus dem weltweiten Netz ausgesetzt sind. Dabei sind die Angriffe heute hochprofessionell und von wirtschaftlichen und geostrategischen Interessen geleitet.

Ist Cyber Security nur ein Thema für Großunternehmen?

Fraunhofer SIT
Nein, im Gegenteil. Wir beobachten ein starkes Ungleichgewicht zwischen den Fähigkeiten der Angreifer, der Nachhaltigkeit ihrer Attacken und dem Sicherheitsstandard und -bewusstsein in den Unternehmen oder auch staatlichen Einrichtungen. Dabei hinken gerade mittelständische Unternehmen dem Potenzial der Angreifer hinterher. Dies ist umso kritischer, da sie mit ihren Innovationen und Technologien das Rückgrat der deutschen Volkswirtschaft bilden.

Die Brisanz wird durch die Tatsache deutlich erhöht, dass mittelständische Unternehmen zudem Elemente in organisationsübergreifenden Wertschöpfungsketten sind. Sie müssen deshalb einen hohen Sicherheitsstandard abbilden, um die Vertraulichkeit und Integrität der Informationen über die gesamte Kette zu gewährleisten.

Deloitte
Cyber-Kriminalität kann jeden treffen: von Privatpersonen über staatliche Institutionen und kritische Infrastrukturen bis zu vernetzten, globalen Konzernen und mittelständischen Betrieben.

Im Vergleich zu Großunternehmen birgt die geringe Kapitalausstattung von KMU[1] ein höheres Risiko: Schließlich können monetäre Verluste nach einem Cyber-Angriff existenzbedrohende Folgen haben. Hinzu kommt, dass KMU immer öfter zur Zielscheibe von Cyber-Kriminellen werden. 2012 stiegen allein die Malware-Attacken auf dieses Unternehmenssegment um 86 Prozent.

Wo liegen die Gefahren? Worauf muss man vorbereitet sein?

Fraunhofer SIT
Dass Cyber-Bedrohungen in vielfältiger Form existieren, ist hinreichend bekannt. Es gibt konventionelle Formen wie Online-Betrug im Zahlungsverkehr oder beim Einkauf im Internet. Eine besondere Bedrohung stellt dabei Cyber-Spionage dar, in deren Fokus dabei nicht nur Wirtschaftsunternehmen, sondern auch staatliche Einrichtungen stehen.

Zunehmend geraten auch Produktionssysteme in den Fokus von Cyber-Attacken. Wenn Einrichtungen kritischer Infrastrukturen wie Energieversorgungssysteme oder die Telekommunikationsinfrastruktur angriffen werden, können über kaskadierende Effekte ganze Bereiche der Wirtschaft betroffen sein. Besondere Herausforderungen entstehen in Zukunft auch durch den verstärkten Einsatz von Maschine-zu-Maschine Kommunikation. Diese bietet im Umfeld von Industrie 4.0-Konzepten große Effizienzpotentiale aber auch entsprechende Angriffsmöglichkeiten, sofern die IT-Sicherheit nicht von Anfang an bedacht wird. Die Forschung hat einige der skizzierten Herausforderungen bereits angenommen. So hat das Fraunhofer SIT zum Beispiel gemeinsam mit Unternehmen bereits zukunftsweisende Konzepte und erste Lösungen entwickelt.

Deloitte
2012 haben wir eine Vielzahl an Angriffen durch Botnetze, Malware, Trojaner und Phishing erlebt. Die Täter setzen dabei auf Qualität und Quantität der Attacken und agieren deutlich professioneller. Cyber-Kriminelle sind heute finanziell besser ausgestattet und zunehmend in Netzwerken

[1] Kleine und mittlere Unternehmen (KMU).

organisiert. Entsprechend werden die Attacken zielgerichteter, ausgeklügelter und sind schwieriger zu erkennen. Die meisten E-Spionage-Fälle werden oft nur durch Zufall entdeckt. Kein Wunder, dass der monetäre Schaden aus Cyber-Spionage für die deutsche Wirtschaft enorm ist. Er wird auf jährlich 50 Milliarden Euro geschätzt.

