COMPUTERWOCHE VOICE OF DIGITAL

CIO

ChannelPartner

TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE CYBER SECURITY 2020

PLATIN-PARTNER

Microsoft

GOLD-PARTNER

cisco Secure

McAfee Together is power.

INFINIGATE Adding Value to Distribution

DriveLock

F-Secure

MICRO FOCUS

TREND MICRO

SILBER-PARTNER

AIRLOCK® SECURE ACCESS HUB

Ein aktuelles Studienprojekt von

IDG RESEARCH SERVICES

Platin-Partner

Microsoft

Gold-Partner

cisco Secure

DriveLock

F-Secure

McAfee Together is power.

INFINIGATE Adding Value to Distribution

MICRO FOCUS

TREND MICRO

Silber-Partner

AIRLOCK® SECURE ACCESS HUB

Alle Angaben in diesem Ergebnisband wurden mit größter Sorgfalt zusammengestellt. Trotzdem sind Fehler nicht ausgeschlossen. Verlag, Redaktion und Herausgeber weisen darauf hin, dass sie weder eine Garantie noch eine juristische Verantwortung oder jegliche Haftung für Folgen, die auf fehlerhafte Informationen zurückzuführen sind, übernehmen.
Der vorliegende Ergebnisberichtsband, einschließlich all seiner Teile, ist urheberrechtlich geschützt. Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen, auch auszugsweise, bedürfen der schriftlichen Genehmigung durch IDG Research Services.

Traue niemandem – außer dieser Studie

Simon Hülsbömer,
Senior Project Manager
Research

Vertrauen ist gut, Kontrolle ist besser. Dieser abgedroschene Spruch ist in der IT-Security-Welt aktueller denn je. Wo Menschen an ihre Grenzen stoßen, müssen technische Vorgaben für die Sicherheit sorgen. Zero Trust heißt der neue Trend. Mehr als 90 Prozent der von uns befragten Unternehmen haben ein solches Konzept zumindest in der Planung. Das Prinzip dahinter ist denkbar einfach: Jeder Nutzer, jede Anwendung, jedes Gerät, das auf bestimmte Daten zugreifen möchte – egal, ob von intern oder extern –, muss sich authentifizieren und wird fortwährend überprüft – vertraut wird niemandem. Nur so lässt sich konsequent verhindern, dass unbefugte Datenzugriffe erfolgen und sensible Informationen aus einem Unternehmen abfließen oder manipuliert werden. Vertrauensvorschuss ist nicht mehr, jede und jeder wird gleichbehandelt und kontrolliert. Das Konzept ist bereits zehn Jahre alt – aber erst jetzt beginnt sein Siegeszug. Was mich zu dem Schluss bringt: Manch gute Idee braucht etwas länger, bis sie auf fruchtbaren Boden stößt.

Eine andere gute Idee, die nicht sofort überall als solche erkannt wurde, ist gerade ebenfalls en vogue: Remote Work. Arbeiten von überall – sofern das Jobprofil es hergibt, versteht sich. Dieses Konzept funktioniert mit Zero Trust besser als ohne – sicherlich ein Grund, warum Letzteres gerade so angesagt ist.

Trotzdem wäre es mir persönlich aufgrund neuer Perspektiven und frischen Innovationsdenkens lieber gewesen, wenn Remote Work (oder in vielen Fällen auch Homeoffice) auch ohne die andauernde Pandemie ihren Weg schneller in deutsche Unternehmen gefunden hätte. Die „Zwangs-Digitalisierung", die das Thema nun vielerorts mit sich gebracht hat, erscheint diesbezüglich für viele Organisationen geradezu heilsam. Ob das Ganze aber auch für die flächendeckende Absicherung der Remote-Arbeit sorgen oder die Security-Lage eher verschlimmbessern wird, ist noch nicht final entschieden.

Zu beiden erwähnten Themen – und vielen, vielen mehr – werden Sie in diesem Berichtsband spannende Erkenntnisse finden, denn vor Ihnen liegt die umfangreichste Studie zur Cyber- und IT-Sicherheit in der Digitalisierung, die die IDG-Marktforschung jemals aufgelegt hat. Mit an Sicherheit grenzender Wahrscheinlichkeit sind auch für Sie aufschlussreiche Inhalte dabei – ganz gleich, für welches Thema Sie sich besonders interessieren oder in welchem Unternehmensbereich Sie tätig sind.

Ich wünsche Ihnen eine ausführliche, gleichwohl kurzweilige Lektüre!

Inhalt

Weitere Studienergebnisse

24

Unsere Studienpartner stellen sich vor

51

Die Studienreihe

71

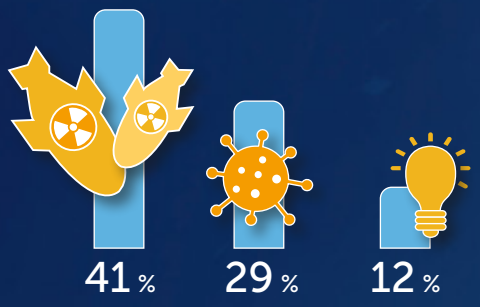
Kontakt / Impressum

75

© shutterstock.com / PopTika

Management Summary

Die Key Findings im Überblick



Cyber-Risiken bleiben das größte Unternehmensrisiko

Auch in Zeiten der Corona-Pandemie sind für 41 Prozent die Cyber-Bedrohungen besonders gefährlich für ihr Unternehmen. Pandemien nennen dagegen 29 Prozent als größtes Unternehmensrisiko, neue Technologien sogar nur zwölf Prozent.

Homeoffice gilt nicht als größtes Security-Problem

Endgeräte und externe Bedrohungen sind die größten Herausforderungen für die Security, nicht etwa Datenschutz, mobiles Arbeiten oder Heimarbeit. Nur vier Prozent des C-Levels nennen das Homeoffice als größte Herausforderung für die Security.

Cyber-Versicherungen sind die Regel, nicht mehr die Ausnahme

Etwa sechs von zehn Unternehmen sind bereits gegen Cyber-Risiken versichert. Größere Unternehmen verzichten nur zu 19 Prozent darauf. Allerdings wissen 17 Prozent gar nicht, ob sie versichert sind oder nicht.

Jedes zweite Unternehmen erlitt Schaden durch Cyber-Attacken

Von Schäden durch Cyber-Angriffe verschont blieben mit 62 Prozent eher die kleinen Unternehmen, während die mittelgroßen zu 54 Prozent und die großen Unternehmen zu 53 Prozent einen wirtschaftlichen Schaden durch Cyber-Attacken hinnehmen mussten.

Security-Investitionen steigen, aber nicht problemorientiert

Mehr als drei Viertel der Unternehmen wollen stärker in Security investieren. Die Security-Vorhaben entsprechen aber nicht immer den genannten Herausforderungen in der Security. Auch fehlen für die geplanten neuen Maßnahmen teilweise die technischen Grundlagen.

Über 70 Prozent sind offen für KI in der Security

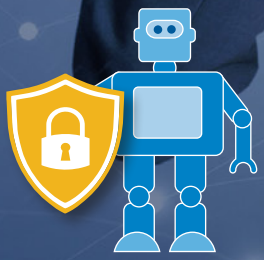
Künstliche Intelligenz (KI) wird nur von 23 Prozent der Unternehmen in der Cyber Security nicht genutzt oder zumindest eingeplant. Die Ablehnung ist bei den kleinen Unternehmen mit 31 Prozent am größten, obwohl sie den Fachkräftemangel besonders spüren.

Die Zahl der Unternehmen ohne Zero Trust geht gegen null

Mehr als neun von zehn Unternehmen setzt bereits Zero Trust ein, implementiert es oder plant es zumindest. Nur sieben Prozent haben dies noch nicht geplant, sodass Zero Trust in der Cyber Security bald zum Unternehmensalltag gehören wird.

Security Outsourcing ist zum Tabuthema geworden

55 Prozent der Unternehmen sagen, dass das Outsourcen der Security für ihr Unternehmen nicht infrage kommt. Nur 13 Prozent sagen, Outsourcing sei bei ihnen kein Tabuthema. Besonders hoch ist die Ablehnung bei kleinen Unternehmen, trotz des Fachkräftemangels.



Security Automation wird genutzt, aber missverstanden

51 Prozent der Unternehmen automatisieren bereits Teile ihrer Security. Dabei wird zum Beispiel die Abwehr automatisiert, nicht aber die Erkennung der Angriffe. Compliance-Vorteile werden teils nicht erkannt, aber die Möglichkeit, den Ressourcenbedarf zu senken.

60 Prozent möchten eine offene Sicherheitsarchitektur

Nur vier Prozent der Unternehmen halten es für unwichtig, ob ihre Security-Systeme offen sind, um Lösungen anderer Anbieter integrieren zu können. Vorständen und Geschäftsführern ist die Offenheit noch wichtiger als der IT-Leitung.

© shutterstock.com / PopTika

Die Key Findings

Cyber Security 2020

1. 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.

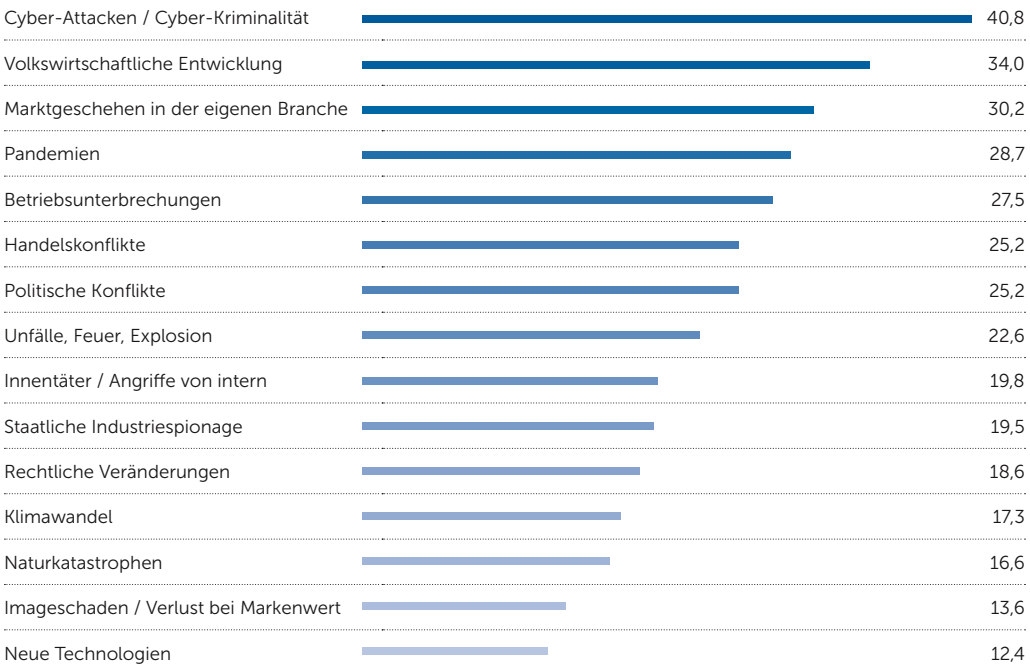
Der Blick auf Geschäftsrisiken hat sich durch die Corona-Pandemie durchaus verändert. Mögliche Risiken durch Pandemien werden stärker wahrgenommen als die Bedrohungen durch Betriebsunterbrechungen, politische Konflikte oder Handelskonflikte. Sorgen wegen der Folgen durch den Klimawandel nennen nur 17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



2. 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.

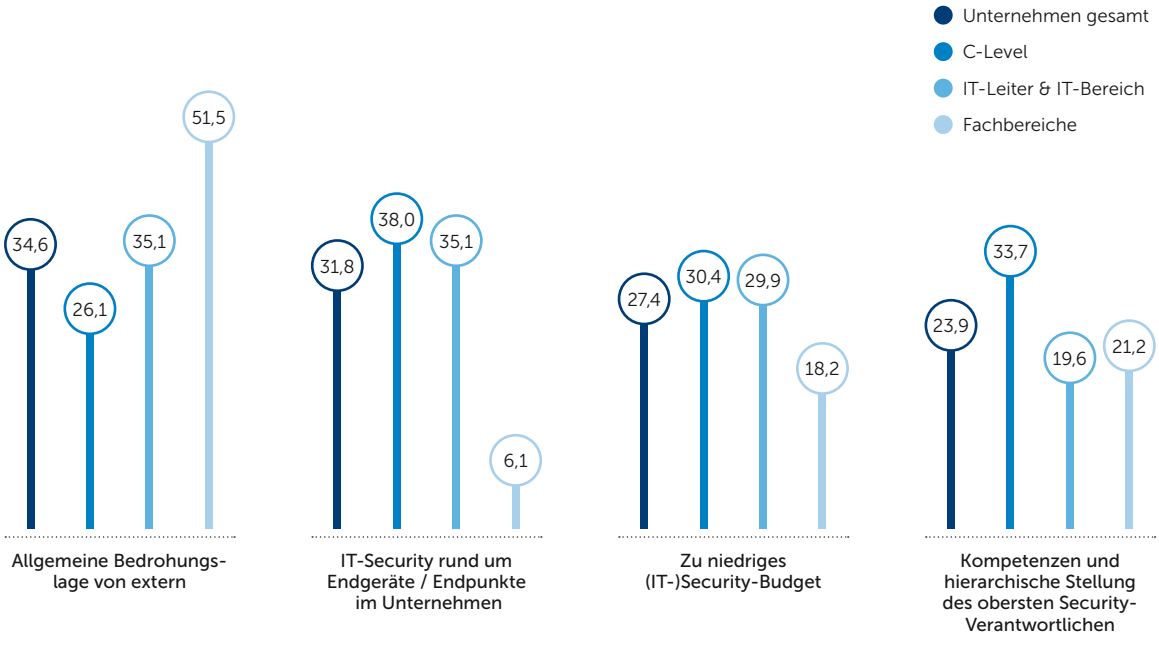
Endgerätesicherheit ist für 38 Prozent der befragten C-Level-Entscheider (Geschäftsführung / Vorstand) die größte Aufgabe für die Security, in der IT-Leitung sind es 35 Prozent, in den Fachbereichen dagegen nur sechs Prozent. Cloud-Risiken nennen 25 Prozent der Befragten aus dem C-Level, 24 Prozent der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

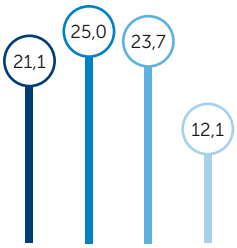
Die auch durch die Corona-Pandemie bedingte Zunahme an Tätigkeiten im Homeoffice sehen nur vier Prozent der C-Level-Angehörigen als Security-Herausforderung, selbst der IT-Bereich denkt dies nur zu elf Prozent, während in den Fachbereichen mehr als jeder Fünfte (21 Prozent) die heimischen Arbeitsplätze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

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

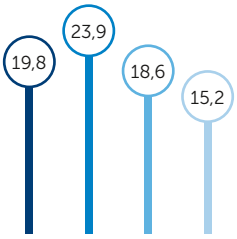
Mehrfachnennungen möglich. Dargestellt sind ausgewählte Antworten. Angaben in Prozent. Basis: n = 318



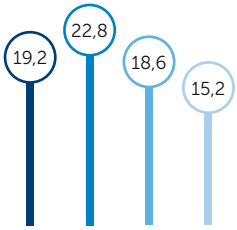
Nicht vergessen werden sollte jedoch, dass Endgerätesicherheit einen hohen Stellenwert im Homeoffice besitzt. Die Sensibilisierung für die Endpoint Security ist insofern zu begrüßen, als sichere Endgeräte besonders dort eine wichtige Rolle spielen.



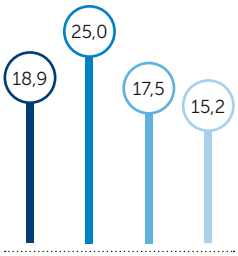
Cloud Security (Daten, Prozesse, Infrastruktur)



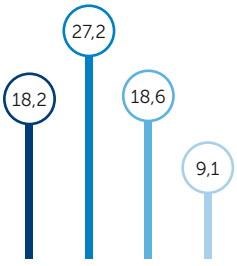
Aus- und Weiterbildung der Security-Mitarbeiter



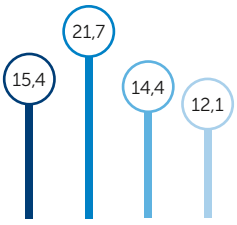
Personelle Ressourcen im Unternehmen (Anzahl der Mitarbeiterstellen)



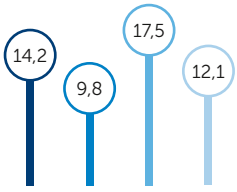
Allgemeine Bedrohungslage von intern



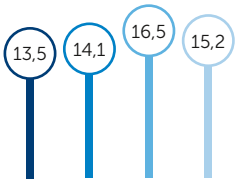
Priorisierung von IT-Security auf Vorstands- und Managementebene



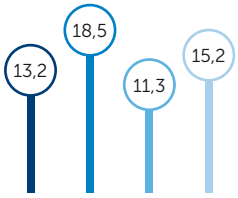
Fehlende Informationen über den Wert bedrohter Daten und Prozesse



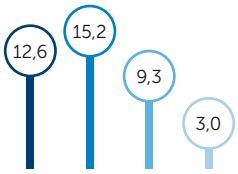
Balance zwischen „erlauben“ und „absichern“



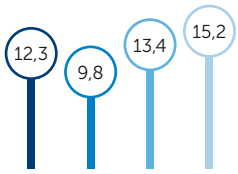
Supply-Chain-Risiken



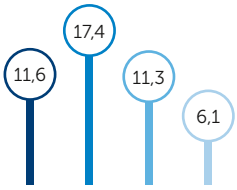
Einbindung von Identity- und Access-Management in Gesamtsicherheitsstrategie



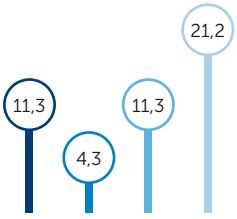
Verhaltens-Monitoring vs. Datenschutz



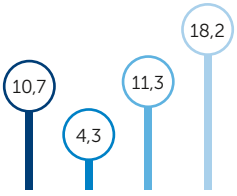
Gesetzliche Vorgaben / Compliance-Anforderungen



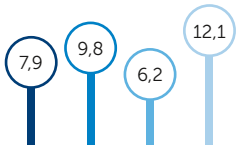
Risikopotenzial, das von internen Mitarbeitern und Vertragspartnern ausgeht



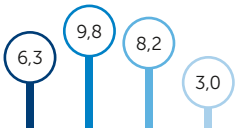
Homeoffice-Nutzung



Mobiles Arbeiten



Automatische Identifizierung der riskantesten Security Events



Schatten-IT

3. Fast 40 Prozent der kleinen Unternehmen erlitten Schäden durch Cyber-Attacken

Größere Unternehmen erleiden mit 20 Prozent Betroffenen häufiger einen massiven wirtschaftlichen Schaden als mittelgroße Betriebe, die zu neun Prozent stark geschädigt wurden. Bei den kleinen Unternehmen sind es nur fünf Prozent, die einen hohen Schaden durch Cyber-Angriffe verzeichneten. Nur 14 Prozent aller Unternehmen denken, dass es bei ihnen bisher keinen unberechtigten Datenzugriff gegeben hat.

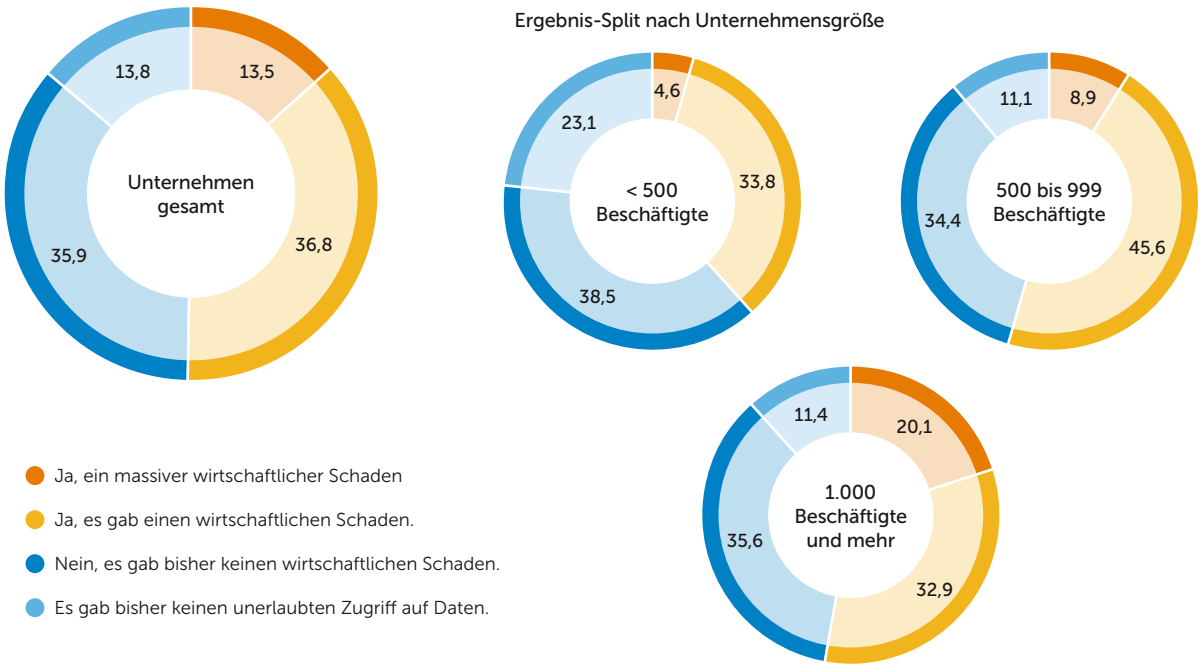
Die Höhe des wirtschaftlichen Schadens hängt auch von der Unternehmensgröße ab: Je kleiner eine Firma ist, desto eher ist die Höhe des Schadens von geringerer Natur.

Während der Anteil der Unternehmen, die bisher keinen wirtschaftlichen Schaden durch Cyber-Angriffe erlitten haben, je nach Unternehmensgröße zwischen 36 und 39 Prozent liegt, dominiert der Anteil mit einem massiven wirtschaftlichen Schaden bei den großen Unternehmen (1.000 Beschäftigte und mehr). Bei den kleinen Betrieben (< 500 Beschäftigte) haben 39 Prozent bisher keinen Schaden, 34 Prozent einen Schaden, aber nur fünf Prozent einen massiven Schaden durch Cyber-Angriffe erlitten.

Dennoch bleibt festzuhalten, dass auch kleinere Firmen Opfer von Cyber-Attacken werden und wirtschaftliche Schäden erleiden, wobei sie oftmals über geringere Budgets verfügen, um sich gegen die Angriffe besser zu schützen.

Ist Ihrem Unternehmen durch einen Cyber-Angriff schon einmal ein wirtschaftlicher Schaden entstanden?

Angaben in Prozent. Basis: n = 318



4. Fast 60 Prozent der Unternehmen haben eine Cyber-Versicherung

Nur 25 Prozent der befragten Unternehmen sagen, sie hätten noch keine Versicherung gegen Cyber-Risiken. Der Anteil derer, die nicht wissen, ob eine Cyber-Versicherung vorhanden ist, liegt bei hohen 17 Prozent. Cyber-Versicherungen werden eher von größeren Unternehmen abgeschlossen, dort liegt der Anteil bei 62 Prozent.

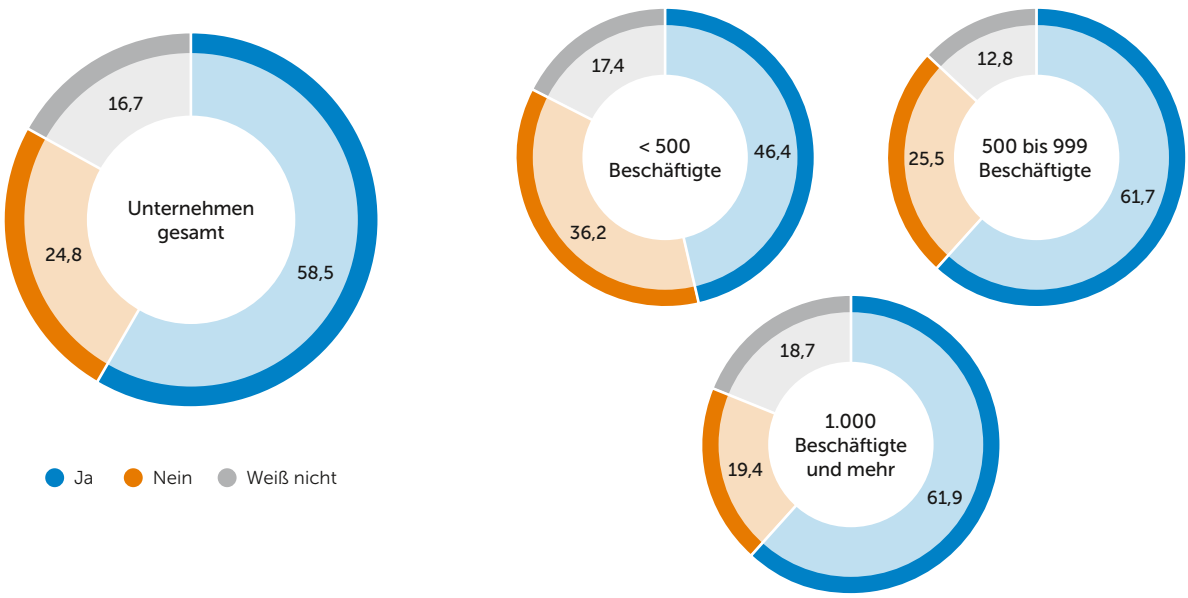
Cyber-Versicherungen sind inzwischen eher die Regel als die Ausnahme. Selbst bei Unternehmen mit weniger als 500 Beschäftigten sind es 47 Prozent, die sich gegen Cyber-Risiken versichert haben, 36 Prozent haben dies noch nicht getan, ganze 17 Prozent der Befragten wissen es nicht genau.

Mit der Größe des Unternehmens beziehungsweise der Anzahl der Beschäftigten wächst der Anteil der Unternehmen mit Cyber-Versicherung auf 62 Prozent, der Anteil der Unternehmen ohne Cyber-Versicherung liegt bei mittelgroßen Betrieben bei 26 Prozent. Sind es mehr als 1.000 Beschäftigte, sinkt die Zahl der Unternehmen ohne Cyber-Versicherung auf 19 Prozent.

Bemerkenswert ist der relativ hohe Anteil der Unternehmensentscheider, vorrangig in den IT- und Fachbereichen, die nicht wissen, ob sie eine solche Versicherung haben oder nicht. Bei kleinen Unternehmen sind sich 17 Prozent unsicher, bei mittelgroßen 13 Prozent, bei den großen Unternehmen sogar 19 Prozent. Betrachtet man die Funktionen der Befragten, relativiert sich das Bild ein wenig: Auf Geschäftsführungsebene trifft die Unkenntnis nur auf zwei Prozent zu. Mehr als jeder zehnte IT-Chef und sogar mehr als jeder fünfte Fachbereichsleiter hat indes keine genaue Kenntnis über das Vorhandensein einer solchen Versicherung. Offensichtlich besteht hier noch ein größerer Aufklärungsbedarf.

