COMPUTERWOCHE VOICE OF DIGITAL | CIO | ChannelPartner | TECCHANNEL IT IM MITTELSTAND

IDG RESEARCH SERVICES

STUDIE CYBER SECURITY 2020

DIE WICHTIGSTEN KEY FINDINGS

PRÄSENTIERT VON MICRO FOCUS

MICRO FOCUS®

Liebe Leserinnen, lieber Leser,

vielen Dank für Ihr Interesse an den Ergebnissen unserer Studie rund um Cyber Security, die in Kooperation mit unserem Studienpartner Micro Focus entstanden ist. An der Umfrage von COMPUTERWOCHE und CIO, die im Juli 2020 online durchgeführt wurde, haben sich insgesamt 655 (IT-) Entscheider aus Unternehmen der D-A-CH-Region beteiligt. Es handelt sich dabei um Verantwortliche aus allen relevanten Unternehmensbereichen, vom C-Level über die Fachbereiche bis hin zum IT-Bereich.

Ob Zero Trust oder Security Automation: Im Corona-Jahr 2020 scheinen einige teils schon länger bekannte Security-Trends frischen Rückenwind zu bekommen. Da lohnt ein genauerer Blick: Wie ist der Status Quo dieser Entwicklungen in den deutschen Unternehmen? Wie entwickeln sich die IT-Sicherheits-Budgets angesichts der aktuellen Gesamtlage? Wie offen müssen und dürfen Security-Infrastrukturen heute sein? Ob die Pandemie nun mittel- bis langfristig Fluch oder Segen für die IT-Sicherheit ist, muss sich zwar erst noch zeigen – unsere Studie gibt aber zumindest kurzfristig viele spannende Einblicke in die aktuelle Marktlage.

Wir freuen uns, Ihnen mit dem hier vorliegenden Whitepaper einige zentrale Ergebnisse der Studie präsentieren zu dürfen. Für weitere Ergebnisse verweisen wir auf die laufende Berichterstattung in unseren Medien und auf unseren Studien-Shop (https://shop.computerwoche.de/portal-9915), in dem die komplette Studie für ein Download bereitsteht.

Wenn Sie Rückfragen zur Studie haben, wenden Sie sich gerne an Frau Sophie Heidenreich von Micro Focus (sophie.heidenreich2@microfocus.com). Weitere Kontaktdaten entnehmen Sie bitte dem Impressum.

Wir wünschen Ihnen eine interessante und aufschlussreiche Lektüre.

Ihre Teams von
Micro Focus und
IDG Research Services

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.

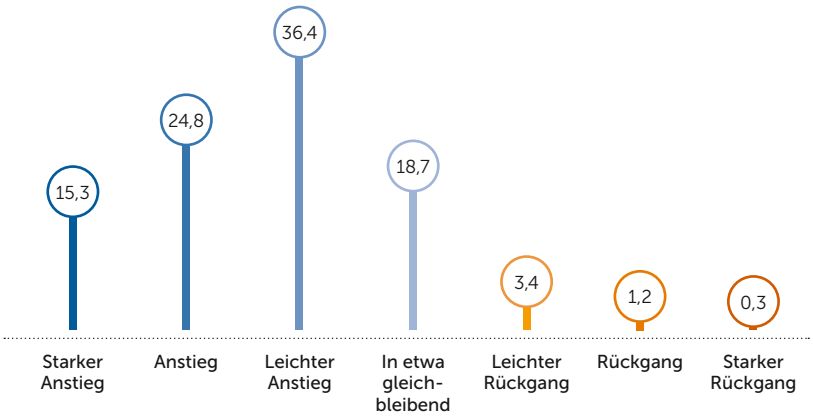
Die Unternehmen, die mit einem leichten bis starken Anstieg des Budgets für Cyber-Sicherheit in 2021 rechnen, haben bereits konkrete Pläne, wo sie die Security-Investitionen tätigen wollen. Die geplanten Anschaffungen für Security stimmen allerdings nicht durchgehend mit den zuvor genannten Herausforderungen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

