IT-Sicherheit bei KMU

IT-Dienstleister als Akteure zur Stärkung der IT-Sicherheit bei KMU in Deutschland

Eine Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie erstellt durch NKMG mH & BIGS gGmbH, 19.02.2021

Studie des BMWi

BIGS

htw. Hochschule für Technik und Wirtschaft Berlin

Abschlussbericht

„IT-DIENSTLEISTER ALS AKTEURE ZUR STÄRKUNG DER IT-SICHERHEIT BEI KMU IN DEUTSCHLAND“

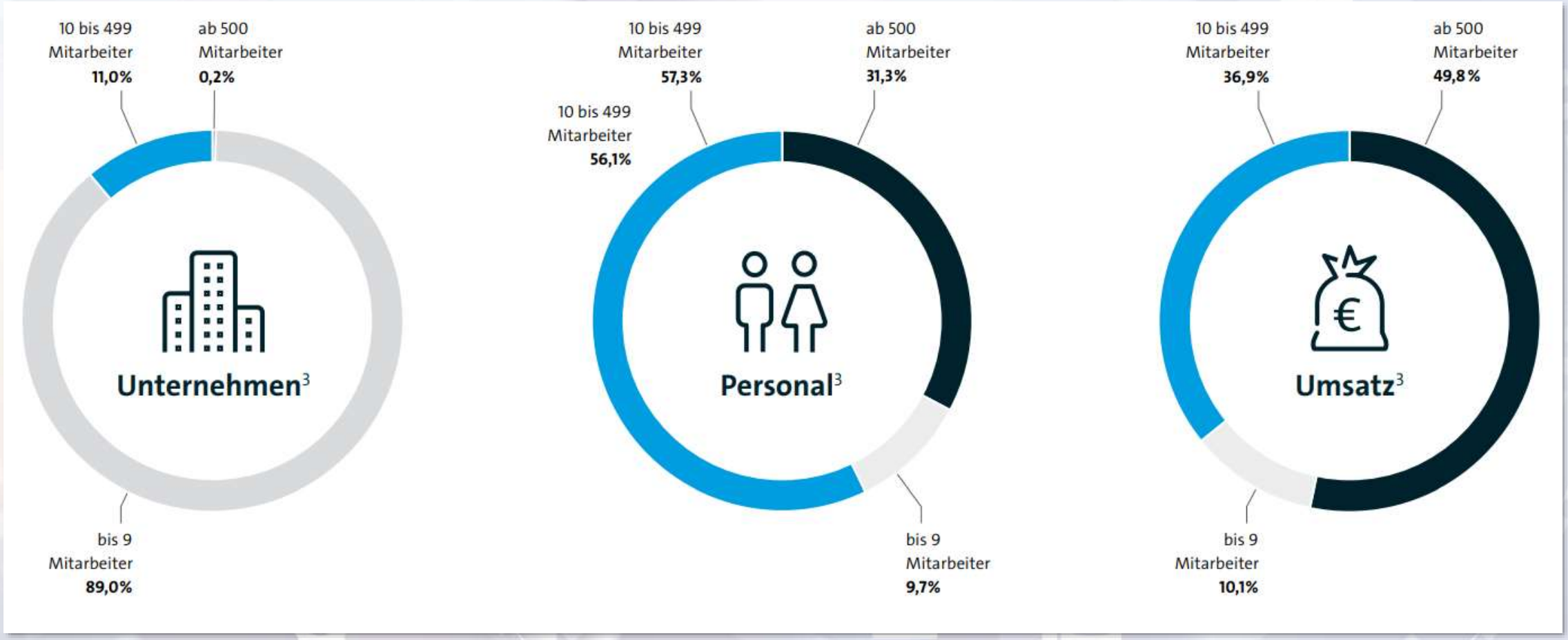
STUDIE IM AUFTRAG DES BUNDESMINISTERIUMS FÜR WIRTSCHAFT UND ENERGIE

AUTORINNEN DER STUDIE:

CHRISTIAN KÖHLER, CHARMAINE RICKERSON, PHILIP STEINKRÜGER, ORTWIN WOHLRAB, STEFFEN KOLB, ESTHER KERN, TIM STUCHTEY, ALEXANDER SZANTO

erstellt durch
HBMG mbH & BIGS gGmbH
19.02.2021

Motivation



Anzahl, Beschäftigte & Umsatz mittelständischer IT-Unternehmen, Quelle: Bitkom 2020a, 7

Aufgabe und Ziele

Aufgabe

Untersuchung und Darstellung eines Lagebilds zur Rolle der IT-Dienstleister für mehr Sicherheit bei KMU

Ziele

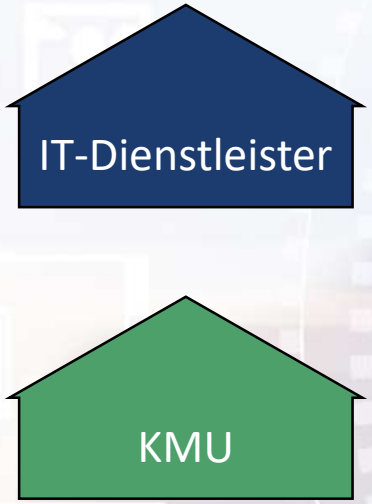
1. Die aktuelle IT-Sicherheitslage von KMU unter Einbindung von IT-Dienstleistern in Deutschland transparenter zu gestalten

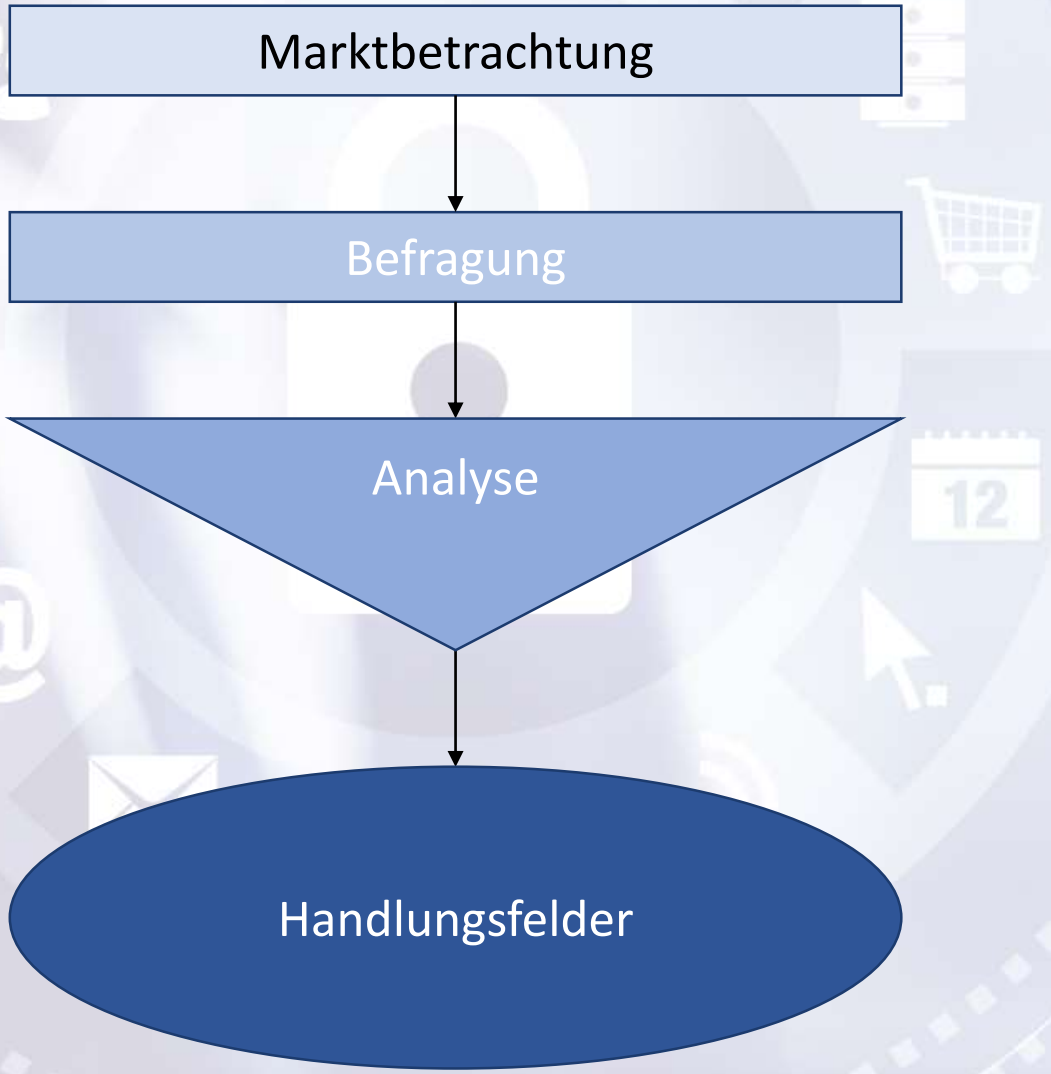
2. Mit Handlungsempfehlungen zur Verbesserung des IT-Sicherheitsniveaus beizutragen