Auch rücken innovative Technologien stärker ins Visier der Cyber-Kriminellen: Der Einsatz von mobilen Privatgeräten und Cloud Services im geschäftlichen Umfeld macht die IT-Landschaft verwundbarer.

Und nicht zuletzt tragen aufgeklärte Mitarbeiter dazu bei, Bedrohungen wirksam zu bekämpfen. Klare Richtlinien, praxisnahe Schulungen und kontinuierliche Informationen schaffen Abhilfe.

Was sind die Voraussetzungen für Cyber Security?

Fraunhofer SIT

Cyber-Sicherheit erfordert angriffsresistente, robuste Systeme mit integrierten und kooperativen Angriffserkennungs- und -abwehrkonzepten. Dabei muss Sicherheit in Hardware- und Software-Architekturen verankert sein. Forschung und Industrie müssen mittelfristig gemeinsam Projekte umsetzen, die sich mit Themen wie Security by Design, neuen Risikomodellen, daraus resultierenden Informationssicherheitsmanagementkonzepten und der Absicherung von mobilen Systemen oder Sicherheit für Industrie 4.0 beschäftigen.

In jedem Fall sind aber die Unternehmen gefragt, ihre Sicherheitsanforderungen und ihren Schutzbedarf zu analysieren und zu bewerten. Die Auswahl der Lösungen muss sich dann an der aktuellen Bedrohungslage orientieren. Tests und Audits, aber auch die Integration von Sicherheitsmetriken im Sicherheitsmanagement sind zum Beispiel Instrumente, um das Sicherheitsniveau im Unternehmen nachhaltig zu verbessern.

Deloitte

Der Schlüssel ist, Cyber Security ganzheitlich zu bedenken. Unternehmen müssen Vorbereitungen treffen, Bedrohungen in Echtzeit auswerten und im Ernstfall koordiniert reagieren. Ausgangspunkt ist die Cyber-Strategie, die vielfältige Aspekte wie Systemsicherheit, Websicherheit oder Passwortsicherheit abdeckt und zugleich auf die aktuellen Trends ausgerichtet ist.

Eine umfassende Vorbereitung setzt voraus, dass Unternehmen mit den verschiedenen Bedrohungsszenarien für ihre Prozesse und Daten bestens vertraut sind. Bereits bestehende Maßnahmen müssen regelmäßig auf ihre Wirksamkeit überprüft werden. Technische und organisatorische Schwächen decken Cyber-Simulationen auf. Auf dieser Basis lässt sich eine integrierte Sicherheitsarchitektur für die Gesamtorganisation planen und umsetzen. Last but not least brauchen die Mitarbeiter Anleitung zum richtigen Umgang mit Informationen.

Beim Monitoring geht es darum, Angriffsversuche sofort zu erkennen und möglichst effektiv abzuwehren. Im Ernstfall kommt es auf schnelles und koordiniertes Handeln an. Ein gutes Krisenmanagement begrenzt den Schaden und sichert die Einbruchsspuren.

Welche Akteure sind beteiligt?

Deloitte

Cyber Security ist kein Thema ausschließlich für die IT- und Sicherheitsexperten im Unternehmen. Sie wird angesichts ihrer wachsenden Bedeutung für den nachhaltigen Unternehmenserfolg zu einer Top-Management-Aufgabe. Die Unterstützung der Geschäftsführung ist entscheidend. Denn zum einen brauchen Sicherheitskonzepte und -maßnahmen eine stabile finanzielle Grundlage. Zum anderen kommt es darauf an, Verhaltensänderungen auf allen Unternehmensebenen zu bewirken.

Fraunhofer SIT

Sicherheitskonzepte und -maßnahmen brauchen eine stabile finanzielle Grundlage. Deshalb ist Cyber Security (auch) eine Managementaufgabe. Das Management muss aber zudem Verhaltensänderungen auf allen Unternehmensebenen steuern. Denn das höchste implementierte Sicherheitsniveau ist nutzlos, wenn auf User-Ebene die Sicherheitssysteme bewusst oder unbewusst umgangen werden.

