COMPUTERWOCHE VOICE OF DIGITAL

CIO

ChannelPartner

TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE CYBER SECURITY 2020

DIE WICHTIGSTEN KEY FINDINGS

PRÄSENTIERT VON McAFEE®

McAfee™ Together is power.

Cyber-Attacken und Cyber Crime werden als größtes Geschäftsrisiko gesehen

Während 41 Prozent der befragten Unternehmen die Bedrohungen aus dem Cyber-Raum besonders fürchten, liegen die volkswirtschaftliche Entwicklung mit 34 Prozent und das Marktgeschehen in der eigenen Branche mit 30 Prozent auf Platz zwei und drei. Pandemien werden inzwischen von 29 Prozent als größte Bedrohung für das eigene Unternehmen eingestuft.

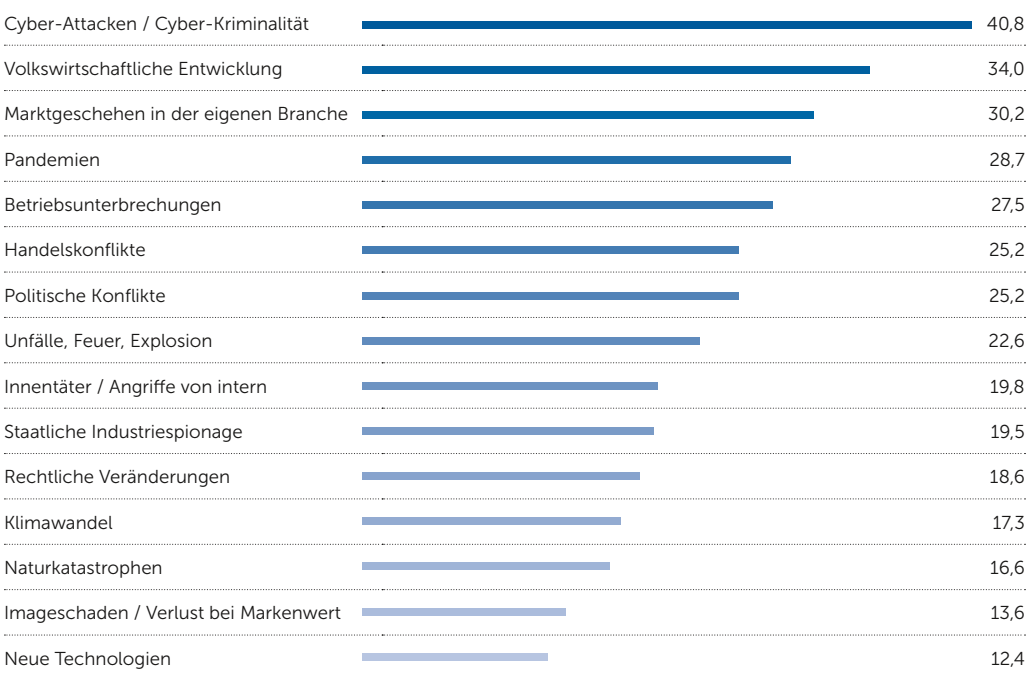
Der Blick auf Geschäftsrisiken hat sich durch die Corona-Pandemie durchaus verändert. Mögliche Risiken durch Pandemien werden stärker wahrgenommen als die Bedrohungen durch Betriebsunterbrechungen, politische Konflikte oder Handelskonflikte. Sorgen wegen der Folgen durch den Klimawandel nennen nur 17 Prozent.

Erstaunlich ist zudem, dass die Bedrohungen durch Innentäter nur knapp 20 Prozent der befragten Unternehmen als besonders hoch erachten. Risiken durch neue Technologien werden sogar nur von zwölf Prozent genannt.

Für die Ausrichtung der Cyber Security kann dies bedeuten, dass viele Unternehmen sich verstärkt gegen externe Cyber-Bedrohungen schützen wollen, die internen Bedrohungen aber dabei nicht ausreichend im Blick behalten. Ebenso scheint der Zusammenhang zwischen Cyber-Attacken und Betriebsunterbrechungen nicht deutlich genug zu sein. So gehören die Betriebsunterbrechungen zu den schwerwiegenden Folgen von Cyber-Attacken und sind oftmals das ausgewiesene Ziel der Angreifer. Eine genauere Risikobetrachtung und -bewertung ist deshalb zu empfehlen.

