



# STUDIE MANAGED SECURITY EXECUTIVE SUMMARY

PRÄSENTIERT VON SYNTAX

## Der Aufwand für die Implementierung und Umsetzung von Sicherheitsvorgaben wird zum Problem

Komplexere Cyber-Angriffe in Verbindung mit einem höheren Aufwand bei der Umsetzung von Sicherheitsmaßnahmen stellen Unternehmen vor wachsende Herausforderungen. Hinzu kommt das mangelnde Bewusstsein der Mitarbeiter für IT-Sicherheit (35 Prozent).

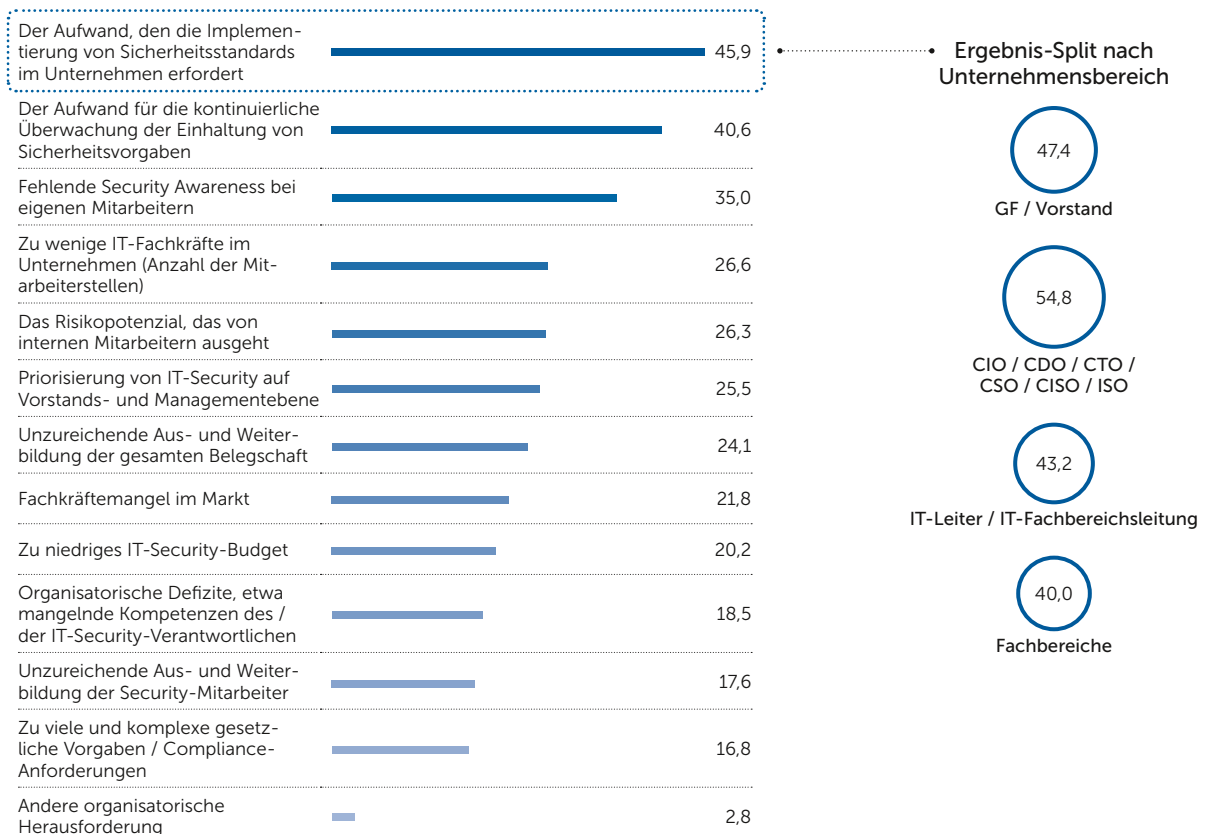
Rund 46 Prozent aller Unternehmen betrachten die Implementierung von IT-Sicherheitsstandards als größte organisatorische Herausforderung im Rahmen von IT-Security. Das sehen vor allem CIOs, CTOs und IT-Sicherheitsverantwortliche so (55 Prozent).

Für 41 Prozent der Unternehmen ist die kontinuierliche Kontrolle der Einhaltung von Security-Vorgaben mit einem hohen Aufwand verbunden.

Eng damit verbunden ist die Problematik, dass Mitarbeiter über ein unzureichendes Bewusstsein für IT-Sicherheit verfügen (35 Prozent). Das gilt vor allem für Unternehmen mit mehr als 500 Mitarbeitern (40 Prozent).