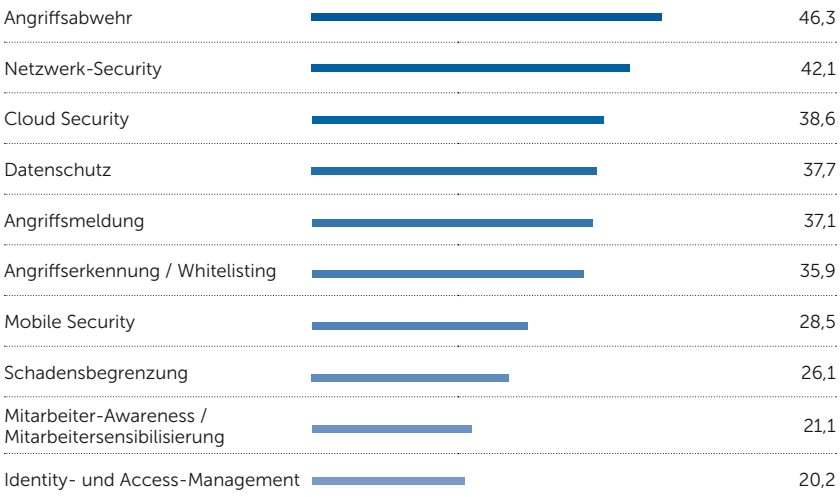


Betrachtet man einzelne Sicherheitsmaßnahmen und die dafür geplanten Projekte in 2021, nennen 61 Prozent den verbesserten Schutz oder die Verschlüsselung sensibler Daten, 46 Prozent die Klassifizierung der Daten, 39 Prozent das Auffinden sensibler Daten und 27 Prozent das Testen und die Absicherung von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

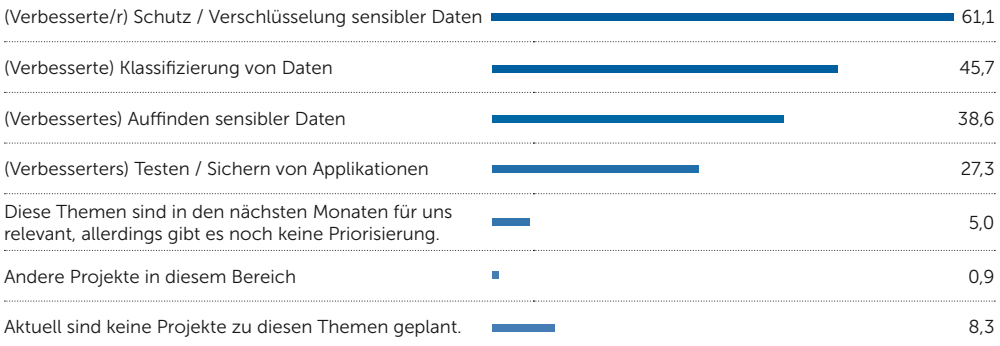
Wo liegen die Schwerpunkte Ihrer Cyber-Security-Investitionen?

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



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.