Hat Ihr Unternehmen eine Cyber-Versicherung abgeschlossen?

Angaben in Prozent. Basis: n = 318



5. Drei von vier Unternehmen erhöhen ihr Security-Budget in 2021

15 Prozent der befragten Unternehmen planen eine starke Erhöhung ihres Security-Budgets für 2021, 25 Prozent erwarten einen Anstieg und 36 Prozent immer noch einen leichten Anstieg. Einen Rückgang im Security-Budget soll es nur bei fünf Prozent geben, bei 19 Prozent werden die Ausgaben in 2021 für Security in etwa gleich bleiben. Die Schwerpunkte der Investitionen werden in der Cyber-Abwehr erwartet.

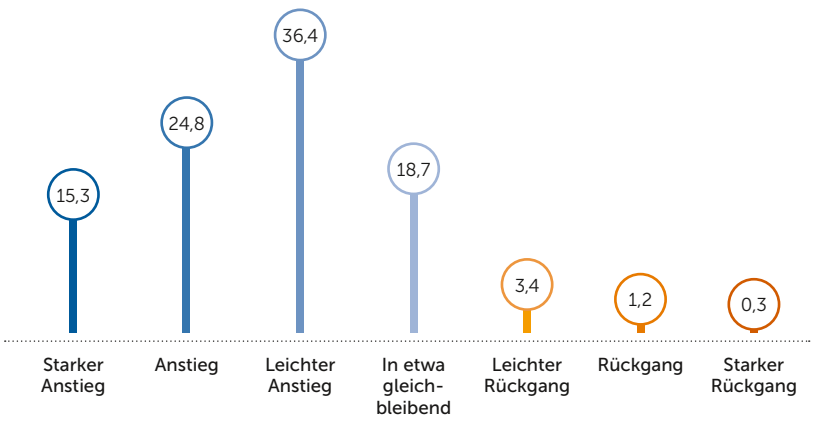
Die Unternehmen, die mit einem leichten bis starken Anstieg des Budgets für Cyber-Sicherheit in 2021 rechnen, haben bereits konkrete Pläne, wo sie die Security-Investitionen tätigen wollen. Die geplanten Anschaffungen für Security stimmen allerdings nicht durchgehend mit den zuvor genannten Herausforderungen der Cyber Security überein.

So wird die als besondere Herausforderung empfundene Endpoint Security nur von 20 Prozent der Unternehmen mit Investitionen in 2021 bedacht werden. Weitaus mehr werden in Netzwerksicherheit und Cloud-Sicherheit investieren, mit 42 Prozent beziehungsweise 39 Prozent. Auch der Datenschutz wird von 38 Prozent mit Investitionen versehen werden. Konzepte wie Zero Trust können nur bei fünf Prozent auf Investitionen hoffen.

Dabei sind es nicht etwa immer die großen Unternehmen, die eher investieren wollen. Für Zero-Trust-Lösungen planen beispielsweise acht Prozent der Unternehmen mit weniger als 500 Beschäftigten Investitionen, die größeren Unternehmen ab 1.000 Beschäftigten sehen den Investitionsbedarf hier hingegen nur in vier Prozent der Fälle. Ähnlich verhält es sich bei den Datenschutzausgaben: Jede zweite kleinere Firma plant, hier zu investieren – bei den größeren Unternehmen ist es indes nur jedes dritte. Man kann also einen gewissen Nachholbedarf bei den kleineren Unternehmen annehmen, der nun behoben werden soll.

Wie wird sich das IT-Security-Budget Ihres Unternehmens in 2021 im Vergleich zum Vorjahr (voraussichtlich) entwickeln?

Angaben in Prozent. Basis: n = 337

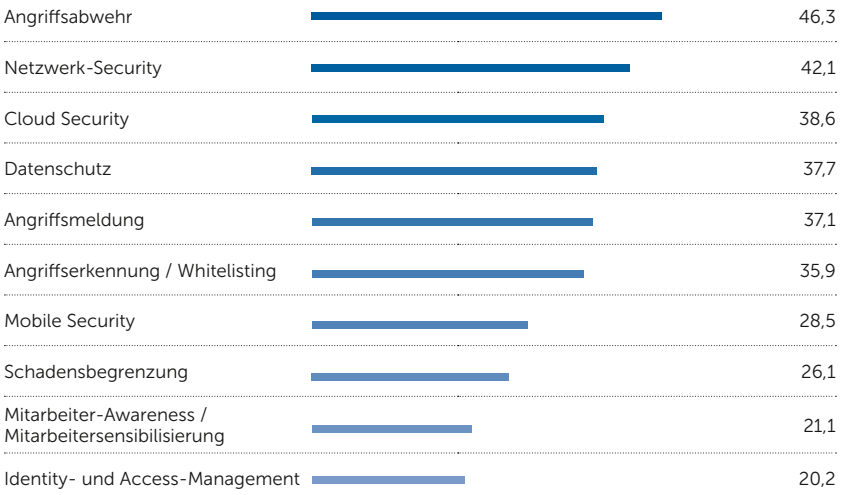


Betrachtet man einzelne Sicherheitsmaßnahmen und die dafür geplanten Projekte in 2021, nennen 61 Prozent den verbesserten Schutz oder die Verschlüsselung sensibler Daten, 46 Prozent die Klassifizierung der Daten, 39 Prozent das Auffinden sensibler Daten und 27 Prozent das Testen und die Absicherung von Applikationen.

Offensichtlich liegt bei vielen Unternehmen noch kein schlüssiges Modell vor, wie denn die angestrebte Verbesserung der Datenverschlüsselung aussehen soll. So sind das Auffinden sensibler Daten und deren Klassifizierung eigentlich die Grundlage für eine sinnvolle, risikoabhängige Verschlüsselung, auch im Hinblick auf Compliance-Vorgaben wie den Datenschutz.

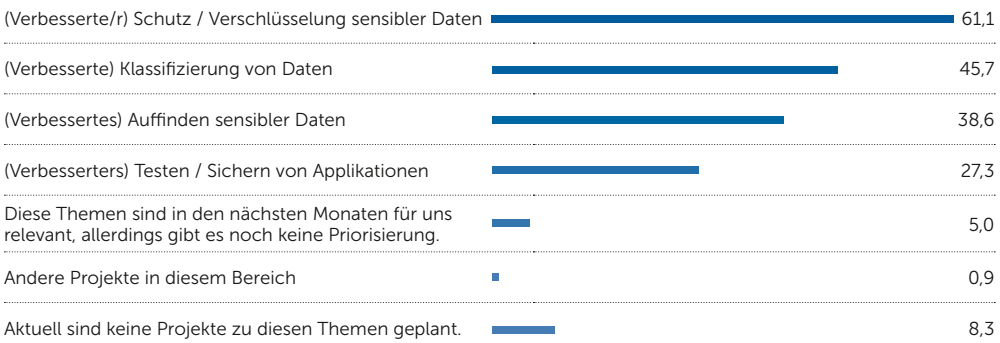
Wo liegen die Schwerpunkte Ihrer Cyber-Security-Investitionen?

Mehrfachnennungen möglich. Angaben in Prozent. Dargestellt sind die Top-10-Antworten. Basis: n = 337



In welchen Bereichen der Application Security, Data Security und / oder Data Governance planen Sie in den nächsten sechs bis zwölf Monaten konkrete Projekte?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 337



6. Zero Trust ist für über 90 Prozent der Unternehmen ein Thema

38 Prozent der befragten Unternehmen setzen bereits auf ein Zero-Trust-Modell, 41 Prozent sind gegenwärtig in der Implementierung. Weitere 14 Prozent planen die Einführung von Zero Trust, nur für sieben Prozent der Unternehmen hat es Zero Trust noch nicht einmal in die Planung geschafft. Damit kann man sagen, dass sich Zero Trust nachhaltig etabliert hat.

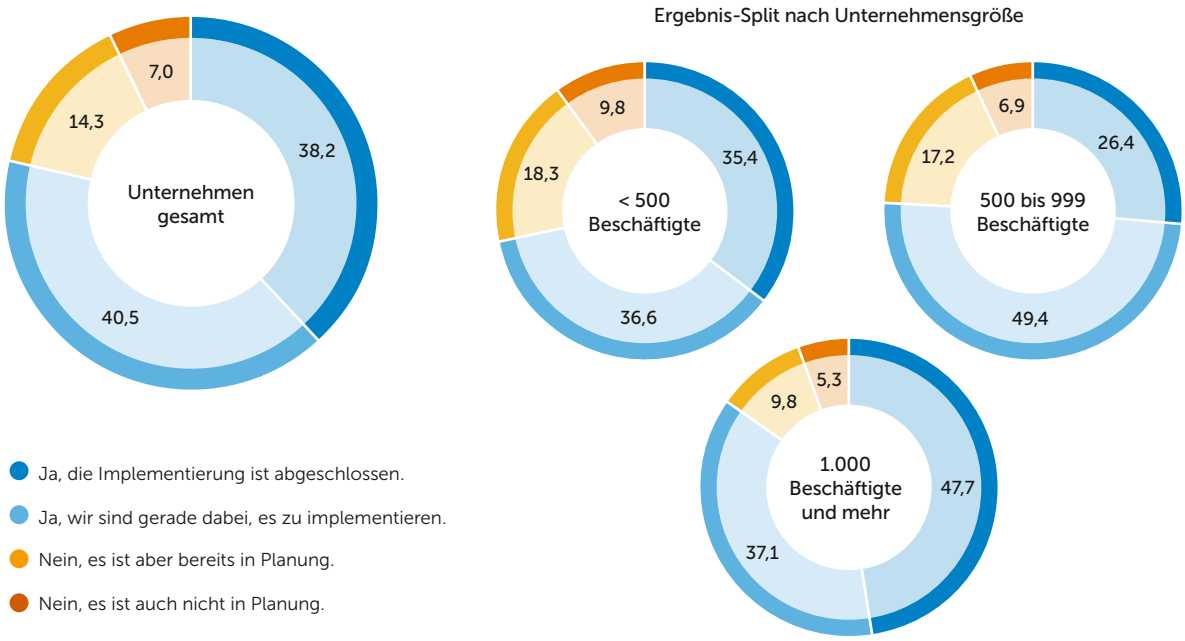
Obwohl nur wenige Unternehmen Investitionen für Zero Trust vorgesehen haben, ist dieser Ansatz bei 55 Prozent in der Implementierung oder in der Planung. Das gilt auch für größere Unternehmen, die sogar noch seltener Investitionen im Bereich Zero Trust vorgesehen haben.

So sind es 37 Prozent der Unternehmen mit 1.000 und mehr Beschäftigten, die Zero Trust einführen, und zehn Prozent, die es planen. Entweder wurden also für Zero Trust bereits Mittel in eine Rücklage eingestellt, oder aber die Projekte könnten Gefahr laufen, ohne geeignete Investition ins Stocken zu geraten.

Es bleibt zu hoffen, dass die Projektplanungen und Budgetplanungen besser in Übereinstimmung gebracht werden, sodass wichtige Projekte wie Zero Trust ohne Verzögerungen umgesetzt werden können.

Haben Sie ein Zero-Trust-Modell implementiert?

Angaben in Prozent. Basis: n = 337



Definition: Ein Zero-Trust-Modell ist ein Sicherheitskonzept, bei dem keinem Gerät, keinem Nutzer und keinem Dienst – weder innerhalb noch außerhalb des Unternehmensnetzes – per se vertraut wird. Sämtliche Anwender und Dienste müssen einzeln authentifiziert werden.

7. 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.

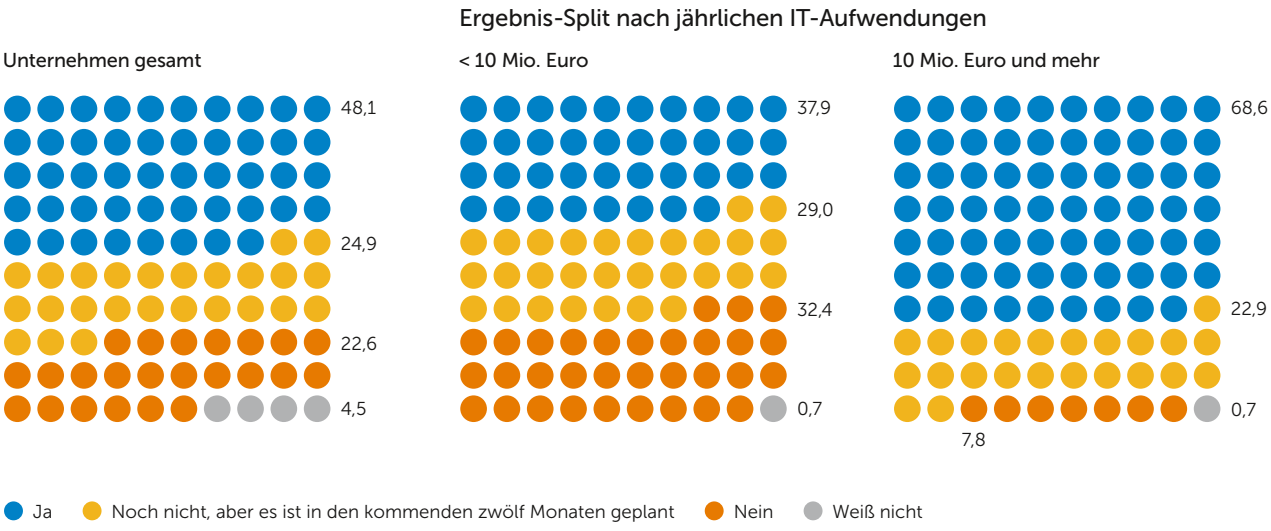
Doch KI in der Cyber Security ist nicht nur eine Frage des Budgets: Unternehmen mit weniger als 500 Beschäftigten sagen bisher in 31 Prozent der Fälle Nein zu KI. Bei 500 bis 999 Beschäftigten sinkt die Ablehnung auf 22 Prozent, ab 1.000 Beschäftigten beträgt sie nur noch 18 Prozent.

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



8. Jedes zweite Unternehmen setzt bereits auf Security Automation

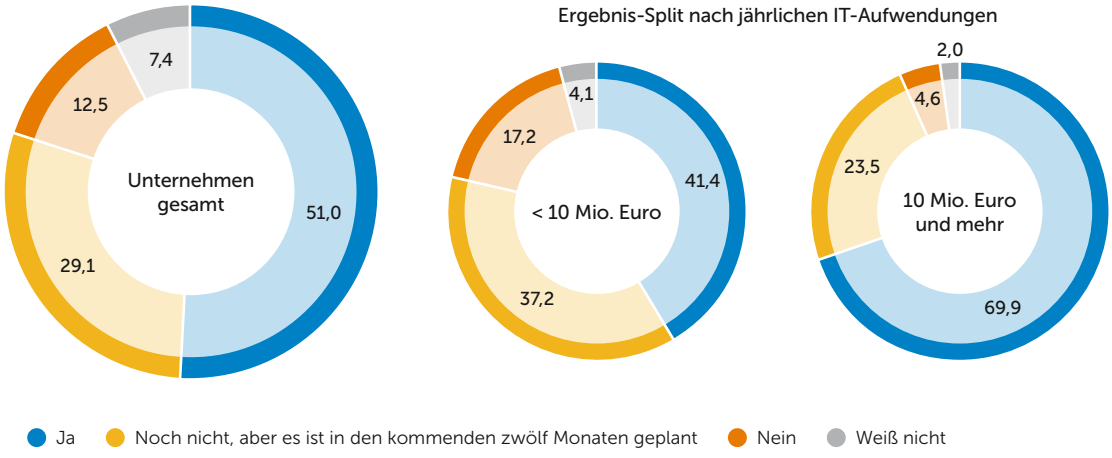
Nur 13 Prozent der befragten Unternehmen planen nicht, ihre Cyber Security (teilweise) zu automatisieren. 29 Prozent planen Security Automation in den nächsten zwölf Monaten. Security-Automatisierung ist bei größeren Unternehmen mit 58 Prozent stärker verbreitet als bei den kleinen mit 46 Prozent. Ein höheres IT-Budget trägt zu mehr Security Automation bei.

Bei einem jährlichen IT-Budget ab zehn Millionen Euro nutzen 70 Prozent der Unternehmen Funktionen zur Automatisierung ihrer Cyber Security, bei unter zehn Millionen Jahresbudget für die IT sind es immer noch 41 Prozent.

Als Gründe für Security Automation nennen 65 Prozent die schnellere Erkennung von Angriffen, 51 Prozent den Fachkräftemangel und 50 Prozent die raschere Abwehr von Angriffen. Die Kostenreduktion ist für 45 Prozent ein Grund, eine bessere Compliance dagegen nur für 26 Prozent.

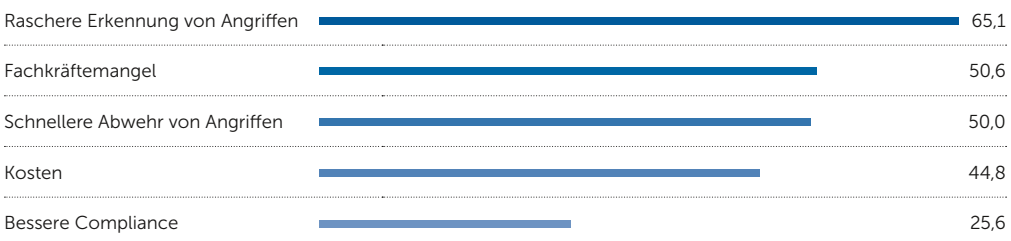
Ist Security Automation Teil Ihrer IT-Security-Strategie?

Angaben in Prozent. Basis: n = 337



Aus welchen Gründen ist Security Automation Teil Ihrer IT-Security-Strategie?

Mehrfachnennungen möglich. Angaben in Prozent. Filter: Unternehmen, die Security Automation einsetzen. Basis: n = 172

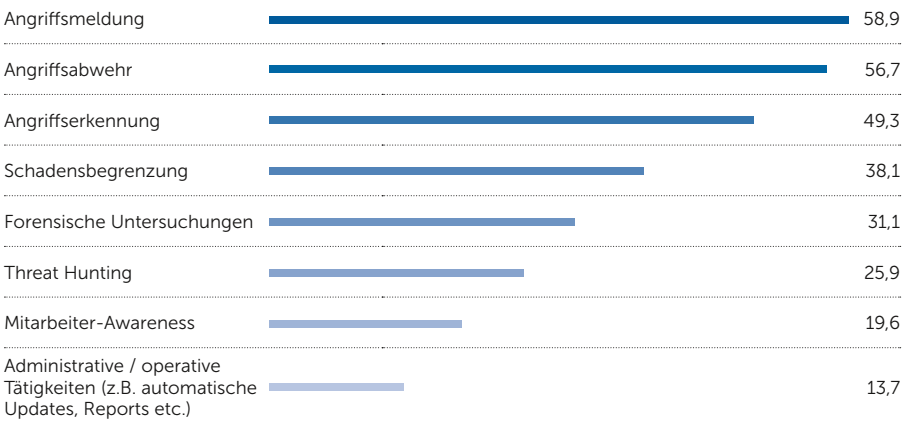


Offensichtlich wird die Bedeutung einer schnellen Abwehr nach der Detektion ebenso unterschätzt wie die Vorteile einer automatisierten Erkennung und Abwehr für die Compliance. So richtet sich zum Beispiel die Höhe des Bußgeldes bei einer Datenschutzverletzung nach DSGVO (Datenschutz-Grundverordnung) auch nach den Maßnahmen, die zur Eindämmung möglicher Schäden ergriffen werden.

Auch bei der Frage danach, welcher Teil der Security automatisiert wurde oder werden soll, zeigen sich Unklarheiten bei den Zusammenhängen: 59 Prozent beziehen die Automatisierung auf die Angriffsmeldung, aber nur 49 Prozent auf die Angriffserkennung. Die Angriffsabwehr wird diesmal von 57 Prozent erwähnt. Wichtig ist allerdings, dass bei der Detektion und Antwort auf Cyber-Attacken ein durchgehender Prozess herrschen muss, der möglichst viel Unterstützung durch Security Automation erfährt. Meldungen ohne Erkennung sind ebenso wenig hilfreich wie eine Abwehr ohne vorherige Detektion.

Welcher Teil Ihrer IT-Security ist automatisiert oder soll automatisiert werden?

Mehrfachnennungen möglich. Angaben in Prozent. Filter: Unternehmen, die Security Automation einsetzen oder den Einsatz planen. Basis: n = 270



9. Über die Hälfte der Unternehmen sagt Nein zum Security Outsourcing

Nur 13 Prozent der Unternehmen sagen, dass das Outsourcing der Cyber Security bei ihnen kein Tabuthema ist. 55 Prozent jedoch halten das Outsourcing für ein No-Go in ihrem Unternehmen. Die Ablehnung von Outsoucing steigt mit dem verfügbaren IT-Budget. Ab zehn Millionen Euro IT-Budget pro Jahr lehnen 64 Prozent das Outsourcing ab.

Obwohl Outsourcing als Weg gegen den vorherrschenden Fachkräftemangel gesehen wird, sind es insbesondere die Unternehmen mit weniger Beschäftigten, die Security Outsourcing ablehnen. Bei weniger als 500 Beschäftigten sagen 59 Prozent der Befragten, Outsourcing der Cyber-Sicherheit sei bei ihnen ein Tabuthema. Ab 1.000 Beschäftigten sind es immer noch 54 Prozent der Unternehmen, die so denken.

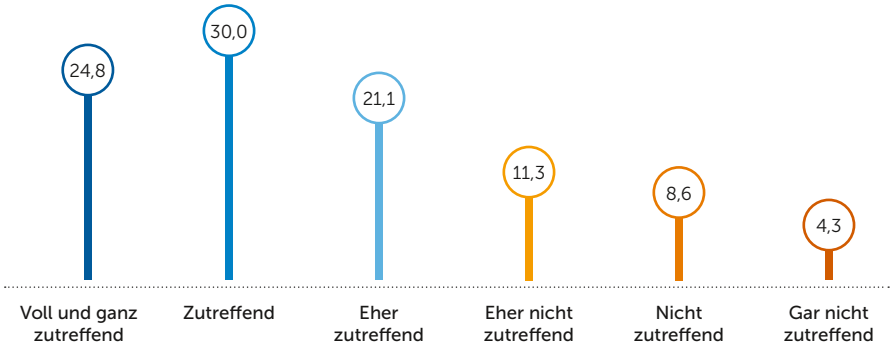
Die Ablehnung des Security Outsourcings hängt auch von der Rolle der Befragten ab. Während die Fachbereiche nur zu 24 Prozent sagen, dass Outsourcing ein Tabuthema sei, sind es im IT-Bereich bereits 56 Prozent und bei Vertretern des C-Levels (Geschäftsführung / Vorstand) sogar 67 Prozent. Da der C-Level in der Regel die Entscheidungen über das Outsourcing trifft, dürfte dies deutliche Folgen für den Outsourcing-Markt haben.

Das jährlich verfügbare IT-Budget hat auch einen Einfluss auf die Einstellung zum Outsourcing von Security-Funktionen. In Unternehmen mit weniger als zehn Millionen Euro IT-Budget im Jahr sind es 49 Prozent, die Outsourcing ablehnen, volle Zustimmung zum Outsourcing signalisieren dagegen 15 Prozent. Ist das IT-Budget höher als zehn Millionen Euro jährlich, sind es sogar 64 Prozent, die das komplette oder teilweise Outsourcen der Security als Tabuthema ansehen. Offensichtlich ist hier der Kostendruck geringer, ein Outsourcing deshalb nicht interessant.

Insgesamt ist diese Entwicklung als Abwendung von Outsourcing in der Security erstaunlich, da der Fachkräftemangel zunimmt und vielfach beklagt wird.

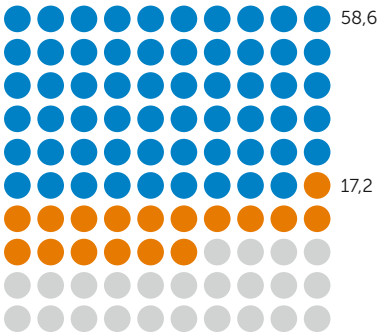
Inwieweit ist die folgende Aussage für Ihr Unternehmen zutreffend?
„Das (komplette oder teilweise) Outsourcen von IT-Security ist für unser Unternehmen ein Tabuthema."

Angaben in Prozent. Basis: n = 337

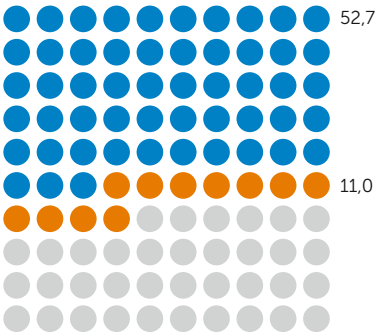


Ergebnis-Split nach Unternehmensgröße

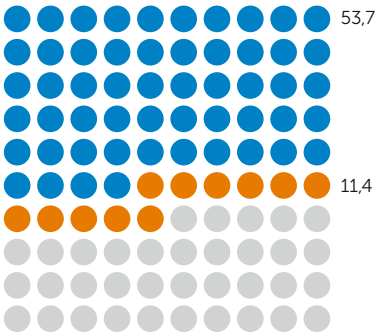
< 500 Beschäftigte



500 bis 999 Beschäftigte



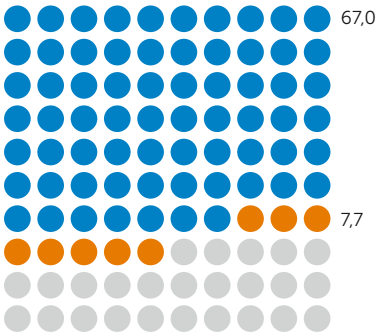
1.000 Beschäftigte und mehr



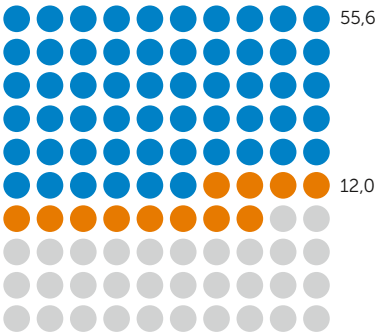
Voll und ganz zutreffend / zutreffend Nicht zutreffend / gar nicht zutreffend

Ergebnis-Split nach Funktion im Unternehmen

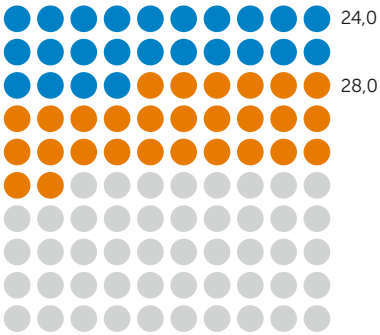
C-Level



IT-Leiter & IT-Bereich



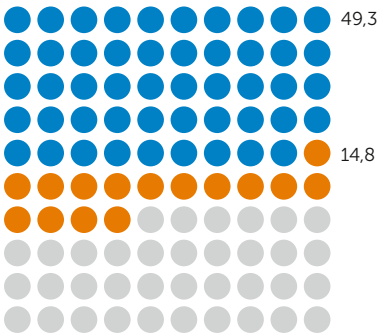
Fachbereiche



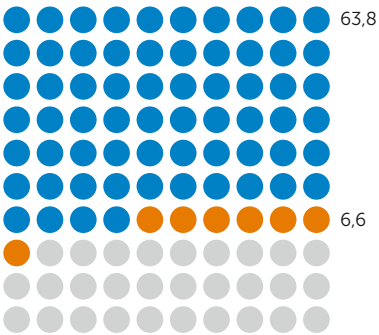
Voll und ganz zutreffend / zutreffend Nicht zutreffend / gar nicht zutreffend

Ergebnis-Split nach jährlichen IT-Aufwendungen

< 10 Mio. Euro



10 Mio. Euro und mehr



Voll und ganz zutreffend / zutreffend Nicht zutreffend / gar nicht zutreffend

10. 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.