### Was sind in Ihren Augen für die Unternehmen die größten organisatorischen Herausforderungen in Bezug auf IT-Security?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 357



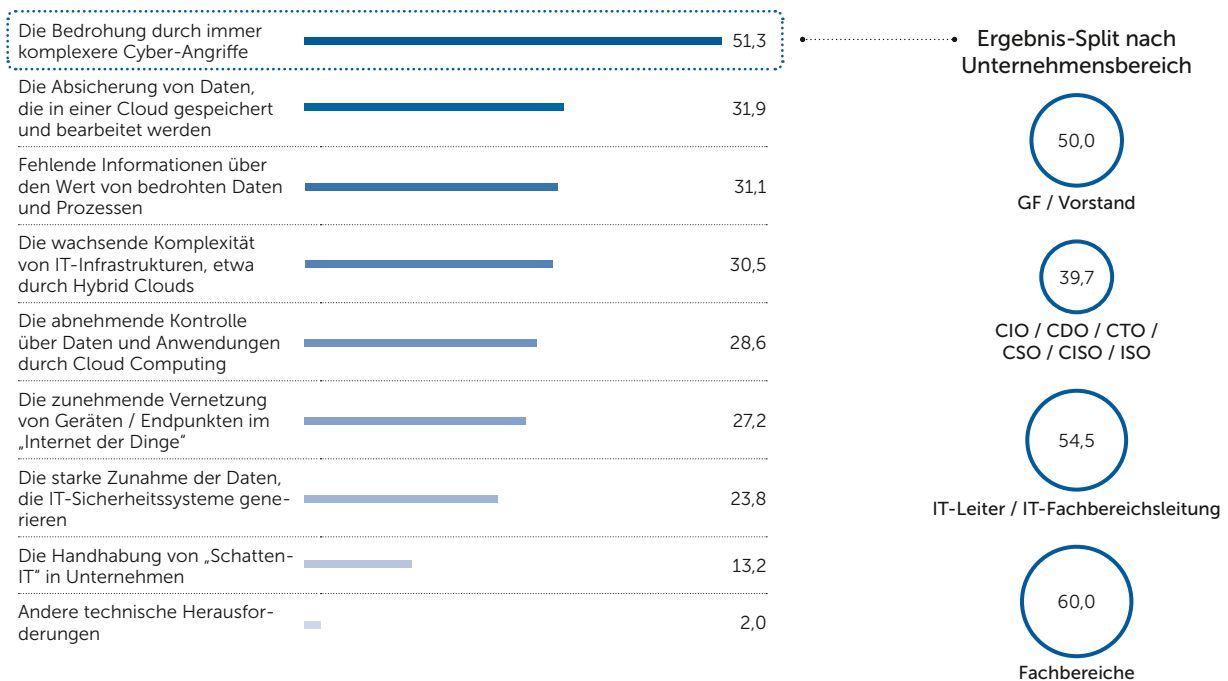


Die größte Herausforderung in technischer Hinsicht ist die wachsende Komplexität von Cyber-Attacken (51 Prozent). Das sehen Geschäftsführung (50 Prozent), IT-Bereichsleiter (55 Prozent) und Fachbereiche (60 Prozent) gleichermaßen so. Dagegen sind nur 40 Prozent der CIOs und Technikvorstände dieser Auffassung.

Der Schutz von Daten in der Cloud (32 Prozent) ist eine weitere technische Herausforderung. Das sehen vor allem CIOs und IT-Vorstände so (47 Prozent) – die darunter angesiedelte Hierarchieebene der IT-Fachbereichsleiter ist nicht unbedingt der gleichen Auffassung. Hier sehen nur 25 Prozent die Absicherung der Cloud als ihre größte technische Security-Herausforderung an.

### Was sind in Ihren Augen für die Unternehmen die größten technischen Herausforderungen in Bezug auf IT-Security?

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 357





## Eine Vielzahl von Sicherheitsmaßnahmen lässt sich auslagern

Unternehmen können sich vorstellen, einen Großteil der IT-Security-Maßnahmen an einen Dienstleister auslagern – von der Überwachung von Sicherheits-Policies bis hin zur Identifizierung und Abwehr von Cyber-Angriffen.

Die Top-8-Themenbereiche, die laut den Befragten für ein Outsourcing infrage kommen, bewegen sich in einem Bereich zwischen 22 und 31 Prozent Zustimmung. Das heißt, Unternehmen sehen ein großes Potenzial für das Verlagern von IT-Sicherheitsaufgaben auf Dienstleister.

