Die Perspektive der Fachleute:

Cyber-Sicherheit in der DACH-Region

FROST & SULLIVAN

Eine Studie von Frost & Sullivan in Zusammenarbeit mit:

(ISC)²

(ISC)² FOUNDATION

A Frost & Sullivan White Paper

Autoren:

Michael Ranke, Vice President, Customer Research

Jarad Carleton, Principal Consultant, Digital Transformation

EINLEITUNG

Seit über einem Jahrzehnt entwickelt und veröffentlicht die (ISC)² globale Studien zum Berufsstand von Informations- und IT-Sicherheitsexperten. Sie bietet damit Einblick in die Herausforderungen der Cyber-Sicherheit und beleuchtet, wie Fachkräfte auf ein sich rasant veränderndes Geschäfts- und Sicherheitsumfeld reagieren. Die Cyber-Sicherheit ist eine Herausforderung globaler Natur – doch die Reaktion darauf ist es oft nicht. Die weltweite Betrachtung ähnlicher Sicherheitsprobleme und ihrer unterschiedlichen Handhabung lässt ein besseres Verständnis der Informationssicherheits-branche zu.

Die (ISC)² Global Information Security Workforce Study von 2015 beruht auf einer Umfrage unter fast 14.000 Fachkräften weltweit, davon über 500 aus der DACH-Region (D für Deutschland, A für Österreich und CH für die Schweiz). Der vorliegende Bericht nimmt diese DACH-Daten genauer unter die Lupe, um die berufliche und geschäftliche Dynamik in der Region zu erhellen.

In der Umfrage gewähren Informations- und IT-Sicherheitsspezialisten der DACH-Region Einblick in ihr Arbeitsumfeld. Ihre Antworten zeigen Stärken und Schwächen im Umgang mit Sicherheitsproblemen auf und markieren Schwerpunkte bezüglich aktueller und künftiger Budgets sowie Personalbedarfe. DACH-Fachkräfte haben dadurch die Möglichkeit, ihr eigenes Unternehmen mit dem regionalen Durchschnitt zu vergleichen (hilfreich für die Geschäftsplanung über die nächsten zwei Jahre) und datengestützte Gespräche mit leitenden Managern zu führen, die besser über die Herausforderungen der Cyber-Sicherheit informiert sein müssen.

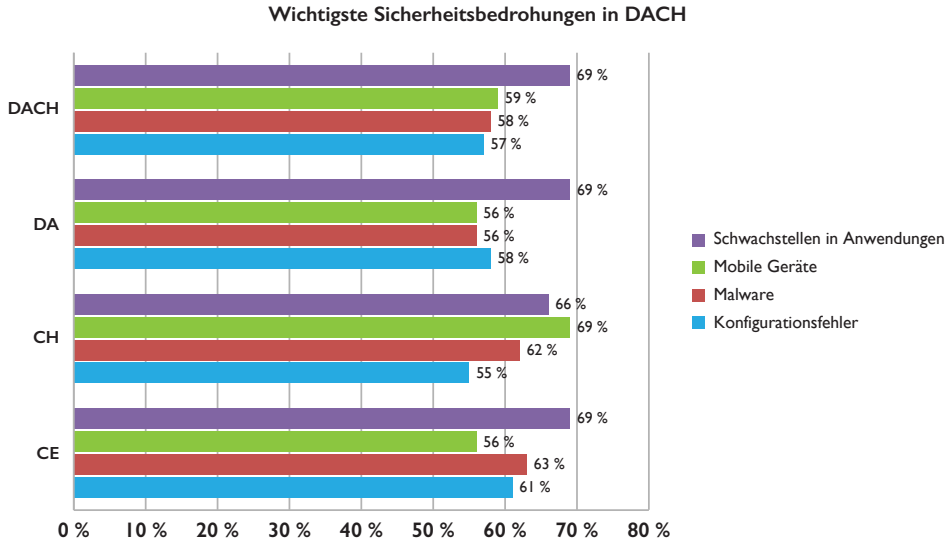
Um einen geeigneten Kontext für Geschäftsplanung und Management-Gespräche zu bieten, werden die Daten in den meisten Fällen für die DACH-Region insgesamt sowie aufgeschlüsselt für DA, CH und CE (Core Europe, Kerneuropa) bereitgestellt.[1]