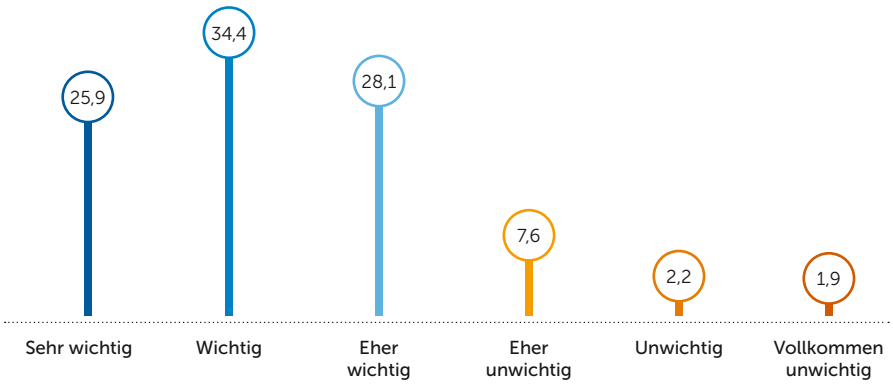
Der Wunsch nach offenen Security-Lösungen hängt auch vom jährlich verfügbaren IT-Budget ab. Beträgt es zehn Millionen Euro und mehr, wollen 71 Prozent eine offene Sicherheitsinfrastruktur. Bei unter zehn Millionen Euro sind immer noch 53 Prozent an der Offenheit der Security interessiert.

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.

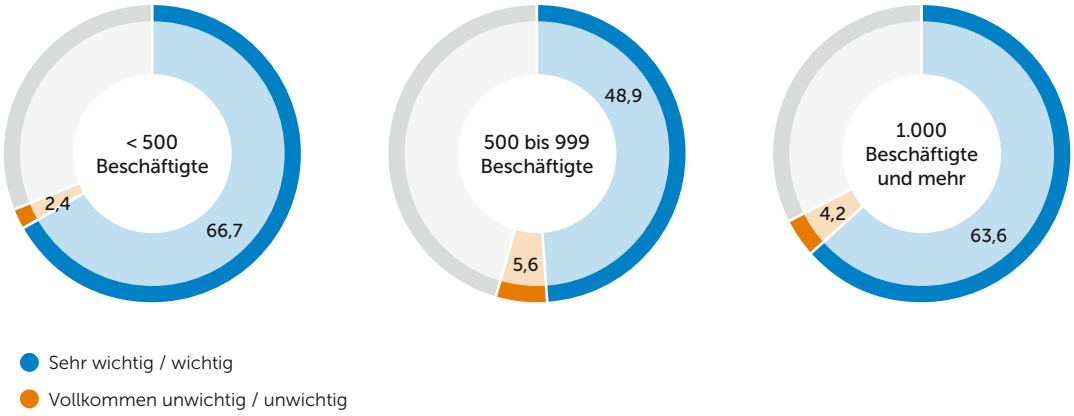
Es ist allerdings zu vermuten, dass die Fachbereiche die Nachteile von Insellösungen in der Security nicht genau genug kennen, die Vertreter des C-Levels hingegen sind mit den Vorteilen der Offenheit offensichtlich vertraut.

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

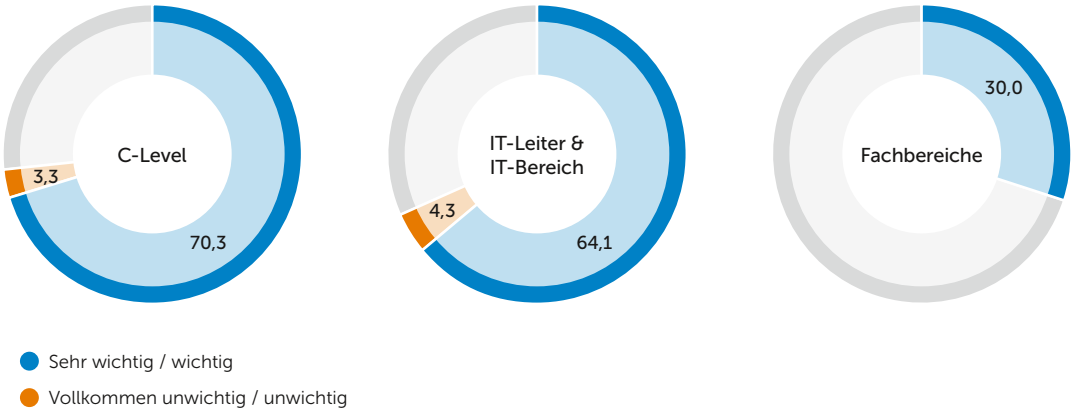
Angaben in Prozent. Basis: n = 337



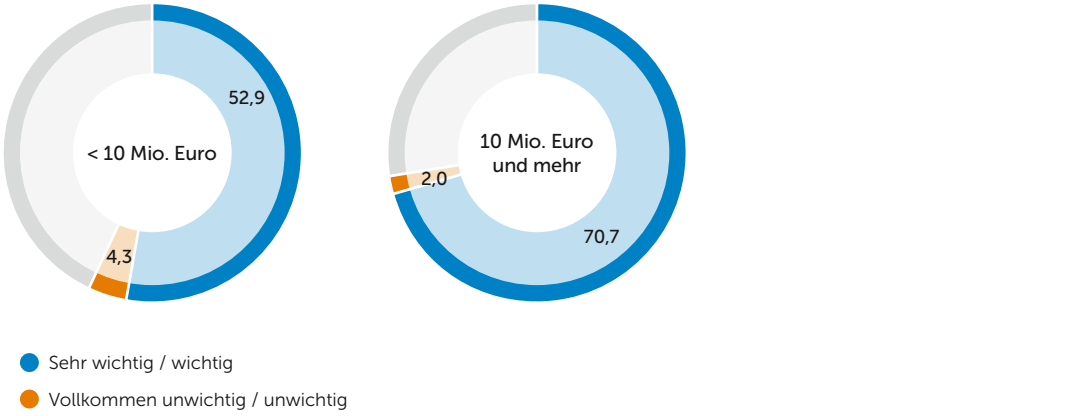
Ergebnis-Split nach Unternehmensgröße



Ergebnis-Split nach Funktion im Unternehmen



Ergebnis-Split nach jährlichen IT-Aufwendungen



Weitere Studienergebnisse

1. Digitalisierungsstrategien teils ohne Security-Grundlage

Die verschiedenen Strategien in den befragten Unternehmen sind nicht immer aufeinander abgestimmt. So gibt es zum Beispiel bei 71 Prozent ein Mobile-Konzept, doch nur 61 Prozent behandeln den häufigen Fall, dass private Geräte auch betrieblich genutzt werden (BYOD, Bring Your Own Device). Ähnlich verhält es sich mit Modern Workplace und Homeoffice.

84 Prozent der Unternehmen haben eine Digitalisierungsstrategie verabschiedet. Was auf den ersten Blick gut aussieht, hat aber gewisse Einschränkungen. Die Cyber-Sicherheit bildet ebenfalls ein Fundament der Digitalisierung. Doch nicht alle Unternehmen, die eine Strategie für die Digitalisierung haben, besitzen auch eine solche für die IT-Security. Diese haben 81 Prozent.

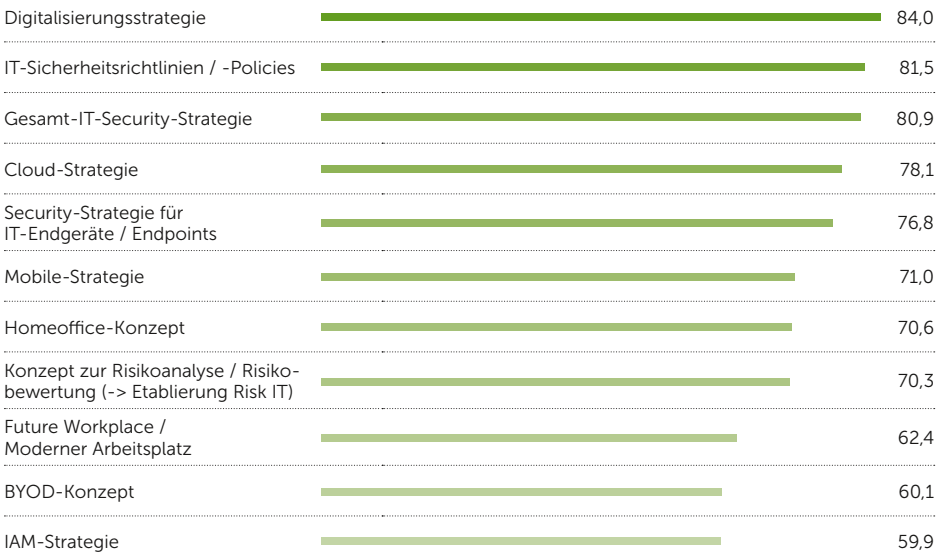
Bedenkt man zudem, dass Endpoints als eine große Herausforderung für die Security gesehen werden, ist es erstaunlich, dass nur 77 Prozent eine Security-Strategie im Bereich Endgeräte entwickelt haben.

Besonders kritisch zu sehen ist, dass nur 70 Prozent ein Konzept zur Risikoanalyse haben, da dieses grundlegend für die Erstellung von Security-Konzepten ist. Ebenfalls fehlt bei 40 Prozent ein Konzept für den wichtigen Bereich IAM (Identity- and Access-Management). Das immer wichtiger werdende Konzept für Homeoffice haben erst 71 Prozent.

Insgesamt zeigt sich, dass das gute Bild, eine Digitalisierungsstrategie zu haben, getrübt wird, wenn man sich die Konzepte und Strategien im Detail ansieht.

Welche der folgenden Strategien und Konzepte gibt es in Ihrem Unternehmen?

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



2. Industriespionage – wenig gefürchtet, aber großes Schadpotenzial

Wenn es um den möglichen Schaden geht, fürchten sich Unternehmen weniger vor Angreifern als vor Angriffsformen. So werden die Risiken durch Industriespione, ehemalige Mitarbeiter oder Partner in der Lieferkette geringer gesehen als die Folgen von Ransomware oder Identitätsdiebstahl. Hier zeigt sich ein Problem in der Risikowahrnehmung.

Berichte über erfolgreiche Cyber-Attacken zeigen, wie hoch der Schaden sein kann, wenn Industriespione oder staatliche Spione angreifen, ebenso wenn es zu Attacken auf die oder aus der Lieferkette kommt. Auch die Risiken durch die Nachlässigkeit der Beschäftigten sind erfahrungsgemäß hoch.

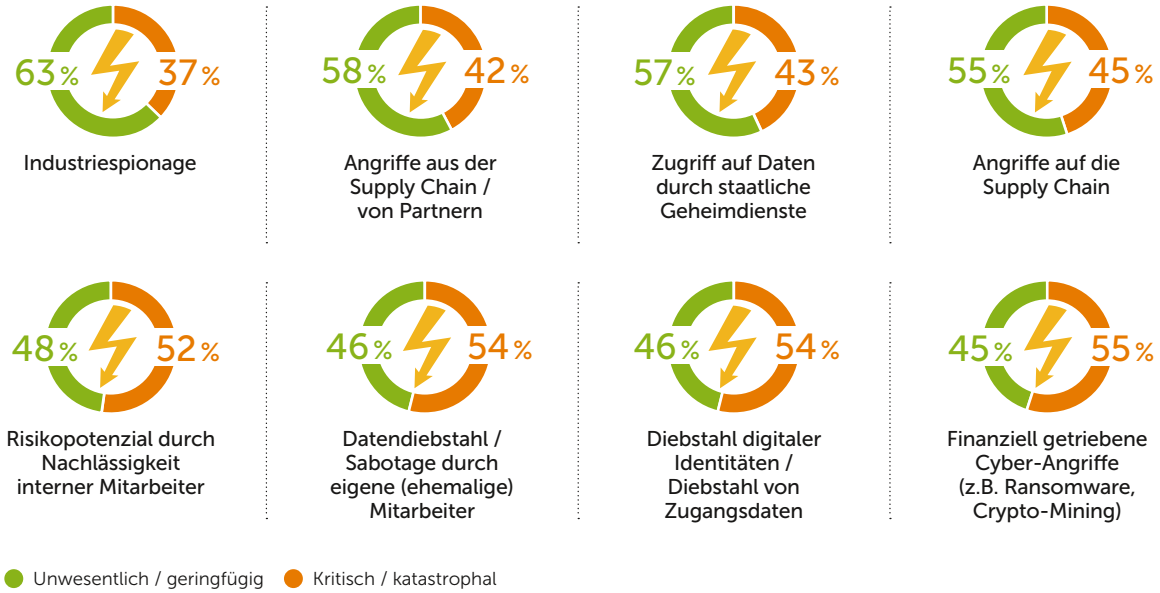
Trotzdem werden die Schäden solcher Vorfälle als geringer eingestuft als zum Beispiel die durch Ransomware-Attacken oder den Diebstahl digitaler Identitäten. Das zeigt, dass bei der Mehrzahl der befragten Unternehmen ein unklares Bild herrscht, wie Industriespione oder Nachrichtendienste vorgehen.

So gehören Erpresserviren ebenso zu den möglichen Werkzeugen der Spione wie der Diebstahl von Zugangsdaten. Auch kann die Nachlässigkeit der Mitarbeiter zum Erfolg von Datendiebstahl oder Ransomware beitragen.

Die Risikobetrachtung in den Unternehmen sollte deshalb die möglichen Instrumente der Angreifer genauer in den Augenschein nehmen, denn die Instrumente werden eher gefürchtet als diejenigen, die diese Werkzeuge einsetzen könnten.

Wie groß würden Sie im schlimmsten Fall das Schadensmaß bei diesen Cyber-Vorfällen einstufen?

Angaben in Prozent. Basis: n = 318



Setzt man das erwartete Schadensausmaß ins Verhältnis zu der in einer weiteren Frage abgefragten erwarteten Eintrittswahrscheinlichkeit bestimmter Cyber-Vorfälle, lassen sich erste grobe Risikoanalysen vornehmen.

Beispiel Industriespionage: Auch wenn fast zwei Drittel der Befragten den erwarteten Schaden durch Industriespionage als unwesentlich oder geringfügig einschätzen, schätzen genauso viele Befragte die Eintrittswahrscheinlichkeit solch eines Ereignisses zumindest als „entfernt vorstellbar" ein. Das hat zur Folge, dass der „inakzeptable Bereich" der Risikomatrix zu „Industriespionage" besonders groß wird. Über 92 Prozent derjenigen Befragten, die das Schadensausmaß von Industriespionage als „katastrophal" bezeichnen, können sich zumindest entfernt vorstellen, dass dieses Ereignis eintreten könnte. Auf der Gegenseite umfasst der „akzeptable Bereich" unter anderem 68 Prozent der Befragten, die das mögliche Schadensausmaß von Industriespionage als „unwesentlich" einstufen und sich gleichzeitig auch nicht oder nur wenig vorstellen können, dass sie Opfer solch eines Incidents werden.

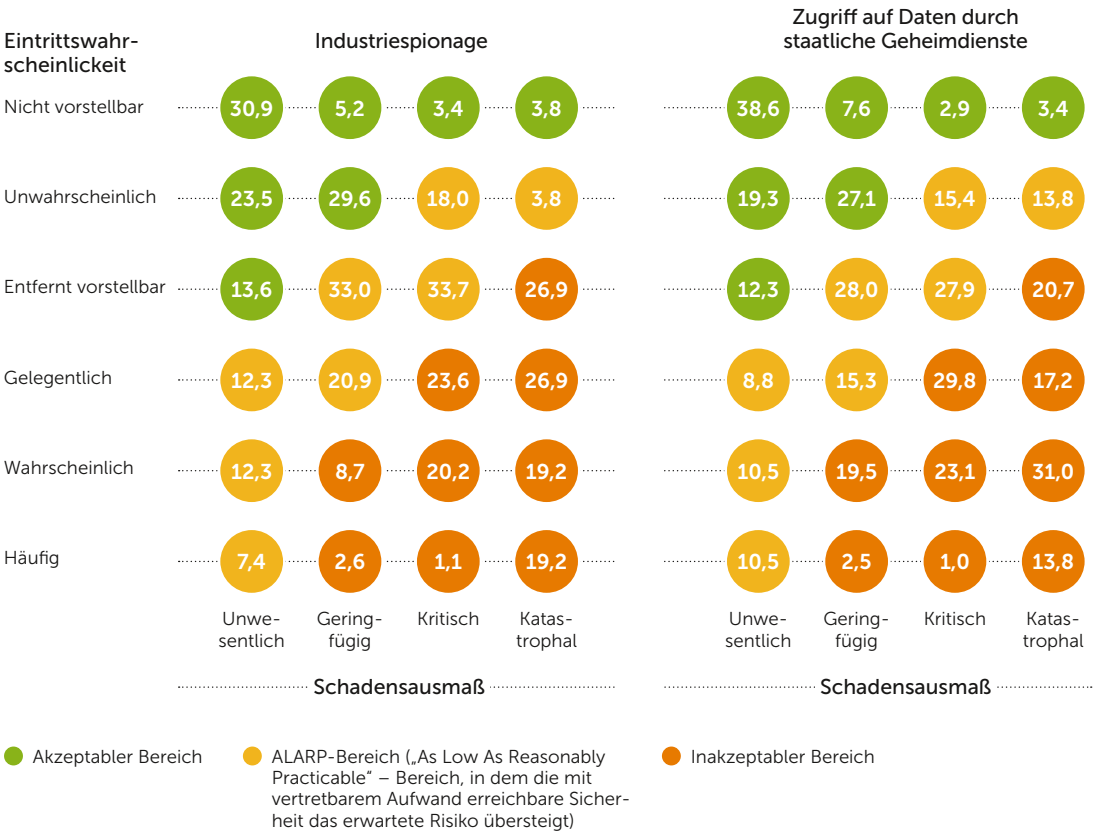
Beispiel „Zugriff auf Daten durch staatliche Geheimdienste": Hier ist der „akzeptable Bereich" besonders groß – man erwartet solch ein Ereignis seltener, der erwartete Schaden ist deutlich geringer.

Fazit: Je realistischer ein Security-Vorfall, desto größer der erwartete Schaden. Je unbekannter ein Incident, desto kleiner.

Wie groß ist Ihrer Einschätzung nach die Eintrittswahrscheinlichkeit in Ihrem Unternehmen für einen Cyber-Vorfall?

Angaben in Prozent. Basis: n = 318

Risikomatrizes mit kombinierten Antworten auf die Fragen nach Schadensausmaß und Eintrittswahrscheinlichkeit



3. Spannende Positionen zu verschiedenen Security-Ansätzen

Die Unternehmen wurden auch befragt, wie sie zu verschiedenen Aussagen rund um die Cyber Security stehen. Der Grad an Zustimmung kann wertvolle Hinweise darauf liefern, wie erfolgreich entsprechende Security-Ansätze im Markt gesehen und umgesetzt werden können. Entsprechende Kommentare ergänzen die Statements.

„Es geht nicht um Netzwerk, Endpoint oder Cloud, sondern um die Daten, die verarbeitet werden"

Kommentar: Datenzentrierte Security hat eine hohe Bedeutung, allerdings darf nicht vergessen werden, dass zur Umsetzung der Datensicherheit auch Maßnahmen im Bereich Netzwerk, Endpoint und Cloud erforderlich sind.

„Die beste Endpoint Security bringt nichts, wenn der Faktor Mensch das größte Sicherheitsrisiko bleibt. Er muss daher Teil des Security-Konzepts werden."

Kommentar: Die Bedeutung des Menschen als Risikofaktor und als „menschliche Firewall" darf nicht unterschätzt werden. Man darf aber auch nicht den Fehler machen, den technischen Schutz zu wenig zu beachten.

„IT-Security ist zu umfangreich und komplex geworden, um sie ohne Hilfe von Partnern oder Dienstleistern umsetzen zu können."

Kommentar: Diese Aussage erstaunt insofern, als an anderer Stelle Outsourcing von der Mehrheit abgelehnt wird. Deshalb sucht man offensichtlich Unterstützung, aber nur im begrenzten Umfang.

„IAM wird immer facettenreicher und kann deshalb künftig nur noch in der Cloud richtig funktionieren."

Kommentar: Trotzdem haben 40 Prozent der Unternehmen kein IAM-Konzept entwickelt, wie sich an anderer Stelle zeigt.

„Eine einheitliche Security-Management-Plattform unterstützt Unternehmen bei der Umsetzung ihrer IT-Security-Strategie besser als Einzellösungen."

Kommentar: Dieses Aussage passt dazu, dass viele Unternehmen die Offenheit von Security-Lösungen wünschen, da diese auch dann eine durchgehende Security ermöglicht, wenn keine zentrale Plattform nur eines Anbieters genutzt wird.

4. Systemfehler und Datenverlust sind die häufigsten Schäden

Kommt es zu einem Cyber-Vorfall, leiden die Unternehmen insbesondere unter den internen Aufwänden zur Fehlerbehebung, dem Datenverlust, den zusätzlichen Kosten für Dienstleister und dem Produktionsstillstand. Imageschäden gegenüber Kunden, Lieferanten und der Öffentlichkeit sind hoch, aber nachrangig, wenn es um die Schadenshöhe geht.

Was genau als größter Schaden nach einem Cyber-Vorfall auftritt oder so angesehen wird, hängt auch von der Größe des betroffenen Unternehmens ab. Kleinere Unternehmen mit weniger als 500 Mitarbeitern klagen mit 48 Prozent besonders über den Verlust geschäftskritischer Informationen.

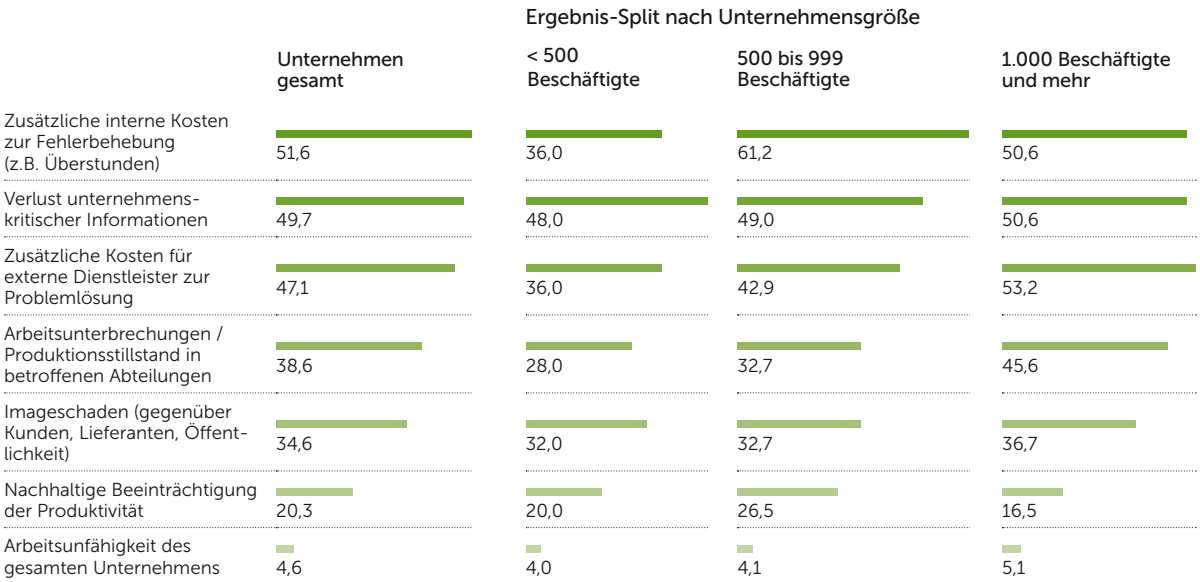
Mittelgroße Unternehmen mit 500 bis 999 Beschäftigten berichten dagegen besonders häufig (61 Prozent), dass ein Schaden durch die internen Kosten entsteht, die die Fehlerbehebung verursacht. Unternehmen ab 1.000 Beschäftigte sehen mit 53 Prozent am häufigsten einen Schaden durch die Kosten, die externe Dienstleister erzeugen.

Das ist insofern überraschend, als mittelgroße Unternehmen offensichtlich eher interne Lösungen einsetzen, die dann Kosten verursachen, während größere Unternehmen auf Dienstleister setzen, um entstandene Schäden einzudämmen.

Die bei Datenpannen besonders gefürchteten Imageschäden sehen größere Unternehmen eher als kleinere (37 gegenüber 32 Prozent).

Welcher Schaden (durch einen Cyber-Angriff) ist genau entstanden?

Mehrfachnennungen möglich. Angaben in Prozent. Filter: Unternehmen, denen durch Cyber-Angriff schon einmal ein wirtschaftlicher Schaden entstanden ist. Basis: n = 153



5. Attacken durch (ehemalige) Mitarbeiter oder Partner kommen häufiger vor

Innentäter erweisen sich als häufiges Risiko. 55 Prozent der Unternehmen haben bereits einen Datendiebstahl durch ehemalige oder aktuelle Beschäftigte festgestellt. Fast genauso viele wurden von Partnern aus ihrer Lieferkette oder Dienstleistern angegriffen.