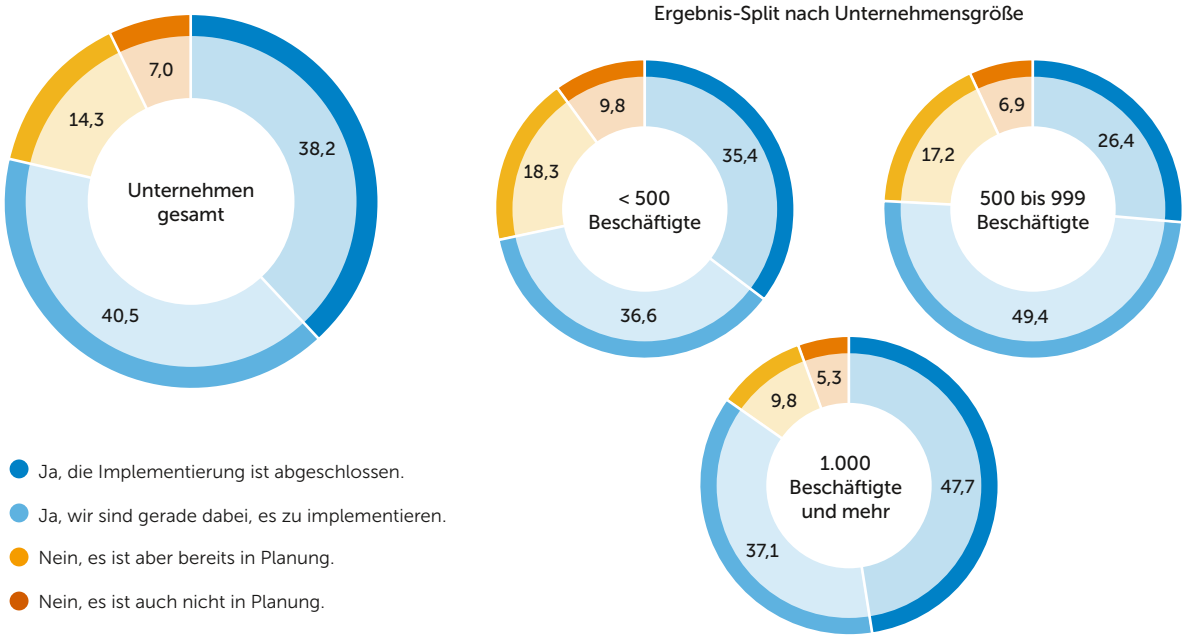
Obwohl nur wenige Unternehmen Investitionen für Zero Trust vorgesehen haben, ist dieser Ansatz bei 55 Prozent in der Implementierung oder in der Planung. Das gilt auch für größere Unternehmen, die sogar noch seltener Investitionen im Bereich Zero Trust vorgesehen haben.

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.

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.

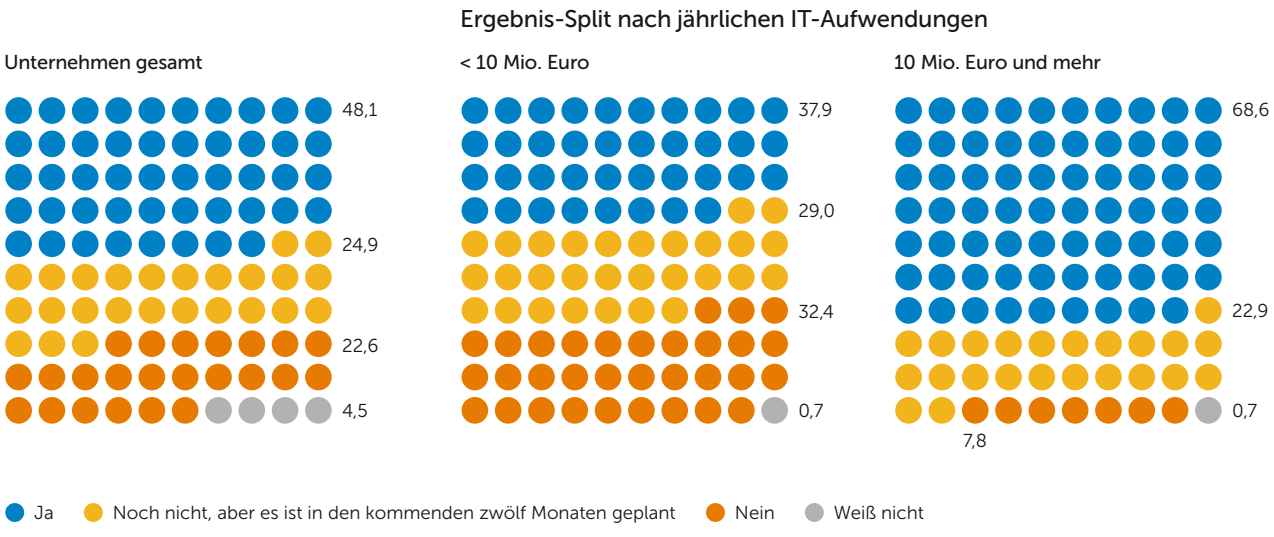
Doch KI in der Cyber Security ist nicht nur eine Frage des Budgets: Unternehmen mit weniger als 500 Beschäftigten sagen bisher in 31 Prozent der Fälle Nein zu KI. Bei 500 bis 999 Beschäftigten sinkt die Ablehnung auf 22 Prozent, ab 1.000 Beschäftigten beträgt sie nur noch 18 Prozent.