Grundsätzlich sind sich DA und CH recht ähnlich. Es gibt allerdings einen großen, allgemein bekannten Unterschied – IT-Sicherheitsspezialisten in CH werden besser bezahlt. Wenn man DACH in zwei Unterregionen aufteilt, zeigt sich, dass Gehälter in DA und CE in etwa übereinstimmen, in CH dagegen um 37 Prozent höher liegen.

1 „Kerneuropa“ ist definiert als das kontinentale Westeuropa, Skandinavien und das Vereinigte Königreich.

Die Bedrohungs-Landschaft: Wichtigste Anliegen und Gefährdungen

Bei der Frage nach den häufigsten Sicherheitsrisiken in der DACH-Region zeigt sich ein interessanter Unterschied zwischen den wichtigsten Risiken einerseits und den am häufigsten festgestellten Risiken andererseits. Fachkräfte in CE und DACH sind mit ähnlichen Bedrohungen konfrontiert, obwohl es einige Unterschiede in der Bewertung ihrer Wichtigkeit gibt.



Quelle: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH und Kerneuropa, N = 2.801

Schwachstellen in Anwendungen wurden in DACH und CE – genau wie im Rest der Welt – als größte Sicherheitsbedrohung identifiziert. Dass Softwareentwickler unter Druck stehen, weil ihre Manager aggressive Markteinführungs-Zeitpläne für neue Produkte vorgeben, ist kein Geheimnis. Dies führt zu nachlässigen Entwicklungspraktiken mit begrenzten oder gänzlich fehlenden Sicherheitstests. Leider ist es nach wie vor wichtiger, ein neues Produkt vor einem Wettbewerber herauszubringen, als eine sichere Anwendung zu entwickeln. Hacker verstehen diese Dynamik genauso wie IT-Sicherheitsexperten.

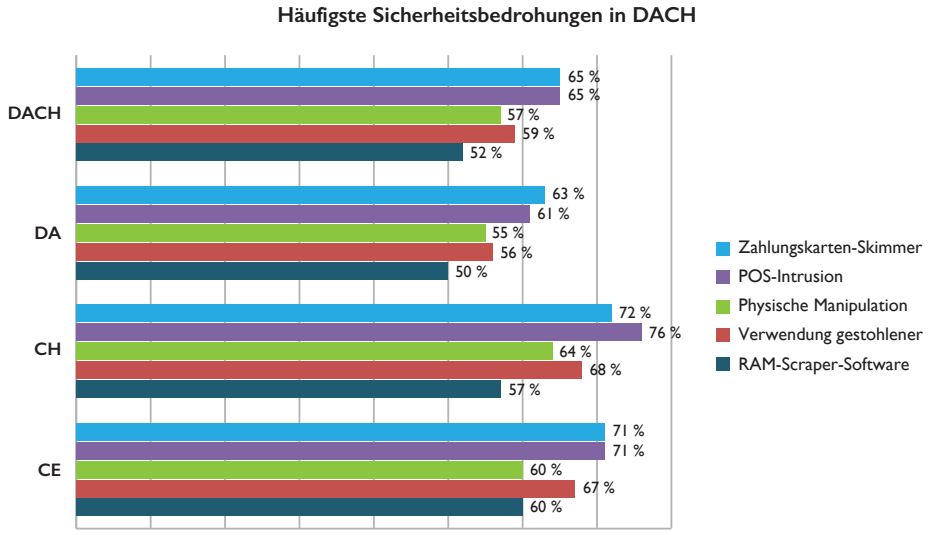
In Bezug auf mobile Geräte zeigt sich in der DACH-Region ein interessanter Unterschied. Während die Sorge im Zusammenhang mit mobilen Geräten weltweit deutlich zurückgegangen ist (wie von den DA- und CE-Daten bestätigt), herrscht in CH eine andere Sicht: Sicherheitsbedenken liegen hier um 13 Prozent höher als in DA. Die stärkere Sensibilisierung in CH lässt sich vermutlich dadurch erklären, dass das Land weltweiter Marktführer bei Offshore-Finanzdienstleistungen ist und erhebliches geistiges Eigentum in seine MEM-[2] sowie Chemie-/ Pharma-Industrien investiert hat.