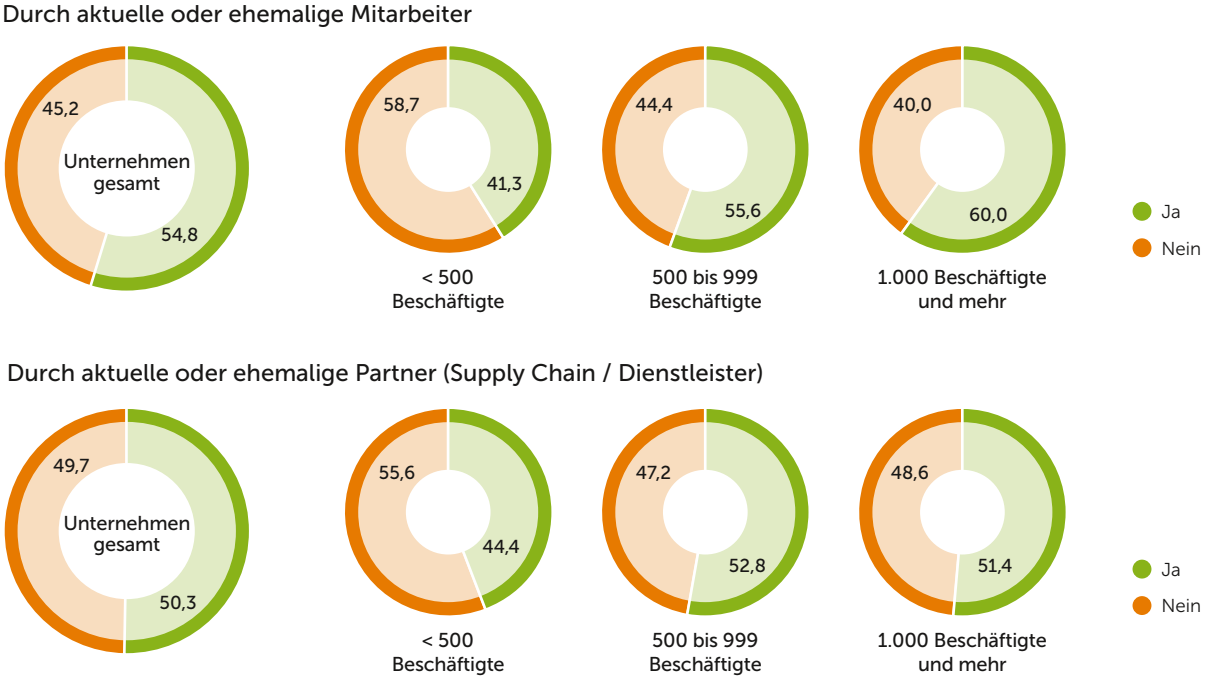
Das sogenannte Insider-Risiko hängt aber von der Größe des Unternehmens ab. Je mehr Beschäftigte ein Unternehmen hat, desto häufiger wurde bereits ein Vorfall mit Innentätern, also ehemaligen oder aktuellen Mitarbeitern festgestellt.

Kleine Unternehmen mit bis zu 500 Beschäftigten berichten zu 41 Prozent von Insider-Attacken. In Unternehmen ab 1.000 Beschäftigten beläuft sich der Anteil der Angegriffenen auf 60 Prozent. Wer also mehr Beschäftigte hat, muss intern fast zwangsläufig auch mit mehr krimineller Energie rechnen.

Im Fall von Supply-Chain-Partnern oder Dienstleistern verhält es sich ähnlich, doch die Unterschiede sind nicht ganz so ausgeprägt. Datendiebstahl durch Partner oder Dienstleister mussten 44 Prozent der kleineren Unternehmen beobachten, bei den größeren Unternehmen waren es dagegen 51 Prozent. Die Vermutung liegt nahe, dass dies auch hier mit der meist größeren Zahl der Partner oder Dienstleister zusammenhängt.

Sind in Ihrem Unternehmen schon einmal wichtige Daten oder Informationen gestohlen, sabotiert oder vorsätzlich gelöscht worden?

Angaben in Prozent. Basis: n = 318



6. Die IAM-Lösungen kommen mehrheitlich aus der Cloud

51 Prozent der Unternehmen nutzen eine cloud-basierte Lösung für IAM (Identity- und Access-Management). Weitere 25 Prozent planen deren Einführung in den nächsten zwölf Monaten. IAM-Lösungen aus der Cloud werden dabei vermehrt von Unternehmen genutzt, die mehr Beschäftigte haben. Der Anteil der Nutzer von Cloud-IAM steigt auf 57 Prozent ab 1.000 Beschäftigten.

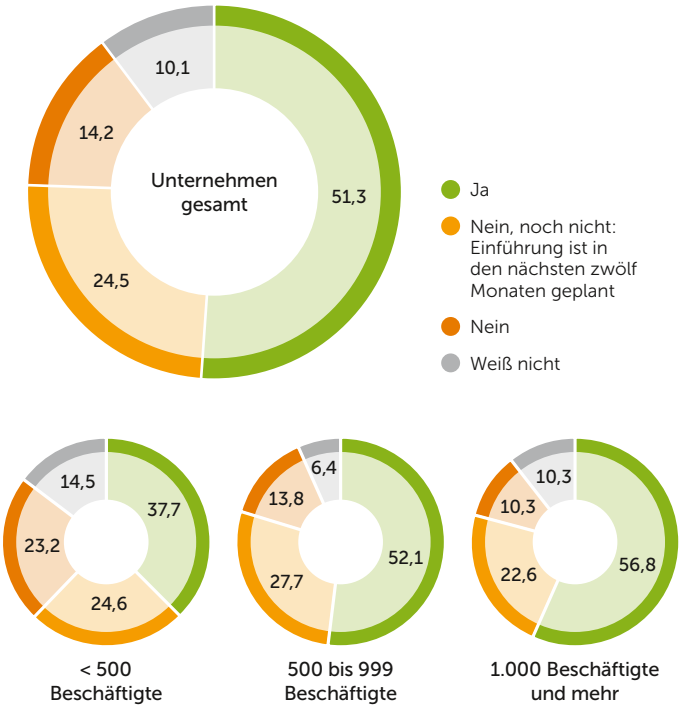
Geplant wird der Bezug von IAM-Lösungen aus der Cloud besonders von Unternehmen mit 500 bis 999 Beschäftigten, dort beträgt der Anteil 28 Prozent, bei kleineren Unternehmen 25 Prozent und bei größeren 23 Prozent.

Keine cloud-basierte Lösung für IAM setzen 23 Prozent der kleinen, 14 Prozent der mittleren und zehn Prozent der größeren Unternehmen ab 1.000 Beschäftigten ein. Offensichtlich sehen größere Unternehmen auch einen höheren Vorteil bei IAM aus der Cloud, da sich solche IAM-Lösungen schneller und einfacher unter den Nutzern ausrollen lassen.

Eine zentrale IAM-Lösung für Cloud-Anwendungen und für On-Premises-Applikationen setzen 30 Prozent bereits seit Längerem ein, 47 Prozent erst seit kurzer Zeit. In Planung ist es bei weiteren 15 Prozent. Man kann also davon ausgehen, dass nun die Zeit für zentrale, übergreifende IAM-Lösungen gekommen ist – gerade in letzter Zeit wurden hier die Weichen entsprechend gestellt.

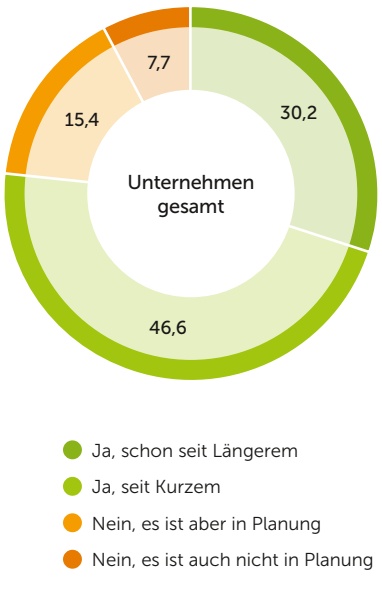
Gibt es in Ihrem Unternehmen ein cloud-basiertes Identity- und Access-Management (IAM)?

Angaben in Prozent. Basis: n = 318



Nutzen Sie eine zentrale Identitäts- und Zugriffsverwaltungsplattform für den Zugriff auf Cloud- und On-Prem-Applikationen verschiedener Hersteller?

Angaben in Prozent. Basis: n = 318



7. Multi-Faktor-Authentifizierung (MFA) muss sicher und integrierbar sein

Nur zwei Prozent der Unternehmen wünschen sich von einer MFA-Lösung die Unterstützung von biometrischen Faktoren. Zehn Prozent achten auf eine Nutzerakzeptanz, 20 Prozent auf den Stand der Technik, ebenso viele auf die Administrierbarkeit der gewünschten Lösung zur Authentifizierung der Nutzer.

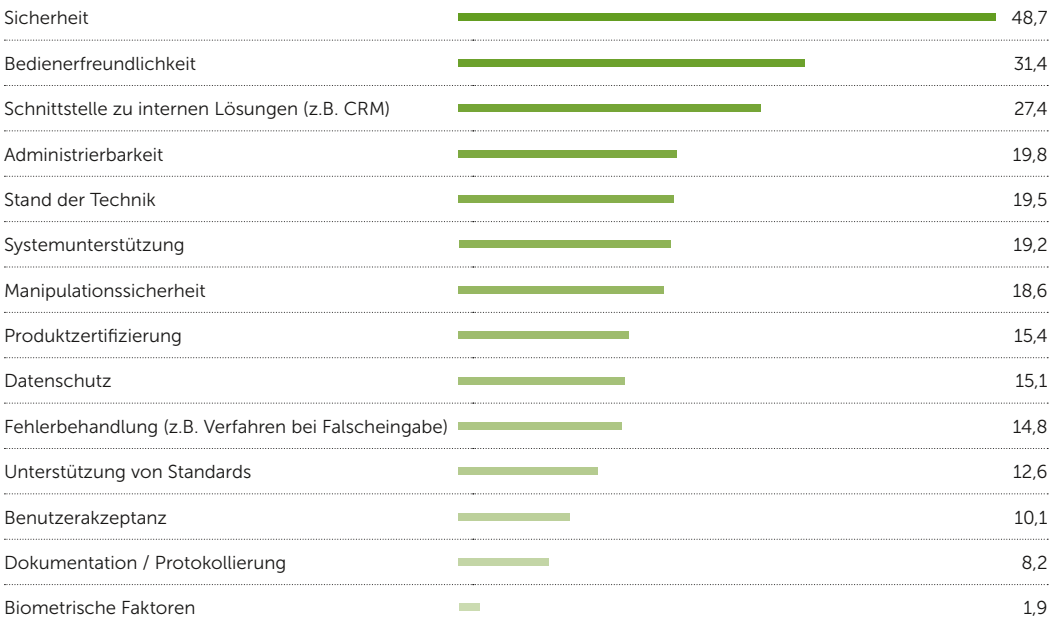
Die Sicherheit einer MFA-Lösung sollte eigentlich für jedes Unternehmen entscheidend sein. Doch nur 49 Prozent nennen diese Anforderung als Top-3-Auswahlkriterium. Die Bedeutung der Sicherheit ist bei den Unternehmen mit weniger Beschäftigten (unter 500) am höchsten und liegt dort bei 59 Prozent. Sind mehr Beschäftigte abzusichern, sinkt der Anteil der entsprechenden Antworten auf 47 Prozent bei 1.000 und mehr Beschäftigten.

Dabei sind die Vertreter des C-Levels (Vorstände, Geschäftsführer) am wenigsten an sicheren MFA-Lösungen interessiert, hier liegt der Anteil nur bei 44 Prozent. Im IT-Bereich liegt der Anteil hier bei 46 Prozent, in den Fachbereichen bei mehrheitlichen 52 Prozent.

Das ist erstaunlich – denn vermuten würde man, dass es den Fachbereichen mehr um Benutzerfreundlichkeit als um Sicherheit geht. Bedienerfreundliche MFA-Lösungen fordern aber nur 24 Prozent der Fachbereiche, 25 Prozent der IT-Bereiche, aber 35 Prozent im C-Level. Entsprechend sollten sich die Unternehmensentscheider mehr damit vertraut machen, was den Nutzern wirklich wichtig ist: Sicherheit vor Benutzerfreundlichkeit.

Was sind für Sie die wichtigsten drei Kriterien zur Auswahl einer (Multi-Faktor-)Authentifizierungslösung, mit deren Hilfe Sie digitale Geschäftsprozesse absichern möchten?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 318



8. Vier von zehn Unternehmen verwenden nur Bordmittel für privilegierte Accounts

45 Prozent der befragten Unternehmen setzen zur Verwaltung und Absicherung der privilegierten Zugänge auf eine IAM-Lösung oder aber PAM-Lösung (Privileged Access Management). 29 Prozent sehen keine besonderen Maßnahmen für den Schutz von Administratorkonten oder anderen Konten mit hohen Berechtigungen.

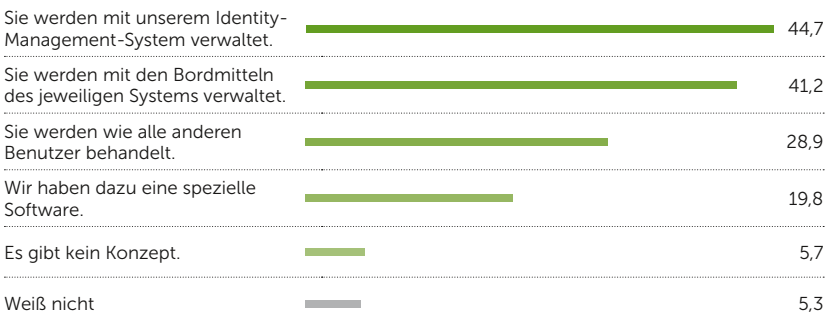
Der Missbrauch privilegierter Zugänge stellt eine besondere Bedrohung für die Cyber-Sicherheit in einem Unternehmen dar. Trotzdem setzt weniger als die Hälfte der befragten Unternehmen spezielle Lösungen für den Schutz dieser Accounts ein. Die Verwendung von Bordmitteln der genutzten Applikationen führt oftmals dazu, dass die Administratorzugänge genauso geschützt werden wie einfache Nutzerzugänge.

Die Umfrage zeigt aber, dass es nicht etwa an einem unzureichenden Budget liegt, wenn privilegierte Zugänge nur so geschützt werden wie einfache. Unternehmen mit einem jährlichen IT-Budget von zehn Millionen und mehr setzen mehrheitlich zu 53 Prozent auf die Bordmittel der genutzten Applikationen und nicht auf spezielle PAM-Lösungen. Bei diesen Unternehmen sind es zudem sogar 36 Prozent, die privilegierte Zugänge nicht besonders schützen.

Offensichtlich muss die Bedeutung der Sicherheit privilegierter Zugänge noch stärker ins Bewusstsein vorrücken, da unsichere privilegierte Zugänge dazu führen können, dass sämtliche Zugänge unsicher werden, wenn Angreifer die Administratorrechte missbrauchen.

Wie gehen Sie in Ihrem Unternehmen mit privilegierten Accounts um?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 318



9. 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.

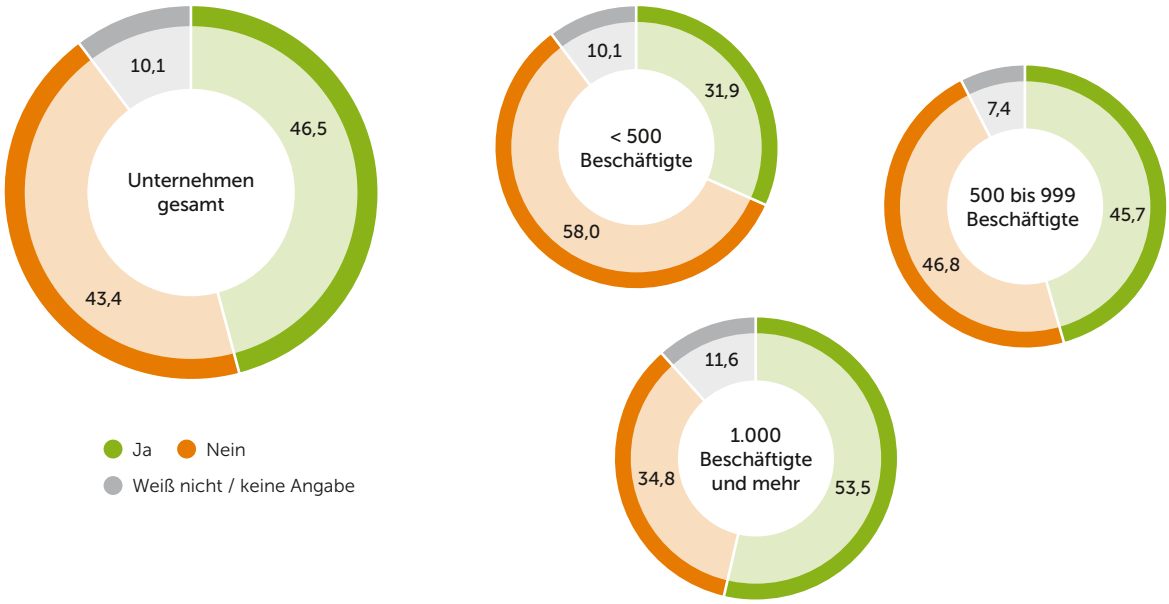
Die befragten Unternehmen vertrauen in Cloud Computing, nur zwei Prozent setzen ausschließlich auf On-Premises-IT. Gleichzeitig hat fast jedes zweite Unternehmen erfahren müssen, dass es über seine Cloud-Dienste angreifbar ist. Jedes zehnte Unternehmen hat noch keine Übersicht darüber, wie es um die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

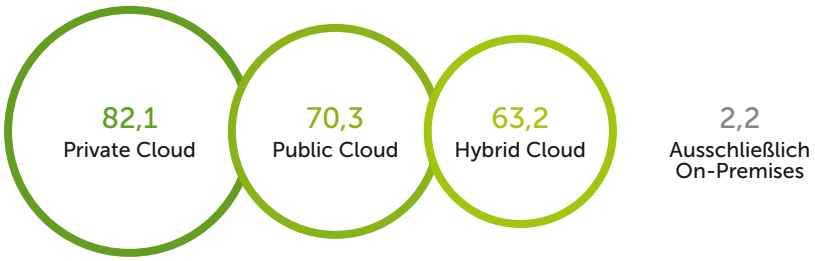
Angaben in Prozent. Basis: n = 318



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

10. Entwicklung und Security arbeiten häufig eng zusammen

Nur sieben Prozent der Unternehmen entwickeln keine eigene Software. Die Sicherheit bei den Eigenentwicklungen stellt bei 34 Prozent die Projektentwicklung selbst sicher, sie tauscht sich aber mit der Security-Abteilung aus.

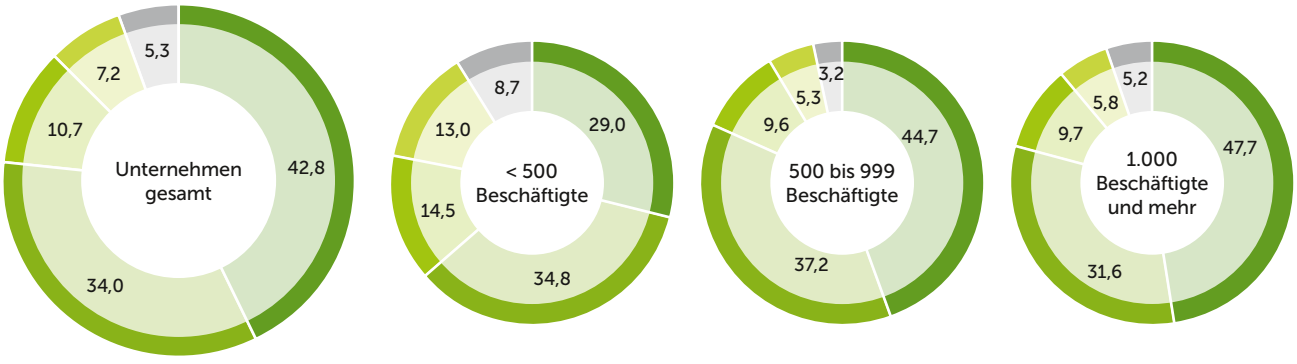
Eigene Softwareentwicklung ohne Security-Maßnahmen darf es nicht geben, sonst kann Security by Design kaum Realität werden. Es stellt sich aber die Frage, wie für die Security gesorgt wird: durch eine enge Zusammenarbeit mit der Security-Abteilung, Austausch mit der Security oder aber eine völlig getrennte Security innerhalb der Projektentwicklung.

Wie dies ausgestaltet ist, hängt auch von der Beschäftigtenzahl und dem jährlichen IT-Budget ab. Die Zusammenarbeit zwischen Entwicklung und Security ist bei Unternehmen mit mehr Beschäftigten intensiver. Bei unter 500 Beschäftigten liegt der Anteil derer, bei denen Security und Entwicklung eng zusammenwirken, bei 29 Prozent. Dies steigt mit der Beschäftigtenzahl auf 48 Prozent bei 1.000 Beschäftigten und mehr. Dies könnte auch daran liegen, dass größere Unternehmen auch häufiger eigenständige Abteilungen für Entwicklung und Security haben.

Ein höheres Budget für IT führt ebenso dazu, dass Security und Entwicklung enger zusammenarbeiten. Bei mehr als zehn Millionen Euro IT-Budget jährlich sind es 51 Prozent, die von einer engen Zusammenarbeit berichten – wohl auch, weil man sich jeweils eigene Abteilungen leisten kann.

Inwiefern werden Entwicklung und Betrieb eigener Softwarekomponenten (z.B. mithilfe von DevOps-Methoden) durch die firmeneigene IT-Security betreut?

Angaben in Prozent. Basis: n = 318



- Projektabteilung und IT-Security-Abteilung arbeiten miteinander. Die IT-Security-Abteilung kann jederzeit den Security-Stand der eigenen Softwareprodukte prüfen und nachweisen.
- Die Projektabteilung entwickelt bzw. implementiert geeignete Security-Mechanismen. Die IT-Security-Abteilung erhält auf Nachfrage Statusberichte.
- Die Softwareentwicklung unterhält Ihre eigenen Security-Kontrollen und -Werkzeuge. Die IT-Security-Abteilung (sofern es sie überhaupt gibt) wird nicht informiert.
- Unser Unternehmen entwickelt keine eigene Software.
- Weiß nicht

11. Bei einigen Security-Maßnahmen herrscht Unzufriedenheit

Viele zentrale Security-Maßnahmen werden in ihrer Bedeutung unterschätzt. So halten die befragten Unternehmen zum Beispiel E-Mail-Sicherheit nur zu 70 Prozent für wichtig, bei IT-Sicherheitsschulungen sind es sogar nur 59 Prozent. Bei vielen Maßnahmen korrespondiert die empfundene Wichtigkeit mit der Zufriedenheit damit, doch es gibt Ausnahmen.

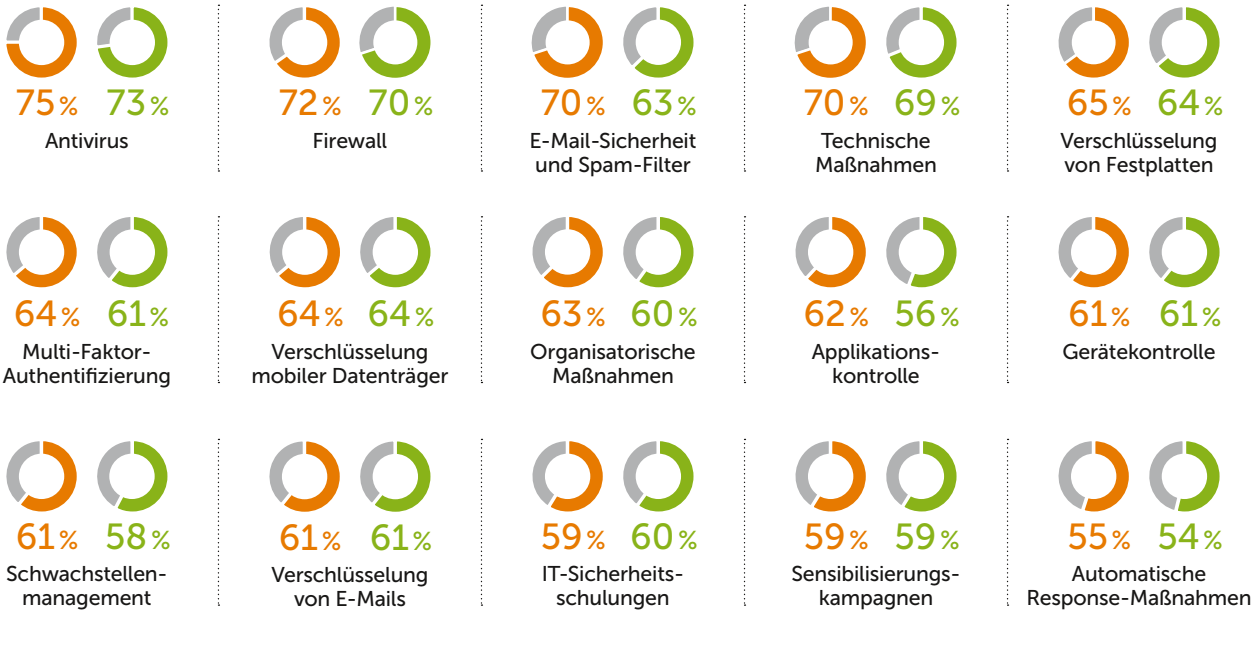
Selbst Basisschutz-Maßnahmen wie Firewall, Antivirus und Schwachstellenmanagement sind nicht für alle der befragten Unternehmen von Bedeutung. Themen wie automatische Response-Maßnahmen, die durch die zunehmend komplexen, intelligenten Attacken und den gleichzeitigen Fachkräftemangel immer wichtiger werden, sehen die befragten Unternehmen nur zu 55 Prozent als bedeutend an.

Allerdings sind die Unternehmen bei den meisten Maßnahmen der Cyber Security zufrieden, trotz der offensichtlichen Erfolge der Angriffe. Ausnahmen bei der Zufriedenheit und damit einen deutlichen Unterschied zur Bedeutung gibt es bei E-Mail-Sicherheit und bei Applikationskontrolle. Hier sagen mehr Unternehmen, es sei wichtig, als es Unternehmen gibt, die mit den ergriffenen Maßnahmen zufrieden sind.

Fragt man direkt nach der Unzufriedenheit, wird der höchste negative Wert bei der IT-Sicherheitsschulung und bei automatischen Response-Lösungen erzielt. Hier besteht also ebenfalls Handlungsbedarf.

Wie wichtig sind Ihrem Unternehmen die folgenden IT-Sicherheitsmaßnahmen und -leistungen, und wie zufrieden sind Sie mit deren Umsetzung?

Angaben in Prozent. Dargestellt sind die Werte für „Esentiell wichtig" und „Sehr zufrieden / zufrieden". Basis: n = 337



12. Orts- und geräteunabhängiges Arbeiten ist noch nicht sehr weit verbreitet

In nur vier Prozent der Unternehmen ist weder das orts- noch das geräteunabhängige Arbeiten möglich respektive erlaubt. Freie Gerätewahl besteht indes nur in drei Prozent der Unternehmen, freie Wahl des Arbeitsorts immerhin bei 21 Prozent. Diese Formen des Arbeitens schlagen sich auch in den Security-Strategien nieder.

Das orts- und / oder geräteunabhängige Arbeiten sollte in der Security-Strategie eines Unternehmens Berücksichtigung finden. Bei den befragten Organisationen ist dies auch der Fall, jedoch nicht durchgehend. So haben nur 47 Prozent das mobile Arbeiten und die Arbeit im Homeoffice in der Security berücksichtigt, obwohl dies durch die Corona-Pandemie deutlich an Bedeutung gewonnen hat und zum „New Normal" gerechnet wird.