Wie können die Beteiligten zur Stärkung der Cyber Security zusammenwirken?

Fraunhofer SIT

Unter den beteiligten Akteuren gibt es einen großen Konsens darin, dass eine Stärkung der Cyber-Sicherheit durch einen Multi-Stakeholder-Ansatz befördert wird. So profitieren sowohl staatliche Einrichtungen als auch Wirtschaftsunternehmen davon, dass Informationen zu aktuellen Bedrohungen, Vorkommnissen und entsprechenden Gegenmaßnamen ausgetauscht werden.

Deloitte

Ich bin davon überzeugt, dass die sich wandelnden Bedrohungen im Cyber Space durch eine engere Kooperation zwischen Unternehmen und Security-Dienstleistern auf der einen Seite und Wirtschaft, Wissenschaft und Politik auf der anderen Seite sich effektiver bekämpfen lassen. Wir brauchen eine „Collective Intelligence", die aus dem Austausch von Informationen über Schwachstellen, Gefährdungen und Gegenmaßnahmen entsteht.

Detaillierte Umfrageergebnisse

Teilnehmer

Etwa 350 Teilnehmer aus privaten und öffentlichen Organisationen, Forschungsinstituten und Industriegruppen aus 31 Ländern aus ganz Europa wurden zu dieser Online-Umfrage eingeladen.

In den privaten Organisationen waren die unterschiedlichen Branchen wie Fertigung, Gesundheitswesen und Naturwissenschaften, Finanzdienstleistungen oder Technologie, Medien und Telekommunikation vertreten. Zu den öffentlichen Organisationen gehörten Ministerien, Behörden für Informations-und Kommunikationstechnologie, Polizei- und Nachrichtendienste & Geheimdienste. Zu den Forschungsinstituten zählten Universitäten, Institute und Laboratorien für Informations- und Kommunikationstechnologie.

Ergebnisse

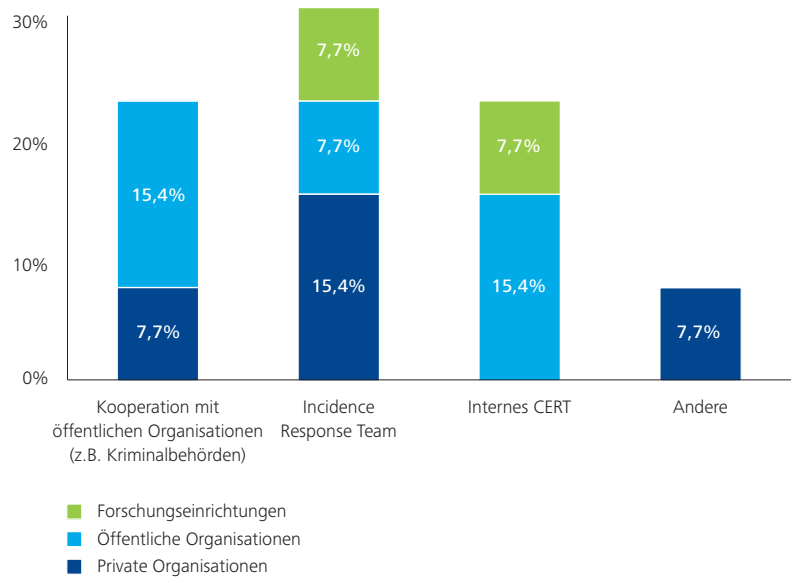
Von allen Teilnehmern, die an der Umfrage teilgenommen haben, waren 31% aus privaten Organisationen, 54% aus öffentlichen Organisationen und 15% aus den Forschungsinstituten. Rund 85% der Teilnehmer waren Organisationen mit weniger als 500 Mitarbeitern (Abb. 2).