Welche der folgenden Gefahren und Risiken gehören aus Ihrer Sicht zu den größten Bedrohungen für Ihr Unternehmen? Welche stellen das größte Geschäftsrisiko dar?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 655



Hacker und Endpoints sind die Herausforderungen

Compliance-Vorgaben wie der Datenschutz oder die Schatten-IT werden deutlich seltener als Herausforderung für die Cyber Security genannt als externe Angreifer, Endgeräte, Budget und Kompetenzen in der Security. Homeoffice und mobiles Arbeiten nennen nur elf Prozent, externe Bedrohungen dagegen 35 Prozent und Endgeräterisiken 32 Prozent.

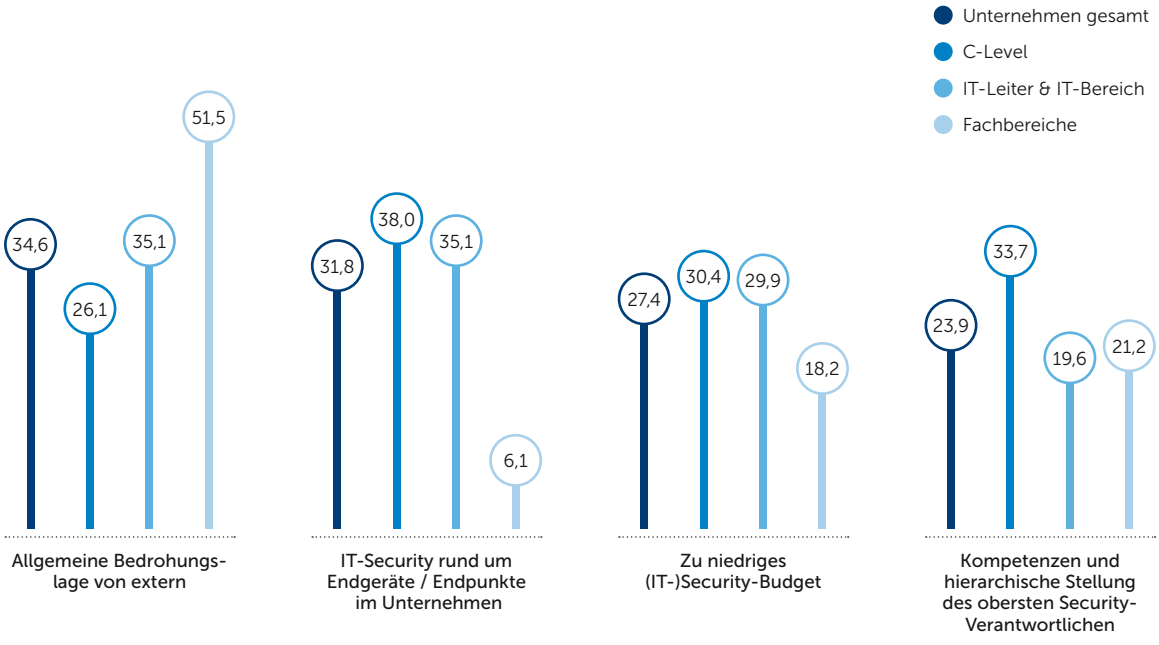
Endgerätesicherheit ist für 38 Prozent der befragten C-Level-Entscheider (Geschäftsführung / Vorstand) die größte Aufgabe für die Security, in der IT-Leitung sind es 35 Prozent, in den Fachbereichen dagegen nur sechs Prozent. Cloud-Risiken nennen 25 Prozent der Befragten aus dem C-Level, 24 Prozent der IT-Experten und zwölf Prozent der Fachbereiche als Security-Problem.

Interne Bedrohungen nehmen die Vertreter des C-Level ebenso stärker als Herausforderung wahr (25 Prozent) als der IT-Bereich (18 Prozent) und die Fachbereiche (15 Prozent).

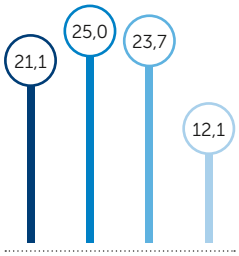
Die auch durch die Corona-Pandemie bedingte Zunahme an Tätigkeiten im Homeoffice sehen nur vier Prozent der C-Level-Angehörigen als Security-Herausforderung, selbst der IT-Bereich denkt dies nur zu elf Prozent, während in den Fachbereichen mehr als jeder Fünfte (21 Prozent) die heimischen Arbeitsplätze als Probleme für die Security einstuft.