Malware bleibt ein Grund zur Sorge für IT-Sicherheitsexperten. Angestellte lassen sich durch Social Engineering weiterhin leicht dazu verleiten, auf Dateien und Links von unbekannten Absendern zu klicken. Insgesamt sind DA-Fachkräfte in Bezug auf Malware etwas weniger besorgt (56 %) als ihre Kollegen in CH und CE (62 % bzw. 63 %). Malware dürfte in DA kaum seltener sein als anderswo – eine mögliche Erklärung wären also unterschiedliche Ansätze bei der Prävention von Datenschutzverletzung oder, dass weniger Angestellte am Arbeitsplatz Zugang zum Internet haben.

2 Die Maschinen-, Elektro- und Metallindustrie

Ein weiterer Punkt in der Liste der wichtigsten Sicherheitsanliegen für DACH und CE sind Konfigurationsfehler (eine neue Option in der diesjährigen Umfrage). Ihre hohe Einstufung zeugt davon, dass das Potenzial einer schwerwiegenden Verletzung der Datensicherheit durch menschliches Versagen bekannt ist. Aufgrund von Personal- und Qualifikationslücken – Themen, auf die weiter unten näher eingegangen wird – dürfte das Risiko von Konfigurationsfehlern leider auch in Zukunft hoch bleiben.

Wenn man die Bedrohungen betrachtet, besteht offenbar ein Missverhältnis zwischen dem, was erkannt wird, und dem, was als wichtigste Bedrohung gilt. Eine praktische Erklärung könnte darin liegen, dass Finanzdienstleistungen, Einzelhandel und der Dienstleistungssektor erhebliche Ressourcen in die Bekämpfung von Kreditkartenbetrug investieren. Dies gilt besonders für CH mit ihrem großen Finanzdienstleistungssektor. Die in der Studie identifizierten wichtigsten Sicherheitsbedrohungen weisen auf Bereiche hin, in denen Fachkräfte mehr Ressourcen brauchen, um sich entwickelnde Risiken effizient zu bekämpfen. Allerdings sollte hierbei angemerkt werden, dass die Bereitschaft von Unternehmen hinter aktuellen Anforderungen hinterherhinken könnte.



Quelle: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH und Kerneuropa, N = 2.801