Aufgrund der unerwartet niedrigen Rückläuferquote betrachten wir die Ergebnisse als nicht repräsentativ. Allerdings zeigt die Auswertung einen Vergleich zwischen privaten und öffentlichen Organisationen mit zusätzlichen Einblicken in die Forschungsinstitute. Industriegruppen sind in den Ergebnissen nicht abgebildet.

Reaktionsfähigkeit auf Cyber-Vorfälle und Eskalationsverhalten

31% der Befragten gaben an, ein lokales Incident Management Team etabliert zu haben. 23% verfügen über ein internes CERT und weitere 23% würden Unterstützung bei lokalen, öffentlichen Organisationen suchen.[1] Für den Fall, dass ein Cyber-Vorfall nicht selbst behandelt werden kann, würde die Mehrheit der Befragten Unterstützung durch öffentliche Organisationen suchen. In den meisten Fällen wurden zentrale oder bundesstaatliche CERTs als Quelle der Unterstützung genannt. Eine geringe Anzahl würde nationale Polizeidienststellen oder die Bundespolizei involvieren (Abb. 1).

Abb. 1 – Cyber-Incident-Möglichkeiten und Eskalations-Verhalten pro Sektor



[1] Die übrigen 23% haben entweder nicht auf die Fragen geantwortet oder sind selbst ein CERT.

Bedeutung des Informationsaustausches für Cyber Security

Die Befragten sind sich der Bedeutung des Informationsaustausches als wichtige Maßnahme in einem Cyber-Security-Programm durchaus bewusst: Rund 92% bewerteten den Austausch von Informationen mit hoher Priorität, 8% mit mittlerer und keiner mit niedriger (Abb. 3).

Vorhandensein und Auswirkungen aktueller nationaler Cyber-Security-Richtlinien oder -Verordnungen

Über alle Branchen hinweg gaben 64% der Befragten an, dass sie keiner bestehenden regionalen/nationalen oder EU-Cyber-Security-Richtlinie oder -Verordnung unterliegen. Die 36%, die bestehenden Richtlinien oder Verordnungen unterliegen, nannten beispielhaft die EU-Richtlinie 2009/140/CE, das portugiesische elektronische Kommunikationsgesetz Nr. 51/2011, die schwedische Regelung SFS 2006:942 über Notfallvorsorge und anderen nationale Gesetze in Bezug auf Cyber Security oder Cyber-Kriminalität. Der Bereich Information Security Governance ist am stärksten vom Informationsaustausch betroffen, gefolgt von Austausch in den Bereichen Technologien und Geschäftsprozesse.

Abb. 2 – Rückmeldung nach Sektor und Größe

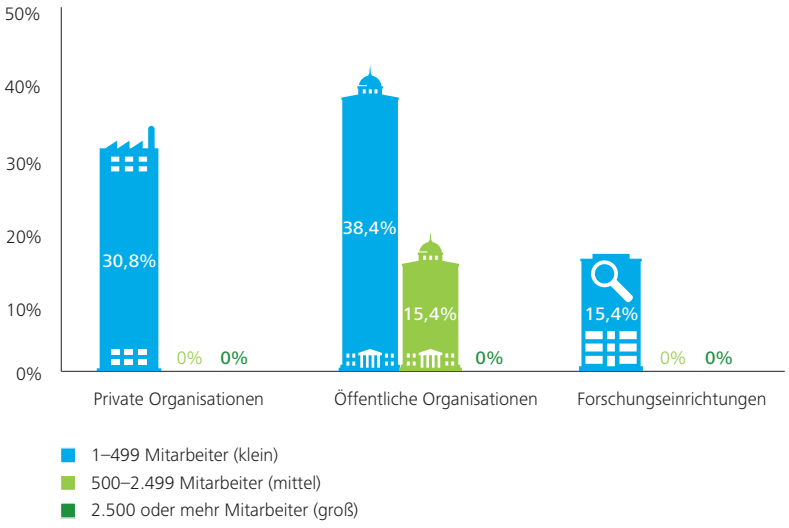
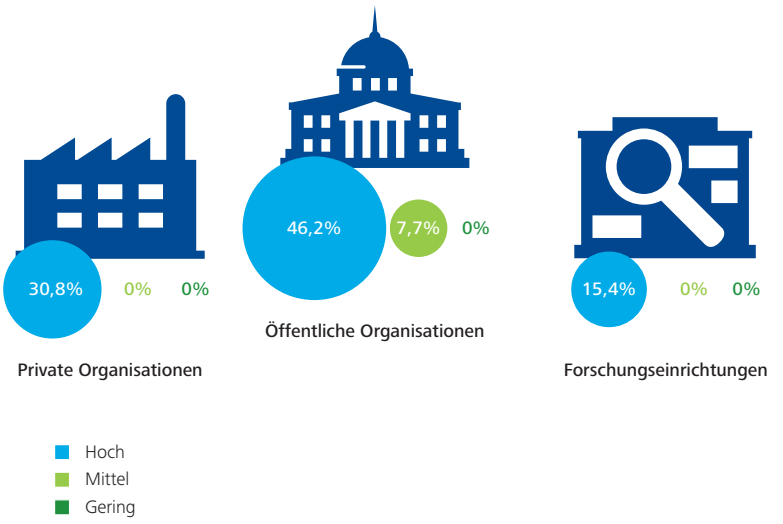