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

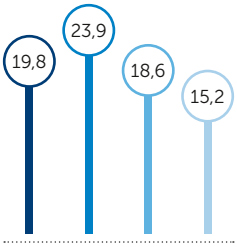
Mehrfachnennungen möglich. Dargestellt sind ausgewählte Antworten. Angaben in Prozent. Basis: n = 318



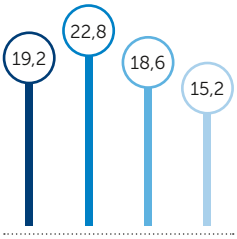
Nicht vergessen werden sollte jedoch, dass Endgerätesicherheit einen hohen Stellenwert im Homeoffice besitzt. Die Sensibilisierung für die Endpoint Security ist insofern zu begrüßen, als sichere Endgeräte besonders dort eine wichtige Rolle spielen.



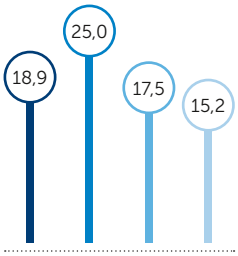
Cloud Security (Daten, Prozesse, Infrastruktur)



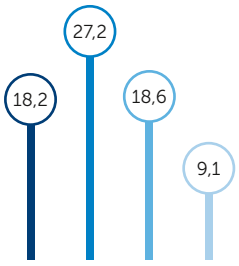
Aus- und Weiterbildung der Security-Mitarbeiter



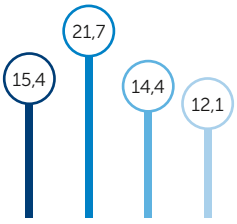
Personelle Ressourcen im Unternehmen (Anzahl der Mitarbeiterstellen)



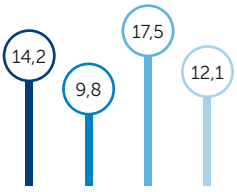
Allgemeine Bedrohungslage von intern



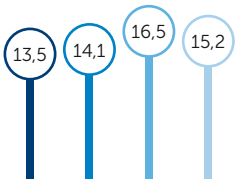
Priorisierung von IT-Security auf Vorstands- und Managementebene



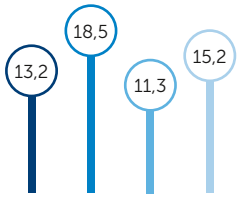
Fehlende Informationen über den Wert bedrohter Daten und Prozesse



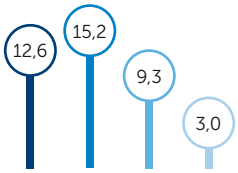
Balance zwischen „erlauben" und „absichern"



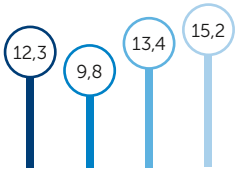
Supply-Chain-Risiken



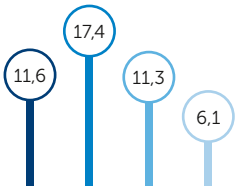
Einbindung von Identity- und Access-Management in Gesamtsicherheitsstrategie



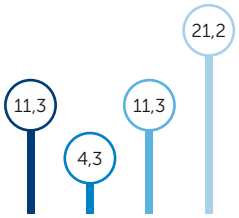
Verhaltens-Monitoring vs. Datenschutz



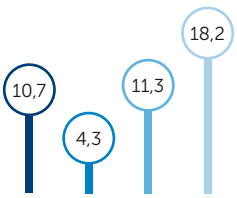
Gesetzliche Vorgaben / Compliance-Anforderungen



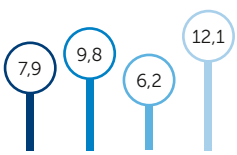
Risikopotenzial, das von internen Mitarbeitern und Vertragspartnern ausgeht



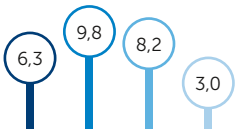
Homeoffice-Nutzung



Mobiles Arbeiten



Automatische Identifizierung der riskantesten Security Events



Schatten-IT

Künstliche Intelligenz hält Einzug bei fast drei Vierteln der Unternehmen

48 Prozent der Unternehmen nutzen bereits KI in ihren Security-Konzepten. Weitere 25 Prozent planen dies in den kommenden zwölf Monaten. Die Ablehnung von KI ist mit 23 Prozent aber noch relativ hoch, zudem gibt es fünf Prozent, die sich noch unsicher sind. Trotzdem hat KI seinen Platz in der Security erobert.