Fragestellungen

- Wie ist die Gruppe der IT-Dienstleister zu definieren?
- Welche IT-Dienstleistungen werden den KMU angeboten?
- Wie arbeiten IT-Dienstleister und ihre (KMU-) Kunden bzgl. der IT-Sicherheit als Teil des Leistungsportfolios von IT-Dienstleistungen zusammen?
- Wie finden KMU geeignete IT-Dienstleister und nach welchen Kriterien wählen sie diese aus?

Vorgehensweise





Marktbetrachtung: Wissenslücken bei IT-Dienstleistern

Push- oder Pull-Faktoren bei IT-Schutzmaßnahmen

Grundlagen für Zusammenstellung des Produktportfolios (Fähigkeiten, Bedrohungslage, etc.)

Arbeitsorganisation/-prozesse in der Zusammenarbeit mit Dritten (IT-/Cybersicherheits-unternehmen) „im Auftrag“ von KMU

Informationsgewinnung/ Quellen zu Bedrohungslagen

Notwendigkeit von Branchenwissen bei kleinen IT-Dienstleistern

Vorgehen bei der Kundenakquisition

Qualifizierungsniveau der MitarbeiterInnen und Aktivitäten der Weiterbildungsmaßnahmen

Marktbetrachtung: Wissenslücken bei KMU

Auswahlfaktoren für einen IT-Dienstleister (Preis, Qualität, Regionalität etc.)

Rolle von Standards und Förderprogrammen für die IT-Sicherheit und die Auswahl der IT-Dienstleister