Zu den Aufgaben, die ein externer Spezialist in erster Linie übernehmen kann, zählen die Überwachung von Security Policies (31 Prozent), die Implementierung von Sicherheitslösungen (28 Prozent) sowie die Analyse von Angriffen (28 Prozent).

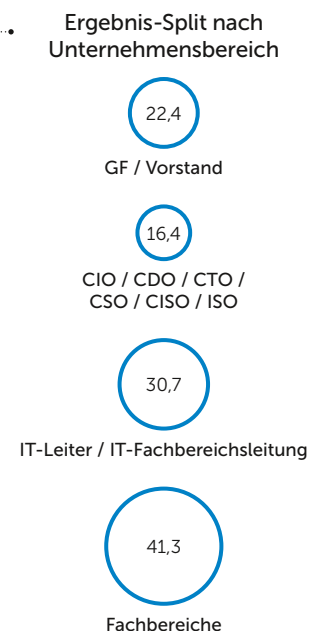
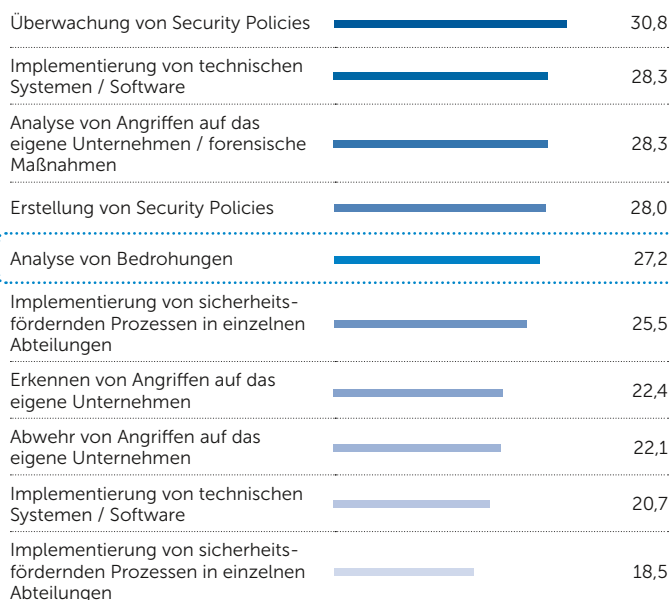
Doch es gibt gravierende Unterschiede: So können sich nur 17 Prozent der Geschäftsführer eine Untersuchung von Cyber-Attacks durch Externe vorstellen, dagegen 38 Prozent der CIOs.

Dagegen würden 41 Prozent der Fachbereiche und 31 Prozent der IT-Leiter und IT-Fachbereichsverantwortlichen auch Bedrohungsanalysen einem Dienstleister übertragen. Das wollen aber nur 16 Prozent der CIOs und 22 Prozent der Führungsspitze eines Unternehmens.

Viele der genannten Security-Themen, die sich nach Meinung der Befragten auslagern lassen, haben wir in unserem Portfolio: z. B. Implementierung von technischen Systemen / Software, Analyse von Angriffen auf das eigene Unternehmen / forensische Maßnahmen, Analyse von Bedrohungen, Erkennen von Angriffen auf das eigene Unternehmen, Abwehr von Angriffen auf das eigene Unternehmen.

### Welche Security-Themen lassen sich Ihrer Meinung nach an einen oder mehrere Dienstleister outsourcen?

Angaben in Prozent. Mehrfachnennungen möglich. Dargestellt sind die Top-10-Antworten. Basis: n = 357



## Mehr als die Hälfte der Unternehmen arbeitet mit IT-Security-Dienstleistern zusammen

An die 54 Prozent der Befragten nutzt externe IT-Sicherheits-Services, weitere 15 Prozent planen dies. Rund 38 Prozent greifen auf die Unterstützung von zwei bis drei Dienstleistern zurück. Das gilt vor allem für größere Unternehmen.

Ein Drittel der befragten Unternehmen arbeitet bereits seit mindestens zwei Jahren mit Dienstleistern im Bereich IT-Sicherheit zusammen. Das ist vor allem bei größeren Firmen mit mehr als 500 Beschäftigten (37 Prozent) der Fall.

Rund 21 Prozent der Unternehmen haben erst vor kurzer Zeit eine entsprechende Kooperation begonnen.

