FROST & SULLIVAN

Absicherung mittelständischer Unternehmen in Europa:

Aktuelle Lücken bei den Ausgaben für Cybersicherheit und der Budgetierung in verschiedenen Branchen

FROST & SULLIVAN WHITEPAPER

T-SECURITY

DER INHALT

Der aktuelle Stand der Cybersicherheit in mittelständischen Unternehmen in Europa

Unternehmen mit 250 oder mehr Beschäftigten sind für etwa ein Drittel aller Arbeitsplätze außerhalb des Finanzsektors in der Europäischen Union[1] und für fast die Hälfte der gesamten Wertschöpfung verantwortlich, obwohl sie nur weniger als 1% der Gesamtunternehmen ausmachen[2]. Für Cyberkriminelle besteht daher ein erheblicher Anreiz, diese Organisationen ins Visier zu nehmen, da erfolgreiche Versuche zu hohen Geldsummen führen können. Ransomware - ein beliebtes Mittel für Cyberkriminelle, um finanzielle Gewinne mit ihren Opfern zu erzielen - zeigt sehr prägnant die potenziellen finanziellen Risiken für Unternehmen auf. Zur Veranschaulichung: Die durchschnittlichen Kosten von Ransomware für Unternehmen sind von 2020 bis 2022 um den Faktor 5 gestiegen[3]. Für größere Unternehmen, die es sich leisten können, das Ransom zu bezahlen, kann dies einen Wert in Millionenhöhe haben.

Darüber hinaus sind 2022 weltweit mehr als 80% der Unternehmen Opfer von Cyberangriffen geworden. Die DACH-Region sowie Frankreich und die Niederlande, die in dieser Studie berücksichtigt werden, weisen eine überdurchschnittlich hohe Rate an potenziell gefährdeten Organisationen auf[4]. Der anhaltende Konflikt an der Ostgrenze Europas hat die Lage zusätzlich verschlimmert, da staatlich sanktionierte Akteure im Hintergrund daran arbeiten, die Netzwerke ihrer Gegner zu infiltrieren.

Regierungsbehörden auf der ganzen Welt haben die zunehmende Bedrohungslage zur Kenntnis genommen und arbeiten aktiv an der Aufklärung ihrer Bürger. In der Europäischen Union hat die Europäische Agentur für Cybersicherheit (ENISA) eine Ad-hoc-Arbeitsgruppe gebildet, um das Bewusstsein für Cybersicherheit zu schärfen, und hat zu diesem Zweck mehrere Kampagnen durchgeführt[5].

[1] Verteilung der Beschäftigung im nichtfinanziellen Sektor der gewerblichen Wirtschaft in den Ländern der Europäischen Union (EU27) im Jahr 2021, nach Unternehmensgröße; Statista; 2022

[2] Großunternehmen stellen etwas mehr als ein Drittel der Beschäftigung; Eurostat

[3] Der Zustand von Ransomware; Sophos; 2022

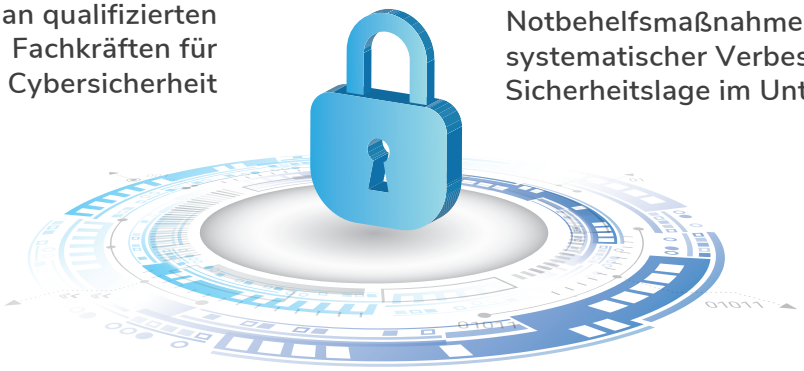
[4] 2022 Cyberthreat Defense Report; CyberEdge Group; 2022

[5] Ad-Hoc-Arbeitsgruppe zur Bewusstseinsbildung; ENISA; 2022

Trotz des wachsenden Bewusstseins für Cyber-Bedrohungen mangelt es den Unternehmen immer noch an der Fähigkeit, Cyber-Bedrohungen zu beseitigen, und zwar aus verschiedenen Gründen:

Mangel an qualifizierten Fachkräften für Cybersicherheit

Notbehelfsmaßnahmen statt systematischer Verbesserungen der Sicherheitslage im Unternehmen



Die Budgets für Cybersicherheit steigen nicht im Einklang mit der zunehmenden Bedrohungslage und der steigenden Zahl von Cybervorfällen

Dies gilt insbesondere für kleinere Unternehmen. Wie die Studie von Frost & Sullivan zeigt, verfügen mehr als 80% der mittelständischen Unternehmen nicht über eine eigene CISO-Position und ein separates Cybersicherheitsbudget innerhalb ihrer Organisation. Stattdessen werden Entscheidungen zur Cybersecurity- innerhalb der IT-Abteilung getroffen und Cybersecurity-Ausgaben sind Teil des größeren IT-Budgets. Da die IT-Budgets nicht mit der sich verändernden Bedrohungslandschaft mitwachsen, ergibt sich eine Unterdeckung bei den Ausgaben im Vergleich zu dem, was für die Aufrechterhaltung eines optimalen Cyberschutzes erforderlich ist.

Wie können Organisationen die idealen Ausgaben für Cybersicherheit ermitteln?

In diesem Papier schlüsselt Frost & Sullivan auf, wie die Ausgaben für Cybersicherheit derzeit getätigt werden und wie Unternehmen die idealen Ausgaben erreichen können. Welche Möglichkeiten gibt es, die Ausgaben europäischer mittelständischer Unternehmen in den Bereichen produzierendes Gewerbe, Automobilindustrie, Gesundheitswesen, , Einzelhandel und Dienstleistungen zu verbessern? In dieser Studie wurden die Länder Deutschland, Österreich, die Schweiz, die Niederlande und Frankreich berücksichtigt. Die empfohlenen Mindestausgaben für ein Unternehmen wurden in diesem Papier anhand der jährlichen Verlusterwartung (Annual Loss Expectancy - ALE) und des Gordon-Loeb-Modells, sowie anhand von Erkenntnissen aus Interviews mit CISOs. Zusätzlich wurde eine Umfrage mit 117 Teilnehmern aus den aufgeführten Branchen in fünf europäischen Ländern ermittelt. Branchentyp, Unternehmensgröße und durchschnittlicher Unternehmensumsatz waren die drei Hauptvariablen, die zur Formulierung der empfohlenen Mindestausgaben verwendet wurden. Dieses Papier soll somit als Leitfaden für eine optimale Verteilung des Cybersecurity-Kapitalaufwands (Capital Expenditure - CAPEX) für mittelgroße und mittelständische Unternehmen in Europa dienen.