Informationsbeschaffung zur Bedrohungslage

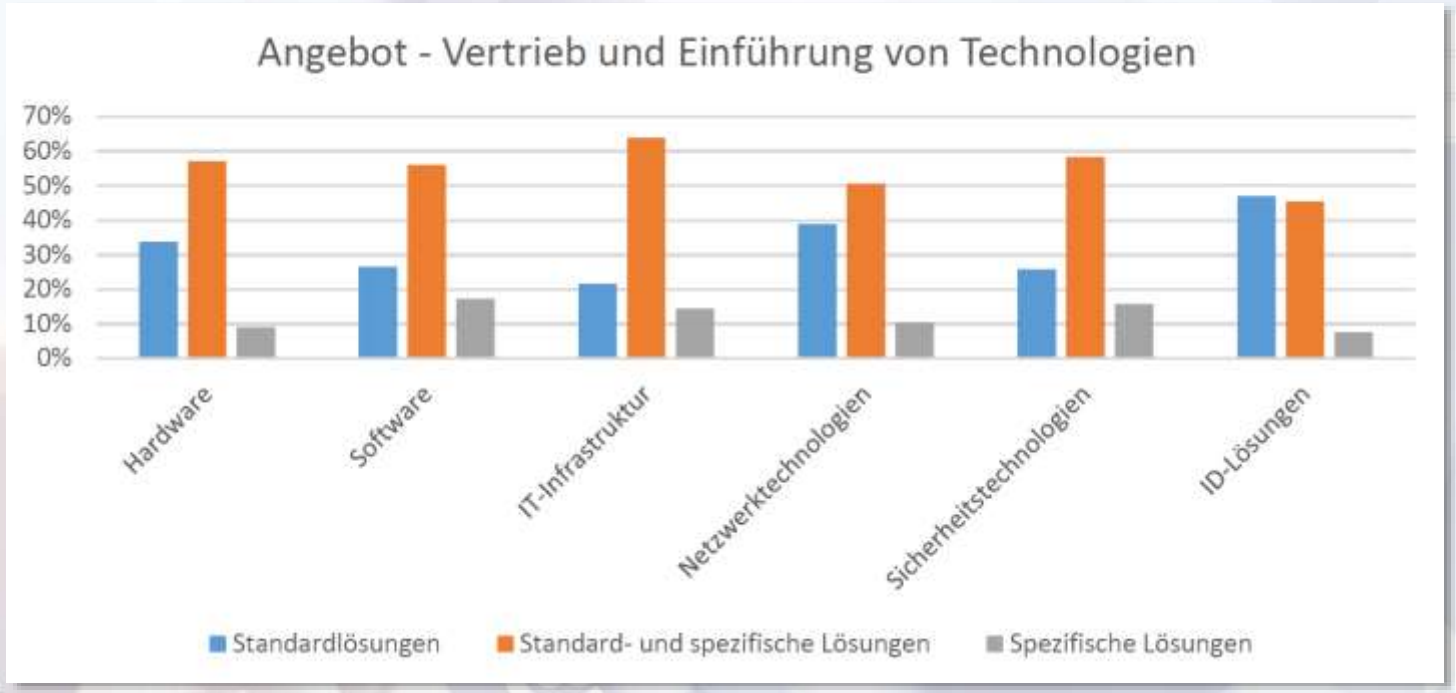
Kommunikationskanäle/ Plattformen für den Austausch/Kontaktpunkte mit IT-Dienstleistern

Entscheidungsprozesse und hierarchische Entscheidungsebene

Entscheidungsprozess des IT-Sicherheitsbudgets

Einfluss des Fachkräftemangels auf Outsourcing-Entscheidungen

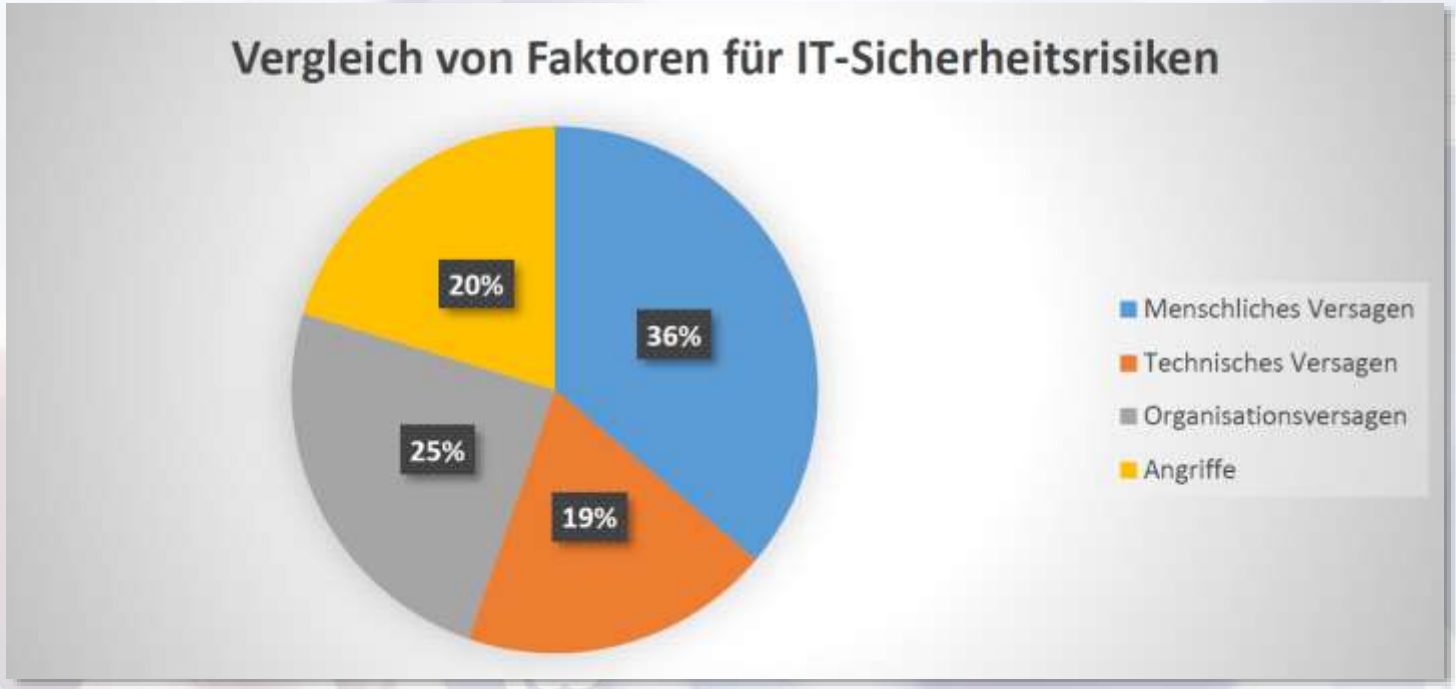
Erkenntnisse: Angebot der IT-Dienstleister



