techconsult
TECHNOLOGY MARKET ANALYSTS

EIN UNTERNEHMEN DER heise group

CSaaS in Deutschland

Cyber Security as a Service in der Praxis

Wie deutsche Unternehmen eine ganzheitliche IT-Security mithilfe von CSaaS gewährleisten

Unterstützt durch

SOPHOS

Informationen zur Studie

Erstellung durch
techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de
Tel.: +49 561 8109 0
Fax: +49 561 8109 101
Web: www.techconsult.de

Erscheinungsjahr
2023

Autor
Ercan Hayvali

techconsult TECHNOLOGY MARKET ANALYSTS | EIN UNTERNEHMEN DER heise group

In Zusammenarbeit mit

SOPHOS

Kontakt

Gustav- Stresemann-Ring 1
65189 Wiesbaden
Telefon: +49 800 2782761

Mehr erfahren

Sonstige Informationen
Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Inhaltsverzeichnis

Einleitung 4

Fachkräftemangel erschwert IT-Security 5

Unternehmen setzen auf Security as a Service 7

Agilität durch CSaaS 9

Strategische Ausrichtung der Security 10

Verschärfung der Bedrohungslage 11

Fazit 13

Studiendesign und Stichprobe 14

Weitere Informationen 15

Einleitung

Für Unternehmen ist die IT-Security in den letzten Jahren zu einem erfolgskritischen Faktor geworden. Nicht nur die voranschreitende digitale Transformation, sondern auch die zunehmende Vernetzung der IT-Infrastrukturen machen es Cyberkriminellen einfach, neue Angriffsvektoren zu identifizieren und Unternehmen anzugreifen. Diese Bedrohungen sind nicht nur vielfältig, sondern auch stetig im Wandel, was Unternehmen vor neue Herausforderungen stellt. Dennoch scheuen viele Unternehmen finanziellen und personellen Aufwand zur Modernisierung der IT-Security. Denn für einen allumfassenden IT-Security-Ansatz müssen dabei nicht nur moderne technische Systeme implementiert werden, sondern auch ausreichend Security-Personal vorhanden sein.

Diese Notwendigkeit wird durch die vorherrschende Angriffsintensität unterstrichen: So wurden 67 Prozent der befragten Unternehmen in den vergangenen 24 Monaten Opfer von Cyberangriffen, von denen 14 Prozent erfolgreich waren.

Dabei kann Cyber Security as a Service (CSaaS) als extern bezogene Leistung einen großen Teil der sicherheitsrelevanten Aspekte übernehmen und den Schutz der IT-Infrastruktur gewährleisten. Doch welche Gründe sprechen für den Einsatz von CSaaS und wie viele Unternehmen setzen derartige Services ein? Welche Herausforderungen im Bereich IT-Security lassen sich gegenwärtig identifizieren und wie gehen Unternehmen mit den Gefahren um? Wie planen Unternehmen eine langfristige IT-Security sicherzustellen und welche Maßnahmen werden dabei fokussiert?

Die vorliegende Studie zielt darauf ab, den aktuellen Stand der IT-Sicherheit in Unternehmen unterschiedlicher Branchen und Größen zu analysieren.

Dabei werden sowohl der vorherrschende Fachkräftemangel als auch die ergriffenen Maßnahmen und Strategien beleuchtet.

Zudem sollen die Sicherheitsansätze untersucht werden, die Unternehmen ergreifen, um in dieser dynamischen und oft herausfordernden Umgebung geschützt zu bleiben.

Abschließend soll ein tiefgreifender Einblick in die Prioritäten, Bedenken und Investitionen von Unternehmen im Bereich IT-Sicherheit gegeben werden.

Als Datengrundlage dient eine Befragung mit 200 IT-Verantwortlichen und -Entscheidern aus deutschen Unternehmen mit 100 bis 999 Beschäftigten.

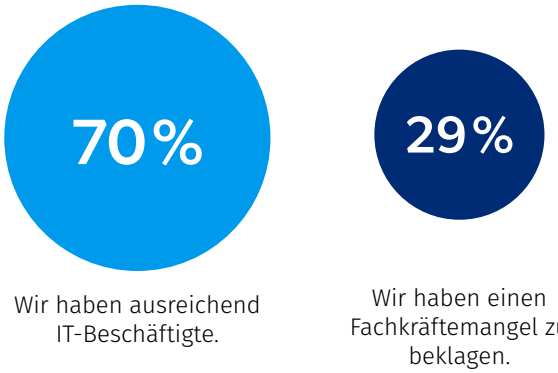
Fachkräftemangel erschwert IT-Security

In Anbetracht der zunehmenden Komplexität von Cyberbedrohungen wird es immer wichtiger, über qualifiziertes IT-Personal zu verfügen. Denn die IT-Sicherheit eines Unternehmens ist entscheidend für den Erfolg und die Wettbewerbsfähigkeit. Dennoch können hier deutliche Defizite bei Unternehmen beobachtet werden. So geben 29 Prozent der befragten IT-Verantwortlichen an, dass sie nicht über ausreichend IT-Beschäftigte verfügen, um einen allumfänglichen Schutz ihrer IT-Infrastruktur gewährleisten zu können; im Umkehrschluss berichten 70 Prozent der Verantwortlichen, dass sie über ausreichend IT-Personal verfügen. Diese Verteilung lässt sich dabei über alle Größenklassen hinweg beobachten, was darauf hindeutet, dass unabhängig von der Unternehmensgröße ein generelles Problem in Bezug auf den Mangel an IT-Sicherheitsexperten besteht.