Komplexität und Architecture Sprawl

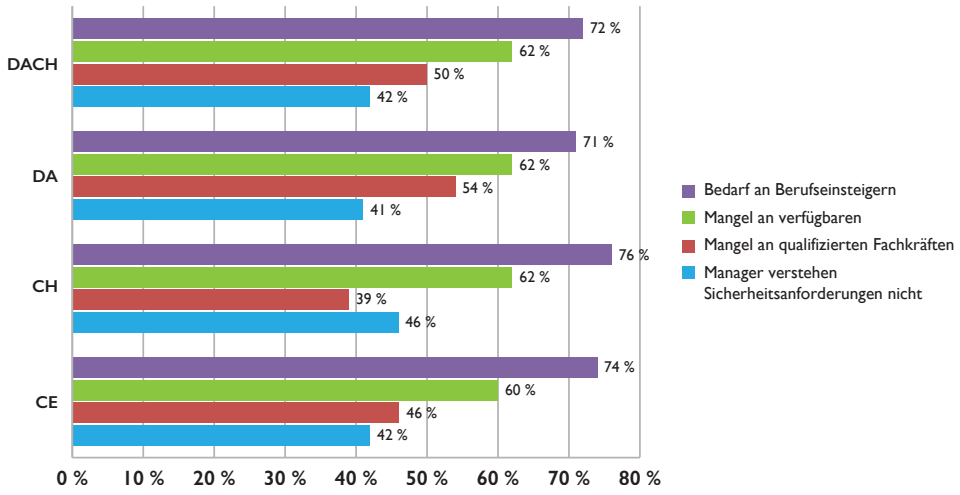
Die Komplexität der Sicherheitslandschaft, in der sich IT-Sicherheitsexperten bewegen, verringert sich offenbar nicht. Der entscheidende Faktor, der hierzu beiträgt, ist der sogenannte „Architecture Sprawl", d. h. die Multiplikation von Architekturen – es gibt immer mehr Sicherheitsanbieter und Konsolen, die Sicherheitslage bessert sich jedoch wenig. Kein Wunder also, dass 57 Prozent der DACH-Fachkräfte diese Multiplikation als betriebliches Risiko identifizieren: Sie stellt eine bedeutende Verwaltungsbelastung für Fachkräfte dar, die gezwungen sind, sich in Sicherheitsprodukte von verschiedenen Anbietern einzuarbeiten und immer mehr Sicherheitsberichte nach tatsächlich relevanten Bedrohungen zu durchkämmen. Deshalb sind 54 Prozent der DACH-Fachkräfte der Ansicht, dass der Architecture Sprawl die Wirksamkeit von Sicherheitsmaßnahmen einschränkt und ihre Unternehmen vor Schulungsprobleme stellt.

Ursachen sind in der DACH-Region der dezentralisierte Einkauf von Sicherheitstechnologie (21 %), Fusionen und Übernahmen (27 %) sowie Bedrohungen, die sich schneller weiterentwickeln als Sicherheitsprodukte (34 %). Ironischerweise trägt auch die sich verändernde Risikolandschaft maßgeblich zum Architecture Sprawl

bei, weil Organisationen als Reaktion auf neue Bedrohungen zusätzliche Sicherheitsprodukte kaufen. Der Wert dieser Vorgehensweise ist allerdings unklar. Heutzutage lassen sich 3 von 5 Datenschutzverletzungen in der DACH-Region auf eine zuvor nicht erkannte Schwachstelle zurückführen. Probleme mit immer neuen Sicherheitsprodukten zu bekämpfen, ist also eindeutig nicht so effektiv, wie einige Seiten vielleicht gehofft haben.

Personallücken

Zentrale personelle Anliegen im Bereich Informationssicherheit



Quelle: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH und Kerneuropa, N = 2.801

Der hohe Bedarf an Berufseinsteigern und der Mangel an Arbeitskräften für die Informationssicherheit der DACH-Region sind in CE wie auch weltweit ein bekanntes Thema. IT-Sicherheitsspezialisten in DACH geben an, dass der Personalbestand im Durchschnitt um 11 Prozent aufgestockt werden müsste. Der größte Bedarf besteht in den folgenden Berufsfeldern:

- Sicherheitsanalysten
- Forensische Analysten
- Sicherheitsarchitekten

Die Nachfrage nach diesen Fachkräften unterstreicht die Probleme, die Unternehmen nach Aussage der Befragten angehen müssen. Ein erstes Beispiel ist die Notwendigkeit einer kritischen Analyse von Malware in einem Unternehmen, ein zweites Beispiel die Analyse der 60 Prozent von Datenschutzverletzungen, die auf unbekannte Schwachstellen zurückgeführt werden. Der Bedarf an Sicherheitsarchitekten steht im Einklang mit der Besorgnis rund um den Technology Sprawl und andere sich entwickelnde Trends, die auf IT-Systeme einwirken, wie die Mobilität.