Unternehmen mit einem jährlichen IT-Budget ab zehn Millionen Euro setzen bereits zu 69 Prozent auf KI in der Security, bei geringerem IT-Budget sind es nur 38 Prozent. Weder im Einsatz noch in Planung ist Security-KI bei Unternehmen mit höherem IT-Budget nur in acht Prozent der Fälle. Ist das IT-Budget geringer, findet KI keinen Zuspruch bei 32 Prozent.

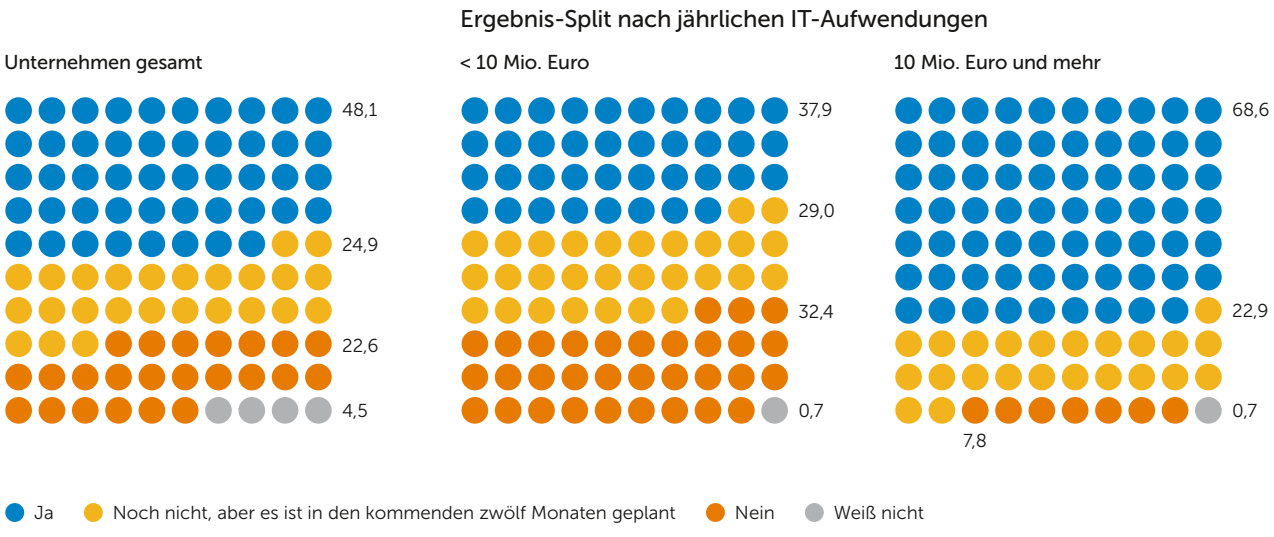
Doch KI in der Cyber Security ist nicht nur eine Frage des Budgets: Unternehmen mit weniger als 500 Beschäftigten sagen bisher in 31 Prozent der Fälle Nein zu KI. Bei 500 bis 999 Beschäftigten sinkt die Ablehnung auf 22 Prozent, ab 1.000 Beschäftigten beträgt sie nur noch 18 Prozent.

Allerdings steigt die Unsicherheit, ob man KI in der Cyber Security nutzen sollte oder nicht, mit der Anzahl der Beschäftigten. Bei weniger als 500 Beschäftigten sind nur drei Prozent unsicher, bei 1.000 und mehr Beschäftigten immerhin sieben Prozent.

Geplant wird der Einsatz von KI je nach Beschäftigtenzahl von 22 bis 29 Prozent der befragten Unternehmen.

Nutzen Sie Künstliche-Intelligenz-Technologie (KI) in Ihrem Security-Konzept?

Angaben in Prozent. Basis: n = 337



Security-Infrastrukturen müssen für die meisten Unternehmen offen sein

Offenheit ist bei Security-Lösungen sehr wichtig, meinen 26 Prozent der befragten Unternehmen. Die Möglichkeit, möglichst viele andere Security-Anbieter einbinden zu können, interessiert nur zwei Prozent nicht, die dies für vollkommen unwichtig halten. Gerade kleinere Firmen mit weniger Beschäftigten achten auf eine offene Security-Infrastruktur.