Es zeigen sich jedoch deutliche branchenspezifische Unterschiede in Bezug auf den Fachkräftemangel in der IT. Während 43 Prozent der Banken und Versicherungen sowie 42 Prozent der Industrieunternehmen von einem solchen Mangel berichten, ist der Anteil im Industriesektor mit 23 Prozent und im Handel mit lediglich neun Prozent deutlich geringer.

Mangel an IT-Fachkräften

Basis: 200 Unternehmen | Weiß nicht/Keine Angabe: 1 %

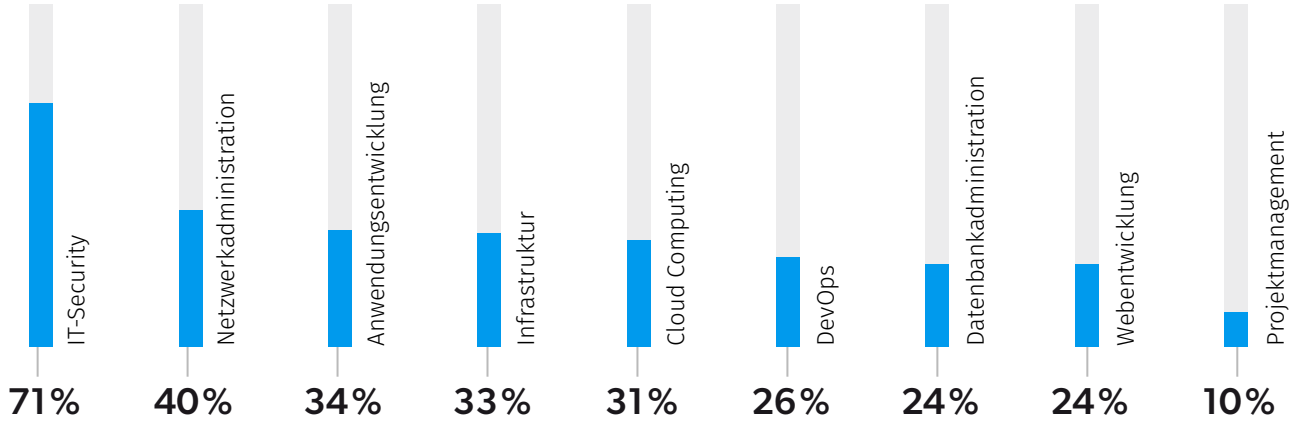


Insbesondere Branchen mit sensiblen Daten sind häufiges Ziel von gezielten und hochspezialisierten Cyberangriffen. Diese Sektoren benötigen daher spezialisiertes Personal für die IT-Security, welches neben dem technischem Know-how auch mit den branchenspezifischen Risiken und Anforderungen vertraut ist.

71 Prozent der Fachkräfte fehlen im Bereich IT-Security und 40 Prozent in der Netzwerkadministration.

Bereiche mit Mangel an IT-Fachkräften

Basis: 58 Unternehmen | Mehrfachauswahl möglich | Filter: Fachkräftemangel



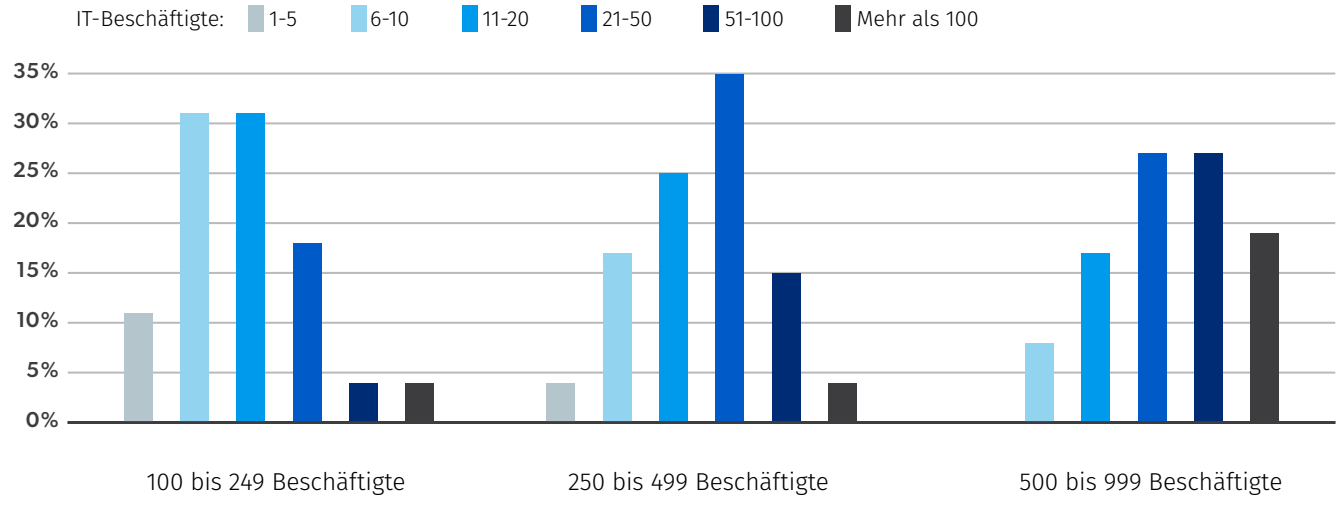
Der Mangel an IT-Beschäftigten betrifft dabei viele unterschiedliche Bereiche im Unternehmen. So fehlen in 71 Prozent der Unternehmen, die ein Fachkräftemangel in ihrer IT verzeichnen, Beschäftigte speziell für die IT-Security.