Abb. 3 – Bewertung der Wichtigkeit von Cyber-Security-Informationsaustausch nach Sektoren

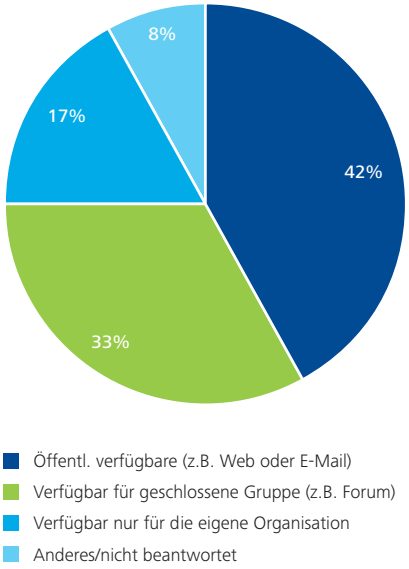


Häufigkeit und Quellen für Cyber-Security-Informationseinholung

62% der Befragten nutzen regelmäßig[2] verfügbare Cyber-Security-Informationen. Quellen sind zu 24% öffentliche Organisationen, zu 24% private Organisationen und zu 15% Forschungsinstitute. Andere Quellen wie Industriegruppen spielen lediglich eine untergeordnete Rolle.

Bei der Wahl der Quellen konnten keine Sektor-spezifischen Präferenzen festgestellt werden. Öffentliche und private Organisationen verwenden gleichermaßen Quellen aus öffentlichen und privaten Organisationen. Die meisten Organisationen bevorzugen allerdings öffentlich zugängliche Informationen (42%), wobei etwa 50% Informationen nutzen, die entweder nur für eine geschlossene Gruppe oder explizit nur der eigenen Organisation zugänglich sind (Abb. 4).

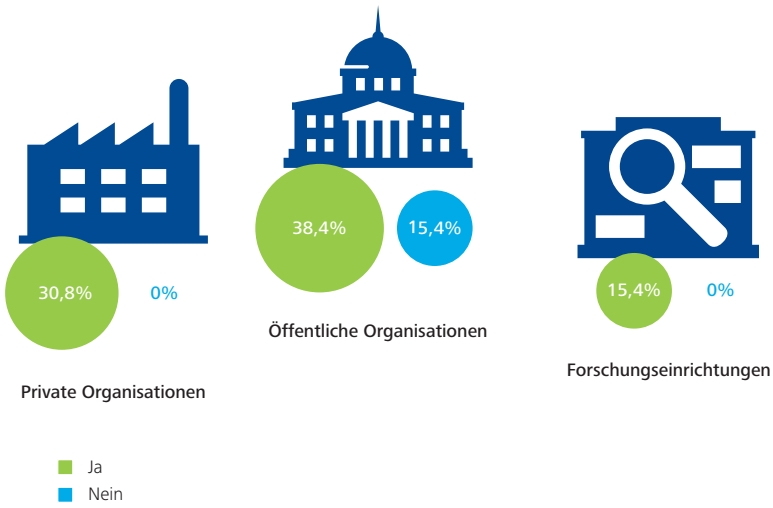
Abb. 4 – Bevorzugte Quellen für Cyber-Security-Informationen