Die empfohlenen Mindestausgaben für ein Unternehmen wurden in diesem Papier anhand der jährlichen Verlusterwartung (Annual Loss Expectancy - ALE) und des Gordon-Loeb-Modells sowie anhand von Erkenntnissen aus Interviews mit CISOs und einer Umfrage unter 117 Befragten aus der Branche in fünf europäischen Ländern ermittelt. Branchentyp, Unternehmensgröße und durchschnittlicher Unternehmensumsatz waren die drei Hauptvariablen, die zur Formulierung der empfohlenen Mindestausgaben verwendet wurden. Dieses Papier soll somit als Leitfaden für eine optimale Verteilung des Cybersecurity-Kapitalaufwands (Capital Expenditure - CAPEX)

Für die Zwecke dieser Studie, sind mittelgroße Unternehmen Organisationen mit 250 bis 1.000 Mitarbeitern und stellen den kleineren der beiden von Frost & Sullivan untersuchten horizontalen Märkte dar. Aufgrund ihrer Größe verfügen mittelgroße Unternehmen oft nicht über robuste Cybersicherheitsstrukturen und es fehlt ihnen oft an dediziertem Cybersicherheitspersonal in Schlüsselpositionen der Organisation. Kleinere Organisationen haben in der Regel weniger Spielraum bei ihren Budgets und konzentrieren sich eher auf vermeintlich geschäftskritische Systeme. Sie sind jedoch nur selten davon ausgenommen, Ziel von Cyberangriffen zu werden[6]

und müssen daher verstärkt aktive Maßnahmen ergreifen, um ihre Gefährdung durch potenzielle Cyberbedrohungen zu verringern.

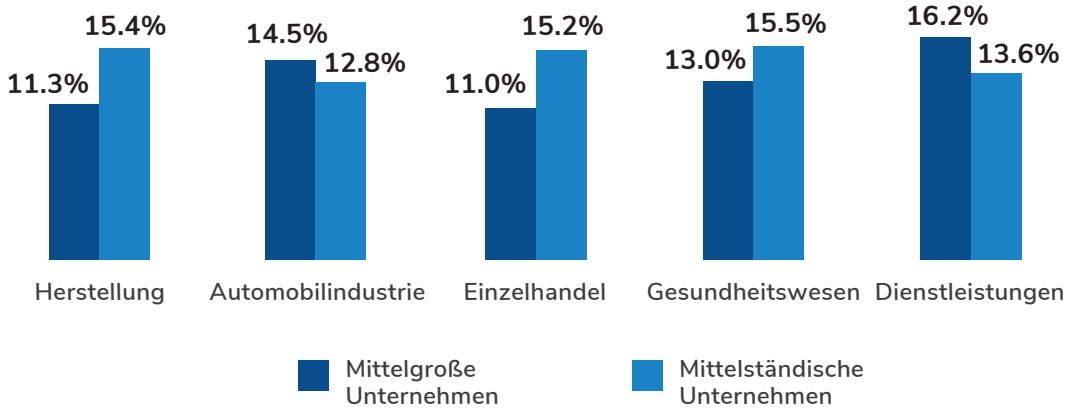
Mittelständische Unternehmen geben in der Regel zwischen 11-16% ihres gesamten IT-Budgets für Cybersicherheit aus. Die Analyse von Frost & Sullivan zu den empfohlenen Mindestausgaben zeigt, dass die Ausgaben für Cybersicherheit in mittelständischen Unternehmen im Durchschnitt 28% zu gering sind. Es wird erwartet, dass mittelständische Unternehmen ihre Ausgaben für Cybersicherheit um 5,4% gegenüber dem Vorjahr erhöhen werden, was die Lücke verringern wird, aber angesichts der sich verändernden Bedrohungslandschaft und der unterschiedlichsten Vektoren von Cyberangriffen müssen sie ihre Investitionen erheblich steigern, um die empfohlenen Mindestausgaben zu erreichen.

Laut einer Analyse von Frost & Sullivan zu den empfohlenen Ausgaben für Cybersicherheit geben mittelständische Unternehmen im Durchschnitt

28%

zu wenig für ihre Cybersicherheit aus.

EXHIBIT 1: Anteil der Cybersicherheit an den jährlichen IT-Ausgaben (%), mittlere und mittelständische Unternehmen



Source: Frost & Sullivan

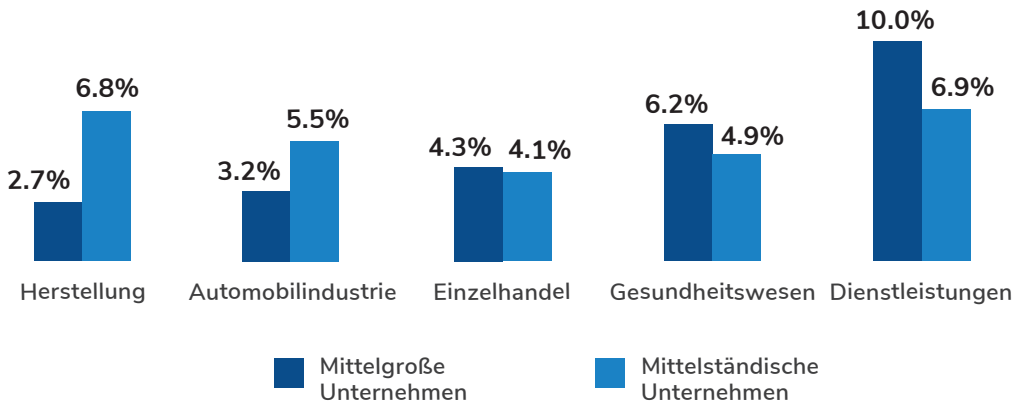
[6]Cybersecurity für KMU - Herausforderungen und Empfehlungen; ENISA; 2021

Mit ihren größeren Budgets und relativ anspruchsvolleren Organisationen schneiden mittelständische Unternehmen (definiert als Unternehmen mit 1.001 bis 5.000 Mitarbeitern) in Europa bei den Ausgaben für Cybersicherheit und der organisatorischen Sicherheitslage besser ab als kleinere (mittelgroße) Unternehmen. Obwohl sie bei weitem nicht überall anzutreffen sind, verfügen mittelständische Unternehmen im Allgemeinen eher über spezielle CISO-Positionen und separate Cybersicherheitsbudgets.

Obwohl sich die prozentualen Ausgaben für Cybersicherheit nicht allzu sehr von denen mittelgroßer Unternehmen unterscheiden (13-16%), ergibt sich in absoluten Zahlen ein erheblicher Unterschied, da sich die Höhe der IT-Budgets deutlich unterscheidet. Da die Kosten für Cybersicherheit jedoch nicht proportional zur Mitarbeiterzahl steigen, geben mittelständische Unternehmen in der Regel weniger pro Mitarbeiter aus als ihre Kollegen aus mittelgroßen Unternehmen. Mit einem erwarteten Wachstum der Cybersicherheitsausgaben von 5,6% gegenüber dem Vorjahr unternehmen mittelständische Unternehmen Schritte in die richtige Richtung, um ein optimales Cybersicherheitsbudget zu erreichen..

> Im Allgemeinen bedeutet dies, dass mittelgroße Unternehmen im Vergleich zum Mittelstand erheblich mehr für Cybersicherheit pro Mitarbeiter ausgeben.

EXHIBIT 2: Jährliches Wachstum der Ausgaben für Cybersicherheit (%)



Source: Frost & Sullivan

In den von Frost & Sullivan untersuchten Märkten liegen die Ausgaben für Cybersicherheit als Prozentsatz des Umsatzes je nach Größe und Branche zwischen 0,3-0,5% für mittelgroße Unternehmen und 0,2-0,4% für mittelständische Unternehmen.