Insellösungen in der Security zu vermeiden ist sechs von zehn Unternehmen wichtig oder sehr wichtig. Bei Unternehmen mit 500 bis 999 Beschäftigten sinkt dieser Wert auf 49 Prozent, um dann bei 1.000 und mehr Beschäftigten auf 64 Prozent zu steigen.

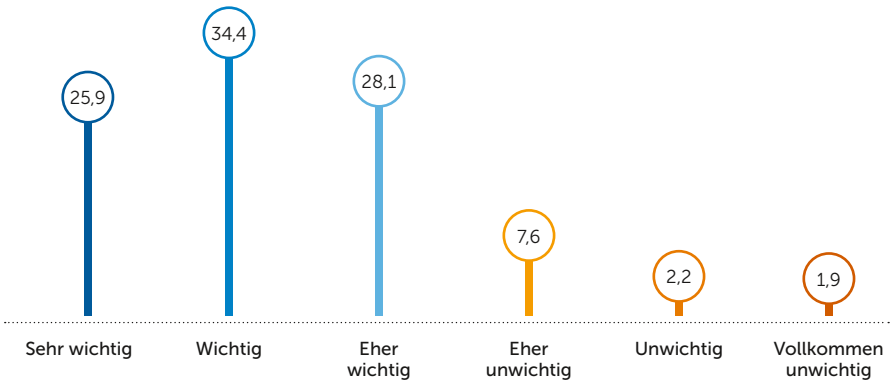
Der Wunsch nach offenen Security-Lösungen hängt auch vom jährlich verfügbaren IT-Budget ab. Beträgt es zehn Millionen Euro und mehr, wollen 71 Prozent eine offene Sicherheitsinfrastruktur. Bei unter zehn Millionen Euro sind immer noch 53 Prozent an der Offenheit der Security interessiert.

Wichtig erscheint zudem die Einschätzung der Offenheit von Security-Lösungen, wenn man sich die verschiedenen Aufgaben und Rollen im Unternehmen anschaut. Vorstände und Geschäftsführer (C-Level) sind in 70 Prozent der Fälle für die Offenheit, nur drei Prozent halten dies für unwichtig. In der IT-Leitung und im IT-Bereich favorisieren 64 Prozent offene Security-Lösungen, in den Fachbereichen nur noch 30 Prozent.

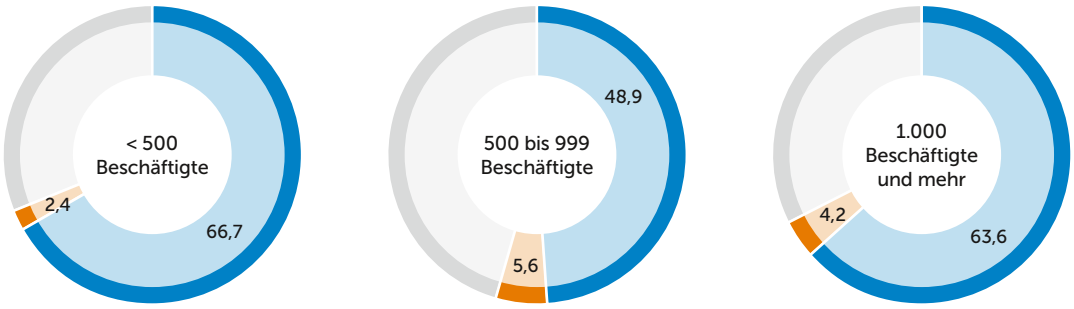
Es ist allerdings zu vermuten, dass die Fachbereiche die Nachteile von Insellösungen in der Security nicht genau genug kennen, die Vertreter des C-Levels hingegen sind mit den Vorteilen der Offenheit offensichtlich vertraut.

Wie wichtig ist Ihnen eine offene Sicherheitsinfrastruktur – also die Möglichkeit, die Sicherheitslösungen möglichst vieler unterschiedlicher Anbieter zu nutzen?