Dieser Mangel unterstreicht die Herausforderung für Unternehmen, mit der rasanten Entwicklung von Cyberbedrohungen Schritt zu halten und ihre IT-Infrastruktur bestmöglich zu schützen. Zudem fehlen in 40 Prozent der Unternehmen Beschäftigte für die Netzwerkadministration und in mehr als einem Drittel (35 Prozent) besteht Bedarf an Experten in der Anwendungsentwicklung, insbesondere in Java und Python. So wird deutlich, dass der Fachkräftemangel nicht nur auf den Bereich der IT-Security beschränkt ist, sondern sich über verschiedene IT-Disziplinen erstreckt.

Dabei kann die Größe des IT-Teams ein entscheidender Faktor für die Fähigkeit eines Unternehmens sein, sich gegen Cyberangriffe schützen und eine effiziente IT-Infrastruktur gewährleisten zu können. Bei mehr als einem Viertel der befragten Unternehmen (27 Prozent), die über ausreichend IT-Personal verfügen, wird die IT-Infrastruktur von 21 bis 50 und bei 24 Prozent von 11 bis 20 IT-Beschäftigten verwaltet. Somit wird deutlich, dass mit der Unternehmensgröße auch die Anzahl der für die IT zuständigen Beschäftigten tendenziell zunimmt.

IT-Mitarbeiter für operative IT-Tätigkeiten

Basis: 141 Unternehmen | Filter: Fachkräftemangel vorhanden



Unternehmen setzen auf Security as a Service

Für einen allumfassenden Cybersecurity-Ansatz müssen Unternehmen über spezialisiertes IT-Personal verfügen, das sich jederzeit um die Sicherheit der IT-Infrastruktur kümmert. Im Falle von IT-Personalmangel bietet Cyber Security as a Service (CSaaS) einen effizienten Ansatz, eine umfassende IT-Security ohne internes Personal sicherzustellen. Somit kann CSaaS den Unternehmen ermöglichen, von der Expertise spezialisierter Sicherheitsexperten zu profitieren und den Schutz ihrer IT-Infrastruktur bestmöglich zu gestalten.

45 Prozent der Unternehmen setzen gegenwärtig auf Cyber Security as a Service (CSaaS).

In der vorliegenden Studie wird deutlich, dass viele Unternehmen bereits die Vorteile dieses Service-Modells erkannt haben. So beziehen bereits 45 Prozent der befragten Unternehmen CSaaS, wobei dieser Anteil bei den Banken und Versicherungen (71 Prozent) besonders ausgeprägt ist. Darüber hinaus tendieren Unternehmen mit einer Größe von 500 bis 999 Mitarbeitern (51 Prozent) stärker zur Nutzung von CSaaS im Vergleich zu Unternehmen, die zwischen 100 und 249 Beschäftigte haben (45 Prozent).

Die Top 5-Gründe gegen den Einsatz von CSaaS

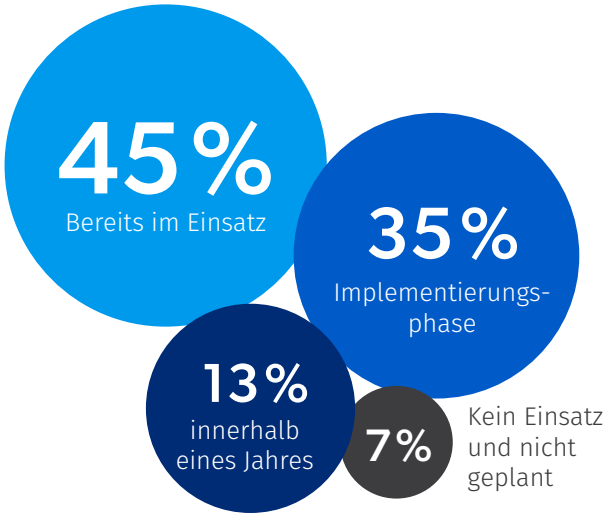
Basis: 14 Unternehmen | Mehrfachauswahl möglich

- **43 %** Kein Bedarf, da unsere IT-Infrastruktur vollständig abgesichert ist
- **36 %** Sehen keine Vorteile gegenüber unserer vorhandenen Infrastruktur
- **36 %** Hohe Abhängigkeit von externen Dienstleister
- **29 %** Bedenken hinsichtlich der Integration mit bestehenden Systemen und Prozessen
- **29 %** Bedenken hinsichtlich der Sicherheit und Vertraulichkeit von sensiblen Daten

Von den befragten Unternehmen, die CSaaS nicht nutzen, führen 43 Prozent eine bereits umfassend gesicherte IT-Infrastruktur als Grund an. Weitere 36 Prozent sehen keinen Mehrwert im Vergleich zu ihrer bestehenden Infrastruktur, während ebenfalls 36 Prozent Bedenken hinsichtlich einer hohen Abhängigkeit von externen Dienstleistern äußern.

Einsatz von Cyber Security as a Service

Basis: 200 Unternehmen



Durch Cyber Security as a Service kann die IT-Infrastruktur nicht nur reaktiv, sondern auch proaktiv gegen mögliche und wahrscheinliche Angriffe geschützt werden. Somit ist proaktives Threat Hunting mit entsprechender Reaktion auf Vorfälle eine optimale Ergänzung zu technischen IT-Security-Maßnahmen. Angesichts dieser Vorteile ist es nicht verwunderlich, dass sich mehr als ein Drittel der befragten Unternehmen (35 Prozent) gegenwärtig in der Implementierung von CSaaS befinden und dass weitere 13 Prozent den Einsatz in den nächsten 12 Monaten planen.

Hier wird deutlich, dass viele Unternehmen aktiv in die Modernisierung ihrer IT-Security-Infrastrukturen investieren und die Vorteile von CSaaS nutzen möchten.