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



Jedes zweite Unternehmen setzt bereits auf Security Automation

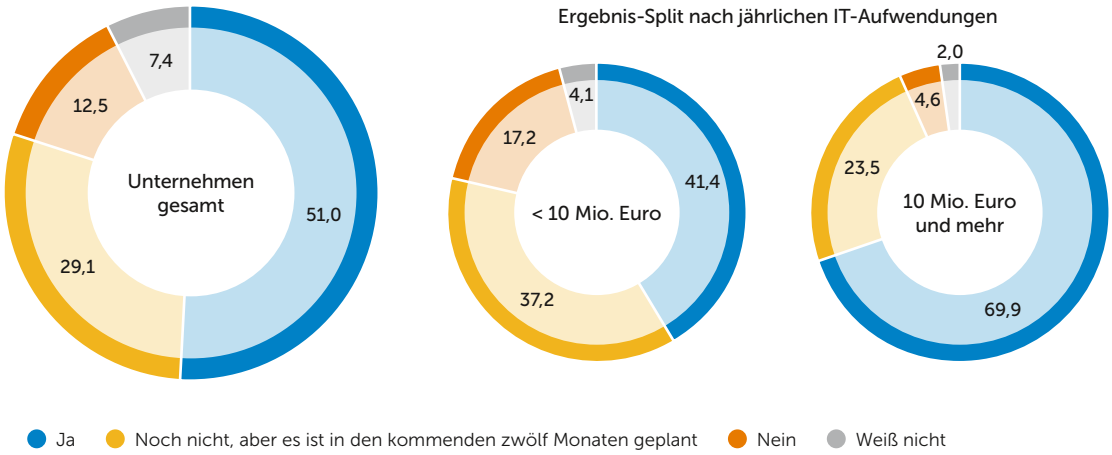
Nur 13 Prozent der befragten Unternehmen planen nicht, ihre Cyber Security (teilweise) zu automatisieren. 29 Prozent planen Security Automation in den nächsten zwölf Monaten. Security-Automatisierung ist bei größeren Unternehmen mit 58 Prozent stärker verbreitet als bei den kleinen mit 46 Prozent. Ein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

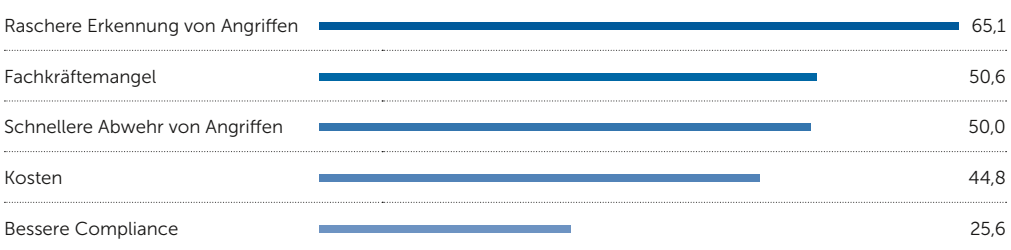
Ist Security Automation Teil Ihrer IT-Security-Strategie?