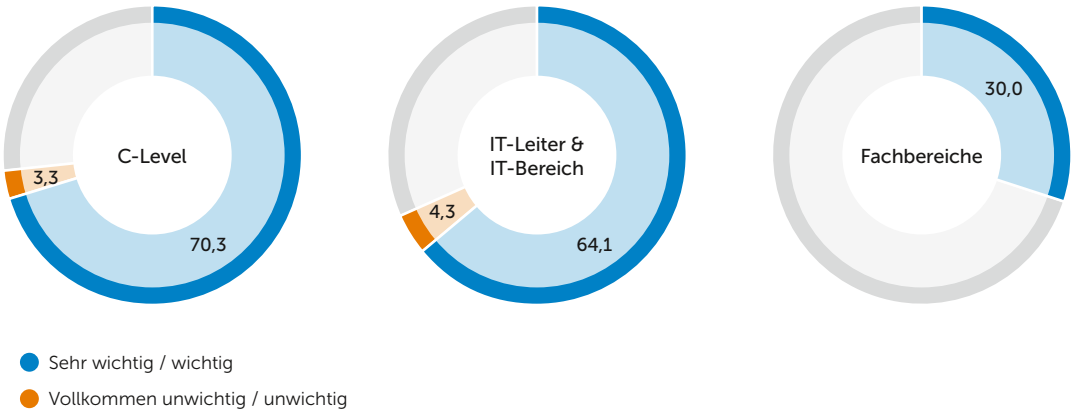
Angaben in Prozent. Basis: n = 337



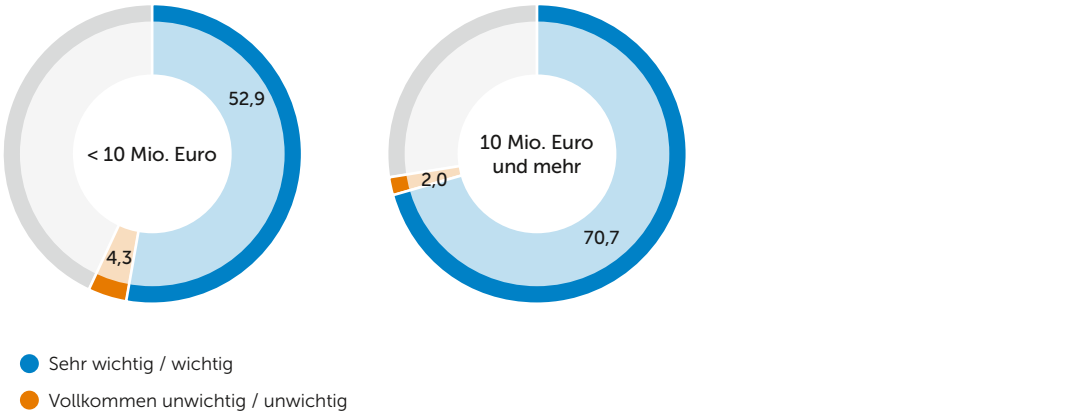
Ergebnis-Split nach Unternehmensgröße



Ergebnis-Split nach Funktion im Unternehmen



Ergebnis-Split nach jährlichen IT-Aufwendungen



Fast die Hälfte der Unternehmen hat bereits eine Cloud-Attacke erlitten

Nur 43 Prozent der Unternehmen sagen, dass sie noch keinen Angriff auf die von ihnen genutzten Cloud-Dienste festgestellt haben. Zehn Prozent wissen nicht, ob ein Cloud-Angriff stattgefunden hat. Unternehmen mit 1.000 und mehr Beschäftigten berichten zu 54 Prozent von einer Cloud-Attacke, bei weniger als 500 Beschäftigten sinkt der Anteil der Betroffenen auf 32 Prozent.

Die befragten Unternehmen vertrauen in Cloud Computing, nur zwei Prozent setzen ausschließlich auf On-Premises-IT. Gleichzeitig hat fast jedes zweite Unternehmen erfahren müssen, dass es über seine Cloud-Dienste angreifbar ist. Jedes zehnte Unternehmen hat noch keine Übersicht darüber, wie es um die Sicherheit der genutzten Cloud-Dienste steht.

Der hohe Zuspruch für Cloud Computing kann auch deshalb erstaunen, weil die Unternehmen Risiken durch Cloud Computing sehen und fürchten. Besonders der Datenverlust mit 35 Prozent, Hacker-Angriffe mit 31 Prozent und Datendiebstahl mit 30 Prozent der Antworten werden als die größten Cloud-Risiken gesehen.