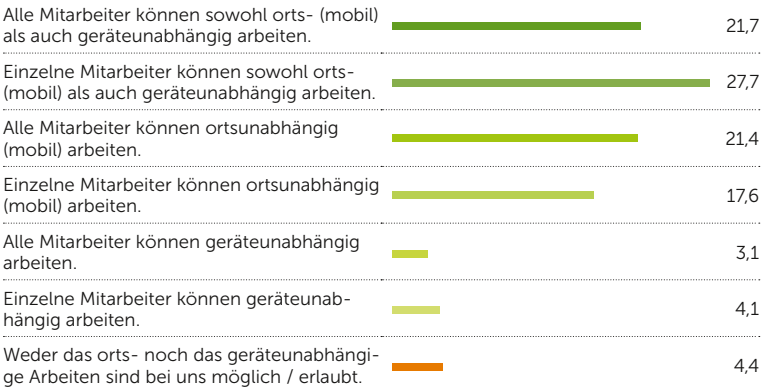
BYOD (Bring Your Own Device) hat bei 37 Prozent Folgen für die Cyber-Security-Konzeption. An die Folgen für den Datenschutz denken rund 20 Prozent der Unternehmen – dabei ist das orts- und geräteunabhängige Arbeiten meist mit Cloud Computing verbunden, mit deutlichen Folgen für den Datenschutz nach Datenschutz-Grundverordnung (DSGVO).

Zwar meinen nur sechs Prozent, dass sie das orts- und geräteunabhängige Arbeiten gar nicht in ihrer Security-Strategie berücksichtigen. Wichtig ist aber auch, an das ganze Spektrum der Folgen für die Security zu denken, nicht nur an einzelne Teile.

Immerhin haben 54 Prozent der befragten Unternehmen sowohl gute als auch schlechte Erfahrungen mit dem orts- und geräteunabhängige Arbeiten der Beschäftigten gemacht. 70 Prozent der Fachbereiche bestätigen dies, die befragten C-Level-Vertreter hingegen berichten dies nur in 51 Prozent der Fälle, scheinen also bisher nicht alle Konsequenzen für die Security wahrgenommen zu haben.

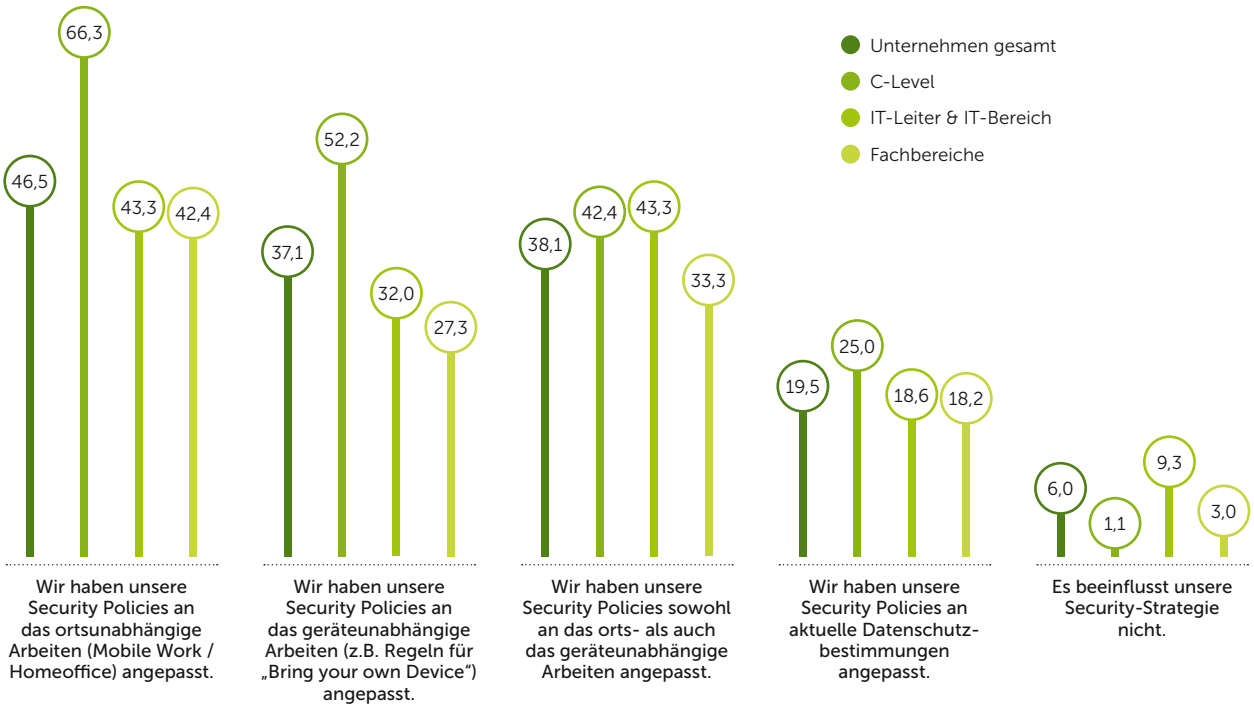
Inwiefern ist in Ihrem Unternehmen das orts- und geräteunabhängige Arbeiten möglich / erlaubt?

Angaben in Prozent. Basis: n = 318



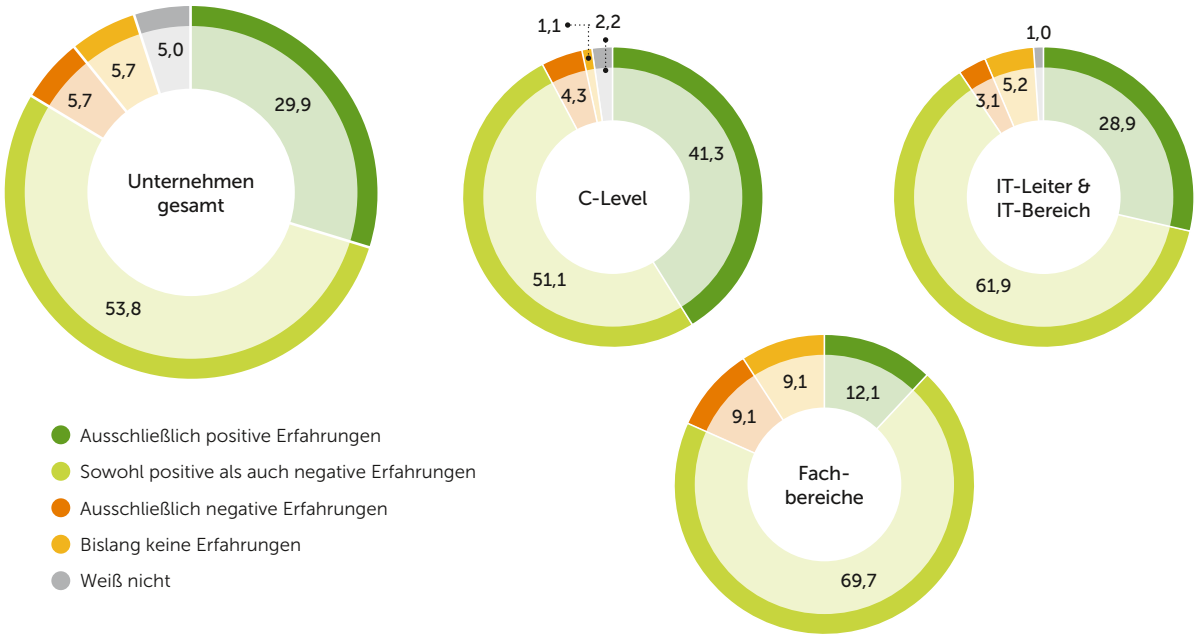
Inwiefern beeinflusst das orts- und / oder geräteunabhängige Arbeiten die Security-Strategie Ihres Unternehmens?

Mehrfachnennungen möglich. Angaben in Prozent. Basis: n = 318



Welche Art von Erfahrungen hat Ihr Unternehmen in Bezug auf seine IT-Sicherheit mit dem orts- und geräteunabhängigen Arbeiten gemacht?

Angaben in Prozent. Basis: n = 318



13. Über die Hälfte der Unternehmen setzt Security Policies zentral durch

Eine zentrale Durchsetzung von Security Policies wird von vielen Security-Experten empfohlen. Die befragten Unternehmen tun dies, allerdings 42 Prozent im Unternehmensnetzwerk und nur 17 Prozent in der Cloud. Dezentral pro Unternehmensstandort setzen nur zehn Prozent der Unternehmen ihre Sicherheitsrichtlinien um. Mit Blick aufs Homeoffice kann dies zum Problem werden.

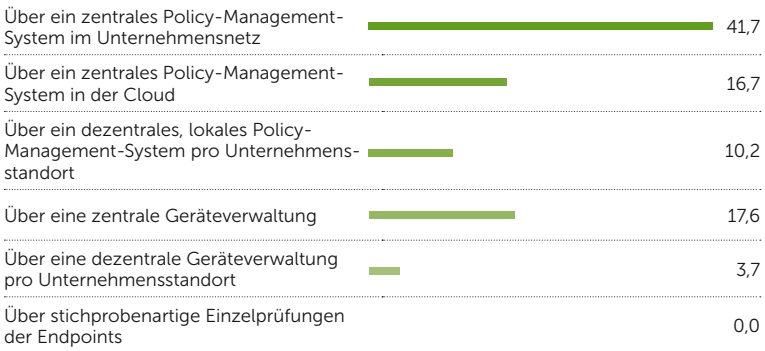
Sowohl das Policy-Management in der Cloud als auch die dezentrale Umsetzung der Durchsetzung von Sicherheitsrichtlinien kann auf das „New Normal" in Zeiten der Corona-Pandemie reagieren. Die meisten Unternehmen, die Sicherheitsrichtlinien über ein Policy-Management durchsetzen, machen dies aber netzwerkbasiert.

Mit den zahlreichen neuen Standorten, den Heimarbeitsplätzen, sollte hier eine Änderung erfolgen, hin zu Cloud-Lösungen im Bereich Policy-Management oder aber zu dezentralen Lösungen, die an den Standorten und damit auch im Homeoffice realisiert werden.

Positiv zu bewerten ist, dass sich kein befragtes Unternehmen darauf verlässt, nur Stichproben durch eine Einzelüberprüfung von Endpoints vorzunehmen. Trotzdem besteht ein dringender Handlungsbedarf im Bereich Policy-Management für Endgeräte, um das mobile und standortunabhängige Arbeiten besser zu berücksichtigen.

Wie setzen Sie definierte Sicherheitsrichtlinien auf den Endpoints in Ihrem Unternehmen durch?

Angaben in Prozent. Filter: Unternehmen, deren IT-Sicherheitsrichtlinien sich (auch) auf Endgeräte beziehen. Basis: n = 108



14. KI versus Security Analyst

Ist KI 300 Mal schneller als jeder Security Analyst? Die Teilnehmerinnen und Teilnehmer an der Studie sind in dieser Frage gespalten, wie die folgenden Statements zeigen. Offen sein für Neues, aber nicht einfach alles glauben – durchaus eine gute Basis, um neuen Security-Technologien zu begegnen.

Was würden Sie antworten, wenn Ihnen jemand sagen würde, dass KI 300 Mal schneller ist als jeder Security Analyst?

Blick in die Zukunft

Cyber Security 2020

Die Cyber Security leidet unter Inkonsistenzen und Missverständnissen

Cyber-Risiken werden als größtes Unternehmensrisiko wahrgenommen. Doch über die Methoden der Angreifer und die Folgen der Attacken herrscht weiter Unklarheit. Die Konsequenzen sind nicht aufeinander abgestimmte Security-Konzepte, verpasste Chancen in der Umsetzung der Security und gefährliche Lücken in der Erkennung und Abwehr von Cyber-Vorfällen.

Von Oliver Schonschek

Vier von sechs Unternehmen sehen in Cyber-Bedrohungen das größte Unternehmensrisiko. Daran haben auch die leidvollen Erfahrungen mit der Corona-Pandemie nichts geändert. Es scheint sogar so, als ob die Folgen der Pandemie, darunter die deutlich gestiegene Nutzung des Homeoffice, weniger im Fokus der Unternehmen stehen, als man wegen der zahlreichen Diskussionen in den Medien hätte erwarten können.

Was die befragten Unternehmen aber als eine der größten Herausforderungen für die Cyber Security sehen, ist die Sicherheit der Endgeräte. Man könnte nun denken, dies wird auch der Security im Homeoffice dienen, denn dort spielt der Einsatz von PCs, Notebooks, Tablets und Smartphones außerhalb des Firmennetzwerkes eine große Rolle.

Doch nur 77 Prozent der befragten Unternehmen haben eine Security-Strategie für Endpoints entwickelt. Der Brückenschlag hin zum Homeoffice gelingt dabei nur bei 71 Prozent, die ein entsprechendes Security-Konzept erstellt haben. Das im Homeoffice häufig anzutreffende BYOD (Bring Your Own Device) wird nur bei 61 Prozent der Unternehmen in einem IT-Sicherheitskonzept behandelt.

Hier zeigt sich beispielhaft, dass die Cyber-Sicherheit bei vielen Unternehmen nicht immer schlüssig und zu Ende gedacht erscheint. Ein möglicher Grund dafür kann in der Risikowahrnehmung gesehen werden, denn auch hier zeigen sich Unstimmigkeiten. So fürchten die Unternehmen besonders die Folgen von Ransomware und Identitätsdiebstahl, halten aber Angriffe von Industriespionen oder die Nachlässigkeit von Mitarbeitern für weniger bedrohlich. Dabei kann es genau bei solchen Vorfällen auch zum Diebstahl digitaler Identitäten oder zu erfolgreichen Ransomware-Angriffen kommen.

Missverständnisse gibt es auch im Bereich der Cloud-Sicherheit. So fürchten 27 Prozent einen Cloud-Ausfall, doch nur sechs Prozent sorgen sich wegen möglicher DDoS-Attacken auf ihre Cloud-Systeme. Dabei gehören DDoS-Angriffe auf Clouds zu den wesentlichen Gründen für einen Cloud-Ausfall.

Auch der Schutz privilegierter Zugänge scheint noch nicht den richtigen Stellenwert zu haben. Zwar werden externe Angriffe auf Zugangsdaten mit großer Sorge gesehen, die besonders interessanten Zugangsdaten der Administratoren jedoch erhalten bei 29 Prozent der Befragten keinen besonderen

Schutz, 41 Prozent verwenden nur die Bordmittel ihrer Fachapplikationen und nicht etwa spezielle Lösungen für PAM (Privileged Access Management).

Die Unklarheiten in den Bereichen Vorgehensweisen der Angreifer, Konsequenzen einer Nachlässigkeit bei Mitarbeitern und Folgen bestimmter Attacken für die IT schlägt sich im Investitionsverhalten der Unternehmen nieder. So wird die als besondere Herausforderung empfundene Endpoint Security nur von 20 Prozent der Unternehmen mit Investitionen in 2021 bedacht.

Ebenso planen 61 Prozent der Unternehmen Projekte zur Verschlüsselung der Daten, doch nur 46 Prozent denken an die dafür grundlegende Klassifizierung der Daten und nur 39 Prozent an eine Verbesserung, wie sich zu schützende Daten überhaupt auffinden lassen.

Trotzdem stehen die Zeichen auf eine weitere Verbesserung der Cyber-Sicherheit in den nächsten Jahren, allerdings sollten die Unternehmen über einige Vorbehalte nochmals nachdenken. Positiv zu sehen ist der hohe Zuspruch oder die bereits weite Verbreitung von Zero Trust, denn dieses Konzept wird auch in Zeiten von Homeoffice und Mobile Work eine wichtige Stütze der Cyber-Sicherheit sein. Nur sieben Prozent der Unternehmen planen kein Zero Trust oder haben es noch nicht eingeführt.

Die Offenheit für künstliche Intelligenz (KI) in der Cyber-Sicherheit ist einerseits positiv, denn KI kann bei der Security Automation helfen, die gerade im Bereich der Erkennung und Abwehr von Cyber-Bedrohungen noch besser werden muss. Die Unternehmen sehen auch durchaus die Grenzen der KI in der Security und betonen in zahlreichen Statements, KI müsse sich erst bewähren, man brauche weiterhin das menschliche Gehirn in der Security.

Doch die Konsequenz daraus, dass Security-Analysten trotz jeder KI noch weiterhin benötigt werden, ist offensichtlich nicht klar genug. Der bekannte, sich sogar noch ausweitende Fachkräftemangel in der Security wird bei vielen Unternehmen nicht zum Anlass genommen, offener für Security Outsourcing zu sein.

Nur 13 Prozent der Unternehmen sagen, dass das komplette oder teilweise Outsourcing der Cyber Security bei ihnen kein Tabuthema ist. 55 Prozent halten das Outsourcing indes für ein No-Go. Sollte es hier kein Umdenken geben, besteht die Gefahr, dass sich viele der genannten Lücken und Ungereimtheiten in den Security-Strategien weiter manifestieren.

Es wäre die Aufgabe der Security-Experten und -Dienstleister, auf diese Lücken aufmerksam zu machen, um die hohe Zahl der Cyber-Vorfälle besser in den Griff zu bekommen. Doch die Unternehmen müssen die Security-Dienstleister auch machen lassen, sprich sich auf eine vertrauensvolle Zusammenarbeit einlassen.

Nur mit der notwendigen Security-Expertise und mit Security-Technologien lassen sich die Angreifer schneller erkennen und besser abwehren. Geschieht dies nicht, muss mit weiter steigenden Zahlen von Cyber-Attacken gerechnet werden.

CIO-Agenda 2020

Daten zur allgemeinen Einschätzung der Marktlage

Exklusive Einblicke: Wie IT-Entscheider das Business in Gegenwart und Zukunft gestalten

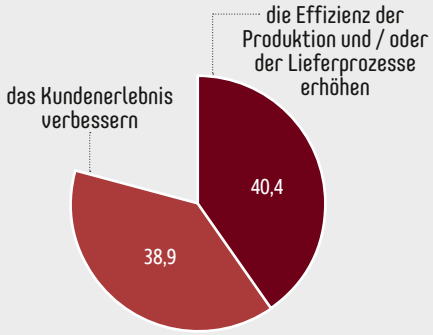
Cyber Security 2020

CIO-Agenda 2020

Alle Angaben in Prozent

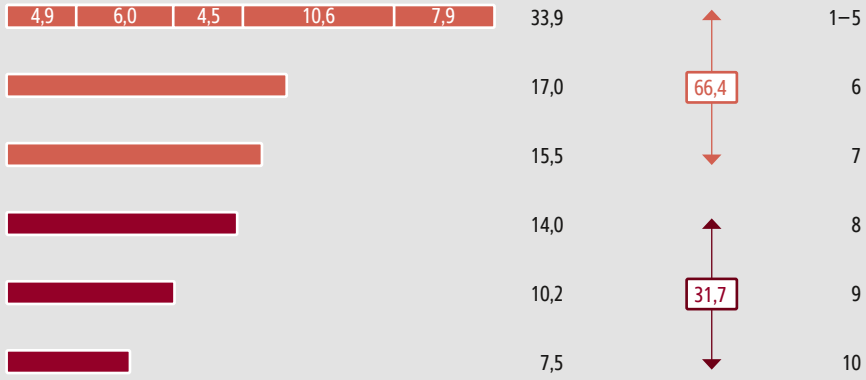
Alles dreht sich um effizientere Prozesse sowie um den Kunden.

Die wichtigsten Ziele, die die Unternehmen für die kommenden drei Jahre verfolgen, drehen sich um die **Verbesserung der Produktionseffizienz und der Lieferprozesse** (40,4 Prozent) und die **Verbesserung des Kundenerlebnisses** (38,9).



Die digitale Transformation ist in den Unternehmen angekommen.

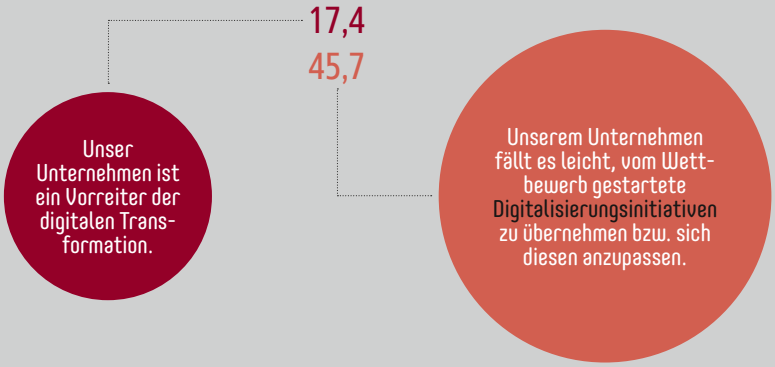
Mehr als 65 Prozent der befragten CIOs sehen sich und ihre Unternehmen bereits auf der zweiten Hälfte des Weges, **fast ein Drittel** der Befragten (31,7 Prozent) sogar auf dem letzten Viertel.



Darstellung in einer Wegstrecke von 1 bis 10

Pioniere und Fast Follower

Fast zwei Drittel der CIOs sehen sich als **Vorreiter** (17,4 Prozent) oder **Fast Follower** (45,7) für Digitalisierungsinitiativen.



Effizienter sein, Umsatz steigern, Kosten senken

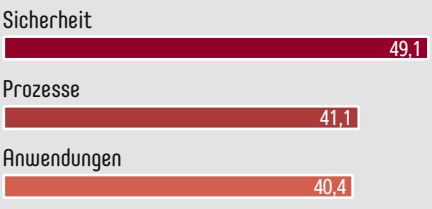
Keine Überraschung sind die Pläne der CIOs, was ihre geschäftlichen Prioritäten im Jahr 2020 angeht: **Operative Effizienz** (40,4 Prozent), **Umsatz- / Geschäftswachstum** (34,7) und die **Senkung der Betriebskosten** stehen ganz oben.

Bei den großen Budgets ist Security Trumpf.

Die substanziellsten Investments der kommenden drei Jahre wollen die CIOs im Bereich „Sicherheit" tätigen, auch Prozesse und Anwendungen stehen auf der Agenda.

Abfrage auf einer Skala von 1 (Starke Veränderung) bis 3 (Keine Veränderung)

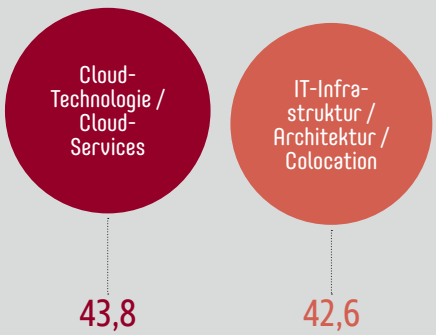
Substanzielles Investment



Auch Cloud und Infrastruktur treiben die Investments.

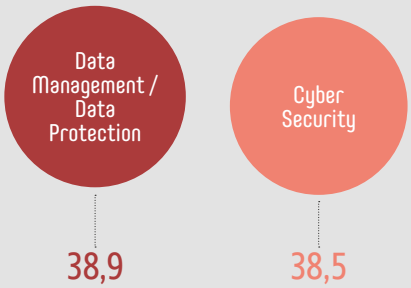
Vor allem in **Cloud-Technologie / Cloud-Services** (43,8 Prozent) und **IT-Infrastruktur / Architektur /Colocation** (42,6) sollen Gelder fließen.

(bis zu 3 Antworten möglich)



Data und Security inhaltlich am relevantesten

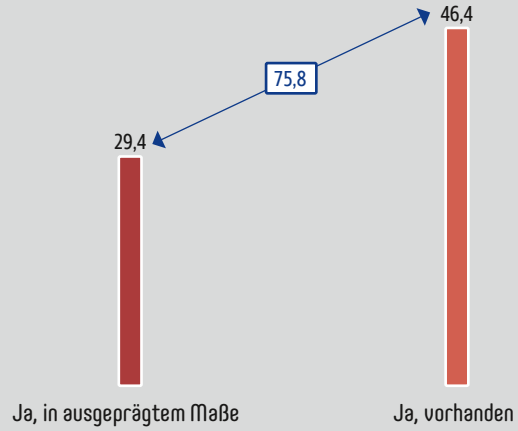
Abgesehen von reinen Investments betrachten die CIOs besonders die Themen **Data Management / Data Protection** (38,9) sowie **Cyber Security** (38,5) als wichtig und relevant für ihre mittelfristige IT-Strategie.



Ein Studienprojekt von IDG Research Services in Kooperation mit der WHU – Otto Beisheim School of Management und der Bechtle AG.

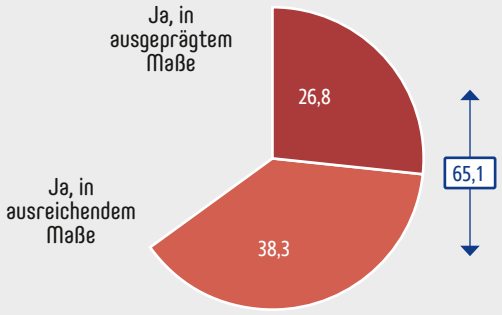
Digitalisierungsstrategie

Drei Viertel haben eine, besonders die großen Unternehmen mit mehr als 100 Mitarbeitern und mehr als einer Milliarde Euro Jahresumsatz.



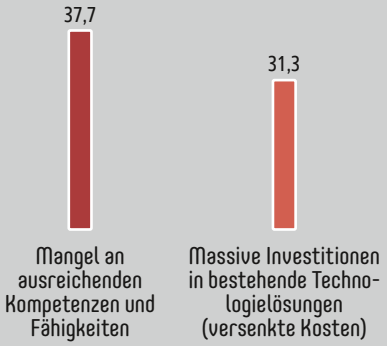
Entwicklung neuer digitaler Geschäftsmodelle

65 Prozent verfügen über grundlegende Prozesse und Strukturen dafür.



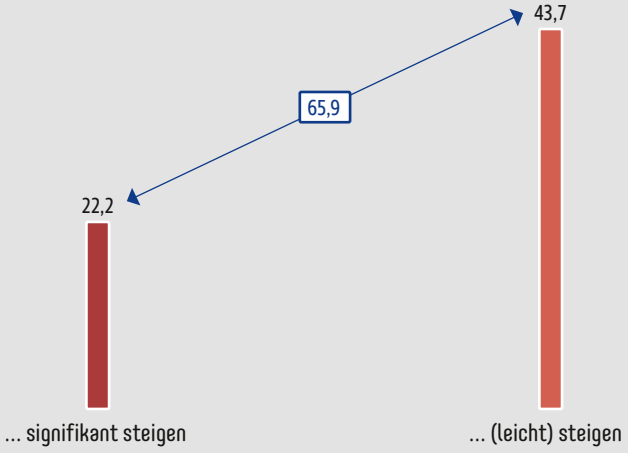
Es mangelt an Know-how und neuer Technik.

Fragt man nach Widerständen und Hindernissen, die die digitalen Ambitionen ihrer Unternehmen behindern, antworten 37,7 Prozent der CIOs zuerst mit dem **Mangel an ausreichenden Kompetenzen und Fähigkeiten**.



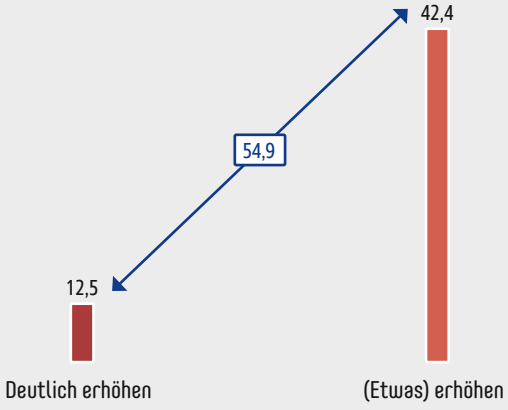
Steigende Investitionen in die digitale Zukunft

Das Gesamt-IT-Budget wird bei **66 Prozent** der Befragten (signifikant) steigen.