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

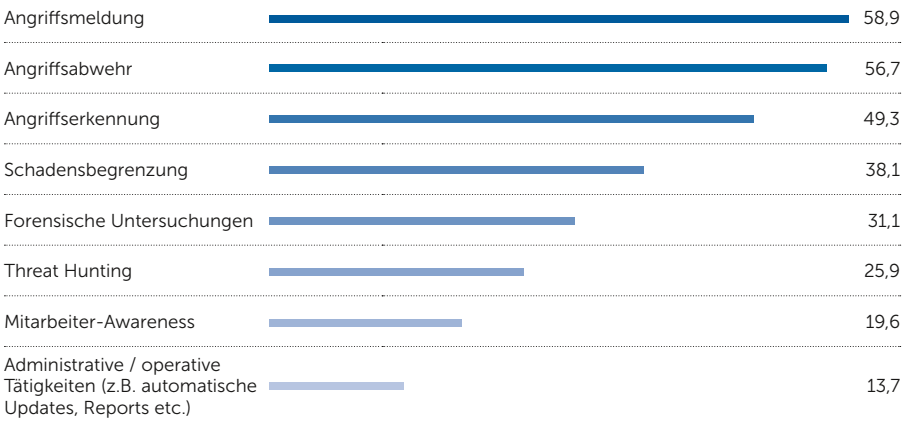


Offensichtlich wird die Bedeutung einer schnellen Abwehr nach der Detektion ebenso unterschätzt wie die Vorteile einer automatisierten Erkennung und Abwehr für die Compliance. So richtet sich zum Beispiel die Höhe des Bußgeldes bei einer Datenschutzverletzung nach DSGVO (Datenschutz-Grundverordnung) 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



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.

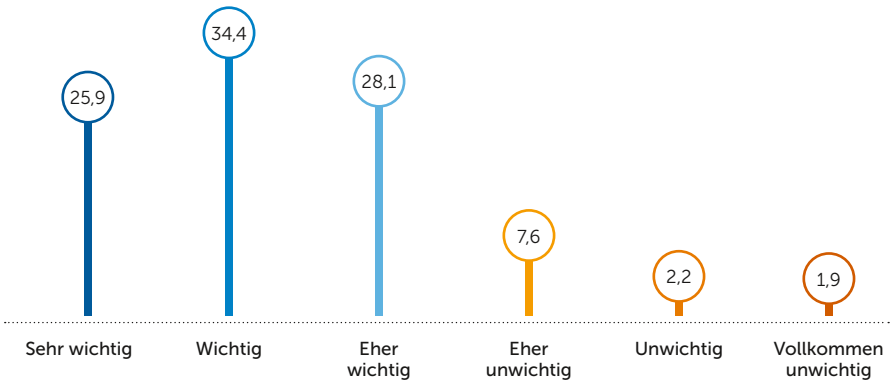
Der Wunsch nach offenen Security-Lösungen hängt auch vom jährlich verfügbaren IT-Budget ab. Beträgt es zehn Millionen Euro und mehr, wollen 71 Prozent eine offene Sicherheitsinfrastruktur. Bei unter zehn Millionen Euro sind immer noch 53 Prozent an der Offenheit der Security interessiert.

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.

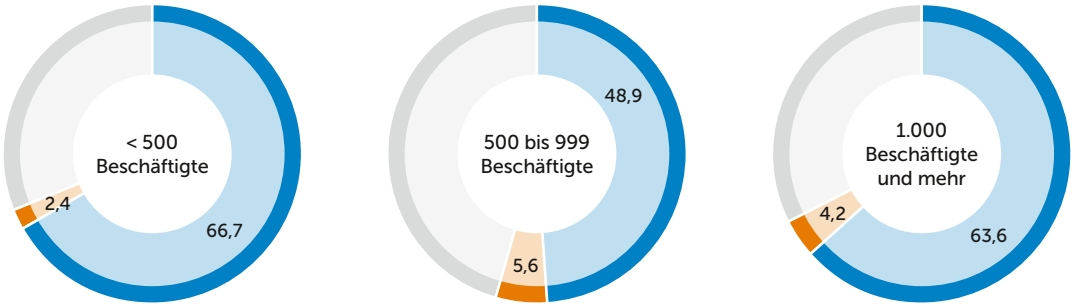
Es ist allerdings zu vermuten, dass die Fachbereiche die Nachteile von Insellösungen in der Security nicht genau genug kennen, die Vertreter des C-Levels hingegen sind mit den Vorteilen der Offenheit offensichtlich vertraut.