Bereitschaft und tatsächliche Umsetzung des Informationsaustausches zu Cyber Security

Rund 85% aller Befragten sind bereit, Cyber-Security-Informationen zu teilen. Die rund 15%, die es ablehnen Informationen auszutauschen, sind ausschließlich öffentliche Organisationen. Zwei Drittel dieser 85% wären bereit, Informationen auf freiwilliger Basis auszutauschen, während ein Drittel angibt, dies nur zu tun, wenn es erforderlich und gesetzlich geregelt ist (Abb. 5).

Abb. 5 – Bereitschaft zum Teilen von Cyber-Security-Informationen nach Sektor



[2] Monatlich, täglich oder häufiger.

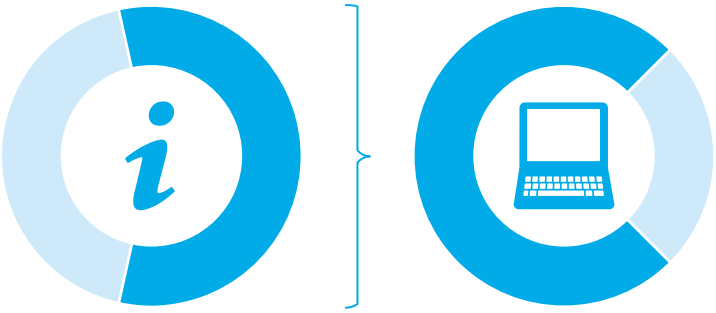
Bei der Frage, ob Organisationen derzeit tatsächlich Informationen zu Cyber Security teilen, zeichnet sich ein anderes Bild. Lediglich 57% sind aktiv an einem Austausch beteiligt; innerhalb dieser Gruppe sind öffentliche Organisationen mit 50% am häufigsten vertreten. Von den Sektoren, die derzeit aktiv an keinerlei Informationsaustausch teilnehmen, sind 60% private Organisationen.

Informationen, die ausgetauscht werden, betreffen hauptsächlich aktuelle Themen zu Cyber-Bedrohungen, gefolgt von Angaben über erfolgreiche Cyber-Attacken, Indikatoren der Gefährdung und Best-Practice-Kontrollen. Am häufigsten erfolgt ein Informationsaustausch mit öffentlichen Organisationen.

Drei Viertel der 57%, die tatsächlich Informationen teilen, nutzen hierzu ein spezielles Software-Tool. Obwohl Kritik an eingesetzen Tools geäußert wurde, z.B. hohe Komplexität, technische Probleme oder Mangel an qualifizierten Teilnehmern, ist die Mehrheit zufrieden mit dem System.

Kenntnis der EU Cyber Security Strategy und erwartete Auswirkungen

Auf die Frage, ob die Teilnehmer die EU Cyber Security Strategy kennen, antworteten doch 57% mit „Ja". Von diesen 57% hat ein Viertel konkrete Maßnahmen geplant, um die Strategie umzusetzen – allesamt private Organisationen. Als größte Einschränkungen für die Einhaltung der Strategie wurden Budget und organisatorische Herausforderungen genannt.