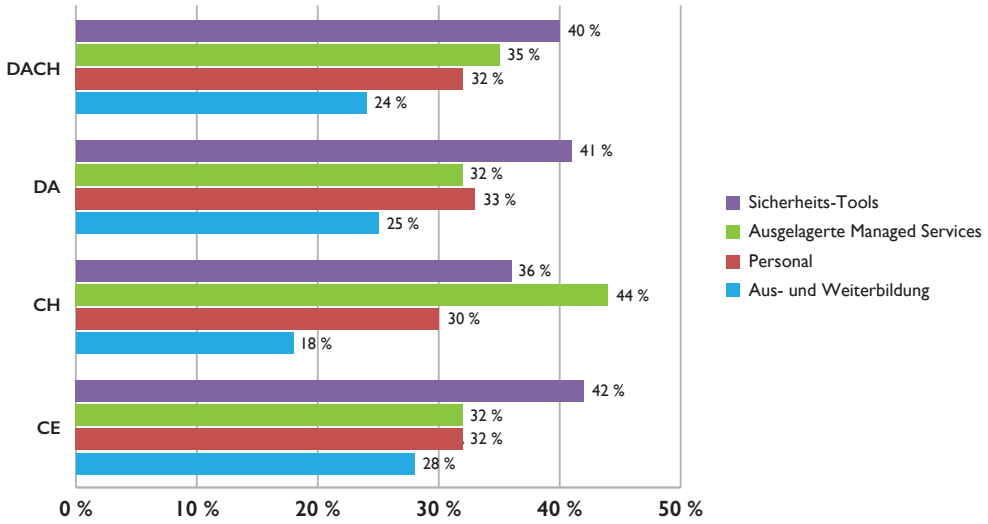
Obwohl sich dieser Fachkräftemangel in der DACH-Region auf mehrere Marktfaktoren zurückführen lässt, ist eines klar: Höhere Gehälter machen es einfacher, die am dringendsten benötigten Fachkräfte zu finden. Dies ist einer der Hauptgründe dafür, dass Unternehmen in CH weniger Schwierigkeiten haben, qualifizierte Mitarbeiter aufzutun und einzustellen.

DIE REAKTION

Sicherheitsbudgets

IT-Sicherheitsausgaben in der DACH-Region belaufen sich im Durchschnitt auf jährlich 3,6 Mio. € pro Organisation[3] – nahezu eine halbe Million Euro mehr als in CE. Angesichts von Personallücken, komplexen Sicherheitsanforderungen infolge von Architecture Sprawl sowie der Unfähigkeit, Datenschutzverletzungen zu stoppen, setzen Organisationen ausgereifte Analytics-Lösungen ein, um Prioritäten für ihre Sicherheitsanstrengungen zu ermitteln.

Die vier wichtigsten Bereiche für höhere Sicherheitsbudgets in den nächsten 12 Monaten



Quelle: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH und Kerneuropa, N = 2.801

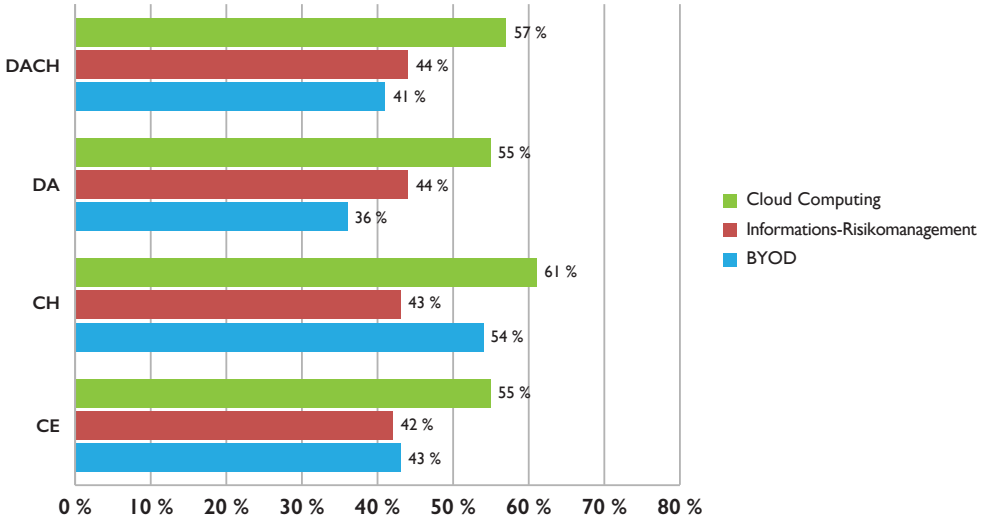
2014 haben 26 Prozent der DACH-Unternehmen bereits eine ausgereifte Analytics-Lösung angewendet, und 15 Prozent sind in der Implementierungsphase. Die Nutzung von Analytics liegt in der DACH-Region etwas höher als in CE (22 Prozent aktuelle Verwendung bzw. 14 Prozent laufende Implementierung) lagen.