Produzierendes Gewerbe

Mit dem Aufkommen der industriellen Revolution 4.0 wurden die einst getrennten Welten der Informationstechnologie (Information Technology - IT) und der Betriebstechnologie (Operational Technology - OT) zusammengeführt, um eine intelligente Fertigung und intelligente Maschinen zu schaffen. Die Konvergenz von IT und OT hat zwar neue Möglichkeiten für den Fertigungsbereich eröffnet, aber auch die Bedrohungslage für Unternehmen vergrößert, da die Bedrohungsvektoren sowohl auf IT- als auch auf OT-Ressourcen abzielen und sich horizontal im Netzwerk ausbreiten können.

Mittelgroße Unternehmen im produzierendem Gewerbe

Eine Möglichkeit für mittelgroße Unternehmen mit Produktion, sich gegen diese neue Bedrohung zu wappnen, ist der Einsatz von sicheren Identitäten. Indem sie darauf abzielen, Bedrohungen durch strenge Zugangskontrollen zu verhindern, können Unternehmen die Häufigkeit von Sicherheitsverletzungen in ihren hochentwickelten Systemen erheblich reduzieren. Sichere Identitäten werden von etwa 83% der mittelgroßen europäischen Hersteller eingesetzt. Im Gegensatz dazu Governance, Risk & Compliance (GRC) mit nur 13% am geringsten verbreitet.

> Trotz durchschnittlich größerer Cybersecurity-Teams ist der Mangel an qualifiziertem Cybersecurity-Personal immer noch eine große Herausforderung für mittelständische Hersteller, da die Bedrohungslandschaft und die Komplexität der Bedrohungen zunehmen.

Was die tatsächlichen Ausgaben betrifft, so gibt das durchschnittliche mittelgroße Produktionsunternehmen 26% zu wenig für die Aufrechterhaltung einer optimalen Cybersicherheit aus. Was die tatsächlichen Ausgaben anbelangt, so entfällt der größte Anteil der derzeitigen Ausgaben auf die Cyberabwehr, die aus Services zur Cyberabwehr, Threat Intelligence und Schwachstellenmanagement besteht. Ein weiterer bemerkenswerter Bereich ist der hohe Anteil der Ausgaben für professionelle Dienstleistungen. Dies ist darauf zurückzuführen, dass mittelgroße Unternehmen stärker auf externes Fachwissen angewiesen sind, da sie in der Regel keine vollwertigen internen Cybersicherheitsteams haben.

Das größte Wachstum im Jahr 2023 wird für mittelgroße Unternehmen im Bereich Industrie- und IoT-Sicherheit erwartet, da sie ihre Fähigkeiten zum Schutz ihrer mittlerweile miteinander vernetzten IT- und OT-Systeme weiter ausbauen. Dennoch müssen mittelgroße Produktionsunternehmen darüber nachdenken, wie sie mehr in Governance Risk und Compliance (GRC) investieren können, um ihre Cybersecurity-Governance-Fähigkeiten zu verbessern.

Der Mangel an qualifizierten Cybersicherheitsexperten innerhalb des Unternehmens ist der größte Einzelfaktor, der die Ausgaben mittelgroßer Produktionsunternehmen in die Höhe treibt. Dieser Mangel betrifft noch immer die meisten Branchen.

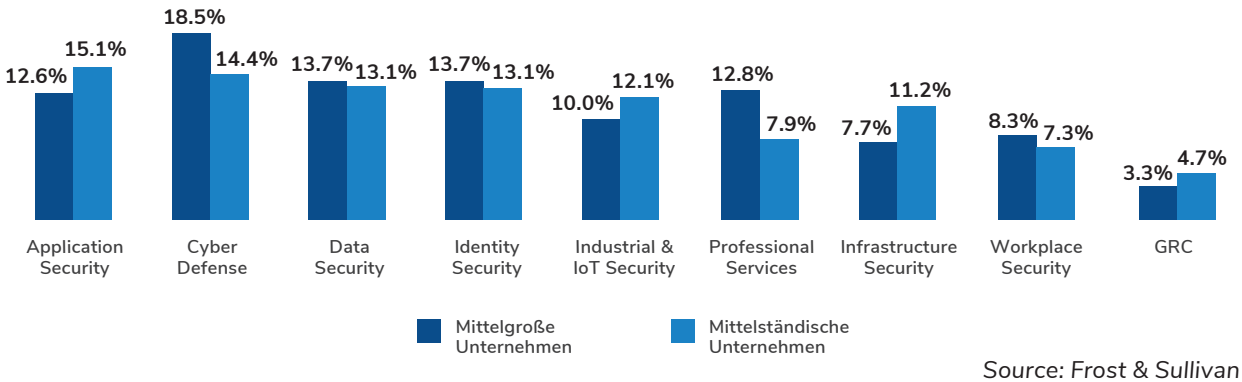
Mittelständische Produktionsunternehmen

Sichere Identitäten sind auch bei mittelständischen Produktionsunternehmen am stärksten verbreitet, während GRC das am wenigsten verbreitete Sicherheitsinstrument ist.

Im Durchschnitt geben mittelständische Produktionsunternehmen 25% weniger für ihre Cybersicherheitsmaßnahmen aus als von Frost & Sullivan empfohlenen. Mittelständische Produktionsunternehmen geben am meisten für die Applikationssicherheit aus, um die verschiedenen internen und externen Anwendungen vor dem Hintergrund der zunehmenden Einführung von Industrie 4.0 zu schützen. Wie bei den kleineren Unternehmen spiegeln die niedrigen Ausgaben für GRC das geringere Bewußtsein hierfür wider. Der prozentuale Anteil des Budgets, der für professionelle Dienstleistungen ausgegeben wird, ist bei den mittelständischen Produktionsunternehmen hingegen geringer, da sie einige der Fähigkeiten intern aufgebaut haben.

Trotz durchschnittlich größerer Cybersecurity-Teams ist der Mangel an qualifiziertem Cybersecurity-Personal immer noch eine große Herausforderung für mittelständische Unternehmen im Produktionsgewerbe, da die Bedrohungslandschaft und die Komplexität der Bedrohungen weiter zunehmen.

EXHIBIT 3: Gewichtung in % der Ausgaben für Cybersicherheit im verarbeitenden Gewerbe



Source: Frost & Sullivan

Automobilindustrie

Der Automobilsektor durchläuft parallel zum Produktionssektor eine IT/OT-Konvergenz. In der Regel sind die Automobilunternehmen in Europa bei der Einführung von Industrie 4.0-Technologien wie Cloud, Big Data und KI im Rückstand. Aufgrund ihrer veralteten Technologielandschaft und -architektur stehen die Automobilunternehmen selbst bei der Einführung von Cybersicherheit vor Herausforderungen.

Mittelgroße Automobilunternehmen

Es ist zu beobachten, dass die Datensicherheit bei den Automobilunternehmen aller Größenordnungen eine viel größere Durchdringung hat. (87,5% bei den mittelgroßen Unternehmen). Datensicherheit ist im Automobilsektor von entscheidender Bedeutung, da ein großer Teil des geistigen Eigentums, wie z. B. Fahrzeugdesigns, gefährdet ist.

Zweitens ähnelt die Akzeptanz von Industrie- und IoT-Sicherheit bei mittelgroßen Automobilherstellern (56%) derjenigen größerer Unternehmen in diesem Sektor, was auf ein hohes Bewusstsein für das Thema hinweist.