45 Prozent der Unternehmen beziehen bzw. möchten CSaaS beziehen, um ihre IT-Infrastruktur 24/7 zu überwachen.

Dabei spielen unterschiedliche Faktoren bei der Entscheidung für den Einsatz von Security-Services eine Rolle. In der vorliegenden Studie wurden die zentralen Beweggründe identifiziert, die Unternehmen zum Einsatz oder zur geplanten Implementierung von CSaaS bewegen. Für 45 Prozent der befragten IT-Verantwortlichen der Unternehmen liegt dabei die 24/7-Überwachung an der Spitze der Gründe für CSaaS. Dies unterstreicht den Bedarf an kontinuierlicher IT-Sicherheit, da Bedrohungen nicht an Geschäftszeiten gebunden sind.

Damit einhergehend stellt die steigende Komplexität von IT-Sicherheitsrisiken für 41 Prozent der Unternehmen einen wichtigen Grund für den Einsatz von CSaaS dar. So werden IT-Infrastrukturen mit immer komplexer werdenden Sicherheitslücken und Angriffsvektoren konfrontiert und müssen mit diesen umgehen. Dies führt zwangsläufig zur Notwendigkeit von präventiven IT-Sicherheitsstrategien, welche von 40 Prozent der befragten IT-Verantwortlichen als Grund für CSaaS genannt werden.

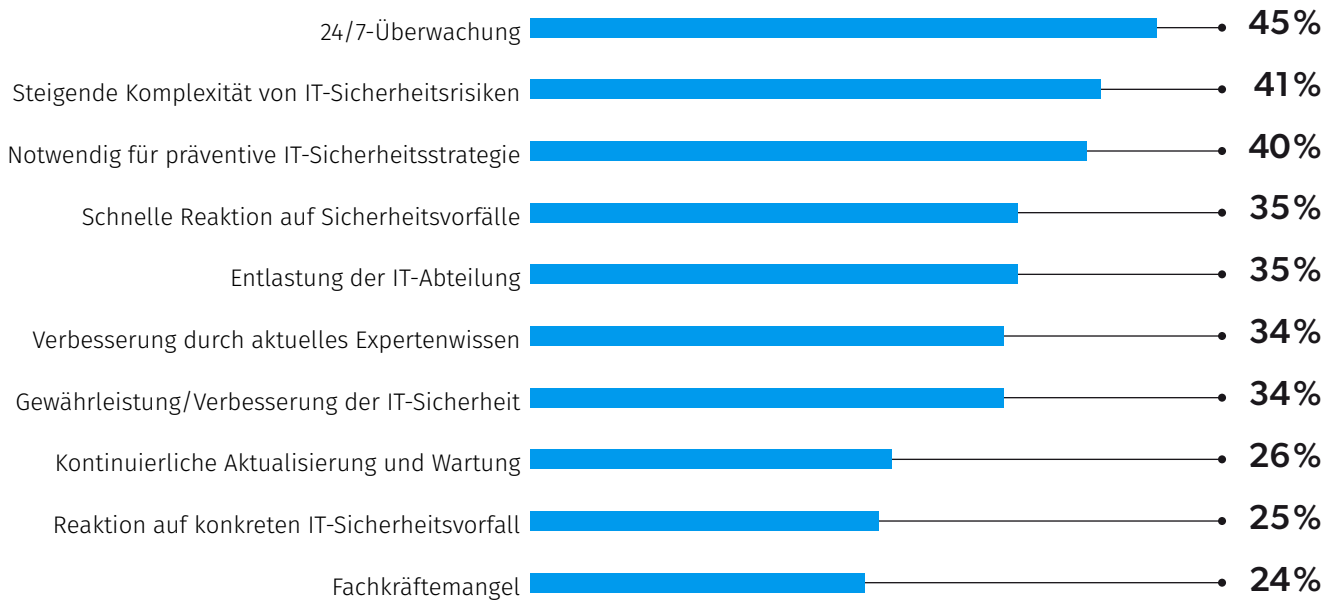
Hier wird ein Wandel von reaktiven Security-Ansätzen zu einem proaktiven Vorgehen sichtbar. Durch proaktives Threat Hunting und das frühzeitige Erkennen potenzieller Risiken können Unternehmen häufig Sicherheitsverletzungen abwenden, noch bevor diese tatsächlich eintreten. Somit möchten Unternehmen nicht nur eine schnelle Reaktion auf Sicherheitsvorfälle (35 Prozent) sicherstellen, sondern auch eine Entlastung der IT-Abteilung (35 Prozent) gewährleisten.

25 Prozent der Unternehmen beziehen bzw. möchten CSaaS aufgrund eines vorangegangenen Sicherheitsvorfalls beziehen.

Zudem hat jedes vierte befragte Unternehmen (25 Prozent) CSaaS nach einem spezifischen Sicherheitsvorfall implementiert. Als Resultat verzeichneten 70 Prozent dieser Unternehmen eine signifikante Verbesserung ihrer IT-Sicherheit und konnten seither keine weiteren Sicherheitsvorfälle feststellen. Insgesamt wird deutlich, dass externe Cybersecurity-Leistungen vor Sicherheitsvorfällen schützen und die internen Teams unterstützen und ergänzen können.