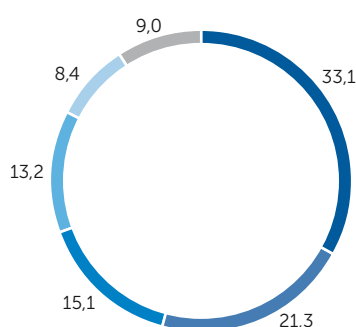
Dagegen sehen 22 Prozent der Befragten keinen Bedarf oder haben sich bewusst gegen ein Outsourcing von IT-Security-Maßnahmen entschieden.

Speziell kleinere Unternehmen mit weniger als 500 Mitarbeitern beschränken sich auf die Zusammenarbeit mit einem einzelnen IT-Security-Spezialisten (42 Prozent). Die Mehrzahl der größeren Unternehmen (45 Prozent) nutzt dagegen zwei bis drei Anbieter.

Relativ klein ist mit 18 Prozent der Anteil der Firmen, die auf bis zu fünf IT-Security-Service-Provider zurückgreifen. Dies sind insbesondere Großunternehmen mit 50 oder mehr internationalen Niederlassungen.

### Arbeitet Ihr Unternehmen mit IT-Security-Dienstleistern zusammen?

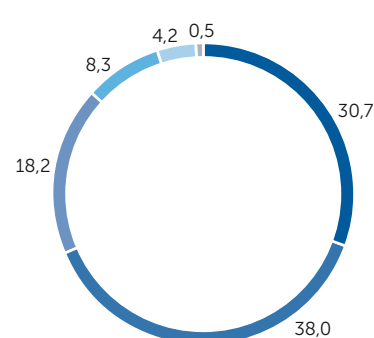
Angaben in Prozent. Basis: n = 357



- Ja, seit mehr als zwei Jahren
- Ja, seit Kurzem
- Noch nicht, aber wir haben es vor.
- Nein, es ist auf absehbare Zeit auch nicht geplant.
- Nein, wir haben uns bewusst dagegen entschieden.
- Weiß nicht

### Mit wie vielen IT-Security-Dienstleistern arbeitet Ihr Unternehmen zusammen?

Angaben in Prozent. Basis: n = 192. Filter: Nur Unternehmen, die mit IT-Security-Dienstleistern zusammenarbeiten



- 1 Dienstleister
- 2 bis 3 Dienstleister
- 4 bis 5 Dienstleister
- 6 bis 9 Dienstleister
- 10 Dienstleister und mehr
- Weiß nicht

### Zusammenarbeit mit bis zu fünf Dienstleistern Ergebnis-Split nach Unternehmensgröße





## Nutzer erwarten technisches Know-how, gute Preise und deutschsprachigen Support

Jeweils rund 31 Prozent der Unternehmen wünschen sich von IT-Security-Services ein gutes Preis-Leistungs-Verhältnis und Support-Hotlines mit deutschsprachigen Mitarbeitern. Am wichtigsten ist jedoch die technische Kompetenz (36 Prozent).

Vor allem größere Unternehmen mit 500 oder mehr Mitarbeitern wollen einen Service-Provider mit profundem technischem Wissen (47 Prozent).

Interessanterweise legen auch 40 Prozent der Geschäftsführer Wert auf Service-Anbieter mit großem Know-how, dagegen nur 30 Prozent der CIOs und CTOs.