Wenn es um die Ausgaben geht, hat die Cyberabwehr bei den mittelgroßen Automobilunternehmen den größten Anteil an den Budgets, während GRC den geringsten Anteil ausmacht. Mittelgroße Automobilunternehmen geben im Durchschnitt 30% weniger als die empfohlenen Mindestausgaben für ihre Cybersicherheitsmaßnahmen aus.

Es wird erwartet, dass sich mittelgroße Automobilunternehmen im nächstenJahr auf den Ausbau ihrer Cyberabwehrkapazitäten konzentrieren werden. In Anbetracht der

Wenn es um die Ausgaben geht, hat die Cyberverteidigung bei den mittelgroßen Automobilunternehmen den größten Anteil an den Budgets, während GRC den geringsten Anteil ausmacht. Mittelgroße Automobilunternehmen geben im Durchschnitt 28% weniger als die empfohlenen Mindestausgaben für ihre Cybersicherheitsmaßnahmen aus.

aktuellen Ausgabenlücken sollten mittelständische Automobilunternehmen in Erwägung ziehen, mehr Mittel für die industrielle und IoT-Sicherheit bereitzustellen und gleichzeitig mehr für Governance Risk & Compliance (GRC) zu tun.

Die wichtigsten Faktoren, die zum erwarteten Anstieg der Ausgaben im nächsten Jahr beitragen, sind der Mangel an qualifizierten Cybersicherheitsressourcen und die zunehmende Nutzung von Clouddiensten. Es wird erwartet, dass die Ausgaben für Cybersicherheit bei mittelgroßen Automobilunternehmen mit 2% im Vergleich zum Vorjahr am wenigsten steigen, was in erster Linie auf die Herausforderungen bei der Erneuerung ihrer bestehenden On-Premise-Infrastruktur zurückzuführen ist.

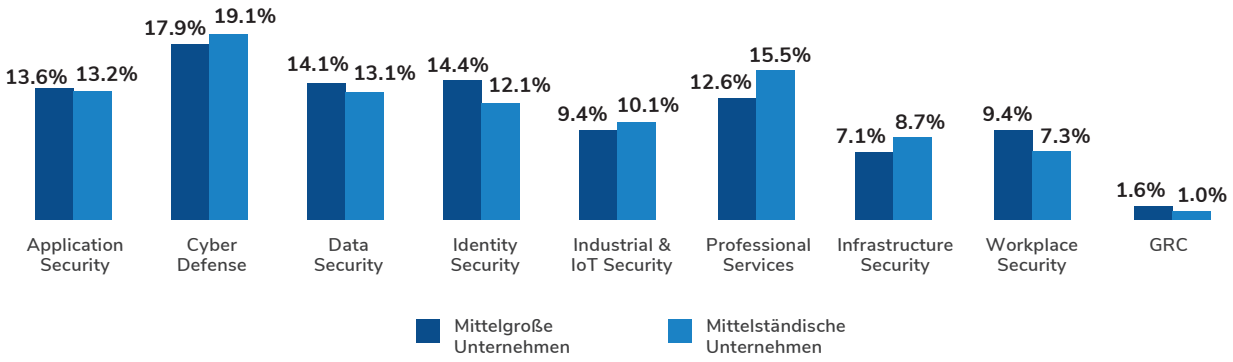
Mittelständische Automobilunternehmen

Neben der Datensicherheit weisen mittelständische Automobilunternehmen auch ein hohes Maß an Cyberabwehr, Applikationssicherheit und Arbeitsplatzsicherheit auf, was ihren höheren Entwicklungsstand im Bereich der Cybersicherheit unterstreicht.

Nach einer Analyse von Frost & Sullivan geben mittelständische Automobilunternehmen 26% zu wenig Geld für ihre Cybersicherheit aus. Der größte Anteil des Gesamtbudgets entfällt auf die Cyberabwehr, während nur 1% des Cybersicherheitsbudgets in GRC investiert wird. Mittelständische Automobilunternehmen investieren mehr in die Einführung von sicheren Identitäten, sowie Industrie- und IoT-Sicherheit, sollten aber auch einen größeren Teil ihrer Budgets für GRC bereitstellen.

Mittelständische Automobilunternehmen haben vor allem Herausforderungen hinsichtlich dem Mangel an qualifizierten Cybersecurityressourcen und den Schwierigkeiten bei der Einführung von Cloud-Diensten, die in den kommenden Jahren die Haupttreiber für höhere Cybersecurity-Ausgaben sind.

EXHIBIT 4: Gewichtung in % der Ausgaben für Cybersicherheit, Automobilindustrie



Source: Frost & Sullivan

Einzelhandel

Der Einzelhandel hat in den letzten drei Jahren eine umfassende Digitalisierung erlebt. Die Covid-19-Pandemie gab dem mobilen und elektronischen Handel einen mehrfachen Schub. Der Einzelhandel gehört zu den größten und schnellsten Anwendern von Cloud-Infrastrukturen für das Hosting und den Betrieb des Tagesgeschäfts. Dies hat der Branche einen Vorteil beim Management ihrer Kosten verschafft und ihr einen relativen Vorsprung bei den Ausgaben für Cybersicherheit und deren Bereitstellung verschafft.

Identitäts- und Applikationssicherheit werden von Einzelhandelsunternehmen in allen Bereichen weitgehend angenommen (>80% Marktdurchdringung für beide Bereiche). Hinsichtlich GRC besteht jedoch eine große Lücke - möglicherweise aufgrund eines mangelnden Bewusstseins für deren Bedeutung. Aufgrund der zunehmenden Nutzung der Cloud helfen GRC-Tools Einzelhändlern dabei, ihre Risikoprofile und Daten-Compliance-Anforderungen im laufenden Betrieb zu verwalten.

Mittelgroße Einzelhändler

Die aktuellen Ausgaben des Einzelhandelssektors für Cybersicherheit liegen relativ nahe an den empfohlenen Mindestausgaben. Die Ausgaben für Cybersicherheit für Einzelhändler dieser Größe konzentrieren sich auf Cyberabwehr und professionelle Dienstleistungen.

Anwendungssicherheit und sichere Identitäten werden bis 2023 im gesamten Einzelhandel am schnellsten wachsen, während mittelgroße Unternehmen voraussichtlich mehr für GRC ausgeben werden. Aufgrund der zunehmenden Bedeutung des IoT im Einzelhandel, z. B. in Form

Der zunehmende Einsatz der Cloud treibt das Wachstum der erwarteten zukünftigen Ausgaben für Einzelhändler in allen Bereichen voran. Die Cloud verschafft dem Einzelhandel einen großen Vorteil bei den Kosten und der Markteinführung, und daher werden die Einzelhändler weiterhin mit einem Cloud-first-Geschäftsmodell innovativ sein.

von intelligenten Sensoren, sollten mittelständische Einzelhändler mehr in die IoT-Sicherheit investieren.

Der zunehmende Einsatz der Cloud treibt das Wachstum der erwarteten zukünftigen Ausgaben für mittelgroße Einzelhändler an. Der Mangel an qualifizierten Cybersicherheitsressourcen wirkt sich in diesem Sektor nicht so stark auf die Ausgabenentscheidungen aus wie in anderen vertikalen Branchen.