Gründe für den Einsatz von Cyber Security as a Service – Top 10

Basis: 200 Unternehmen | Mehrfachauswahl möglich



Agilität durch CSaaS

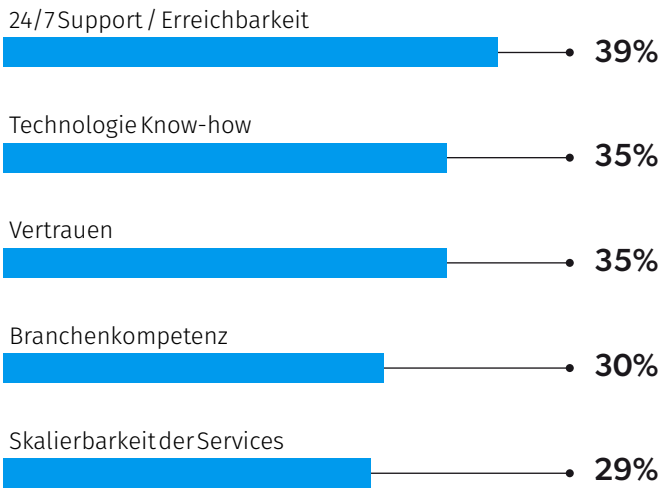
In der sich ständig wandelnden Landschaft der Cybersicherheit ist es von entscheidender Bedeutung, dass Unternehmen schnell und effizient auf Sicherheitsbedrohungen reagieren können. Cyber Security as a Service (CSaaS) bietet Unternehmen genau diese Agilität, um den vielfältigen und ständig wechselnden Bedrohungen entgegenzuwirken. So geben nur 12 Prozent der Befragten an, während des Einsatzes von CSaaS keinen IT-Sicherheitsvorfall erlebt zu haben. Das bedeutet, dass 88 Prozent der Unternehmen während ihrer Nutzung von CSaaS mit Sicherheitsvorfällen konfrontiert wurden. Dabei berichten 52 Prozent dieser Unternehmen, dass sie durch CSaaS in der Lage waren, die Sicherheitsvorfälle frühzeitig zu erkennen. So wird deutlich, dass Cyber Security as a Service Unternehmen ermöglichen, Bedrohungen proaktiv zu identifizieren. Darüber hinaus konnten 46 Prozent der Unternehmen schnell auf die Gefahrenlage reagieren und in ihre normalen Betriebsprozesse übergehen. Die Vorteile von CSaaS zeigen sich zudem in der Tatsache, dass 45 Prozent der Befragten von einem Zugriff auf spezialisiertes Fachwissen und fortschrittliche Technologien profitieren. Ebenfalls 45 Prozent hoben die bessere Isolierung und Verhinderung weiterer Schäden hervor, während 42 Prozent eine gesteigerte Effizienz bei der Reaktion und Behebung von Vorfällen betonten.

Nachdem die direkten Auswirkungen von CSaaS auf die Erkennung und Reaktion auf Sicherheitsvorfälle beleuchtet wurden, ist es ebenso relevant, die Auswahlkriterien für solche Dienstleistungen zu betrachten. So zeigt sich, dass 39 Prozent der Unternehmen den 24/7-Support als primären Faktor bei der Beschaffung von CSaaS-Diensten sehen. Dies unterstreicht die Notwendigkeit für Unternehmen, ständig auf potenzielle Sicherheitsbedrohungen reagieren zu können. Vertrauen in den Dienstleister und das Technologie-Know-how sind ebenfalls zentrale Faktoren, die von jeweils 35 Prozent der befragten IT-Verantwortlichen hervorgehoben werden. Dies spiegelt die Bedeutung von Vertrauenswürdigkeit und Expertise in einem so kritischen Bereich wie der Cybersicherheit wider.

Darüber hinaus legen 30 Prozent der befragten IT-Verantwortlichen Wert auf die Branchenkompetenz des Serviceproviders. So sollten die CSaaS-Provider nicht nur über allgemeines Wissen im Bereich Cybersicherheit verfügen, sondern auch branchenspezifische Herausforderungen und Anforderungen verstehen. Zudem legen 29 Prozent der befragten IT-Verantwortlichen Wert auf die Skalierbarkeit der Dienste, sowohl technisch als auch kommerziell. So suchen Unternehmen nach flexiblen Lösungen, die mit ihren wachsenden Anforderungen und sich ändernden Geschäftslandschaften mithalten können.

Darauf achten IT-Verantwortliche bei CSaaS - Top 5

Basis: 200 Unternehmen | Mehrfachauswahl möglich



Die Gesamtergebnisse verdeutlichen, dass Unternehmen bei der Auswahl von CSaaS-Diensten nicht nur technische Expertise und permanente Verfügbarkeit priorisieren, sondern auch auf Flexibilität, Branchenkenntnisse und Vertrauenswürdigkeit achten. Diese Kriterien spiegeln die zunehmenden und vielfältigen Anforderungen an Cybersicherheitslösungen in der heutigen digitalen Geschäftswelt wider.

Strategische Ausrichtung der Security

Ein Security Operations Center (SOC) stellt in der modernen IT-Landschaft einen Kernbestandteil proaktiver Sicherheitsstrategien dar. Es fungiert als zentrale Einheit, die sich auf die Erkennung, Analyse und Reaktion auf Sicherheitsvorfälle konzentriert. Dies minimiert das Risiko von Sicherheitsverstößen und stellt sicher, dass Unternehmen ihre geschäftskritischen Prozesse und Daten schützen.

Die vorliegenden Ergebnisse machen deutlich, dass die Mehrheit der Unternehmen die Vorteile eines SOCs erkannt und entsprechende Maßnahmen umgesetzt haben. So sind in fast drei von vier Unternehmen (73 Prozent) Security Operations Center aktiv im Einsatz, um eine effiziente Bedrohungsanalyse sicherstellen zu können. Dabei setzen 41 Prozent auf externe SOC-Services von Dienstleistern, während lediglich 32 Prozent ihre SOCs intern betreiben. Trotz dieser positiven Tendenz verzichten fast ein Viertel der Unternehmen (24 Prozent) auf ein SOC und drei Prozent können dahingehend keine Angaben machen. Doch welche zusätzlichen Maßnahmen sehen Unternehmen als erforderlich an, um die IT-Security zu optimieren?