Daneben ist die strategische Auslagerung spezifischer Sicherheitsfunktionen offenbar ein weiterer Ansatz, um Personalengpässe zu überwinden, und steht bei Unternehmen in CH 2015 weit oben auf der Tagesordnung. Ausgaben für berufliche Aus- und Weiterbildung zeigen ebenfalls eine steigende Tendenz – ein klares Indiz, dass das Ausmaß der Veränderungen in diesem Bereich erkannt wurde.

3 Basierend auf dem Wechselkurs von USD -> EUR von 0,884 vom 27. August 2015.

Berufliche Bildung, Zertifizierung, Erfahrung und Kommunikationsfähigkeiten

Die wichtigsten Themen für die berufliche Bildung: 2015 – 2018

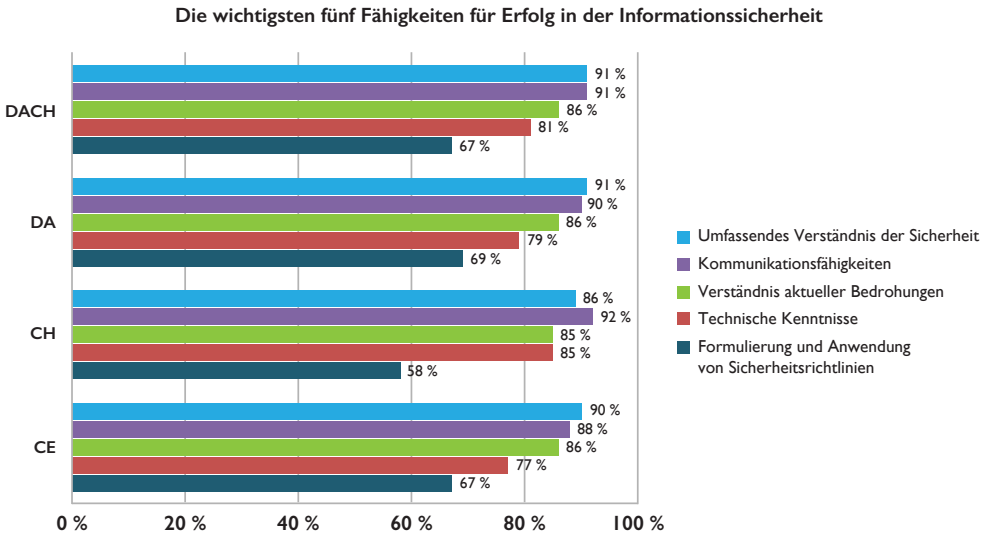


Quelle: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH und Kerneuropa, N = 2.801

Das Spitzenthema für die berufliche Bildung in der DACH-Region ist Cloud Computing – 43 Prozent der hier angesiedelten Unternehmen nutzen heute Cloud Services und weitere 10 Prozent planen dies innerhalb der nächsten zwei Jahre. Schulungen im Bereich Informations-Risikomanagement stellen ebenfalls eine Priorität dar. Dies überrascht kaum. Unternehmen sind bemüht, ihre Prozesse für die Klassifizierung ihrer geschäftskritischen Daten, die Ermittlung von Schwachstellen und die Wahl geeigneter Maßnahmen zu verbessern. Mobile Geräte stellen das wichtigste Sicherheitsanliegen in CH dar. Demnach wird der BYOD-Schulung eine hohe Priorität für Unternehmen beigemessen.