Technologiebereiche in denen IT-Dienstleister verschiedene Lösungen vertreiben. Quelle: Studie, Abbildung 20

- Stark fragmentierte Anbieterlandschaft, recht unterschiedliche Produktportfolios
- Kleinstanbieter versuchen Nachfragen abzudecken, große Anbieter mit kompletter Notfallhilfe, Forensik etc.
- Standardprodukte und spezifische Einzellösungen

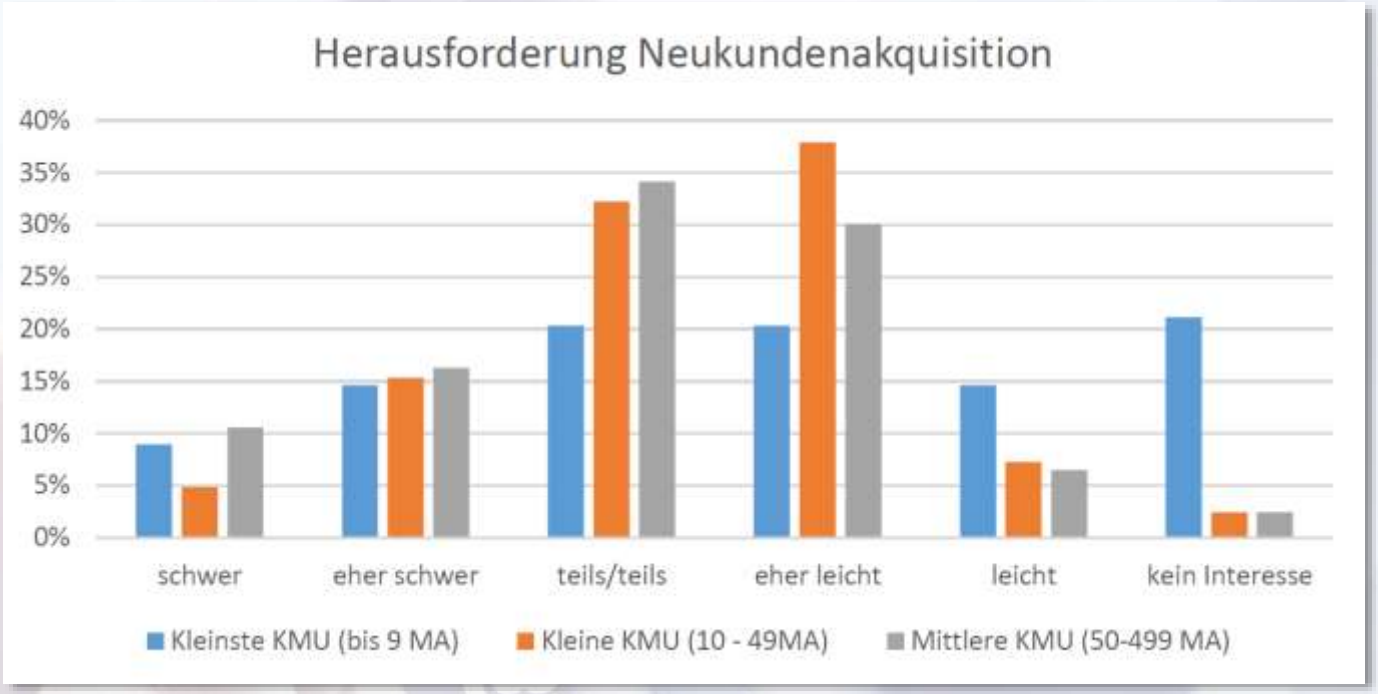
Erkenntnisse: Risikoeinschätzung der IT-Dienstleister