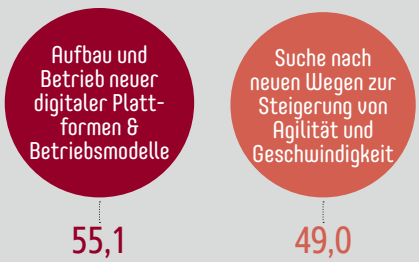
Mehr IT-Mitarbeiter für den Erfolg

Die Zahl der IT-Mitarbeiter soll in **mehr als der Hälfte der Unternehmen** (deutlich) erhöht werden. Interessant: Das gilt besonders für Unternehmen mit weniger als zehn Millionen Euro IT-Budget (47,7 Prozent).



CIO Agenda 2025 – neue digitale Plattformen und Betriebsmodelle stehen im Mittelpunkt.

Der Fokus des CIOs und des IT-Bereichs wird sich vor allem im **Aufbau und Betrieb neuer digitaler Plattformen und Betriebsmodelle** niederschlagen.



Grundgesamtheit:
Oberste (IT-)Verantwortliche von Unternehmen in der D-A-CH-Region: strategische (IT-)Entscheider im C-Level-Bereich und in den Fachbereichen (LoBs), IT-Entscheider & IT-Spezialisten aus dem IT-Bereich

Gesamtstichprobe:
265 abgeschlossene und qualifizierte Interviews

Untersuchungszeitraum:
14. November bis 18. Dezember 2019

Methode:
Online-Umfrage (CAWI)

Deutsche Unternehmen spielen Catenaccio

Digitalisierung in Deutschland: Die Mehrheit der Unternehmen verfolgt eine „Catenaccio-Strategie", die rein auf Effizienzsteigerung und Gefahrenabwehr ausgerichtet ist.

Von Prof. Dr. Dries Faems

Bis in die 1970er-Jahre wandten vor allem italienische Fußballteams den Catenaccio als taktisches System an, das den Schwerpunkt auf die Verteidigung legte, weltweit aber der Benchmark für das erfolgreiche Spiel war. Bis heute ist „Catenaccio" als Synonym im Fußball gebräuchlich – allerdings eher negativ besetzt – für eine destruktive Spielweise, die nur auf Verteidigung und knappe 1:0-Siege ausgelegt ist.

Die aktuelle Studie „CIO-Agenda 2020" von CIO, WHU – Otto Beisheim School of Management und Bechtle zeigt, dass der Catenaccio auch heute noch praktisch angewandt wird – in der Wirtschaft. Die Mehrheit der deutschen Unternehmen verfolgt nämlich eine Catenaccio-Strategie, die vor allem auf Effizienzsteigerung und Abwehr der Schattenseiten der Digitalisierung ausgerichtet ist. Für diese Unternehmen ist es eine Kernherausforderung, die notwendigen Kompetenzen zu finden, einen „digitalen Catenaccio" umzusetzen. Obwohl solch eine defensive Strategie sicherlich helfen kann, bestehende Produktionsprozesse und Angebote zu verbessern, ist es ebenso wichtig, digitale Innovationen zu entwickeln, um das langfristige Überleben und den Erfolg zu sichern.

Investitionen in die Verteidigung

Digitale Technologien verändern das Geschäftsleben grundlegend. Die Befragten der „CIO-Agenda 2020" sind sich einig, dass sich alle Geschäftsfunktionen durch die Digitalisierung in den kommenden drei Jahren verändern werden. So erwarten 82 Prozent der Befragten beispielsweise Veränderungen in der Personalfunktion, ähnliche Zahlen werden für Funktionen wie Vertrieb, Produktion, Finanzen und Forschung vermutet. Die Unternehmen sind sich auch bewusst, dass diese Veränderungen zusätzliche Investitionen in digitale Technologien erfordern werden. 66 Prozent der Befragten erwarten, dass das IT-Budget in den nächsten drei Jahren weiter steigen wird. 27 Prozent gehen davon aus, dass das Budget relativ stabil bleibt, während nur 7 Prozent mit einem Rückgang des IT-Budgets rechnen.

Im Catenaccio-Fußball konzentrieren sich die Teams vor allem auf den Aufbau einer gut organisierten und effektiven Backline-Verteidigung, die darauf ausgerichtet ist, gegnerische Angriffe auszuschalten und Torchancen zu verhindern. In ähnlicher Weise widmen deutsche Unternehmen dem Aufbau einer starken Abwehr gegen die Schattenseiten der Digitalisierung große Aufmerksamkeit. Auf die Frage nach den wichtigsten IT-Themen für ihr Unternehmen nennen die Befragten Datenschutz und Datensicherheit. Bei der Frage nach den obersten Digitalisierungszielen heben die Befragten zudem hervor, wie wichtig es ist, die bestehenden Produktions- und Lieferprozesse weiter zu verbessern und die Erfahrung der bestehenden Kunden zu optimieren. Mit anderen Worten: Die Unternehmen wollen mit ihren digitalen Investitionen vor allem das verteidigen und nach vorne bringen, was sie bereits haben.

Dieser Fokus auf die Verteidigung stimmt auch mit dem Selbstverständnis der meisten deutschen Unternehmen überein. 46 Prozent der Befragten kategorisieren sich als

Prof. Dr. Dries Faems
ist Inhaber des Lehrstuhls für Entrepreneurship, Innovation und Technologische Transformation an der WHU – Otto Beisheim School of Management

„erfolgreiche Digital Follower“ – das heißt, sie sind in der Lage, sich auf neue digitale Initiativen, die von anderen gestartet werden, einzustellen. Nur 17 Prozent sehen sich selbst als „digitale Vorreiter“, was bedeutet, dass sie selbst digitale Veränderungen initiieren. 25 Prozent der Befragten bezeichnen sich als „erfolglose Digital Follower“, die restlichen zwölf Prozent sehen sich als „digitale Nachzügler“.

Fehlende digitale Kompetenzen als zentraler Hemmschuh

Eine erfolgreiche Catenaccio-Fußballmannschaft lebt von Spielern, die Erfahrung und Kompetenzen mitbringen, diese Strategie umsetzen zu können. In ähnlicher Weise erfordert der Aufbau einer sicheren und effizienten digitalen Architektur nicht nur finanzielle Investitionen, sondern auch qualifizierte und erfahrene Mitarbeiter. Die Frage nach den Kernfaktoren, die Unternehmen bei der Realisierung ihrer digitalen Ambitionen behindern, wird von 38 Prozent der Befragten mit dem Mangel an Kompetenzen und Fähigkeiten beantwortet. Die Altlasten vergangener technologischer Investitionen (31 Prozent) und die mangelnde Veränderungsbereitschaft innerhalb der Organisation (29 Prozent) werden als weitere Hemmschuhe benannt, die die Fähigkeit der Unternehmen zur digitalen Transformation behindern.

Persönlicher Kommentar von Prof. Faems:

Die Ergebnisse der Studie „CIO-Agenda 2020“ zeigen: Die Mehrheit der Unternehmen hat erkannt, dass eine bessere Wettbewerbsposition im Markt nur über Investitionen in digitale Technologien möglich ist. Ich bewerte die Aufmerksamkeit für Themen wie Datenschutz und Datensicherheit ebenso positiv: Ich denke, wir sind an einem Wendepunkt angelangt, an dem Unternehmen es sich nicht mehr leisten können, naiv mit Themen wie Lösegeld, Cyber-Spionage und Datenschutz umzugehen. Die Tatsache, dass Entscheider diesen Themen Priorität einräumen, ist eine positive und wichtige Entwicklung.

Gleichzeitig würde ich mir aber wünschen, dass man sich nicht nur auf einen rein defensiven Ansatz beschränkt: Es genügt nicht, nur in digitale Technologien zu investieren, um bestehende Werte zu erhalten. Das wird den Unternehmen das langfristige Überleben nicht sichern. Wir stellen schon heute in verschiedenen Branchen Disruptionen durch digitale Technologien und alternative Geschäftsmodelle fest. In einem solchen Umfeld ist eine rein defensive Strategie wahrscheinlich nicht ausreichend. Es braucht einen proaktiveren Ansatz, bei dem Unternehmen neue technologische Möglichkeiten erforschen. Die gute Nachricht ist, dass sie sich im Gegensatz zum Fußball nicht nur auf ihre eigene Mannschaft verlassen müssen, um offensiver zu werden. Es ist möglich, mit externen Akteuren wie Start-ups zusammenzuarbeiten, um neben einer starken Verteidigung gegen digitale Bedrohungen eine ebenso offensivstarke Mannschaft zu entwickeln. Auf diese Weise lässt sich eine erfolgreiche Catenaccio-Strategie mit offensiveren Ansätzen kombinieren, um langfristig wettbewerbsfähig zu bleiben.

Hintergrund zur Studie

Die Studie „CIO-Agenda 2020“ wurde vom 14. November bis zum 18. Dezember 2019 von IDG Research Services (COMPUTERWOCHE / CIO) in Zusammenarbeit mit der WHU und der Bechtle AG durchgeführt. Es nahmen 265 CIOs, Geschäftsführer, Vorstände, C-Führungskräfte und Abteilungsleiter aus verschiedenen Unternehmensbereichen aller Branchen in Deutschland, Österreich und der Schweiz an der Online-Befragung teil.

Corona-Update

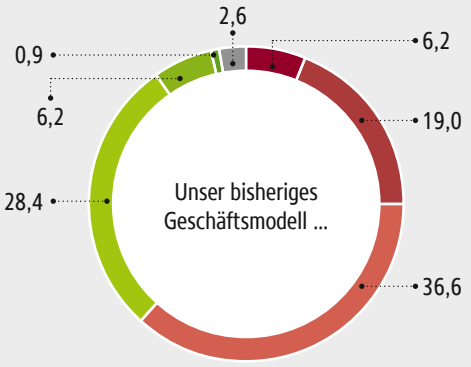
Alle Angaben in Prozent

Mehr als 60 Prozent der befragten Unternehmenslenker geben zu Protokoll, dass ihr Geschäftsmodell durch die Covid-19-Pandemie zumindest ein wenig negativ beeinflusst wird, ein weiteres Drittel kann indes keine Veränderungen zu vor der Krise feststellen.

Ob negativ beeinflusst oder nicht - reagiert wird dennoch allerorten: Mehr als vier von fünf Unternehmen haben ihr Geschäftsmodell aufgrund der Krise (leicht) angepasst. Der Zusammenhang mit dem Grad der eigenen Digitalisierung ist offensichtlich: Dieser ist seit dem Corona-Ausbruch in fast 70 Prozent der befragten Unternehmen gestiegen.

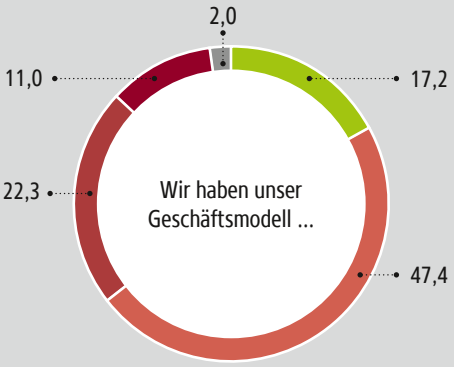
Was die Budgets angeht, wird vor allem in der IT gespart: Satte 40 Prozent der befragten Unternehmensentscheider geben zu Protokoll, dass die Situation rund um Covid-19 dort zu (starken) Kürzungen oder gar einem kompletten Budgetstopp geführt habe. Zur Wahrheit gehört aber auch, dass in jeweils rund einem Drittel der Unternehmen sowohl Investitions- als auch IT-Budgets zwischen Corona-Ausbruch im März und dem Zeitpunkt der Befragung Ende Juli unverändert geblieben sind.

Inwiefern beeinflusst die Covid-19-Pandemie das Geschäftsmodell Ihres Unternehmens?



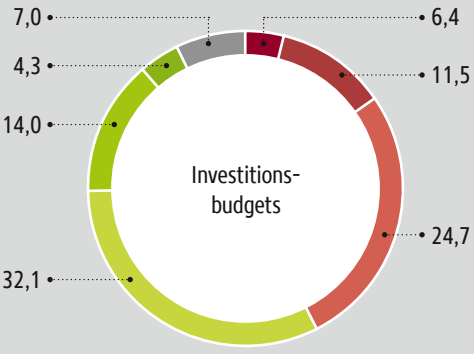
- ... wurde durch Covid-19 komplett ausgehebelt
- ... wurde durch Covid-19 zu großen Teilen ausgehebelt
- ... funktioniert noch, wurde aber durch Covid-19 negativ beeinflusst
- ... funktioniert noch wie vorher.
- ... funktioniert: Wir sind sogar leichter Krisengewinnler
- ... funktioniert: Wir sind sogar klarer Krisengewinnler
- Weiß nicht

In welchem Umfang haben Sie das Geschäftsmodell Ihres Unternehmens aufgrund der aktuellen Situation verändert?



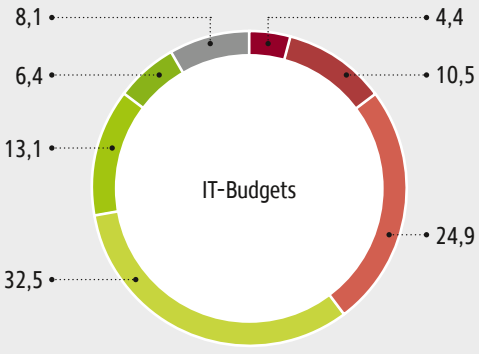
- ... nicht verändert
- ... nur wenig verändert
- ... verändert
- ... stark verändert
- Weiß nicht

Inwiefern hat sich die Situation um Covid-19 auf die Investitionsbudgets Ihres Unternehmens ausgewirkt?



- Es gab einen Investitionsstopp
- Die Investitionsbudgets wurden stark gekürzt
- Die Investitionsbudgets wurden etwas gekürzt
- Die Investitionsbudgets sind unverändert geblieben
- Die Investitionsbudgets wurden etwas erhöht
- Die Investitionsbudgets wurden stark erhöht
- Es gibt diesbezüglich noch immer keine Entscheidung / Lässt sich noch immer nicht abschätzen

Inwiefern hat sich die Situation um Covid-19 auf die IT-Budgets Ihres Unternehmens ausgewirkt?



- Es gab einen kompletten Budgetstopp
- Die IT-Budgets wurden stark gekürzt
- Die IT-Budgets wurden etwas gekürzt
- Die IT-Budgets sind unverändert geblieben
- Die IT-Budgets wurden etwas erhöht
- Die IT-Budgets wurden stark erhöht
- Es gibt diesbezüglich noch immer keine Entscheidung / Lässt sich noch immer nicht abschätzen

Studiensteckbrief „Corona-Update“:

Die Zahlen wurden vom 20. bis 28. Juli 2020 im Rahmen der Studie "Cyber Security 2020" erhoben. An der Online-Befragung nahmen 655 CIOs, Geschäftsführer, Vorstände, C-Führungskräfte und Abteilungsleiter aus verschiedenen Unternehmensbereichen aller Branchen in Deutschland, Österreich und der Schweiz teil. Die Umfrage wurde ganz überwiegend unter Unternehmen mit mehr als 100 Mitarbeitern durchgeführt.

Unsere Studienpartner stellen sich vor

Cyber Security 2020

MICROSOFT INITIATIVEN FÜR CYBER-SICHERHEIT

Um Unternehmen wie Privatanwender zu schützen, investiert Microsoft jährlich eine Milliarde Dollar in Cyber Security – insbesondere in die Bereiche Forschung und Entwicklung. Hierbei verfolgt Microsoft einen ganzheitlichen Ansatz, um Kunden umfassende Sicherheitslösungen zu bieten und zu ihren Anforderungen zu beraten. Microsofts Security-Initiativen umfassen sowohl Maßnahmen, die Hacker davon abhalten, ins Firmennetzwerk einzudringen (Pre-Breach), als auch Maßnahmen, die greifen, wenn der Einbruch ins Firmennetzwerk bereits erfolgt ist (Post-Breach).

Mehr als 3.500 Sicherheitsexperten im Cyber Defense Operations Center, in der Digital Crimes Unit und dem Microsoft Threat Intelligence Center sind täglich im Einsatz, um Kunden zu schützen. Microsoft setzt auf intelligente Technologien wie erweiterte KI, um 6,5 globale Signale hinsichtlich Gefahren auszuwerten, Bedrohungen zu erkennen und Maßnahmen zu ergreifen. Moderne Lösungen von Microsoft profitieren nachhaltig von diesen Erkenntnissen.

MICROSOFT DEUTSCHLAND GMBH

Die Microsoft Deutschland GmbH ist die 1983 gegründete Tochtergesellschaft der Microsoft Corporation / Redmond, USA., des weltweit führenden Herstellers von Standardsoftware, Services und Lösungen mit 125,8 Mrd. US-Dollar Umsatz (Geschäftsjahr 2019; 30. Juni 2019). Der Nettogewinn im Fiskaljahr 2019 betrug 36,8 Mrd. US-Dollar.

Neben der Firmenzentrale in München-Schwabing ist die Microsoft Deutschland GmbH bundesweit mit sechs Regionalbüros vertreten und beschäftigt rund 2.700 Mitarbeiterinnen und Mitarbeiter. Im Verbund mit rund 30.000 Partnerunternehmen betreut sie Firmen aller Branchen und Größen.

Darauf aufbauend bietet Microsoft Unternehmen einen ganzheitlichen Ansatz für professionelle und höchste Sicherheit auf dem Stand der Technik. Microsoft Secure bietet Firmenkunden Sicherheitsmaßnahmen, Technologien und Partnerschaften, um sich in der komplexen digitalen Welt zu behaupten. Die Microsoft-Security-Lösungen sind integrierter Bestandteil von beispielsweise Microsoft 365 und Azure, bieten aber auch Schutz für Drittanbietergeräte, Betriebssysteme und Cloud-Dienste.

VIER SÄULEN FÜR DIE UMSETZUNG EINES ZERO TRUST MODELLS IM DIGITALEN ZEITALTER

Werkzeuge für Identitäts- und Zugriffsverwaltung ermöglichen es Kunden, die Identitäten ihrer Nutzer zu schützen und den Zugang zu wichtigen Ressourcen je nach Risikoniveau durch bedingten Zugriff zu kontrollieren. Stichwort „Bring Your Own Device" (BYOD): Mitarbeiter erwarten, mit verschiedensten Geräten – ob firmeneigene oder private – auf wichtige Geschäftsdaten und -Tools zugreifen zu können, die sie für produktives Arbeiten benötigen. Hierfür stellt Microsoft umfangreiche Lösungen zur Verfügung, die den Schritt in Richtung Multi-Faktor-Authentifizierung (MFA) erleichtern sollen: So ersetzt beispielsweise die App Microsoft Authenticator unsichere Logins mit Passwörtern durch PIN, sowie biometrische Merkmale wie den Fingerabdruck und erhöht neben der Sicherheit auch den Benutzerkomfort. Komplizierte Passwörter gehören damit

schon bald der Vergangenheit an. Weitere Lösungen zum Identitätsschutz umfassen Angebote wie Azure Active Directory, Multi-Faktor-Authentifizierung (MFA), biometrische Authentifizierung via Windows Hello sowie Microsoft Defender Credential Guard.

Lösungen für den Informationsschutz unterstützen Firmen dabei, sensible Daten sowohl On-Premises als auch in der Cloud zu klassifizieren und zu schützen. Umständliche Einschränkungen auf mobilen Geräten, für Anwendungen sowie beim Remote-Zugriff können die IT-Abteilung belasten und zugleich die Geduld der Mitarbeiter auf eine harte Probe stellen. Benutzer erwarten, dass sie Informationen und Dateien praktisch überall erstellen, auf diese zugreifen und mit anderen Anwendern austauschen können. Doch zugleich muss die IT dafür sorgen, dass diese Aktionen auf sichere und geschützte Weise erfolgen. Microsoft bietet Sicherheitslösungen, mit denen Anwender ihre Dokumente einfach ausfindig machen, klassifizieren, nachverfolgen und schützen können, um versehentliche Datenlecks oder den Zugriff durch unautorisierte Nutzer zu verhindern. Konkrete Angebote umfassen hierbei unter anderem Azure Information Protection, Office 365 Data Loss Prevention, Windows Information Protection, Lösungen für sichere Cloud-Dienste sowie Microsoft Intune.

Intelligente Funktionen für den Schutz vor Bedrohungen liefern das Rüstzeug, um den präventiven Schutz für E-Mail- und Kollaborations-Dienste zu stärken sowie Endpunkte durch Maßnahmen abzusichern, die direkt in die jeweilige Hardware eingebettet sind. Zudem kann die Unternehmens-IT die Detektion von Schädlingen nach einem erfolgten Angriff durch intelligente Tools optimieren, einschließlich Memory- und Kernel-Schutz, und Reaktionen mithilfe von automatisierten Prozessen einleiten. Selbst der vorsichtigste Anwender kann unwissentlich eine infizierte Datei öffnen oder auf einen schädlichen Link klicken. Um sich vor versehentlichen Verletzungen zu schützen, müssen Firmen sämtliche Angriffsvektoren absichern und Richtlinien etablieren, mit denen potenziell schädliche Aktivitäten erkannt, verfolgt und darauf reagiert werden kann. Hierfür bietet Microsoft eine große Auswahl an intelligenten Tools aus der Cloud für die wichtigsten Anwendungs- und Produktbereiche – beispielsweise Azure Advanced Threat Protection (ATP), Microsoft Defender ATP oder auch Office 365 ATP. Diese wehren nicht nur Bedrohungen ab, sondern unterstützen im Fall eines Angriffs auch eine rasche Wiederherstellung. Und auch hier sprechen wieder die Vorteile für die Cloud: Künstliche Intelligenz, Machine Learning und Big Data sind heutzutage unverzichtbar, wenn es um intelligenten Schutz geht.

Tools für das Sicherheitsmanagement bieten hohe Transparenz sowie Kontrolle über eingesetzte Sicherheitslösungen und praktische Anleitungen, um beispielsweise Firmenrichtlinien zentral zu verwalten. Klar ist, das IT-Personal kann das Management moderner Sicherheitsfunktionen nicht mehr allein schaffen: Um ein umfassendes Sicherheitskonzept umsetzen und immer wieder an neue Anforderungen anpassen zu können, braucht die Firmen-IT Unterstützung über intelligente Tools. Microsoft-Sicherheitslösungen bieten integrierte Werkzeuge, mit denen Firmen die Compliance wahren, Schatten-IT sowie neue Bedrohungen automatisiert aufspüren und individuelle Richtlinien definieren können. Über zentralisierte Sicherheitslösungen kann sich die IT ein umfassendes Bild von der Sicherheitssituation im gesamten Unternehmen machen. Wichtige Angebote von Microsoft in diesem Bereich sind das Azure Security Center, Office 365 Security Center oder Microsoft Defender Security Center.

Für weitere Informationen hier klicken.

Microsoft

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München
Deutschland
Telefon: +49 89 31 76 0
Fax: +49 89 31 76 1000

Cisco Secure

Cisco (NASDAQ: CSCO) hilft als weltweit führender IT-Anbieter Unternehmen dabei, schon heute die Geschäftschancen von morgen zu nutzen. Durch die Vernetzung von Menschen, Prozessen, Daten und Dingen entstehen unvergleichliche Möglichkeiten. Unternehmen können damit Prozesse optimieren, Ressourcen effizienter nutzen und sich so Vorteile gegenüber Wettbewerbern verschaffen.

CISCO IN DEUTSCHLAND

Im Rahmen der Initiative „Deutschland Digital" investiert Cisco gezielt in die Beschleunigung der Digitalisierung in Deutschland – insbesondere in den drei Schwerpunkten Innovation, Cyber-Sicherheit und Bildung. Die Investitionen umfassen Anschubfinanzierungen für konkrete Digitalisierungsprojekte, Forschungsgelder, den Ausbau des Cisco-Networking-Academy-Programms, direkte Investitionen in einen Venture Fund sowie zusätzliche Personal- und Infrastrukturausgaben.

In Deutschland unterhält Cisco Standorte in Garching bei München, Berlin, Bonn, Düsseldorf, Eschborn, Hamburg, Mannheim und Stuttgart. Seit 2019 ist Uwe Peter Vice President und Vorsitzender der Geschäftsführung von Cisco Deutschland. Das Unternehmen setzt auf den indirekten Vertrieb über rund 2.200 zertifizierte Partner in Deutschland.

Das Unternehmen entwickelt und vertreibt Produkte auf Basis des IP-Protokolls in den Bereichen Security, Core Networking, Video und Collaboration, Access (Wired und Mobile), Unified Datacenter und Services. Dabei konzentriert sich das Unternehmen auf die Marktsegmente Enterprise (Großunternehmen, kleine und mittelständische Unternehmen sowie die öffentliche Hand) und Service-Provider.

UMFASSENDE SICHERHEIT

Cisco ist ein seit Jahrzehnten erfolgreicher Anbieter und Experte für integrierte IT-Security-Lösungen. Im Jahr 2018 blockierte Cisco weltweit 20 Milliarden Cyber-Bedrohungen – pro Tag. Dabei baut es auf eine umfangreiche Erfahrung mit internen Netzwerken auf. Denn jeden Tag schützt Cisco 122.000 interne und externe Mitarbeiter, das eigene Netzwerk mit mehr als 40.000 Routern, 26.000 Büroanbindungen, 2.500 IT-Anwendungen, 1.350 Testlaboren sowie 500 Cloud-Anwendungen in 170 Ländern. Der ganzheitliche Security-Ansatz basiert auf drei Bereichen:

Das Security & Trust Office (STO) Deutschland ist Teil der weltweiten Security & Trust Organization, in der mehr als 650 Mitarbeiter tätig sind. Es unterstreicht Ciscos kontinuierliches Engagement für mehr Cyber-Sicherheit. Das STO Deutschland dient als zentrale Kontaktstelle für Kunden zur Klärung strategischer

Anforderungen bei Cyber Security, Datenschutz oder Datensicherheit. Zusätzlich unterstützt es die Cisco Networking Academy dabei, Training und Schulungsmaterial zum Thema Cyber Security zu entwickeln.

Das Intuitive Network lässt die Vision eines Netzes, das Aktionen vorhersieht und automatisiert, Sicherheitsgefahren abwehrt und sich durch Lernprozesse selbstständig weiterentwickelt, wahr werden. Das neue Netz baut auf der Cisco Digital Network Architecture (DNA) auf und bietet Software und Hardware mit neuen Technologien und Services. Damit verändert Cisco die Basis für Netzwerke von einem hardwarezentrierten zu einem softwaregetriebenen Ansatz. So profitieren Kunden von deutlich höherer Sicherheit, Agilität, Produktivität und Performance.

Die Cisco Talos Intelligence Group ist eines der weltweit größten kommerziellen Teams für Bedrohungsanalyse mit erstklassigen Forschern, Analysten und Entwicklern. Es wird durch führende Telemetrie und intelligente Systeme unterstützt, um genaue, schnelle und umsetzbare sicherheitsbezogene Informationen für Kunden, Produkte und Dienstleistungen von Cisco zu erstellen. Talos schützt sie vor bekannten und neuen Bedrohungen und entdeckt neue Schwachstellen in gängiger Software.