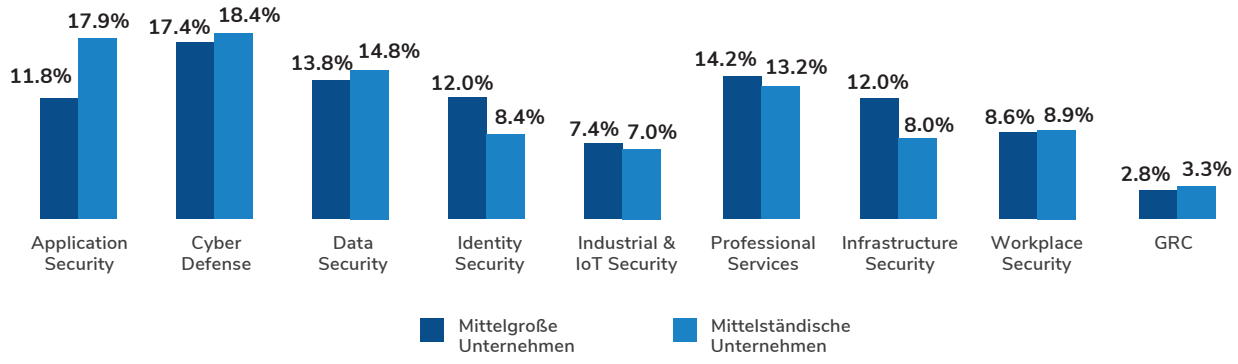
Mittelständische Einzelhändler

Mittelständische Einzelhändler sind im Allgemeinen recht nah an den von Frost & Sullivan empfohlenen Mindestausgaben. Dies ist in erster Linie auf die höhere Akzeptanz von Identitätssicherheit, Applikationssicherheit, professionellen Dienstleistungen und GRC-Lösungen zurückzuführen. Da das Geschäftsmodell des Einzelhandels agil ist, ist es für Einzelhandelsunternehmen relativ einfach, Proof of Concepts (POCs) neuerer Technologien durchzuführen und diese zu übernehmen, wodurch sie in der allgemeinen Reifekurve einen Vorsprung haben.

Die Applikationssicherheit und die Identitätssicherheit haben beide einen Verbreitungsgrad von mehr als 85% bei mittlgroßen Einzelhändlern, was dem höheren Bedarf von Unternehmen entspricht, die große Mengen an Kundendaten verarbeiten. Für professionelle Dienstleistungen werden 13-14% des gesamten Cybersicherheitsbudgets in mittelgroßen und großen Einzelhandelsunternehmen ausgegeben, was auf die Bereitschaft hinweist, die Expertise von externen Sicherheitsexperten zu nutzen, um ihre Cybersicherheitslage zu verbessern.

Im Umgang mit Kundendaten, Kreditkarten- und anderen Finanzdaten sind Einzelhändler im Falle einer Datenschutzverletzung einer strengen Prüfung unterworfen. Dies zwingt sie dazu, ihre Sicherheitsmaßnahmen zu verstärken und die Einhaltung der Vorschriften zu gewährleisten, während sie gleichzeitig neue Technologien einsetzen.

EXHIBIT 5: Gewichtung in % der Ausgaben für Cybersicherheit, Einzelhandel



Source: Frost & Sullivan

Gesundheitswesen

Die Gesundheitsbranche gehört zu den Hauptangriffszielen von Cyberkriminellen, da sie über eine große Menge an personenbezogenen Patientendaten verfügt. Ransomware-Akteure haben gesehen, dass sie von Gesundheitsdienstleistern Lösegeld in Höhe von mehreren Millionen Dollar verlangen können, um die Daten nach einem Angriff zu entschlüsseln, wohl wissend, dass die Datensysteme die Lebensader eines jeden Krankenhauses oder Gesundheitsdienstleisters sind. Der Gesundheitssektor verzeichnete 2022 einen Anstieg der durchschnittlichen wöchentlichen Cyberangriffe um 74% im Vergleich zu 2021 - der höchste prozentuale Anstieg und der drittgrößte in absoluten Zahlen[7]. Branchenuntersuchungen ergaben, dass die durchschnittlichen Kosten einer Sicherheitsverletzung im Gesundheitswesen 10,1 Mio. US-Dollar (9,5 Mio. Euro) betragen und damit etwa 57% höher sind als der weltweite Durchschnitt[8] für andere Branchen.

Der Gesundheitssektor verzeichnete im Jahr 2022 einen Anstieg der durchschnittlichen wöchentlichen Cyberangriffe um 74% gegenüber 2021 - der höchste prozentuale Anstieg und der drittgrößte in absoluten Zahlen . Branchenuntersuchungen ergaben, dass die durchschnittlichen Kosten einer Sicherheitsverletzung im Gesundheitswesen 10,1 Mio. US-Dollar (9,5 Mio. Euro) betragen und damit etwa 57% höher sind als der weltweite Durchschnitt für andere Branchen.

[7]Check Point Research berichtet über einen 38%igen Anstieg der weltweiten Cyberangriffe im Jahr 2022; Check Point; 2022

[8]Kosten einer Datenschutzverletzung 2022, Ein millionenschwerer Wettlauf um Erkennung und Reaktion; IBM; 2022

Mittelgroße Unternehmen des Gesundheitswesens

Die Ausgaben eines durchschnittlichen mittelgroßen Unternehmen im Gesundheitssektor sind derzeit 39% unter den empfohlenen Mindestausgaben, um sich angemessen gegen Cyberbedrohungen zu schützen. Obwohl die Unternehmen des Gesundheitswesens bereits eine beträchtliche Summe für Cybersicherheit ausgeben, bleiben sie immer noch hinter den empfohlenen Mindestausgaben zurück. Grund dafür sind die hohen Kosten, die mit einer Datenschutzverletzung von Gesundheitsdaten verbunden sind, sowie potenziell lebensbedrohliche Situationen, die entstehen können, wenn das Netzwerk eines Gesundheitsdienstleisters durch einen Cyberangriff lahmgelegt wird.

Da Datenverlust zu den größten Risikofaktoren gehört, mit denen sich Organisationen im Gesundheitswesen auseinandersetzen müssen, ist es nicht verwunderlich, dass die Datensicherheit in diesem Sektor eine Durchdringung von über 80% aufweist. Darüber hinaus ist die Arbeitsplatzsicherheit im Gesundheitswesen weit verbreitet, da der Schutz der verschiedenen Endgeräte entscheidend für die Aufrechterhaltung einer ausreichenden Sicherheitslage ist.

Die tatsächlichen Ausgaben sind relativ gleichmäßig verteilt, aber mehr als 30% der mittelgroßen Budgets für Cybersicherheit im Gesundheitswesen entfallen auf Cyberabwehr und Datensicherheit. Auch hier ist die Datensicherheit für Gesundheitsdienstleister von entscheidender Bedeutung, da die potenziellen Folgen von Datenschutzverletzungen enorm sind - ein Kostenfaktor, den viele kleinere Unternehmen einfach nicht tragen könnten.

Am stärksten werden die Ausgaben für die Cyberabwehr bei mittelgroßen Unternehmen steigen, da sie einen vollständigen Überblick über ihre aktuelle Cyberlage erlangen möchten. Da IoT-Geräte im in Gesundheitseinrichtungen immer häufiger zum Einsatz kommen und die Vorschriften für die Datenverarbeitung verschärft werden, können Unternehmen des Gesundheitswesens von höheren Investitionen in IoT-Sicherheits- und GRC-Lösungen profitieren.