Im Vergleich die Eintrittswahrscheinlichkeiten eher hoch und sehr hoch für die jeweiligen Bedrohungen für KMU aus Sicht ihrer IT-Dienstleister. Quelle: Studie, Abbildung 15

- Selbsteinschätzung der Bedrohungslagen der KMU teilweise problematisch
- IT-D. leisten einen entscheidenden Beitrag zur Steigerung des Sicherheitsniveaus in KMU
- Intensivere Bemühungen sind notwendig um die Wahrnehmung für das Thema zu schärfen

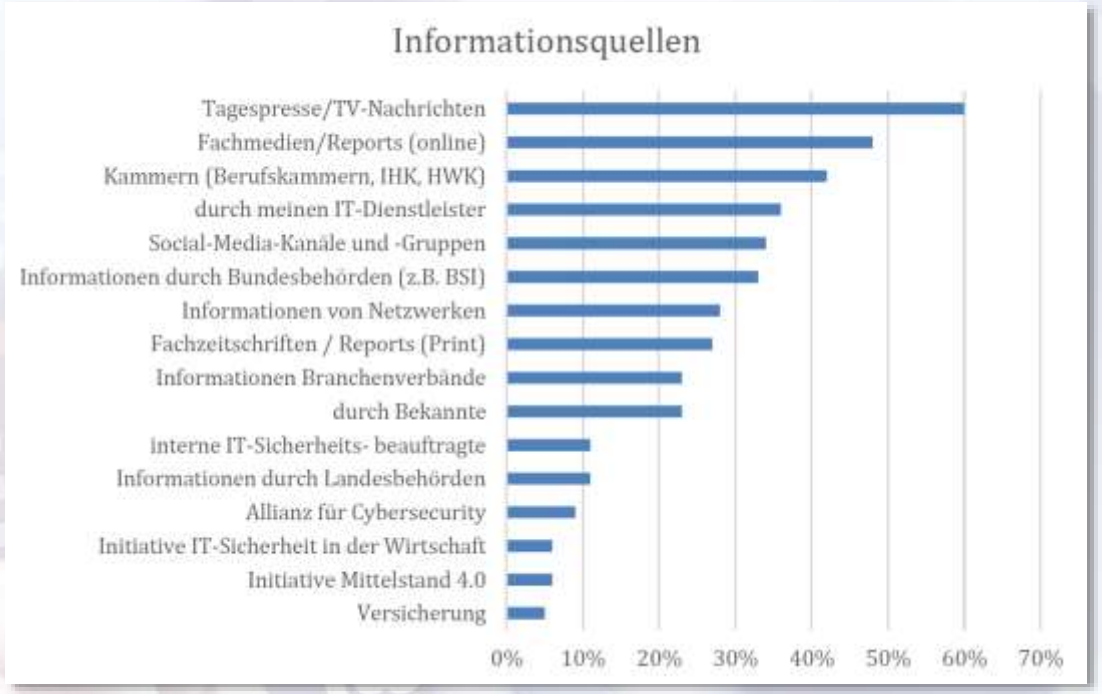
Erkenntnisse: Neukundenakquisition der IT-Dienstleister