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

Angaben in Prozent. Basis: n = 337

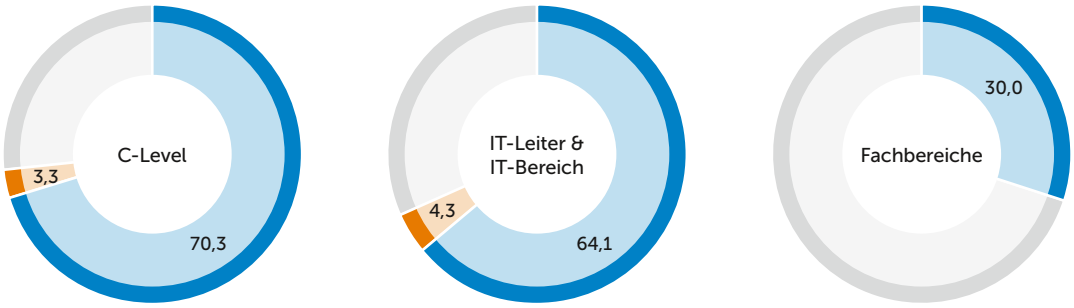


Ergebnis-Split nach Unternehmensgröße



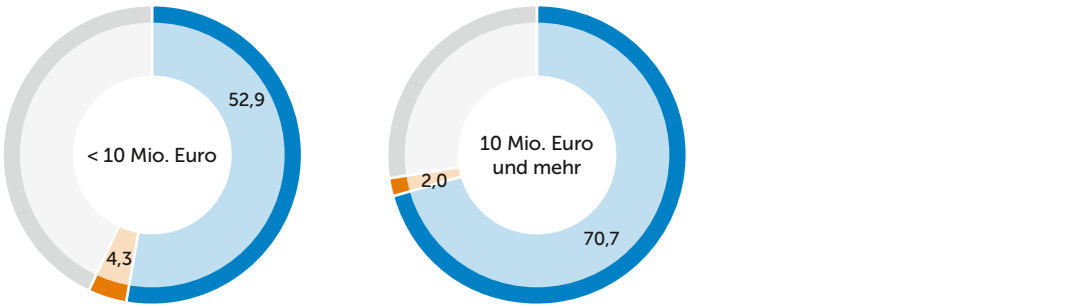
- Sehr wichtig / wichtig
- Vollkommen unwichtig / unwichtig

Ergebnis-Split nach Funktion im Unternehmen



- Sehr wichtig / wichtig
- Vollkommen unwichtig / unwichtig

Ergebnis-Split nach jährlichen IT-Aufwendungen



- Sehr wichtig / wichtig
- Vollkommen unwichtig / unwichtig

Micro Focus ist ein führender, weltweit agierender Softwareanbieter, der Unternehmen bei der Ausweitung vorhandener Investitionen und der gleichzeitigen Einführung neuer Technologien in einer Welt der hybriden IT unterstützt.

Micro Focus stellt seinen Kunden ein erstklassiges Portfolio an skalierbaren Unternehmenslösungen mit integrierten Analysen zur Verfügung und sorgt damit für kundenzentrierte Innovationen in den Bereichen Enterprise DevOps, Hybrid IT Management, Security, Risk & Governance sowie Predictive Analytics.