Mangelhafte Cloud-Konfigurationen gelten als eine der wichtigsten Ursachen dafür, dass es zu Cloud-Attacken kommen kann, doch nur vier Prozent sorgen sich deshalb. Ebenso werden DDoS-Attacken auf Cloud-Dienste weiterhin unterschätzt, nur sechs Prozent sehen sie als Risiko, während einen Cloud-Ausfall 27 Prozent als Risiko nennen. Offensichtlich werden die Folgen von DDoS-Attacken auf Cloud-Dienste noch nicht umfassend verstanden, denn DDoS-Angriffe können zu einem Cloud-Ausfall führen.

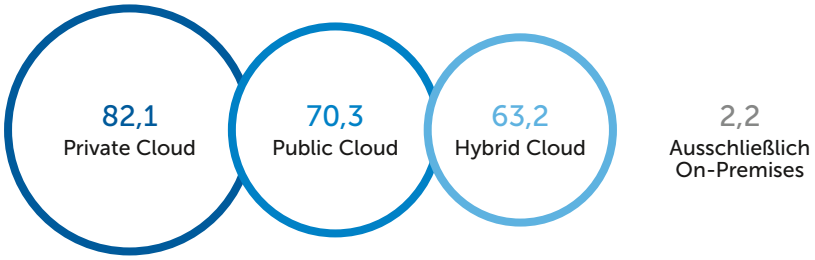
Waren die Cloud-Services Ihres Unternehmens schon einmal Ziel eines Cyber-Angriffs?

Angaben in Prozent. Basis: n = 318

Auch die Datenschutzrisiken bei Cloud Computing nennen nur 20 Prozent, obwohl diese im Hinblick auf die Datenschutz-Grundverordnung (DSGVO) nicht unterschätzt werden sollten. Da nur drei Prozent der befragten Unternehmen nicht sagen konnten, welche Cloud-Risiken sie fürchten, kann man davon ausgehen, dass man sich durchaus mit den Cloud-Risiken befasst hat, trotzdem aber nur in den wenigsten Fällen auf die Cloud verzichtet. Offensichtlich verhindert die oft noch unzureichende Cloud-Sicherheit nicht, dass Cloud-Dienste rege genutzt werden.

Welches Cloud-Bezugsmodell nutzt Ihr Unternehmen bereits oder ist für die Nutzung grundsätzlich vorstellbar?

Angaben in Prozent. Basis: n = 318



Was schätzen Sie ganz allgemein als größtes Security-Risiko bei Cloud-Services ein?

Bis zu drei Antworten möglich. Angaben in Prozent. Basis: n = 318

Datenverlust	34,9
Hacker-Angriffe	31,1
Datendiebstahl	30,2
Cloud-Ausfall (mangelnde Belastbarkeit)	26,7
Datenveränderung / fehlende Daten-integrität / fehlende Datenkonsistenz	24,5
Mangelhafter Datenschutz nach EU-DSGVO	19,5
Mangelhafter virtueller Zugriffsschutz	18,2
Schwachstellen bei Cloud-Technologien	17,0
Unsichere Cloud-Schnittstellen	12,9
Mangelhafter physischer Zugriffsschutz	9,1
APTs (Advanced Persistent Threats)	9,1
Missbrauch der Cloud durch Innentäter (z.B. Datenabfluss)	8,5
DDoS-Attacken	6,0
Mangelnde Datentrennung zwischen verschiedenen Kunden / Mandanten	5,7
Mangelhafte Cloud-Konfigurationen	4,1

McAfee – the Device-to-Cloud Cyber Security Company

McAfee® ist ein globales Cyber-Sicherheitsunternehmen, das besonders mit seinen Cloud-Sicherheitslösungen den Fokus auf die ganzheitliche Absicherung von Endgeräten bis in die Cloud legt. Durch die Bereitstellung von integrierten Lösungen, die mit Produkten anderer Hersteller zusammenarbeiten, unterstützt McAfee Unternehmen und Organisationen dabei, Cyber-Umgebungen abzusichern, Bedrohungen zu erkennen und Schwachstellen zu beheben.

McAfee verfolgt in Sachen Cloud- und Cyber-Sicherheit einen ganzheitlichen Ansatz, dessen Grundlage das **MVISION-Sicherheitsportfolio** bildet. Basierend auf den Grundpfeilern von **MVISION Cloud** und **MVISION Endpoint**, vereint MVISION Bedrohungsabwehr, Datenschutz und Compliance zu einer nativen und offenen Cloud-Plattform, die über eine zentrale, integrierte Konsole – dem **MVISION ePolicy Orchestrator® (ePO™)** – verwaltet wird.