Maßnahmen zur Optimierung der IT-Security

Basis: 200 Unternehmen | Mehrfachauswahl möglich

- **49%** Ganzheitliches IT-Sicherheitskonzept (z.B. Multi-Layer, Zero Trust)
- **49%** Stärkere Sensibilisierung der Mitarbeiter
- **42%** Größeres IT-Security-Budget
- **42%** Auslagerung der IT-Sicherheit mithilfe von Cyber Security as a Service
- **29%** Einsatz ergänzender Security-Lösungen
- **14%** Einbeziehen von externen Experten

Hinsichtlich der Optimierung der IT-Sicherheit sieht fast jedes zweite Unternehmen (49 Prozent) die Mitarbeitersensibilisierung als essenziellen Faktor an. So müssen die Beschäftigen über potenzielle Sicherheitsrisiken aufgeklärt und ein optimales Verhalten sichergestellt werden. Gleichzeitig betonen 49 Prozent der befragten Unternehmen die Bedeutung eines ganzheitlichen IT-Sicherheitskonzepts.

Ein derartiges Konzept sollte fortschrittliche Ansätze integrieren wie die Multi-Layer-Sicherheit, die verschiedene Abwehrmechanismen auf unterschiedlichen Ebenen vorsieht sowie das Zero-Trust-Prinzip, welches grundsätzlich keinem Zugriff vertraut und stets Verifizierungen erfordert.

42 Prozent der Unternehmen sehen die Auslagerung der IT-Sicherheit mithilfe von Cyber Security as a Service als Maßnahme zur Optimierung der IT-Security.

Eine weitere mögliche Maßnahme zur Verbesserung der IT-Security ist die Auslagerung von Sicherheitsdienstleistungen. So sehen 42 Prozent der befragten Unternehmen die Auslagerung der IT-Security durch Cyber Security as a Service als Mittel, um ihre Sicherheitsinfrastruktur zu stärken und aktuelle Herausforderungen effizienter zu bewältigen. Als weitere Maßnahmen werden größere IT-Budgets (42 Prozent), Einsatz ergänzender Security-Lösungen (29 Prozent) sowie das Einbeziehen von externen Experten (14 Prozent) genannt. Insgesamt zeigt sich, dass Unternehmen die strategische Relevanz einer robusten Sicherheitsinfrastruktur erkennen und in entsprechende Lösungen und Bildungsmaßnahmen investieren, um sich gegen die stetig wachsenden Cyberbedrohungen zu wappnen.

Verschärfung der Bedrohungslage

Die digitale Landschaft entwickelt sich ständig weiter, und mit ihr ändert sich auch die Bedrohungslage durch Cyberangriffe. Mehr als die Hälfte der befragten Unternehmen (53 Prozent) erwartet in den kommenden Jahren eine deutliche Zunahme der Cyberbedrohungen, während 43 Prozent glauben, dass das aktuelle Niveau an Cyberangriffen konstant bleiben wird.

Lediglich fünf Prozent der Befragten gehen davon aus, dass die Anzahl der Angriffe abnehmen wird. Insgesamt verdeutlichen diese Erfahrungen das steigende Bewusstsein für Cybersicherheitsrisiken und die Notwendigkeit, ständig wachsam und vorbereitet zu sein, um sich gegen zukünftige Bedrohungen zu schützen.

53 Prozent der Unternehmen erwarten eine deutliche Anspannung der Bedrohungslage.

Zusätzlich dazu lässt sich ein positiver Trend im Bereich der Cyberversicherungen beobachten. Bereits 85 Prozent der Unternehmen haben proaktiv eine Cyberversicherung abgeschlossen, um sich gegen finanzielle Risiken von Sicherheitsvorfällen abzusichern.

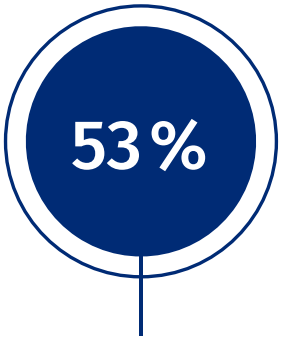
Bemerkenswert ist, dass die Hälfte dieser versicherten Unternehmen (50 Prozent) innerhalb der letzten 12 Monate bessere Konditionen aushandeln konnte, nachdem sie ihre Sicherheitsmaßnahmen verstärkt haben. Dennoch bleibt eine Minderheit von 10 Prozent der Befragten, die sich gegen Cyberangriffe noch nicht versichert haben.

70 Prozent der Unternehmen sind der Ansicht, dass die Sicherheit ihrer IT-Systeme mittel- bis langfristig externen Sicherheitsdienstleistern anvertraut werden sollte.

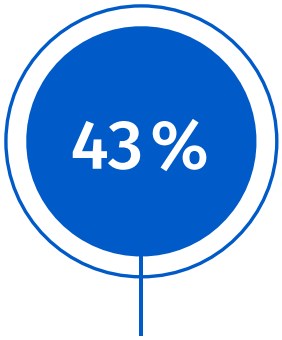
Zusätzlich zu Cyberversicherungen setzen Unternehmen auf verschiedene Strategien, um ihre IT-Sicherheit zu gewährleisten. So sind rund 70 Prozent der befragten IT-Verantwortlichen der Ansicht, dass die Sicherheit ihrer IT-Systeme mittel- bis langfristig externen Sicherheitsdienstleistern anvertraut werden sollte.