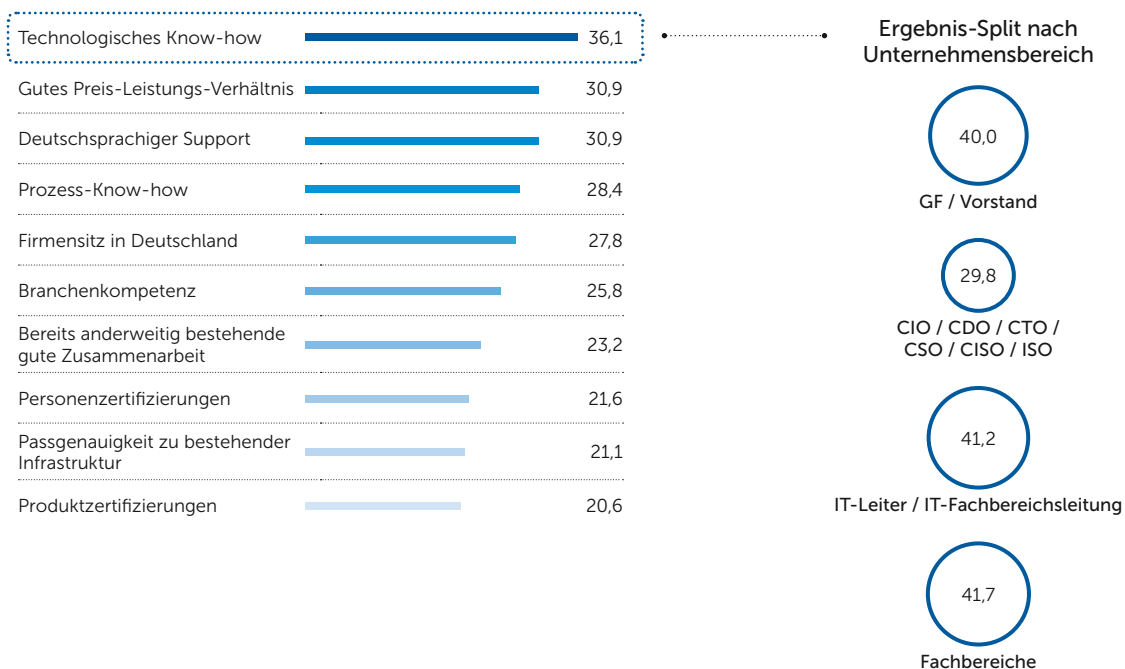
Der IT-Security-Dienstleister sollte aus Sicht von 35 Prozent der kleineren Unternehmen in Deutschland beheimatet sein. Für größere Mittelständler und Großunternehmen ist dies weniger wichtiger (26 Prozent).

Für 23 Prozent der Unternehmen ist die gute Zusammenarbeit in einem anderen Bereich ein Grund, einem IT-Dienstleister das Vertrauen zu schenken. Das heißt für Anbieter, dass sie gute Chancen haben, mit Bestandskunden auch im Bereich Managed Security ins Geschäft zu kommen.

Fachwissen im Bereich Prozesse ist für 28 Prozent der Befragten ein wichtiges Kriterium bei der Wahl eines Anbieters von IT-Security-Diensten.

### Was sind für Sie entscheidende Kriterien bei der Auswahl eines externen IT-Security-Dienstleisters?

Angaben in Prozent. Mehrfachnennungen möglich. Dargestellt sind die Top-10-Antworten. Basis: n = 194  
Filter: Nur Unternehmen, die mit IT-Security-Dienstleistern zusammenarbeiten





**Peter Schütte**  
VP, Head of Global  
Marketing & Communi-  
cations Syntax Systems  
pschuette@syntax.com

## ÜBER SYNTAX

SYNTAX ist ein global agierender IT-Dienstleister und einer der führenden Managed Cloud Provider für den Bereich Enterprise Critical Applications. Hauptsitz des 1972 gegründeten Unternehmens ist Montreal, Kanada. Im März 2019 wurden mit der ehemaligen Freudenberg IT (FIT) sowie dem amerikanischen AWS Spezialisten EMERALDCUBE zwei etablierte IT Unternehmen in die Syntax Organisation integriert.

Weitere Informationen unter [www.syntax.com](http://www.syntax.com)



### Herausgeber:

IDG Business Media GmbH  
Lyonel-Feininger-Str. 26  
80807 München  
Telefon: 089 36086 – 0  
Fax: 089 36086 – 118  
E-Mail: [info@idgbusiness.de](mailto:info@idgbusiness.de)

Vertretungsberechtigter  
York von Heimburg  
Geschäftsführer

Registergericht  
Amtsgericht München  
HRB 99187

Umsatzsteueridentifikations-  
nummer: DE 811 257 800

Weitere Informationen unter:  
[www.idg.de](http://www.idg.de)

### Studienkonzept /

**Fragebogenentwicklung:**  
Simon Hülsbömer,  
IDG Research Services  
Matthias Teichmann,  
IDG Research Services

### Endredaktion /

**CvD Studienberichtsband:**  
Simon Hülsbömer,  
IDG Research Services

### Analysen /

**Kommentierungen:**  
Bernd Reder, München

### Umfrageprogrammierung:

Thamar Thomas-Ißbrücker  
IDG Research Services  
auf EFS Survey Fall 2017

### Grafik:

Patrick Birnbreier, München

### Umschlagkonzept:

Sandra Schmitt,  
IDG Research Services  
(unter Verwendung eines  
Farbfotos für Vorder- und  
Rückseite von © sdecoret /  
shutterstock.com

### Lektorat:

Dr. Renate Oettinger,  
München

### Druck:

Peradruck GmbH  
Hofmannstr. 7b  
81379 München



INSIGHTS  
INTENT &  
ENGAGEMENT