Künftige Ausgaben für Cybersicherheit bei mittelgroßen Gesundheitsdienstleistern werden durch die zunehmende Nutzung der Cloud und die digitale Transformation angekurbelt, da Innovationen im Gesundheitswesen wie beispielsweise Telemedizin die Art und Weise der Gesundheitsversorgung verändern werden.

Mittelständische Unternehmen des Gesundheitswesens

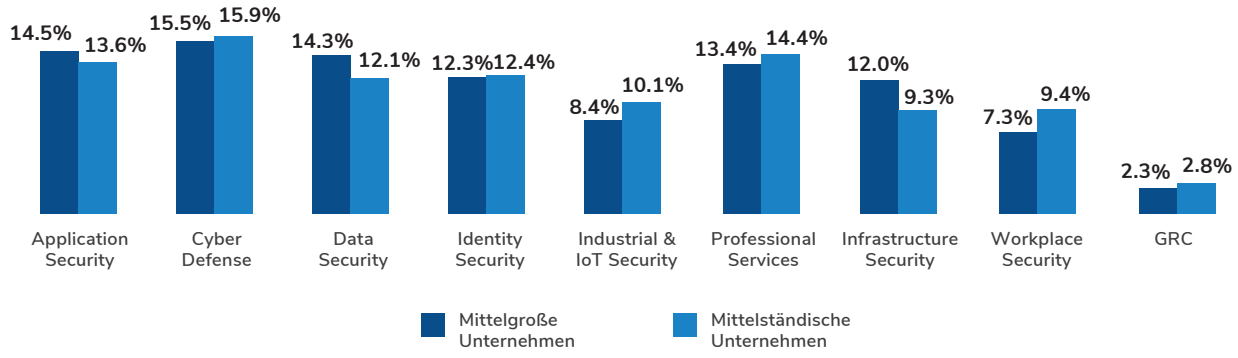
Mittelständische Gesundheitsdienstleister geben angesichts der aktuellen Bedrohungslage durchschnittlich 30% zu wenig für die Aufrechterhaltung einer angemessenen Cybersicherheit aus. Mittelständische Gesundheitsorganisationen verfügen über einige der höchsten Budgets für Cybersicherheit, stehen aber immer noch vor großen Herausforderungen im Umgang mit der sich veränderten Bedrohungslandschaft. Neben der Datensicherheit sind auch die Applikationssicherheit und die Arbeitsplatzsicherheit bei mittelständischen Gesundheitsdienstleistern nahezu durchgängig eingeführt.

Was die aktuellen Ausgaben betrifft, so geben mittelständische Gesundheitsdienstleister den größten Teil ihres Budgets für die Cyberabwehr aus, um ein hohes Maß an Netzwerktransparenz und Cyberbereitschaft aufrechtzuerhalten. Sie geben auch einen großen Teil ihrer Budgets für professionelle Dienstleistungen aus, da ihre Cybersicherheitsanforderungen sehr spezifisch sein können. Zusätzlich entscheiden sich sich Unternehmen den Betrieb der Cybersicherheit an Dritte auszulagern, wenn sie feststellen, dass ihre internen Fähigkeiten für die notwendigen Aufgaben nicht ausreichen.

Laut der Umfrage von Frost & Sullivan werden Gesundheitsdienstleister im mittleren Marktsegment ihre Ausgaben für sichere Identitäten und IoT-Sicherheit am stärksten erhöhen, da eine größere Anzahl von OT-Geräten wie Röntgengeräte, MRT-Scanner usw. mit den Krankenhausnetzwerken verbunden werden und aus der Ferne bedient werden können. Die Verbesserung der Identitäts- und der OT-Sicherheit wird Gesundheitsdienstleistern dabei helfen, ihre Einrichtungen vor unbefugtem Zugang sowie Zugriff und Angriffen aus der Ferne zu schützen, die in diesem Sektor zunehmend zu beobachten sind.

Die Ausrichtung auf die Priorisierung der Cybersicherheit als geschäftskritische Komponente ist der Hauptgrund für die höheren Ausgaben für Cybersicherheit bei mittelständischen Unternehmen - wiederum untermauert durch die schieren Kosten erfolgreicher Angriffe. Die laufenden Initiativen zur digitalen Transformation innerhalb des Sektors haben die Unternehmen auch dazu veranlasst, sich gegen neue Bedrohungen zu wappnen.

EXHIBIT 6: Gewichtung in % der Ausgaben für Cybersicherheit, Gesundheitswesen



Source: Frost & Sullivan

Dienstleistungen

Die Dienstleistungsbranche verzeichnete zwischen 2021 und 2022 etwa 12% aller gemeldeten Cybervorfälle, die vierthöchsten unter den Industriesektoren in der Europäischen Union[9]. Mit der zunehmenden digitalen Ausrichtung der Dienstleistungsbranche steigt auch die Gefährdung durch Cyberbedrohungen sowie das Risiko der Veröffentlichung von Kundendaten und geschützten Unternehmensdaten, was eine stärkere Ausrichtung auf die Cybersicherheit erforderlich macht.

Mittelgroße Dienstleistungsunternehmen

Mittelgroße Dienstleistungsunternehmen geben im Durchschnitt 30% zu wenig für ihre Cybersicherheitsanforderungen aus. Der Sektor weist die höchste Durchdringung bei der Applikationssicherheit in allen Unternehmensgrößen auf. Dienstleistungsunternehmen sind für ihren Betrieb auf verschiedene interne und externe Anwendungen angewiesen und verarbeiten oft sensible Kundendaten, die strengen Vorschriften wie Datengrundschutzverodnung GDPR[10] unterliegen. Mittelgroße Dienstleistungsunternehmen reservieren der Studie zufolge auch einen der höchsten Anteile ihrer IT-Budgets für die Cybersicherheit.

> Die Einführung der Cloud, die digitale Transformation, die Gefährdung durch Bedrohungen und der Wechsel von Geschäftsleuten sind die Hauptgründe für die steigenden Ausgaben für Cybersicherheit im Dienstleistungssektor.

Der größte durchschnittliche prozentuale Anstieg der Ausgaben unter den vertikalen Branchen wird für den Dienstleistungssektor erwartet, sowohl für mittelgroße als auch für große Unternehmen. In der Vergangenheit waren die Ausgaben des Dienstleistungssektor zu gering für die Cybersicherheit. In Verbindung mit der Ausweitung der Bedrohungslage und der zunehmenden Nutzung der Cloud haben Dienstleistungsunternehmen nun einen viel höheren Bedarf der Absicherung ihrer Netzwerke.

[9]ENISA Threat Landscape 2022; ENISA; 2022

[10]Complete guide to GDPR compliance; GDPR; 2023

Um den Anforderungen der verschiedenen Bereiche der Cybersicherheit gerecht zu werden, sollten mittelgroße Dienstleister einen wesentlich höheren Anteil ihres Budgets für GRC bereitstellen. Investitionen in GRC können mittelständischen Dienstleistern helfen, eine bessere Kontrolle über ihre Governance- und Compliance-Prozesse zu erlangen, die für Unternehmen, die mit personenbezogenen Daten umgehen, ein erhebliches Risiko darstellen.

Die Einführung der Cloud, die digitale Transformation, die Gefährdung durch Bedrohungen und der Wechsel von Fachkräften sind die Hauptgründe für den Anstieg der Ausgaben für Cybersicherheit im gesamten Dienstleistungssektor. Dienstleistungsunternehmen sind in der Lage, den Mangel an Cybersecurity-Talenten mit Outsourcing-Verträgen zu bewältigen, da ihre Sicherheitsanforderungen nicht an branchenspezifische Vorschriften gebunden sind.