Als Teil des MVISION Cloud-Portfolios verbindet **MVISION Unified Cloud Edge (UCE)** die Funktionen von McAfee Cloud Access Security Broker (CASB), Secure Web Gateway (SWG) und Data Loss Prevention (DLP) in einer einzigen Plattform. So setzt DLP Sicherheitsrichtlinien im lokalen Netzwerk durch, während CASB diese auf die Cloud-Umgebung überträgt und das McAfee Web Gateway für eine sichere Internetverbindung sorgt. Somit entsteht ein einheitlicher „Device-to-Cloud"-Schutz: Unternehmen erhalten umfassende Transparenz sowie konsistente Kontrolle über sämtliche Unternehmensdaten und schützen sie auf dem Endgerät, auf dem Weg in oder aus der Cloud sowie innerhalb von SaaS-Cloud-Diensten.

Die nativen, KI-basierten Endpoint Detection and Response (EDR)-Funktionen von McAfee unterstützen Unternehmen bei der proaktiven Identifizierung von Cyber-Bedrohungen. Dadurch lassen sich Gefahrenpotenziale, sicherheitsrelevante Vorfälle und komplexere Angriffe wesentlich effektiver einordnen, priorisieren und schneller auflösen. IT-Teams erhalten somit detaillierte Informationen zum Ursprung der Gefährdung sowie zum Schadensausmaß. **MVISION Insights** erweitert das EDR-Repertoire, indem es Bedrohungen noch vor einem Angriff erkennt, kontextualisiert und unterbindet.

Da Sicherheitsteams heute mit immer größeren sicherheitsrelevanten Datenmengen konfrontiert werden, müssen sie einen Weg finden, relevante Warnungen vom Gesamtrauschen zu unterscheiden. Wenn es um die Einhaltung von Compliance und den Datenschutz geht, ist Zeit Gold. Security Information and Event Management (SIEM)-Tools schaffen an dieser Stelle Abhilfe: So unterstützt der cloudbasierte McAfee **Enterprise Security Manager (ESM)** Sicherheitsteams, schädliche Vorfälle herauszufiltern und gleichzeitig die Reaktionszeit auf Events zu verkürzen. Das bewerkstelligt die Lösung, indem sie automatisiert sämtliche Unternehmensdaten auf auffällige Muster hin untersucht und verwertbare Analysen zur Priorisierung und Beschleunigung von Untersuchungen bereitstellt.

McAfee™
Together is power.

In Kooperation mit dem McAfee-Distributor

INFINIGATE
.... Adding Value to Distribution

Herausgeber:
IDG Business Media GmbH
Lyonel-Feininger-Str. 26
80807 München
Telefon: +49 (0) 89 36086 – 0
Fax: +49 (0) 89 36086 – 118
E-Mail: info@idg.de

Vertretungsberechtigter
York von Heimburg
Geschäftsführer

Registergericht
Amtsgericht München
HRB 99187

Umsatzsteueridentifikations-
nummer: DE 811 257 800

Weitere Informationen unter:
www.idg.de

Gold-Partner:
McAfee Germany GmbH
Ohmstraße 1
85716 Unterschleißheim
Telefon: +49 (0) 89 3707 – 0
Web: www.mcafee.com/de

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar / München
Telefon: +49 (0) 89 048 – 0
Web: www.infinigate.de

Studienkonzept / Fragebogenentwicklung:
Simon Hülsbömer,
Matthias Teichmann,
IDG Research Services

Endredaktion / CvD Studienberichtsband:
Simon Hülsbömer,
Armin Rozsa,
IDG Research Services

Analysen / Kommentierungen:
Oliver Schonschek, Bad Ems

Hosting / Koordination Feldarbeit:
Armin Rozsa,
IDG Research Services

Umfrageprogrammierung und Ergebnisauswertungen:
Armin Rozsa,
IDG Research Services
auf EFS Survey

Grafik:
Patrick Birnbreier, München

Lektorat:
Dr. Renate Oettinger, München

Ansprechpartner:
Matthias Teichmann,
Director Research
IDG Research Services
Telefon: +49 (0) 36086 – 131
mteichmann@idg.de