57%
sind aktiv an einem Austausch beteiligt

3/4 dieser nutzen ein spezielles Software-Tool zum Informationsaustausch

Zusammenfassung

Allen Sektoren und Branchen betrachten den Austausch von Cyber-Security-Informationen als sehr wichtig. Die Mehrheit der Teilnehmer ist bereit, sich an einem Cyber-Informationsaustausch zu beteiligen, und würde dies auf freiwilliger Basis tun. Jedoch teilen derzeit 43% keinerlei Informationen zu Cyber Security. Hauptgründe hierzu sind primär rechtliche Bedenken oder geschäftliche Belange sowie ein Mangel an Ressourcen oder geeignetem Personal. Weitere Rückmeldungen, die wir während der Einladungsphase erhielten, deuten an, dass viele Organisationen das Thema Cyber-Security-Informationsaustausch bisher noch nicht in ihre jeweiligen Cyber-Security-Governance- Programme integriert haben[3]. Die niedrige Teilnahmequote gibt daher auch einen Hinweis darauf, dass viele Organisationen scheinbar noch nicht bereit sind, Informationsaustausch als wichtige Quelle für die Verbesserung ihrer Cyber Security anzusehen.

Mehr als die Hälfte der Teilnehmer kennen die EU Cyber Security Strategy, wobei die Kenntnis bei privaten Organisationen proportional viel höher ist als in jedem anderen Sektor. Dies und Statistiken über geplante Maßnahmen zeigen, dass private Organisationen Cyber-Security-Gesetzen und -Vorschriften sowie deren möglichen Auswirkungen auf ihr Geschäft große Beachtung schenken.

Die Umfrage zeigt außerdem, dass sich vor allem kleine bis mittlere Organisationen im Falle eines schwerwiegenden Cyber-Vorfalles nicht an Polizeibehörden wenden würden. Gründe dafür können mangelndes Vertrauen, Unwissenheit bezüglich potenzieller Unterstützung oder Interessenkonflikte sein. Dies könnte ein interessantes Thema für weitere Untersuchungen sein.

[3] Potenzielle Teilnehmer – primär aus den Bereichen „mittel" und „groß" (siehe Abb. 2) – gaben an, dass in ihren Organisationen Policies oder Rollen & Verantwortlichkeiten für den Austausch von Cyber-Security-Informationen fehlen. Aus diesem Grund würden sie nicht an der Studie teilnehmen.

Wo Sie uns finden

10719 Berlin
Kurfürstendamm 23
Tel: +49 (0)30 25468 01

01097 Dresden
Theresienstraße 29
Tel: +49 (0)351 81101 0

40476 Düsseldorf
Schwannstraße 6
Tel: +49 (0)211 8772 01

99084 Erfurt
Anger 81
Tel: +49 (0)361 65496 0

60486 Frankfurt am Main
Franklinstraße 50
Tel: +49 (0)69 75695 01
Consulting:
Franklinstraße 46–48
Tel: +49 (0)69 97137 0

06108 Halle (Saale)
Bornknechtstraße 5
Tel: +49 (0)345 2199 6

20355 Hamburg
Dammtorstraße 12
20354 Hamburg
Tel: +49 (0)40 32080 0

30159 Hannover
Georgstraße 52
Tel: +49 (0)511 3023 0
Consulting:
Theaterstraße 15
Tel: +49 (0)511 93636 0

50672 Köln
Magnusstraße 11
Tel: +49 (0)221 97324 0

04317 Leipzig
Seemannstraße 8
Tel: +49 (0)341 992 7000

39104 Magdeburg
Hasselbachplatz 3
Tel: +49 (0)391 56873 0

68165 Mannheim
Reichskanzler-Müller-Straße 25
Tel: +49 (0)621 15901 0

81669 München
Rosenheimer Platz 4
Tel: +49 (0)89 29036 0

90482 Nürnberg
Business Tower
Ostendstraße 100
Tel: +49 (0)911 23074 0

70597 Stuttgart
Löffelstraße 42
Tel: +49 (0)711 16554 01

69190 Walldorf
Altrottstraße 31
Tel: +49 (0)6227 7332 60

Ihre Ansprechpartner

Für mehr Informationen

Peter Wirnsperger
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Thomas Donner
Tel: +49 (0)89 29036 8614
tdonner@deloitte.de

Für weitere Informationen besuchen Sie bitte unsere Webseite auf www.deloitte.com/de/cyber

Stand 10/2013