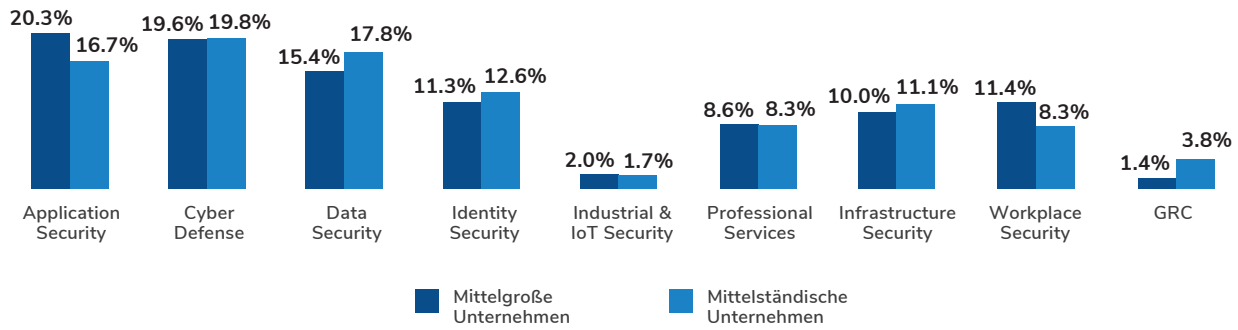
Mittelständische Dienstleistungsunternehmen

Mittelständische Dienstleister geben angesichts der aktuellen Bedrohungslage im Durchschnitt 24% weniger als die empfohlenen Mindestausgaben aus. Anwendungssicherheit, Cyberabwehr und Datensicherheit sind die drei wichtigsten Produktbereiche, für die Cybersicherheitsbudgets ausgegeben werden.

Die Ausgaben für GRC werden im nächsten Jahr das höchste relative Wachstum verzeichnen - im Gegensatz zu den wesentlich geringeren relativen Ausgaben mittelgroßer Dienstleistungsunternehmen in diesem Bereich. Mittelständische Dienstleistungsunternehmen können professionelle Cybersicherheitsdienstleister in Anspruch nehmen, wenn sie vor der Herausforderung stehen, ihre Cybersicherheitsteams intern zu vergrößern.

Dienstleistungsanbieter im mittleren Marktsegment werden durch genau dieselben Faktoren zu höheren Ausgaben für Cybersicherheit veranlasst wie mittelgroße Unternehmen, nämlich durch die Einführung der Cloud, die digitale Transformation, die erhöhte Bedrohungslage und die Neuausrichtung der Fachkräfte hinsichtlich Cybersicherheit.

EXHIBIT 7: Gewichtung in % der Ausgaben für Cybersicherheit, Dienstleistungen



Source: Frost & Sullivan

Der Weg nach vorn

Obwohl die Ausgaben für Cybersicherheit im Laufe der Zeit steigen sollen, haben einige Unternehmen in Europa den Anteil ihrer IT-Budgets für Cybersicherheit von 2021 auf 2022 reduziert[11]. Die Steigerung der Cybersicherheit wird auch durch einen fragmentierten Cybersicherheitsmarkt und öffentliche Förderprogramme verlangsamt, die nicht ausreichend koordiniert sind[12]. In Anbetracht dieser Entwicklungen ist es für mittelgroße und mittelständische Unternehmen wichtig, die Ausgaben für Cybersicherheit zu erhöhen, da das derzeitige Niveau in Betracht des Risikos erheblicher Schäden durch Schwachstellen nicht ausreichend ist.

Europa macht weiterhin Fortschritte in der Cyber- und Informationssicherheit - die Entstehung von Datensicherheitsgesetzen und regulatorischen Rahmenbedingungen auf der ganzen Welt werden nach dem Vorbild der GDPR gestaltet. Dank der gemeinsamen Anstrengungen verschiedener Regierungsstellen in der Europäischen Union ist das Bewusstsein für die Herausforderungen im Cyberraum in mittelgroßen und mittelständischen Unternehmen größer als je zuvor. Mit den richtigen Budgetzuweisungen und Ausgaben können europäische Organisationen ihre Resilienz erheblich steigern.

In Anbetracht der in dieser Studie vorgestellten Ergebnisse sollten europäische mittelständische Unternehmen folgendende zentralen Empfehlungen berücksichtigen, um die Lücke bei den Ausgaben für Cybersicherheit zu schließen:

- ☑ Für mittelgroße Unternehmen ist es von entscheidender Bedeutung, über ein separates, vom IT-Budget abgekoppeltes Budget für Cybersicherheit zu verfügen. Es hat sich gezeigt, dass die IT-Budgets nicht im Gleichschritt mit der sich verändernden Bedrohungslandschaft wachsen. Ein Großteil der traditionellen IT-Ausgaben stagniert , was das Wachstum der Cybersicherheitsausgaben begrenzt, wenn sie nicht aus dem IT-Budget des Unternehmens ausgegliedert werden.
- ☑ Die Studie hat gezeigt, dass viele mittelgroße Unternehmen keine Vollzeitstelle eines Chief Information Security Officer (CISO) im Unternehmen haben. Es ist wichtig, dass Organisationen über dedizierte Cybersicherheitsbeauftragte innerhalb des Unternehmens verfügen, die dafür verantwortlich sind, Cybersicherheitsbudgets angemessen zu gestalten und den entsprechenden Return on Investment zu erzielen.

[11]Cybersicherheitsinvestitionen in der EU: Reicht das Geld aus, um die neuen Cybersicherheitsstandards zu erfüllen?; ENISA; 2022

[12]Europäische Investitionsplattform für Cybersicherheit; Europäische Investitionsbank; 2022

- ☑ Unternehmen sollten den Reifegrad ihrer Cybersicherheit regelmäßig anhand von Industriestandards bewerten und entsprechende Massnahmen planen, um schrittweise weiterzukommenihren Reifegrad zu erhöhen. Es ist wichtig, den aktuellen Status vollständig und unvoreingenommen zu verstehen um sich auf den zukünftigen bzw. angestrebten Zustand zu entwickeln.
- ☑ Unternehmen sollten regelmäßig Schwachstellenbewertungen und Penetrationstests (Vulnerability Assessments & Penetration Tests - VAPT) durchführen, um Schwachstellen in ihrer Infrastruktur (Netzwerk, Endgeräte, Cloud) zu erkennen, bevor ein Angreifer dies tut. Weiter sollten Unternehmen über angemessene Projektpläne zur Installation von Software-Patches verfügen.
- ☑ Die Cybersicherheit ist nur so stark wie ihr schwächstes Glied - der Mensch. Es ist von entscheidender Bedeutung, regelmäßige Cybersicherheitsschulungen für die Mitarbeiter des Unternehmens durchzuführen, um böswillige Akteure zu erkennen und sie dem Cybersicherheitsteam zu melden, damit umgehend Gegenmaßnahmen getroffen werden können.
- ☑ Es zeigt sich, dass viele Unternehmen in dieser Studie zum Schutz ihrer Endgeräte auf Endpoint Detection & Response (EDR) vertrauen, was ein Schritt in die richtige Richtung ist. Um ihre Bedrohungsabwehr und Netzwerktransparenz weiter zu verbessern, sollten Unternehmen die Evaluierung von Managed Detection & Response (MDR) und Extended Detection & Response (XDR) Tools in Betracht ziehen.
- ☑ Führungskräfte sollten die Cybersicherheit nicht als Kostenfaktor betrachten, sondern als einen Faktor, der das Geschäft fördert. Unternehmen können mehr von der Cybersicherheit profitieren (und viel mehr verlieren, wenn sie sie nicht nutzen), wenn sie die Bedrohungslandschaft in ihrem Unternehmen ganzheitlich betrachten.