CISCO IN ZAHLEN

Im Geschäftsjahr 2018 erzielte Cisco einen Umsatz von 49,3 Milliarden US-Dollar mit mehr als 70.000 MitarbeiterInnen (Stand: Juli 2018) weltweit. CEO ist Chuck Robbins. Die Geschäftstätigkeiten von Cisco sind in die Regionen Americas, EMEAR (Europa, Naher Osten, Afrika und Russland) und Asia Pacific / Japan / Großchina gegliedert.

PRESSEKONTAKT:

Lars Gurow,
PR Manager Deutschland

Kurfürstendamm 22
10719 Berlin

Telefon: 030-9789-2203
Mobil: 0172-3898713
E-Mail: Lgurow@cisco.com

EINFACH UND SOFORT VERFÜGBAR

„Cloud-basierte Endpoint Security nach dem Zero-Trust-Modell“

DriveLock ist mit seinen Endpoint-Security-Lösungen seit über 15 Jahren erfolgreich. Das Münchner Unternehmen ist einer der international führenden Spezialisten für IT- und Datensicherheit.

„Die Digitalisierung und der exponentielle Anstieg von Schadsoftware und Cyber-Angriffen machen Unternehmen verwundbar. Speziell in der Pandemie mit mehr Online-Aktivität, -Kommunikation und Nutzung von IT-Systemen von zu Hause aus, müssen Unternehmen den Endgeräteschutz noch ernster nehmen und konsequent umsetzen.“

ANTON KREUZER, CEO, DriveLock SE

Herr Kreuzer, was zeichnet DriveLock aus?

Anton Kreuzer: „Die Digitalisierung lässt Unternehmensgrenzen schmelzen. In der Vergangenheit wurde der Schutz gegen Angriffe von außen maximiert. Heute müssen Unternehmen davon ausgehen, dass sie jederzeit und überall kompromittiert werden können. Damit wird die IT-Landschaft komplexer. Traditionelle Sicherheitsmaßnahmen wie Antivirus und Firewall reichen nicht mehr.

Unser Produktportfolio entwickelt sich dynamisch, und das ist auch nötig bei stetig wachsenden und sich verändernden Cyber-Risiken.

Mit unserer Zero-Trust-Plattform bieten wir mehrere Schutzmechanismen und eine Kombination von Security Tools: von der Verschlüsselung über Applikations- und Device-Kontrolle hin zu Detection & Response.”

Wie beherzigen Sie den Zero-Trust-Ansatz konkret in Ihrer Produktstrategie?

Anton Kreuzer: „Die DriveLock-Zero-Trust-Plattform hat in den vergangenen Monaten viele neue Funktionen und Features bekommen. Wir orientieren unser Produktportfolio an den vier Schritten auf dem Weg zu mehr IT-Sicherheit nach dem Zero-Trust-Modell: Discover, Prevent, Detect und Respond.

Zu allen Steps bieten wir Lösungen:
von Schwachstellenanalyse, Ermittlung der Security-Situation, klassischen Präventionswerkzeugen wie Verschlüsselung und Applikationskontrolle bis zu forensischen Detection-Werkzeugen und automatischer Reaktion auf schädliche Angriffe.”

Das deutsche Unternehmen DriveLock SE wurde 1999 gegründet und gehört zu den international führenden Spezialisten für IT- und Datensicherheit mit Niederlassungen in Deutschland, Frankreich, Australien, Singapur, Middle East und USA.

Schutz von Daten, Geräten und Systemen in Unternehmen

In Zeiten der digitalen Transformation hängt der Erfolg von Unternehmen maßgeblich davon ab, wie zuverlässig Menschen, Unternehmen und Dienste vor Cyber-Angriffen und vor dem Verlust wertvoller Daten geschützt sind.

DriveLock hat sich zum Ziel gesetzt, Unternehmensdaten, -geräte und -systeme zu schützen. Hierfür setzt das Unternehmen auf neueste Technologien, erfahrene Security-Experten und Lösungen nach dem Zero-Trust-Modell.

Zero Trust bedeutet in heutigen Sicherheitsarchitekturen einen Paradigmenwechsel nach der Maxime „Never trust, always verify". So können auch in modernen Geschäftsmodellen Daten zuverlässig geschützt werden.

Die DriveLock-Zero-Trust-Plattform

Die DriveLock-Zero-Trust-Plattform ist entlang der einzelnen Schritte Discover, Prevent, Detect und Respond für effektive IT-Sicherheit nach Zero Trust aufgebaut. Sie vereint die Elemente:

- Data Protection
- Endpoint Protection
- Endpoint Detection & Response
- Identity & Access Management

Die Lösung ist made in Germany und „ohne Backdoor":

- Mehrere Millionen verwaltete Endgeräte in 30 verschiedenen Ländern
- Kundenumgebungen mit über 180.000 verwalteten Endgeräten
- Made in Germany: Entwicklung und technischer Support aus Deutschland

DriveLock

DriveLock SE
Landsberger Straße 396, 81241 München
Telefon: +49 (89) 546 36 49-0
E-Mail: info@drivelock.com
www.drivelock.de

MIT F-SECURE ANGRIFFE ZUVERLÄSSIG ABWEHREN

WIE MAN GEZIELTE CYBER-ATTACKEN ERKENNT

Gegründet im Jahr 1988 ist F-Secure der Spezialist für Cyber Security und dabei ein rein europäisches Unternehmen – Fachleute wissen, was das bedeutet. F-Secure erfüllt alle IT-Sicherheitsanforderungen Ihres Unternehmens; vom branchenbesten Endgeräteschutz über ausgeklügelte Cyber-Sicherheitsstrategien bis hin zu ultraschnellen Reaktionen auf Vorfälle.

Wir alle wissen es: Die Bedrohungslandschaft entwickelt sich rasend schnell weiter. Doch die hochentwickelte Technologie von F-Secure kombiniert die Leistungsfähigkeit maschinellen Lernens mit menschlichem Know-how, um so Ihr Unternehmen und seine Daten umfassend und optimal zu schützen. Und dabei erwies sich F-Secure als der im Wettbewerbsvergleich beste Anbieter: Allein von AV-TEST bekamen sie bereits zu sechsten Mal den »Best Protection Award« verliehen – nur eine unter vielen anderen Auszeichnungen und Referenzen.

Heutzutage ist die Absicherung Ihrer Unternehmensressourcen in der Cloud unverzichtbar. Die richtungsweisenden Schutzlösungen von F-Secure bieten Ihnen ein Höchstmaß an Sicherheit und Kontrolle über Ihr Netzwerk, Ihre E-Mail-Anwendungen und die Software von Drittanbietern.

Zu diesem Gesamtpaket gehört auch das Schwachstellen-Management – ein wichtiger Bestandteil der IT-Risikoanalyse. Die Lösungen von F-Secure für das Schwachstellen-Scanning und -Management helfen Unternehmen, ihre Transparenz von IT-Ressourcen und ihren Sicherheitsstatus zu gewährleisten sowie geltende Vorschriften – wie PCI und DSGVO – einzuhalten.

TRÜGERISCHE SICHERHEIT

Und dieses Gesamtpaket ist meist auch dringend nötig. Denn den IT-Sicherheitsspezialisten in Unternehmen stehen zwar

allerlei Abwehrmechanismen gegen Cyber-Attacken zur Verfügung – von Firewalls bis hin zur klassischen Endpoint Protection. Dieser Schutz wird gerne als Rundum-Schutz betrachtet, der kaum Lücken für erfolgreiche Attacken lässt. Jedoch gibt dies den Unternehmen ein falsches Gefühl von Sicherheit – wie die bedrohliche Realität zeigt.
Gezielte Attacken umgehen nämlich die präventiven Sicherheitsmaßnahmen. Es dauert im Schnitt ganze 69 Tage, bis ein Sicherheitsvorfall überhaupt entdeckt wird. Fortschrittliche Angreifer wissen ganz genau, wie sie die präventiven Sicherheitsebenen umgehen und sich unbemerkt im Unternehmensnetzwerk bewegen können. Solche Attacken können nur durch eine Verhaltensanalyse erkannt werden.
Und genau hier kommt EDR ins Spiel – Endpoint Detection & Response. Der Einsatz einer EDR-Lösung ist der schnellste Weg, Möglichkeiten zur Erkennung sowie Reaktionen auf fortschrittliche und gezielte Attacken zu etablieren.

DIE LÖSUNG: ENDPOINT DETECTION & RESPONSE

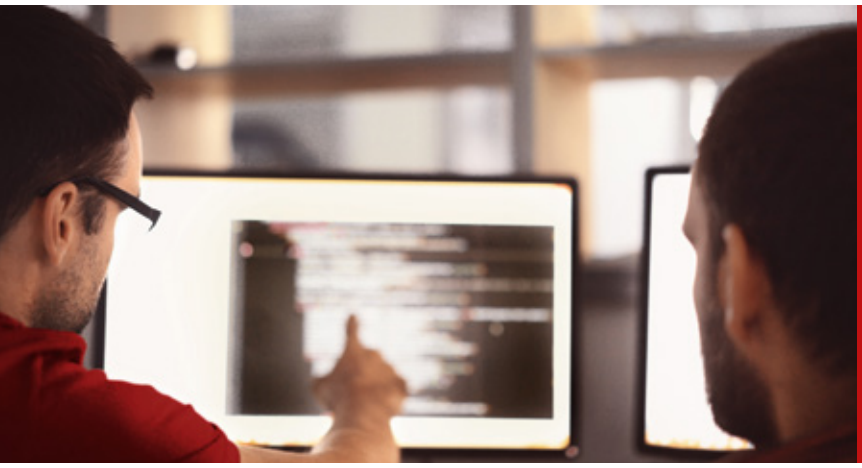
Die Sicherheit für Endpunkte steht bei der Cyber Security an erster Stelle. Die preisgekrönten Lösungen von F-Secure nutzen modernste Technologie, heuristische Analysen und hochentwickelte Lern-Algorithmen, um all Ihre Geräte umfassend abzusichern.
Das Thema EDR stand lange Zeit nur bei großen Unternehmen mit einem besonders ausgeprägten Sicherheitsbedürfnis auf der Agenda. Das hat sich drastisch geändert – inzwischen haben auch kleine und mittelständische Unternehmen die Bedeutung von EDR erkannt. Der Hintergrund: Früher waren es fast ausschließlich die von Regierungen oder Behörden finanzierten Bedrohungsakteure, die anspruchsvolle und zielgerichtete Cyber-Attacken auf andere Nationen oder Großkonzerne durchführen konnten. Seit geraumer Zeit stehen diese ausgefeilten Techniken aber auch den durchschnittlichen Cyber-Kriminellen zur Verfügung – und geben ihnen nun die Möglichkeit, komplexe Angriffe gegen Unternehmen jeglicher Größe zu fahren. Diese Angriffe werden immer zielgerichteter und anspruchsvoller. Die Abwehr dagegen muss entsprechend standhalten.
EDR-Lösungen haben eine hohe Verfügbarkeit, sind im Vergleich zu einem eigenen SOC (Security Operations Center) deutlich günstiger und dabei auch noch leicht zu implementieren. Während bei einem SOC mit In-house-Lösung das erforderliche Know-how erst aufgebaut werden muss, »kauft« sich das Unternehmen mit EDR nicht nur eine rein technische Lösung, sondern zusätzlich auch noch ein ganzes Team von hochqualifizierten Sicherheitsfachleuten.

MENSCH UND MASCHINE – DIE PERFEKTE ABWEHR

Die EDR-Lösung RDR (Rapid Detection & Response) von F-Secure bietet 24/7-Dienste zur Bedrohungsüberwachung, Erkennung und Reaktion an. Hierbei werden Sensoren eingesetzt, um Metadaten von den Systemen eines Unternehmens zu sammeln. Machine Learning analysiert dann diese Metadaten auf Anzeichen von Kompromissen hin.
Ein konkretes Beispiel: In einem mittelgroßen Unternehmen mit etwa 650 Sensoren gibt es jeden Monat über eine Milliarde Alarme, doch nur etwa zehn dieser Vorfälle müssen aktiv von Abwehr-Experten angegangen werden. Die menschliche Expertise ist also nach wie vor unverzichtbar; in Kombination mit den RDR-Lösungen von F-Secure ist sie unschlagbar.

F-Secure

F-Secure GmbH
Kistlerhofstr. 172c
81379 München
+49-89-787467-0
www.f-secure.com



„Kriminelle arbeiten äußerst professionell zusammen. Ich denke, dass der offene und gemeinsame Ansatz von McAfee genau die richtige Sicherheit für unsere Seite liefert."

PETER NEUHAUSER
Leiter des CERT, Bundesagentur für Arbeit

ANWENDERBERICHT

MEHRSTUFIGER SCHUTZ STÄRKT SICHERHEITSLAGE EINER BUNDESBEHÖRDE

Die Bundesagentur für Arbeit vereinfacht die Sicherheitsverwaltung und stärkt den Schutz dank der integrierten Sicherheitsplattform von McAfee.

Durch die Einführung einer integrierten Sicherheitsinfrastruktur, die McAfee Endpoint Security, McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense sowie McAfee SIEM-Lösungen umfasst, konnte die Bundesagentur für Arbeit einen mehrstufigen Schutz einrichten, der die Zeitspanne bis zur Bedrohungseindämmung verkürzt und die allgemeine Sicherheitslage verbessert.

KUNDENPROFIL

Bundesbehörde, die für Entgeltersatzleistungen, Arbeitsvermittlung und andere arbeitsmarktbezogene Aufgaben verantwortlich ist

Herausforderungen

- Zuverlässiger Schutz vor raffinierten Angriffen, einschließlich Ransomware und hochentwickelter Malware
- Verringerung des Verwaltungsaufwands für den Schutz der Infrastruktur und der 160.000 Endgeräte
- Einhaltung des ISO-27001-Standards und der gesetzlichen Vorschriften für kritische Infrastrukturen

Seit mehr als 20 Jahren setzt die Bundesagentur für Arbeit McAfee-Lösungen ein, angefangen mit dem McAfee-Virenschutz. Die Lösungen bieten kontinuierlich zuverlässigen Schutz und halten mit der sich ändernden Bedrohungslandschaft sowie der zunehmenden Zahl und Raffinesse Schritt.

VEREINFACHTE SICHERHEITSVERWALTUNG BEI WENIGER AUFWAND

Die zentrale Verwaltungskonsole McAfee ePolicy Orchestrator (McAfee ePO) hat sich bei der Verwaltung und dem Schutz der zahlreichen Endgeräte als unverzichtbar erwiesen. Das Team verwendet die McAfee ePO-Software zur Verwaltung verschiedenster Sicherheitsprodukte für die gesamte physische und virtuelle Infrastruktur. Mithilfe des anpassbaren Dashboards behält das operative Team den Überblick über eine Vielzahl von Endgeräten und kann diese hierüber entsprechend verwalten und schützen.

„Durch die Vernetzung von McAfee Endpoint Security, McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense erhalten wir unverzichtbaren, mehrstufigen Schutz vor Zero-Day-Angriffen. Dank der Echtzeit-Informationen aus der Cloud in Kombination mit dem bidirektionalen Bedrohungsdatenaustausch über DXL können wir Malware bereits bei ‚Patient Null' stoppen."

PETER NEUHAUSER
Leiter des CERT, Bundesagentur für Arbeit

Darüber hinaus konnten viele kritische Prozesse automatisiert werden, so dass sich das Team darauf konzentrieren kann, die Automatisierung zu verbessern und im Ernstfall manuell zu reagieren.

VERBESSERTER AUSTAUSCH VON BEDROHUNGSINFORMATIONEN

Parallel zum Endgeräteschutz implementierte die Bundesagentur für Arbeit eine Threat-Intelligence-Lösung, die auf eine offene Kommunikationsplattform zurückgreift. Diese besteht aus einer Datenbank, auf die alle vernetzten Systeme Zugriff haben, was einen verbesserten Austausch lokaler sowie globaler Bedrohungsinformationen begünstigt.

INNOVATIVES POSTFACH FÜR SICHERHEITSPRÜFUNGEN

Täglich erreichen die Bundesagentur für Arbeit rund 30 Millionen verdächtige E-Mails. Über die integrierte Sicherheitslösung lässt sich ein „Postfach für Sicherheitsprüfungen" erstellen, mit dem die Mitarbeiter der Bundesagentur für Arbeit aktiv zur Sicherheit beitragen können. Wenn Behördenmitarbeiter eine E-Mail erhalten und sich über die Echtheit nicht sicher sind (z.B., wenn sie nicht in deutscher Sprache verfasst ist oder einen unbekannten Link bzw. einen unerwarteten Anhang enthält), können sie sie an eine spezielle E-Mail-Adresse, das sogenannte „Postfach für Sicherheitsprüfungen", weiterleiten. Ein CERT-Mitarbeiter erhält eine E-Mail und kann verdächtige Inhalte über die intuitive Benutzeroberfläche analysieren lassen.

SIEM RUNDET DIE STRATEGISCHE SICHERHEITSPARTNERSCHAFT AB

Im Rahmen der integrierten Lösung setzt die Bundesagentur für Arbeit ein Security-Information-and-Event-Management-Tool ein (SIEM). „Durch die SIEM-Lösung erhalten wir einen Überblick über jeden der 300 Millionen Sicherheitszwischenfälle, die wir jeden Tag erfassen", sagt Peter Neuhauser. „Wir können umsetzbare, nützliche Berichte zentral abrufen. Die Dashboards und Berichte machen unsere Sicherheitsmaßnahmen sichtbar und helfen uns dabei, die Compliance-Anforderungen einzuhalten."

Peter Neuhauser sieht in McAfee einen wichtigen Partner im IT-Sicherheitsumfeld. Die Bundesagentur für Arbeit verwendet zahlreiche McAfee-Produkte und nutzt bei Bedarf den hauseigenen Service, zum Beispiel zur Unterstützung bei der Erstellung von Zwischenfallreaktionsplänen. „Kriminelle arbeiten äußerst professionell zusammen. Ich denke, dass der offene und gemeinsame Ansatz von McAfee genau die richtige Sicherheit für unsere Seite liefert", schlussfolgert Peter Neuhauser.

Den kompletten Anwenderbericht finden Sie hier.

McAfee
Together is power.

McAfee Germany GmbH
Ohmstr. 1
85716 Unterschleißheim
www.mcafee.com/de

In Kooperation mit:

INFINIGATE
Adding Value to Distribution

DAS ZEITALTER DER **DIGITALEN TRANSFORMATION**

Die digitale Transformation steht bei praktisch jeder Organisation ganz oben auf der Liste, da technologischer Fortschritt, sich ändernde Kundenerwartungen oder neue Geschäftsmodelle Führungskräfte dazu zwingen, existierende IT-Strategien zu überdenken und neue Ansätze zu implementieren – angefangen bei hybriden Infrastrukturen bis hin zur Integration von Cloud-Technologien. Hinzu kommen neue Bereiche wie künstliche Intelligenz, Internet of Things oder Machine Learning. Die digitale Transformation bietet die Chance, differenzierte und überzeugende Ergebnisse zu erzielen – bringt aber auch neue Herausforderungen mit sich.

HERAUSFORDERUNG: **SICHERHEIT IM FOKUS**

Die Menge an Cyber-Bedrohungen nimmt immer weiter zu. Vermehrt werden Sicherheitsverletzungen in den Medien bekannt und veranlassen uns, über den Schutz unserer Daten nachzudenken. Ransomware, Phishing und andere Angriffe sind längst zur neuen Realität geworden. Es gibt viele wichtige Gründe, neben Wachstum auch auf einen angemessenen Schutz digitaler Ressourcen und der Infrastruktur zu setzen. Nicht zuletzt muss die Einhaltung regulatorischer Aspekte sichergestellt werden, um die Anforderungen an die Compliance zu erfüllen. Der Schutz von Identitäten, Anwendungen und Daten war immer wichtig – aber vielleicht nie so wichtig wie in der jetzigen Zeit, in der sich Prozesse und Technologien schnell weiterentwickeln.

UNSERE BEREICHE DER **SICHERHEITSEXPERTISE**

Identity-und Access-Management wird durch die wachsende Anzahl digitaler Identitäten und die Frage von bewusster Anonymität immer bedeutsamer. Unsere Lösungen können dabei helfen, Identitäts- und Zugriffsmanagement-Richtlinien schnell und kostengünstig in lokale,

„Ein ganzheitliches Cyber-Security-Konzept ist ein Muss bei der digitalen Transformation eines Unternehmens, das heißt, die Verantwortlichen der Fachbereiche müssen Hand in Hand mit den Security-Teams arbeiten. Security wird dadurch zum Business-Enabler und wird nicht länger als Kostenfaktor angesehen."

SARAH **TRUNK** | Director Security Business DACH | Micro Focus GmbH

mobile und Cloud-Umgebungen zu integrieren. Sie verwenden integrierte Identitätsinformationen zur Erstellung, Änderung und Stilllegung von Identitäten und zur Kontrolle ihres Zugriffs.

Security Operations ist in Zeiten wachsender Cyber-Bedrohungen besonders wichtig.
Wir bieten eine umfassende SIEM-Lösung und eine fortschrittliche Analyseplattform, die Sicherheitsanalysten und Betriebsteams dabei unterstützt, schneller auf Kompromissindikatoren zu reagieren, und sie in Echtzeit auf reale Bedrohungen hinweist. Durch automatische Identifizierung und Priorisierung von Bedrohungen vermeiden Ihre Teams die Kosten, die Komplexität und den Mehraufwand, die mit der Jagd nach Fehlalarmen verbunden sind.

Application Security sollte möglichst früh Teil des Software Development Lifecycles (SDLC) werden, um im besten Fall Schwachstellen in Anwendungen gar nicht erst entstehen zu lassen. Unsere Lösungen können durch umfangreiche Integrationsmöglichkeiten in vorhandene Prozesse direkt integriert werden. Mit statischen, dynamischen und mobilen Application-Security-Tests und kontinuierlicher Überwachung für Webanwendungen, können Sie Ihren SDLC ganzheitlich abdecken.

Data Privacy Protection ermöglicht es Unternehmen, den Geschäftswert durch vertrauenswürdige Anwendungen, Datenportabilität und Datenschutz zu steigern und gleichzeitig Risiken zu reduzieren. Unsere Lösungen erlauben fortschrittliche, formaterhaltende Verschlüsselung, sichere zustandslose Tokenisierung und zustandsloses Schlüsselmanagement zum Schutz von Unternehmensanwendungen, Datenverarbeitungsinfrastruktur, Cloud-Umgebungen und hybrider IT.

Secure Content Management hilft Ihnen, die Anforderungen an Zusammenarbeit und Produktivität mit Informationssicherheit, Datenschutz und Compliance in Unternehmenssystemen in Einklang zu bringen. Der autorisierte Zugriff, die Veröffentlichung und die fortlaufende Nutzung von Inhalten aus Geschäftsanwendungen (einschließlich E-Mails und SharePoint/O365) und Datenbankanwendungen wird mit weniger Risiko, Komplexität und Kosten verwaltet.

Micro Focus gehört zu den zehn größten Softwareunternehmen weltweit und unterstützt Unternehmen bei der digitalen Transformation mit Softwarelösungen für die Bereiche Enterprise DevOps, Hybrid-IT-Management, Predictive Analytics und Security, Risk & Governance.

Unsere Cyber-Security-Lösungen erstrecken sich über die vier Schlüsselbereiche AppSec for Modern Development, Data Lifecycle Management & Protection, Zero Trust und Next-Generation SOC. Sie bilden eines der branchenweit umfassendsten Angebote und basieren auf einem ganzheitlichen, analysegesteuerten Ansatz, der Sie bei der Sicherung Ihrer Identitäten, Anwendungen und Daten – ob vor Ort oder in der Cloud – auf Ihrem Weg der digitalen Transformation unterstützt.

MICRO FOCUS

Micro Focus GmbH | Herrenberger Straße 140 | 71034 Böblingen | **microfocus.com**

TREND MICRO

INTELLIGENTER SCHUTZ FÜR EINE VERNETZTE WELT

Als einer der weltweit führenden Anbieter von IT-Sicherheit hilft Trend Micro dabei, eine sichere Welt für den digitalen Datenaustausch zu schaffen. Mit über 30 Jahren Sicherheitsexpertise, globaler Bedrohungsforschung und beständigen Innovationen bietet Trend Micro Schutz für Unternehmen, Behörden und Privatanwender.

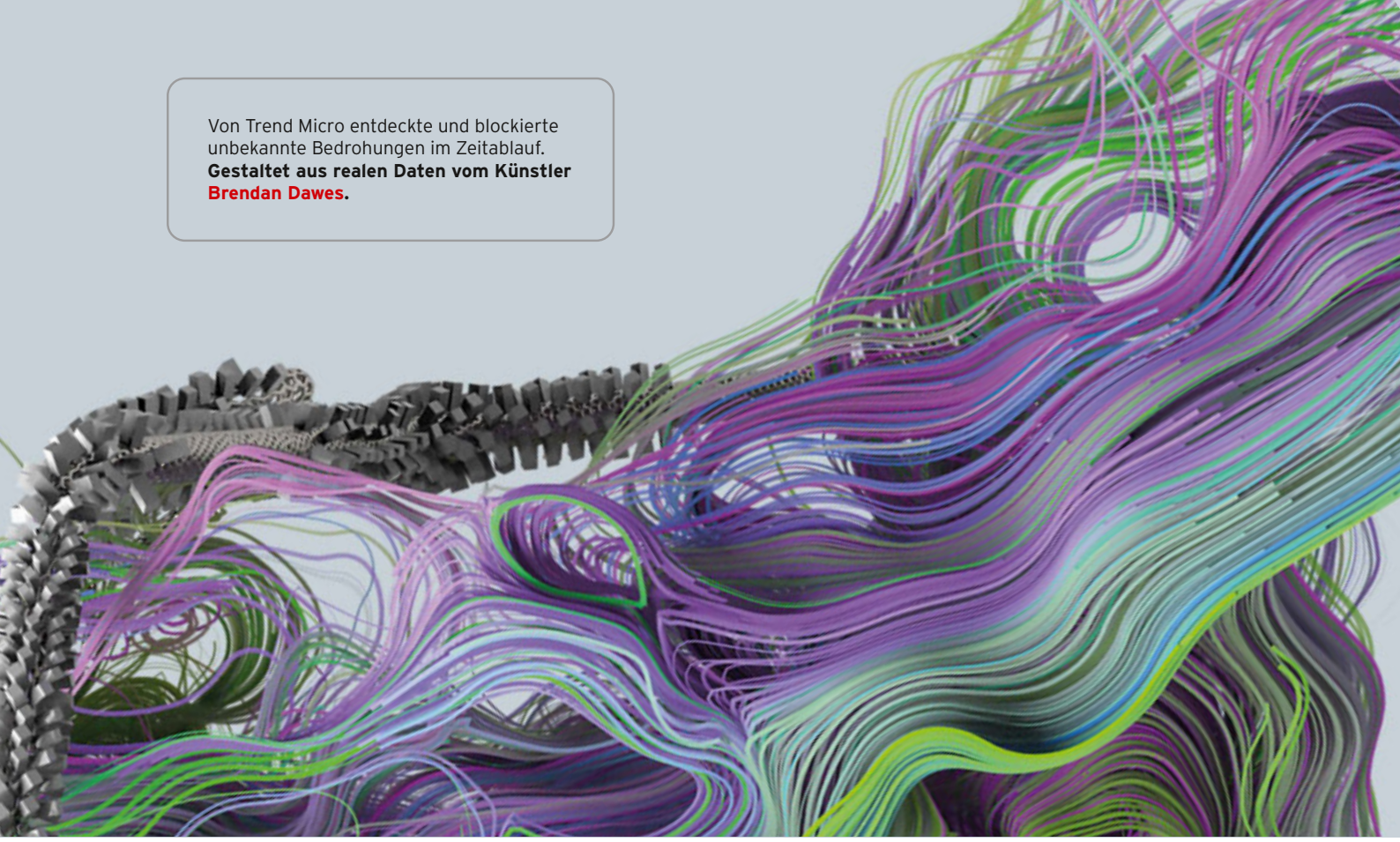
Die vernetzten Lösungen sind für Cloud-Workloads, Endpunkte, E-Mail, das IIoT und Netzwerke optimiert und bieten zentrale Sichtbarkeit über das gesamte Unternehmen, um Bedrohung schneller erkennen und darauf reagieren zu können. Mit über 6.700 Mitarbeitern in 65 Ländern und der weltweit fortschrittlichsten Erforschung und Auswertung globaler Cyber-Bedrohungen ermöglicht Trend Micro Unternehmen, ihre vernetzte Welt zu schützen.