ACCELERATE APPLICATION DELIVERY

Mit den Application Delivery Management-Lösungen von Micro Focus können Unternehmen qualitativ hochwertige Software und Services schnell und sicher bereitstellen.

SIMPLIFY YOUR IT TRANSFORMATION

Unternehmen können Hybrid IT mit den Lösungen von Micro Focus agil angehen und eine Brücke zwischen traditionellen und transformativen IT-Services schlagen – von Mainframe über Mobile bis zur Cloud.

STRENGTHEN YOUR CYBER RESILIENCE

Micro Focus bietet das branchenweit umfangreichste Portfolio an Cybersicherheits-Lösungen. Deren analyticsgetriebener Ansatz hilft Unternehmen zu sichern, was am meisten zählt: Identitäten, Anwendungen und Daten.

ANALYZE IN TIME TO ACT

Datenschätze sind nur wertvoll, wenn Unternehmen daraus auch einen Wert ziehen können. Die Lösungen von Micro Focus ermöglichen es, dies mit Hilfe von Machine Learning zu tun. Durch Echtzeit-Analysen sind Unternehmen in der Lage, Vorhersagen zu treffen, mit denen sie Geschäftsergebnisse schnell und effizient beeinflussen können.

CYBER RESILIENCE IM FOKUS
UNSERE BEREICHE DER SICHERHEITSEXPERTISE

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.

ZERO TRUST

Identity & Access Management wird durch die wachsende Anzahl digitaler Identitäten und die Frage von bewusster Anonymität immer bedeutsamer.
Die Micro Focus Lösungen können dabei helfen, Identitäts- und Zugriffsmanagement-Richtlinien schnell und kostengünstig in lokale, mobile und Cloud-Umgebungen zu integrieren. Sie verwenden integrierte Identitätsinformationen zur Erstellung, Änderung und Stilllegung von Identitäten und zur Kontrolle ihres Zugriffs.

APPLICATION SECURITY FOR MODERN DEVELOPMENT

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.
Die Micro Focus 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

Unsere Lösungen erlauben fortschrittliche, formaterhaltende Verschlüsselung, sichere zustandslose Tokenisierung und zustandsloses Schlüsselmanagement zum Schutz von Unternehmensanwendungen, Datenverarbeitungsinfrastruktur, Cloud-Umgebungen und hybrider IT. Mit unseren Lösungen können Unternehmen Ihren Geschäftswert durch vertrauenswürdige Anwendungen, Datenportabilität und Datenschutz steigern und gleichzeitig Risiken reduzieren.

NEXT-GENERATION SECURITY OPERATIONS

Micro Focus bietet 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.

Zu den Kunden von Micro Focus zählen u. a. Accenture, Accor Hotels, Allianz, BMW und Orange sowie Unternehmen aus den unterschiedlichsten Branchen, darunter Finanzen, Luft- und Raumfahrt, Pharma, Telekommunikation und Versorgung. Micro Focus wurde 1976 gegründet. Der Firmensitz befindet sich in Newbury, England.

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

Vertretungsberechtigter
York von Heimburg
Geschäftsführer

Registergericht
Amtsgericht München
HRB 99187

Umsatzsteueridentifikations-
nummer: DE 811 257 800

Weitere Informationen unter:
www.idg.de

Gold-Partner:
Micro Focus Deutschland GmbH
Sophie Heidenreich,
Marketing Manager
Herrenberger Straße 140
71034 Böblingen
E-Mail: sophie.heidenreich2@microfocus.com

Bei Lösungsanfragen:
Telefon: +49 (0) 3221 107 6466
Web: microfocus.com/contact/contactme
www.microfocus.com/srg

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

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

Analysen / Kommentierungen:
Oliver Schonschek, Bad Ems

Hosting / Koordination Feldarbeit:
Armin Rozsa,
IDG Research Services

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

Grafik:
Patrick Birnbreier, München

Lektorat:
Dr. Renate Oettinger, München

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