Abschließend lässt sich sagen, dass Unternehmen danach streben, das Mindestmaß an Cybersicherheitsausgaben zu erreichen, das erforderlich ist, um in der aktuellen Bedrohungslandschaft geschützt zu sein. Die Deutsche Telekom kann Unternehmen dabei helfen, ihre Cybersicherheitsbudgets effizient einzusetzen und eine bessere Kapitalrendite zu erzielen, indem sie verschiedene Cybersicherheitslösungen für den europäischen Mittelstand anbietet.

Wichtige Kontakte

Alexander Kühnlein
Senior Expert Strategy
Deutsche Telekom Security

Als Senior Expert Strategy treibt Alexander die Strategie der Deutsche Telekom Security voran.

Alexander verfügt über mehr als 10 Jahre Erfahrung im Bereich Strategie und Marketing für Security Service Provider. Vor seiner Zeit bei der Telekom hatte er mehrere Positionen im Airbus Defence and Space, bei Siemens und in der Beratung.

Kontakt: alexander.kuehnlein@telekom.de

Ralf Schneider
Head of Security Consulting
Deutsche Telekom Security

Leitet das globale Security Consulting bei der Telekom Security – mit der Mission, den optimalen Wertbeitrag von Security für das Kundenbusiness zu erreichen.

Ralf profitiert von über 20 Jahren Erfahrung in der technologischen Strategie- und Transformationsberatung als Berater und C-Level Advisor bei der Detecon International. Er entwickelte und verantwortete als Partner die Themen IT-Sourcing & Transformation, sowie Business Technology Strategy & Security.

Kontakt: Ralf-schneider@telekom.de

Vinay Biradar
Associate Director-
Cybersecurity Consulting
Frost & Sullivan

Mit über 12 Jahren Erfahrung in den Bereichen Cybersicherheit und digitale Transformation berät Vinay Kunden zu Geschäfts- und Produktstrategien. Vor Frost & Sullivan hat er für Unternehmen wie British Telecom, Wipro Technologies & HCL Technologies gearbeitet.

Er zeigt aktives Interesse und verfolgt die bevorstehende Forschung in den Bereichen Cybersicherheit, ICT und digitale Transformation. Er hat an mehreren Podiumsdiskussionen teilgenommen und auf Veranstaltungen in verschiedenen Teilen Asiens präsentiert.

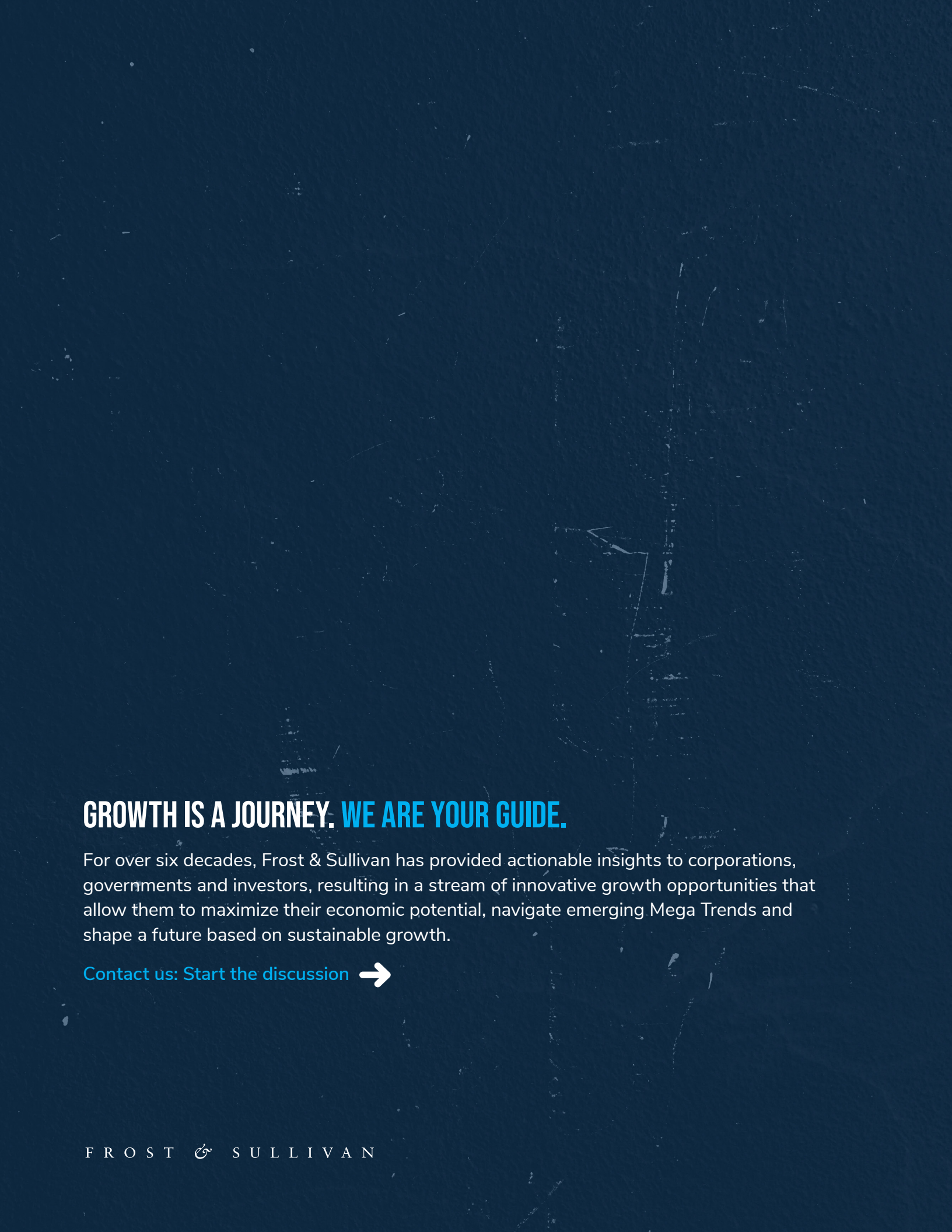
Kontakt: vinay.biradar@frost.com

DISCLAIMER

Über Telekom Security

Telekom Security bietet als Managed Security Service Provider (MSSP) hochwirksame und professionelle Sicherheitsmaßnahmen für den Schutz vor Cyberangriffen. Mit über 25 Jahren Erfahrung ist die eigenständige Gesellschaft unter dem Dach der Deutsche Telekom AG Marktführer in DACH und einer der europäischen Leader in der Cyber Security Branche. Für das breite Portfolio – von Cyber Defense über Cloud Security bis zu OT Security – kooperiert die Telekom Security mit weltweit führenden Unternehmen und bietet so digitale Sicherheit aus einer Hand – von der Beratung über individuelles Design bis zur Implementierung.

T SECURITY



GROWTH IS A JOURNEY. WE ARE YOUR GUIDE.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion →

FROST & SULLIVAN