MARKTFÜHRER FÜR CLOUD SECURITY

Nach Einschätzung des Analystenhauses IDC ist Trend Micro mit einem Marktanteil von 29,5 Prozent der weltweit führende Anbieter für den Schutz von Workloads in hybriden Cloud-Umgebungen. Dabei umfasst das Portfolio auch Lösungen für die sichere, agile Entwicklung und Bereitstellung von Anwendungen im Rahmen von DevOps- bzw. DevSecOps-Prozessen.

SCHUTZ FÜR DIE GESAMTE INFRASTRUKTUR

Die Mehrzahl aller Bedrohungen kann zwar mit bewährten Methoden abgewehrt werden, aber Angreifer versuchen unaufhörlich, bestehende Sicherheitsmaßnahmen mit neuen, komplexeren Attacken zu überwinden. Trend Micro XDR bietet Detection & Response über mehrere Schichten der Infrastruktur hinweg und untersucht Aktivitäten mittels effektiver künstlicher Intelligenz und erprobter Analytik. Dadurch werden weniger, aber dafür genauere Alarme produziert.



Von Trend Micro entdeckte und blockierte unbekannte Bedrohungen im Zeitablauf. **Gestaltet aus realen Daten vom Künstler Brendan Dawes.**

Trend Micro XDR geht dabei weit über Endpoint Detection & Response (EDR) hinaus: Aus E-Mail, Endpunkten, Servern, Cloud-Workloads und Netzwerken werden Daten gesammelt und korreliert. Dies ermöglicht ein Höchstmaß an Sichtbarkeit und Analysetiefe.

IMMER AUF DEM NEUESTEN STAND

Die Technologie von Trend Micro wird rund um die Uhr mit Bedrohungsinformationen von Trend Micro Research, einem globalen Netzwerk aus Zentren für Bedrohungsforschung, sowie der Schwachstellenforschung der Zero Day Initiative versorgt. Angesichts ständig neuer Bedrohungen und Schwachstellen liefert Trend Micro Sicherheit mit globaler Reichweite und lokaler Präsenz. Zudem profitieren die Lösungen von XGen Security, einer generationsübergreifenden Kombination von Abwehrtechniken. Vernetzte Bedrohungsinformationen ermöglichen dabei besseren und schnelleren Schutz.

WELTWEITE VERNETZUNG

Intelligente Sicherheit beginnt mit weltweiten Bedrohungsdaten. Das Trend Micro Smart Protection Network nutzt Big-Data-Analysen, um kontinuierlich über 15 Terabyte an Daten aus der Cloud zu identifizieren, proaktiven Schutz bereitzustellen und Daten schnellstmöglich zu sichern. Allein im Jahr 2019 blockierte das Smart Protection Network mehr als 52 Milliarden Bedrohungen– das bedeutet mehr Sicherheit für Nutzer weltweit.

The Art of Cybersecurity

Trend Micro hat Cyber-Sicherheit in eine Kunstform verwandelt und weltbekannte Künstler damit beauftragt, Sicherheitsdaten des Unternehmens zu visualisieren und in inspirierende Bilder zu verwandeln. Eines der Kunstwerke sehen Sie oben. Künstler verbinden wesentliche Elemente miteinander, um ihre Werke zu erschaffen. Trend Micro kombiniert wie kein anderer bewährte Weitsicht mit vernetzter Sicherheit und engagierten Mitarbeitern – und verwandelt damit Cyber-Sicherheit in Kunst.

www.theartofcybersecurity.com

TREND MICRO™

Securing Your Connected World

Trend Micro Deutschland GmbH
Parkring 29 | 85748 Garching b. München
+49 (0)89 839329-700 | www.trendmicro.com

INTEGRIERTE LÖSUNGEN STATT SPOT SOLUTIONS

Warum „gemeinsam stärker" auch in der IT-Security gilt

Die Anforderungen an die IT-Security steigen ständig. Darum sind heute integrierte Lösungen gefragt, die beides können: maximale Sicherheit gewährleisten und agile Entwicklungsprozesse ermöglichen.

Aus Ihrer Sicht als Security-Experte – was sind die großen Sicherheitsthemen, mit denen Unternehmen heute konfrontiert werden?

Vereinfach lässt sich sagen: Im Zuge der Digitalisierung werden Prozesse agiler. Damit steigt aber auch die Komplexität. Und mit dieser zunehmenden Komplexität muss die IT-Security heute umgehen können – sowohl aus sicherheitstechnischen als auch aus unternehmerischen Gründen.

Welche sind die sicherheitstechnischen Herausforderungen, die Sie ansprechen?

Immer mehr Applikationen, APIs, Microservices und Identitäten werden über die Grenzen der Unternehmens-IT hinaus exponiert. Darum reichen klassische WAF-Technologien, die für den Schutz von traditionellen HTML-Seiten gebaut wurden, heute einfach nicht mehr aus. Denn WAFs müssen heute auch APIs schützen, API Gateways müssen Web Security beherrschen, und APIs brauchen ein kohärentes Identity- und Access-Management.

Die Lösung ist also, statt einer WAF einfach einen API Gateway zu kaufen?

Ganz so einfach ist es leider nicht, denn traditionelle API Gateways können moderne Single-Page Applications (SPA) nur unvollständig absichern. Der Grund hierfür: Herkömmliche Gateways sind mit SOAP Webservices groß geworden, die Enterprise-Service-Busse benötigen und im Korsett komplexer Standards gefangen sind. Diese starre Struktur passt aber schlecht zur schönen neuen REST-Welt, die durch Agilität und Leichtgewichtigkeit geprägt ist.

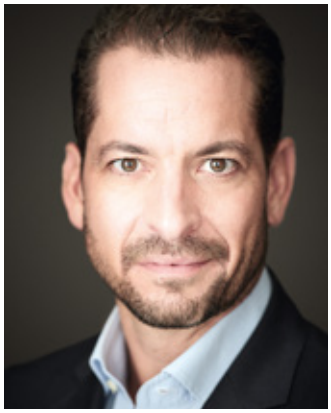
Welche Lösung passt denn am besten zur REST-Welt?

Moderne APIs werden heute von ganz unterschiedlichen Clients genutzt – von herkömmlichen Webapplikationen, SPAs, Smartphone Apps, „Things" und anderen Softwaresystemen. Und diese Clients sind dort exponiert, wo heute das Leben spielt – im wilden, heterogenen Internet. Darum braucht es für APIs Schutzkonzepte, die WAFs schon lange bieten. Und es braucht ein leistungsstarkes Identity- und Access-Management, da immer mehre interne und externe User auf Applikationen zugreifen.

Das heißt ganz konkret?

Grundsätzlich gibt es zwei Lösungsansätze: Entweder man setzt auf Spot Solutions – also auf singuläre Lösungen für singuläre Herausforderungen. Oder man baut auf das, was immer mehr Experten bevorzugen: auf kohärente, integrierte Systeme.


© shutterstock.com / Corepics VOF



„Mehr IT- und Investitions-Sicherheit in einem – der Secure Access Hub ist heute die effizienteste Lösung für die IT-Security."

ROMAN HUGELSHOFER,
Managing Director Application Security, Ergon Informatik AG

Integrierte Systeme – das klingt natürlich gut. Doch was sind die Vorteile?

Bildlich gesprochen werden bei integrierten Systemen vormals lose Enden zuverlässig miteinander verknüpft. So entsteht ein dichtes Sicherheitsnetz, das Unternehmen vor den aktuell größten Gefahren schützt: vor Angriffen auf Applikationen und Identitäten. Deshalb setzen wir bei unserem Secure Access Hub auf die drei Komponenten WAF, API Gateway und Customer IAM mit integrierter Zwei-Faktor-Authentifizierung aus einer Hand.

Neben dem Schutz von APIs haben Sie das Access-Management erwähnt. Warum ist dieser Aspekt so wichtig?

Neben dem Filtern von Inhalten über WAF und API Security wird die Verwaltung und Überprüfung von Identitäten und deren Berechtigungen heute immer wichtiger. Denn erstens greifen immer mehr externe Identitäten auf APIs zu. Und zweitens: Die Ansprüche an einen reibungslosen Authentisierungs-Flow werden immer größer, und Features wie Social Logins, Single Sign-On oder User Self-Services werden fast schon als Selbstverständlichkeit erwartet. Die Lösung für diese komplexe Herausforderungen sind Customer-IAM-Systeme (cIAM), da sie eine nahtlose User Experience garantieren und sich einfach skalieren lassen. Ein weiterer wichtiger Punkt: Mit cIAM-Lösungen lassen sich Zwei-Faktor-Authentifizierungen (2FA) implementieren – und an der kommen viele Unternehmen schon aus regulatorischen Gründen kaum mehr vorbei.

Sicherheitstechnische Anforderungen sind das eine, unternehmerischen Anforderungen das andere. Welche Benefits kann ein moderner Secure Access Hub hier bieten?

Die einfache Antwort: Intelligente und standardisierte Systeme lassen sich vorgelagert und zentralisiert über alle Applikationen und APIs hinweg an neue Aufgaben anpassen. So wird eine agile und flexible Softwareentwicklung ermöglicht, die ein schnelles Time-to-Market sicherstellt – mit allen Wettbewerbsvorteilen, die sich so für Unternehmen eröffnen. Zusätzlich ergeben sich geringere Betriebskosten oder auch eine effizientere Erfüllung von Compliance-Anforderungen.

Und die komplexe Antwort?

Egal ob von DevOps-Prozessen gesprochen wird oder der Einsatz von flexiblen Containern gefragt ist – der grundsätzliche Vorteil von integrierten Sicherheitslösungen ist derselbe: Sie basieren auf kohärenten Frameworks, sodass der Sicherheitsaspekt durchgängig in die Applikationsentwicklung integriert ist. Unternehmen profitieren so von All-in-One-Lösungen – z.B. für Authentisierung, Registrierung, die Anbindung von Directories, das Login sowie Single Sign-on und User Self-Services.

Das klingt ja alles sehr gut. Doch sehr gut – das heißt doch auch sehr teuer?

Unsere klare Antwort: Nein! Denn eine Vollkostenrechnung zeigt, dass ein integrierter Ansatz zu einem wesentlich tieferen TCO führt. Zudem steigern integrierte Ansätze nicht nur die IT-, sondern auch die Zukunfts- und Investitionssicherheit. So gesehen ermöglicht ein Secure Access Hub eine klassische Win-win-Situation – sowohl für die IT als auch für das Business.

AIRLOCK®
SECURE ACCESS HUB

Ergon Informatik AG
Merkurstraße 43, CH-8032 Zürich
Telefon: +41 44 268 89 00
E-Mail: info@ergon.ch

Studiendesign

Cyber Security 2020

Studiensteckbrief

Herausgeber	COMPUTERWOCHE, CIO, TecChannel und ChannelPartner
Studienpartner	**Platin-Partner:** Microsoft Deutschland GmbH **Gold-Partner:** Cisco Systems GmbH DriveLock SE F-Secure GmbH Infinigate Deutschland GmbH McAfee Germany GmbH Micro Focus Deutschland GmbH Trend Micro Deutschland GmbH **Silber-Partner:** Ergon Informatik AG (Airlock)
Grundgesamtheit	Oberste (IT-)Verantwortliche von Unternehmen in der D-A-CH-Region: strategische (IT-)Entscheider im C-Level-Bereich und in den Fachbereichen (LoBs), IT-Entscheider & IT-Spezialisten aus dem IT-Bereich
Teilnehmergenerierung	Stichprobenziehung in der IT-Entscheider-Datenbank von IDG Business Media; persönliche E-Mail-Einladungen zur Umfrage
Gesamtstichprobe	655 abgeschlossene und qualifizierte Interviews Stichprobe 1: 318 Stichprobe 2: 337
Untersuchungszeitraum	20. Juli bis 28. Juli 2020
Methode	Online-Umfrage (CAWI)
Fragebogenentwicklung	IDG Research Services in Abstimmung mit den Studienpartnern
Durchführung	IDG Research Services
Technologischer Partner	Questback GmbH, Köln
Umfragesoftware	EFS Survey

Stichprobenstatistik

Branchenverteilung*	Land- und Forstwirtschaft, Fischerei, Bergbau	4,1 %
	Energie- und Wasserversorgung	8,5 %
	Chemisch-pharmazeutische Industrie, Life Science	10,4 %
	Medizin- und Labortechnik	5,8 %
	Metallerzeugende und -verarbeitende Industrie	14,4 %
	Maschinen- und Anlagenbau	13,9 %
	Automobilindustrie und Zulieferer	7,0 %
	Herstellung von elektrotechnischen Gütern, IT-Industrie	12,2 %
	Konsumgüter-, Nahrungs- und Genussmittelindustrie	3,4 %
	Medien, Papier- und Druckgewerbe	2,6 %
	Baugewerbe, Handwerk	3,7 %
	Groß- und Einzelhandel (inklusive Online-Handel)	8,5 %
	Banken und Versicherungen	16,8 %
	Transport, Logistik und Verkehr	12,1 %
	Dienstleistungen für Unternehmen	11,1 %
	Hotel- und Gastgewerbe, Tourismus	5,6 %
	Öffentliche Verwaltung, Gebietskörperschaften, Sozialversicherung	7,9 %
	Schule, Universität, Hochschule	4,0 %
	Gesundheits- und Sozialwesen	3,4 %
	Andere Branchengruppe	5,8 %
Unternehmensgröße deutschlandweit	Weniger als 499 Beschäftigte	24,3 %
	500 bis 999 Beschäftigte	28,5 %
	1.000 bis 9.999 Beschäftigte	35,6 %
	10.000 Beschäftigte und mehr	11,6 %
Umsatzklasse deutschlandweit	Weniger als 100 Millionen Euro	20,6 %
	100 bis 999 Millionen Euro	27,2 %
	1 bis unter 2 Milliarden Euro	23,2 %
	2 bis unter 5 Milliarden Euro	16,9 %
	5 Milliarden Euro und mehr	12,1 %
Jährliche Aufwendungen in IT-Systeme	Weniger als 1 Million Euro	13,9 %
	1 bis unter 10 Millionen Euro	28,1 %
	10 bis unter 100 Millionen Euro	32,7 %
	100 Millionen Euro und mehr	14,5 %
	Keine Angabe / weiß nicht	10,8 %

*** Mehrfachnennungen möglich**

Studienreihe / Autoren / Kontakt / Impressum

Das Studienkonzept

Die Multi-Client-Studien von IDG Research Services sind mehr als nur Befragungen von C-Level-Entscheidern und IT-Spezialisten. Hinter den Marktforschungsprojekten steht ein nachhaltiges Studienkonzept, das auf eine Laufzeit von mindestens sechs Monaten ausgelegt ist.

Die Veranstaltung der initialen redaktionellen Round Tables, moderiert von leitenden Redakteuren der COMPUTERWOCHE, steht immer zu Beginn eines jeden Studienprojekts.

Über den Verlauf der Round-Table-Veranstaltungen wird ausführlich berichtet, und die Themen, die den Branchenexperten besonders „auf den Nägeln brennen", werden auch bei der Entwicklung des Studienfragebogens mitberücksichtigt. Die Unternehmen, die das Projekt als Partner begleiten, können eigene Ideen und Fragestellungen einbringen.

Etwa drei Monate nach der methodischen und inhaltlichen Ausgestaltung der Studie liegen die zentralen Ergebnisse in Form eines hochwertigen Survey Reports vor. Die Studienergebnisse werden auf Messen und Events, wie der Hannover Messe, dmexco oder it-sa, präsentiert, zum Teil in Form von Podiumsdiskussionen, bei denen sich die Studienpartner einem interessierten Fachpublikum stellen können. Oder es wird zu einem Ergebnis-Round-Table ins IDG Conference Center eingeladen.

Begleitet wird das gesamte Studienprojekt durch kontinuierliche Berichterstattung von COMPUTERWOCHE und CIO, zum Thema im Allgemeinen und zur Studie im Speziellen. Fachwissen und Kompetenz unserer Autoren und Redakteure tragen maßgeblich dazu bei, dass die Ergebnisse der Multi-Client-Studien von IDG Research Services richtig eingeordnet werden können. Berichtet und kommentiert wird auf allen modernen Medienkanälen; Infografiken, Bildergalerien und Videointerviews tragen dazu bei, dass die IDG-Studien mittlerweile auf großes Interesse stoßen.

Das Redaktionsteam

Heinrich Vaske:
Chefredakteur

Heinrich Vaske ist Editorial Director von COMPUTERWOCHE und CIO. Seine wichtigste Aufgabe ist die inhaltliche Ausrichtung beider Medienmarken. Vaske verantwortet außerdem inhaltlich die Sonderpublikationen, Social-Web-Engagements und Mobile-Produkte und moderiert Veranstaltungen.

Wolfgang Herrmann:
Editorial Manager CIO Magazin

Wolfgang Herrmann ist Editorial Manager des CIO Magazins. Zu seinen thematischen Schwerpunkten gehören Cloud Computing, Big Data / Analytics und Digitale Transformation.

Manfred Bremmer:
Senior Editor IoT und Mobile

Manfred Bremmer beschäftigt sich mit Mobile Computing und Communications. Er nimmt mobile Lösungen, Betriebssysteme, Apps und Endgeräte unter die Lupe und überprüft sie auf ihre Business-Tauglichkeit.

Alexandra Mesmer:
Redakteurin

Seit 18 Jahren ist „Karriere in der IT" ihr Leib- und Magenthema. Zudem ist Mesmer verantwortlich für die IDG Career Services mit Dienstleistungen rund um Employer Branding und Recruiting.

Martin Bayer:
Editorial Manager COMPUTERWOCHE

Spezialgebiet Business-Software: Business Intelligence, Big Data, CRM, ECM und ERP; Betreuung von News und Titelstrecken in der Print-Ausgabe der COMPUTERWOCHE.

Jürgen Hill:
Chefredaktuer Future Technologies

Thematisch befasst sich der studierte Diplom-Journalist und Informatiker mit allen Facetten rund um Digitalisierung, KI/ML, IoT und Industrie 4.0.

Hans Königes:
Ressortleiter

Hans Königes ist Ressortleiter Jobs & Karriere und damit zuständig für alle Themen rund um Arbeitsmarkt, Jobs, Berufe, Gehälter, Personalmanagement, Recruiting sowie Social Media im Berufsleben.

Jens Dose:
Redakteur

Jens Dose ist Redakteur des CIO-Magazins. Neben den Kernthemen rund um CIOs und ihre Projekte beschäftigt er sich auch mit der Rolle des CISO und dessen Aufgabengebiet.

Der Autor dieser Studie

Oliver Schonschek
Oliver Schonschek ist freier Analyst und Fachjournalist und schreibt für führende Fachmedien über IT, Sicherheit und Datenschutz, darunter COMPUTERWOCHE und CIO. Er ist Herausgeber und Autor mehrerer Fachbücher und wurde in den USA mehrfach als Influencer und Media Leader für Technologien wie Blockchain, KI, VR / AR und Mobile Computing ausgezeichnet.

Unser Autorenteam

Alexander Jake Freimark
Alexander Jake Freimark wechselte 2009 von der Redaktion der COMPUTERWOCHE in die Freiberuflichkeit. Er schreibt für Medien und Unternehmen, sein Auftragsschwerpunkt liegt im Corporate Publishing. Dabei stehen technologische Innovationen im Fokus, aber auch der Wandel von Organisationen, Märkten und Menschen.

Gerhard Holzwart
Gerhard Holzwart begann 1990 als Redakteur der führenden IT-Wochenzeitung COMPUTERWOCHE und leitete ab 1996 das Ressort Unternehmen & Märkte. Ab 2005 verantwortete er den Bereich Kongresse und Fachveranstaltungen der IDG Business Media GmbH und baute „IDG Events" mit jährlich rund 80 Konferenzen zu einem der führenden Anbieter von ITK-Fachveranstaltungen in Deutschland aus. Seit 2010 ist Gerhard Holzwart geschäftsführender Gesellschafter der h&g Editors GmbH und in dieser Funktion als Event Producer, Direktmarketingspezialist und ITK-Fachredakteur tätig.

Jürgen Mauerer
Jürgen Mauerer arbeitet seit Oktober 2002 als freiberuflicher IT-Fachjournalist in München. Er schreibt vorwiegend über aktuelle Themen und Trends rund um IT und Wirtschaft für Publikationen wie COMPUTERWOCHE, com! professional oder ZD.NET. Darüber hinaus berät und unterstützt er PR-Agenturen sowie IT-Unternehmen bei der Erstellung von Anwenderberichten, Whitepapers, Fachartikeln oder Microsites und moderiert Podiumsdiskussionen und Veranstaltungen.

Bernd Reder
Bernd Reder ist seit rund 30 Jahren als Fachjournalist für Medien, PR-Agenturen und Unternehmen tätig. Zu seinen thematischen Schwerpunkten zählen die Informations- und Netzwerktechnik, Cloud Computing, IT-Security und Mobility. Bevor er sich selbstständig machte, war Reder in den Redaktionen führender Fachpublikationen tätig. Dazu zählen Elektronik, Network World, Digital World und Network Computing.

Michael Schweizer
Michael Schweizer ist freier Redakteur und Autor in München. Oft schreibt er über Menschen, Personal- und Karrierefragen mit IT-Bezug. Besonders interessiert ihn alles, was mit Wissenschaft zu tun hat, also zum Beispiel unabhängige Studien zu komplizierten Themen. Als freier Schlussredakteur ist er unter anderem für die Print-Ausgaben der IDG-Publikationen COMPUTERWOCHE, CIO und ChannelPartner zuständig. Er übernimmt auch Buchlektorate.

Sales-Team

Regina Hermann
Account Manager Research
IDG Research Services
Telefon: +49 (0) 89 36086 –384
rhermann@idg.de

René Krießan
Account Manager Research
IDG Research Services
Telefon: +49 (0) 89 36086 –322
rkriessan@idg.de

Bastian Wehner
Account Manager Research
IDG Research Services
Telefon: +49 (0) 89 36086 – 169
bwehner@idg.de

Projektmanagement

Simon Hülsbömer
Senior Project Manager
IDG Research Services
Telefon: +49 (0) 89 36086 – 177
shuelsboemer@idg.de

Armin Rozsa
Junior Project Manager
IDG Research Services
Telefon: +49 (0) 89 36086 – 184
arozsa@idg.de

Sandra Baumgarten
Junior Project Manager
IDG Research Services
Telefon: +49 (0) 89 36086 – 116
sbaumgarten@idg.de

Gesamtstudienleitung

Matthias Teichmann
Director Research
IDG Research Services
Telefon: +49 (0) 89 36086 – 131
mteichmann@idg.de

Unsere Studienreihe

Erhältlich in unserem Studien-Shop auf **computerwoche.de/studien**

Laufende Studienberichterstattung auf **computerwoche.de/p/research,3557**

Für Rückfragen zu demnächst kommenden Studien: **research@idg.de**

Für regelmäßige Infos: **https://www.idg.de/media/research-services/**

Oder folgen Sie uns gerne auf Twitter: **https://twitter.com/IDGResearch_DE**

oder auf LinkedIn: **https://www.linkedin.com/ showcase /idg-research-services-germany/**

Studienpartner

Platin-Partner:

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München
Telefon: +49 (0) 89 3176 – 0
Fax: +49 (0) 89 3176 – 1000
Web: www.microsoft.com

Gold-Partner:

Cisco Systems GmbH
Parkring 20
85748 Garching
Telefon: +49 (0) 89 51657 1000
Web: www.cisco.com

DriveLock SE
Landsberger Straße 396
81241 München
Telefon: +49 (0) 89 5463 649 – 0
E-Mail: info@drivelock.com
Web: www.drivelock.de

F-Secure GmbH
Kistlerhofstraße 172c
81379 München
Telefon: +49 (0) 89 787 467 – 0
E-Mail: vertrieb-de@f-secure.com
Web: www.f-secure.com

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar / München
Telefon: +49 (0) 89 89048 – 0
E-Mail: info@infinigate.de
Web: www.infinigate.de

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

Micro Focus Deutschland GmbH
Herrenberger Straße 140
D-71034 Böblingen
Telefon: +49 (0) 3221 107 6466
E-Mail: microfocus.com/contact/contactme
Web: www.microfocus.com/srg

Trend Micro Deutschland GmbH
Parkring 29
85748 Garching b. München
Telefon: +49 (0) 89 839 329 – 700
E-Mail: salesinfo_de@trendmicro.com
Web: www.trendmicro.com

Silber-Partner:

Airlock eine Security Innovation der Ergon Informatik AG
Merkurstraße 43
CH-8032 Zürich
Telefon +41 (0) 44 268 87 00
E-Mail: info@airlock.com
Web: www.airlock.com

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

Kommentierungen CIO-Agenda 2020:
Simon Hülsbömer,
IDG Research Services

Hosting / Koordination Feldarbeit:
Armin Rozsa,
IDG Research Services

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

Artdirector & Grafik CIO-Agenda 2020:
Daniela Petrini, Reutte

Grafik:
Patrick Birnbreier, München

Umschlaggestaltung unter Verwendung eines Farbfotos von ©stockphoto-graf / shutterstock.com

Lektorat:
Dr. Renate Oettinger, München

Druck:
Peradruck GmbH
Hofmannstr. 7b
81379 München

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

Herausgeber:

IDG Business Media GmbH

Anschrift:
Lyonel-Feininger-Str. 26
80807 München
Telefon: +49 (0) 89 36086 – 0
Fax: +49 (0) 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

INSIGHTS INTENT & ENGAGEMENT

Studie

CYBER SECURITY

PLATIN-PARTNER

Microsoft

GOLD-PARTNER

cisco Secure

McAfee Together is power.

INFINIGATE ... Adding Value to Distribution

DriveLock

F-Secure

MICRO FOCUS

TREND MICRO

SILBER-PARTNER

AIRLOCK® SECURE ACCESS HUB