Entwicklung der Bedrohungslage durch Cyberangriffe

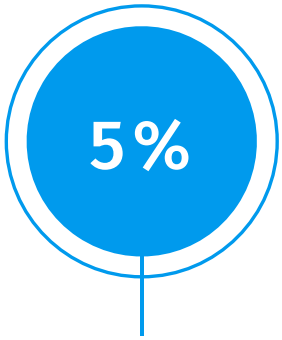
Basis: 200 Unternehmen



Wir erwarten eine deutliche Anspannung der Bedrohungslage.



Wir glauben, dass die Häufigkeit von Cyberangriffen unverändert bleibt.



Wir erwarten ein Absinken der Cyberangriffe.

Dies ist ein Zeichen dafür, dass die interne Expertise oder Ressourcen oft als unzureichend empfunden werden, um den ständig wachsenden und sich verändernden Bedrohungen gerecht zu werden. Zusätzlich dazu setzen 60 Prozent der Befragten auf technologiegetriebene Sicherheitslösungen, die durch verhaltensbasierte Erkennungsmethoden und künstliche Intelligenz (KI) ergänzt werden. Diese Kombination ermöglicht eine präzisere und proaktive Bedrohungserkennung. Trotz dieser fortschrittlichen Ansätze gibt es auch Bedenken. So sind 57 Prozent der Befragten der Meinung, dass präventive Maßnahmen allein nicht ausreichen, um zukünftige Cyberangriffe abzuwehren. Alarmierend ist jedoch auch, dass ebenfalls 57 Prozent zugeben, erst nach einem tatsächlichen Sicherheitsvorfall in umfassende Sicherheitsmaßnahmen zu investieren. Ein reaktiver Security-Ansatz, bei dem Maßnahmen erst nach einem Sicherheitsvorfall ergriffen werden, kann langfristige Schäden verursachen und die Unternehmensreputation gefährden.

74 Prozent der Unternehmen können mit Cyber Security as a Service Compliance-Anforderungen erfüllen.

Abschließend dazu sehen Unternehmen auch einen weiteren positiven Aspekt von CSaaS im Bereich der Compliance. So sehen drei Viertel der Unternehmen (74 Prozent) in CSaaS eine Möglichkeit, Compliance-Anforderungen zu erfüllen, was auf die wachsende Anerkennung dieser Dienstleistung als effektives und regelkonformes Sicherheitsinstrument hinweist. Somit wird insgesamt deutlich, dass die Unternehmen eine wachsende Bedrohung durch Cyberangriffe erkennen und die Vorteile von CSaaS anerkennen.

Fazit

Im Zuge der Digitalisierung sind Unternehmen verstärkt den Bedrohungen durch Cyberkriminelle ausgesetzt. Die vorliegenden Erkenntnisse machen deutlich, dass IT-Sicherheit für Unternehmen nicht nur eine technische, sondern auch eine strategische Bedeutung hat. Die Auswirkungen eines erfolgreichen Cyberangriffs können weit über monetäre Schäden hinausgehen und den Ruf eines Unternehmens schaden. Angesichts des wachsenden Fachkräftemangels im Bereich IT-Sicherheit sind Unternehmen dringend gefordert, innovative und moderne Security-Lösungen zu implementieren und diese mit Cyber Security as a Service anzureichern, um den Bedrohungen zu begegnen. Das Bewusstsein für die Relevanz von Mitarbeiterschulungen und einem integrierten IT-Sicherheitsansatz wächst kontinuierlich. Dennoch sind reaktive Sicherheitsansätze noch weit verbreitet. Überraschenderweise scheuen viele Unternehmen immer noch den finanziellen und personellen Aufwand für moderne IT-Security, oft mehr aus Furcht vor der Umsetzung und den damit verbundenen Kosten als vor dem eigentlichen Angriff selbst.

So bietet CSaaS Unternehmen zahlreiche Vorteile, darunter eine konstante Überwachung der IT-Systeme, Zugang zu Expertenwissen und modernsten Technologien sowie die Möglichkeit, rasch auf sicherheitsrelevante Vorfälle zu reagieren. Vor allem für Unternehmen, die intern nicht über die nötigen Ressourcen oder Kenntnisse verfügen, stellt CSaaS einen strategischen Mehrwert dar. Dabei bietet es eine Anpassungsfähigkeit, die es Unternehmen ermöglicht, ihre Sicherheitsstrategien dynamisch an die ständig wechselnde Bedrohungslandschaft anzupassen. Aufgrund dessen greifen viele Unternehmen nach Cybervorfällen zu CSaaS, um proaktiv weitere Angriffe zu verhindern.

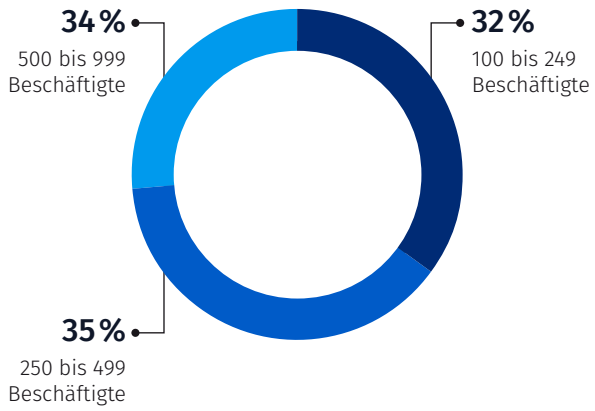
Insgesamt ist es von entscheidender Bedeutung, dass Unternehmen den Fokus nicht allein auf moderne technologische Lösungen legen. Die Ausbildung und das Bewusstsein der Mitarbeiter, kombiniert mit einer umfassenden 24/7-Sicherheitsstrategie sind zentrale Säulen für einen strategischen IT-Sicherheitsansatz.