Professionelle Zertifizierungen zeigen sehr deutlich, dass Fachkräfte ihre Erfahrungen belegen möchten und proaktiv ihre Fähigkeiten erweitern, um in ihrem Beruf erfolgreich zu sein. 59 Prozent der Befragten in der DACH-Region gaben an, dass professionelle Zertifizierungen für sie „wichtig“ oder „sehr wichtig“ sind.

Darüber hinaus äußerten sich die IT-Sicherheitsexperten zu den Fähigkeiten, die ihrer Meinung nach für den Berufserfolg wesentlich sind. Interessant ist, dass technische Kenntnisse weniger wichtig sind, als das umfassende Verständnis von Sicherheitskonzepten, sowie gute Kommunikationsfähigkeiten. Dies steht in deutlichem Gegensatz zu den maßgeblichen Trends beim Technology Sprawl.

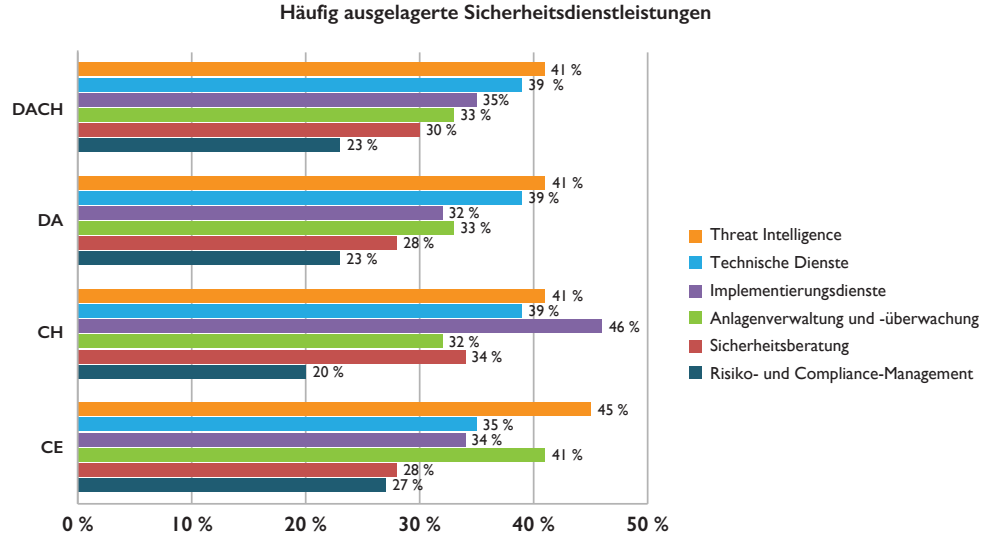


Quelle: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH und Kerneuropa, N = 2.801

Outsourcing

Sicherheitsrisiken unterliegend einem ständigen Wandel und qualifizierte Fachkräfte sind knapp. Um personelle Engpässe zu schließen, lagern immer mehr Unternehmen in der DACH-Region Sicherheitsaufgaben an externe Anbieter aus – und eines der wichtigsten Kriterien für die Wahl eines Sicherheitsdienstleisters ist die Anzahl und Qualität der Sicherheitsfachkräfte.

Zwei der häufigst ausgelagerten Dienstleistungen in der DACH-Region sind Threat Intelligence und Implementierungsdienste. Diese Aufgaben ergänzen sich gegenseitig, weil sie Unternehmen in die Lage versetzen, die von den Fachkräften identifizierten Sicherheitsbedrohungen effizienter zu bekämpfen. Unternehmensspezifische Threat Intelligence (d. h. die Bereitstellung von Informationen über Sicherheitsbedrohungen) bietet Fachkräften in der DACH-Region einen besseren Überblick auf die Gefahrenumgebung sowie Handlungsempfehlungen zur Beseitigung von Schwachstellen. Wird dies mit Implementierungsdiensten kombiniert, können auch personell unterbesetzte DACH-Organisationen schnell auf neue Bedrohungen reagieren, und deshalb besitzen beide Services einen so hohen Stellenwert.



Quelle: Frost & Sullivan 2015 (ISC)² Global Information Security Workforce Study, DACH und Kerneuropa, N = 2.801

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041