Studiendesign und Stichprobe

Die Studie „Cybersecurity as a Service in der Praxis“ wurde von der techconsult GmbH im Auftrag von Sophos konzipiert und durchgeführt. Als Datenbasis dient eine durchgeführte Befragung mit 200 deutschen Unternehmen mit 100 bis 900 Beschäftigten. Die Befragung erfolgte über einen Online-Fragebogen. Die Stichprobe umfasst Unternehmen aus allen Branchen ohne Einschränkungen. Ansprechpartner waren in erster Linie IT-Verantwortliche, IT-Entscheider sowie Entscheidungsträger für die IT-Security-Infrastruktur.

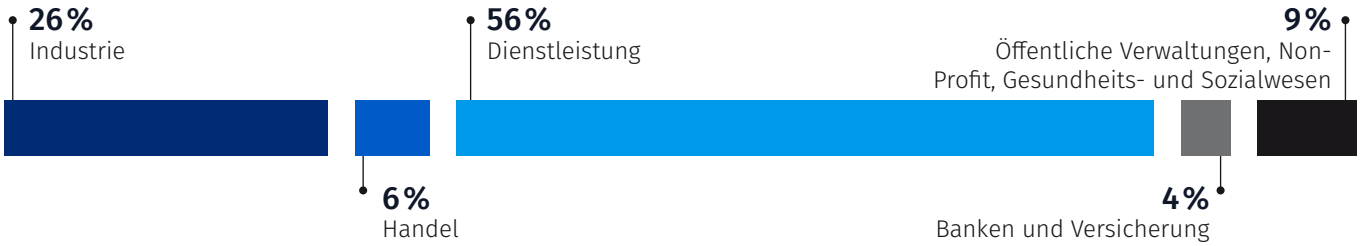
Größenklassenverteilung

Basis: 200 Unternehmen



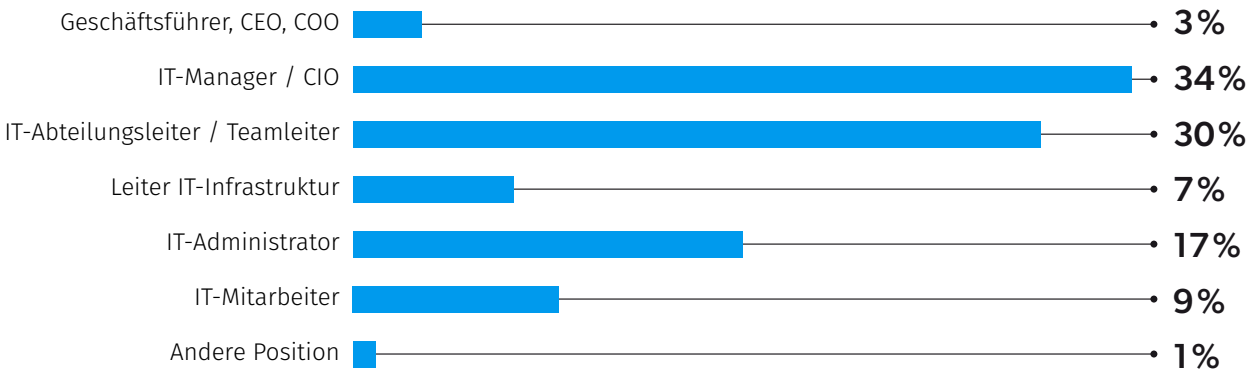
Branchenverteilung

Basis: 200 Unternehmen



Positionsverteilung

Basis: 200 Unternehmen



Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.

Weitere Informationen

Autor der Studie

Ercan Hayvali
Analyst

Telefon: +49 561 8109 178
E-Mail: ercan.hayvali@techconsult.de

Impressum

techconsult GmbH
Baunsbergstr. 37
D-34131 Kassel

Telefon: +49 561 8109 0
Fax.: +49 561 8109 101
Web: www.techconsult.de

Über techconsult GmbH

Seit über 30 Jahren ist techconsult - als Research- und Analystenhaus – ein verlässlicher Partner für Anbieter und Nachfrager digitaler Technologien und Services.

Mehr als 35.000 Interviews/Jahr mit Entscheidern, auf der Business- und Technologie-Ebene, Lösungsanwendern sowie Technologie- und Serviceanbietern, bilden die neutrale Grundlage unserer Beratungs- und Projektaktivitäten.

So werden Nachfrager in ihrer digitalen Standortbestimmung und strategischen Planung ebenso unterstützt, wie in konkreten Sourcing-Prozessen, um fundierte Entscheidungen auf Basis datengestützter Fakten zu treffen.

In der Entwicklung und Umsetzung individueller Go-To-Market-Strategien, profitieren Anbieter sowohl strategisch als auch taktisch von der marktorientierten Unterstützung unserer Analysten und des tc-Partnernetzwerks.

In Zusammenarbeit mit

SOPHOS

Kontakt

Gustav- Stresemann-Ring 1
65189 Wiesbaden
Telefon: +49 800 2782761

Mehr erfahren

Über Sophos

Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.

Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen. Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.

Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.

Weitere Informationen unter: www.sophos.de

Eine Studie von

techconsult
TECHNOLOGY MARKET ANALYSTS
EIN UNTERNEHMEN DER heise group

Impressum
techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de

Telefon: +49 561 8109 0
Telefax: +49 561 8109 101
Web: www.techconsult.de

Unterstützt durch

SOPHOS