Neukundenakquisition nach KMU Größe und Schwierigkeitsgrad. Quelle: Studie, Abbildung 35

- Kleinste KMU sind als Kunden weniger interessant
- Vertrauen und Empfehlungen wichtig
- Angespannte Situation auf dem Arbeitsmarkt, gepaart mit einer hohen Nachfrage nach IT-Dienstleistungen, erfordert den möglichst effizienten Einsatz von Ressourcen

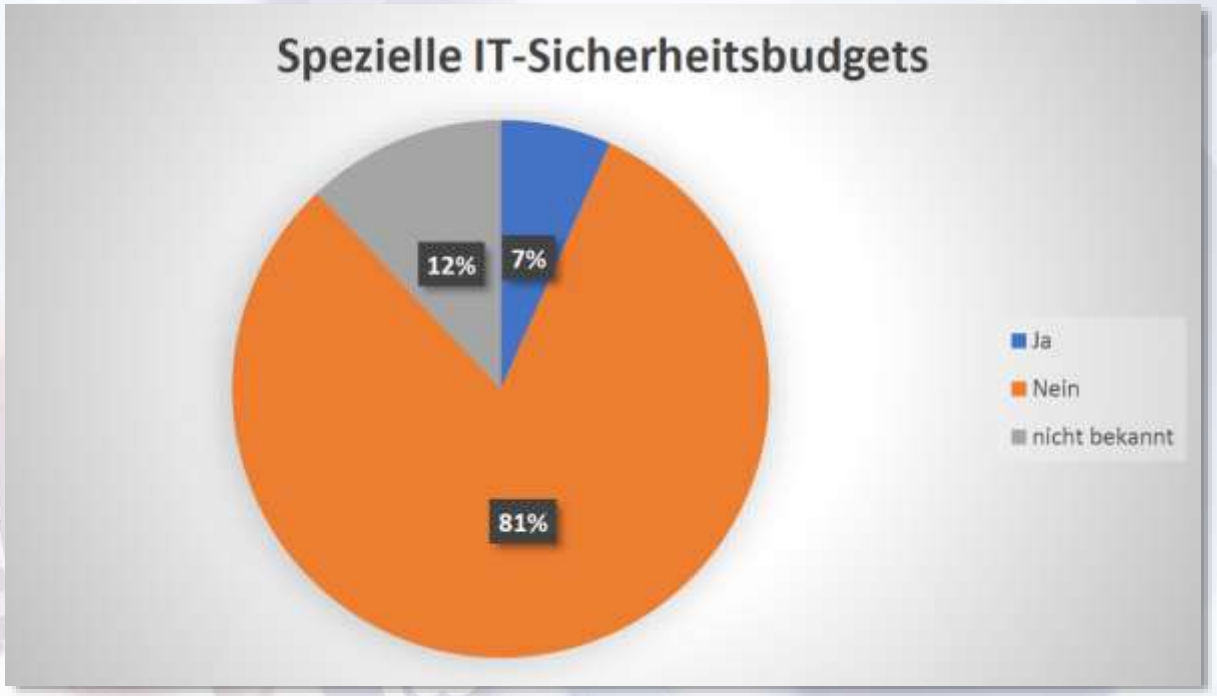
Erkenntnisse: Informationsbeschaffung für KMU



Informationsquellen der KMU zu Angriffen und IT-Sicherheitsrisiken. Quelle: Studie, Abbildung 54

- Oftmals unverständlich für KMU aufgrund hoher Fachlichkeit
- Zusätzlicher Aufwand um sich mit der Thematik auseinanderzusetzen wird als groß erachtet
- Unregelmäßige Informationsbeschaffung (nur bei Bedarf)

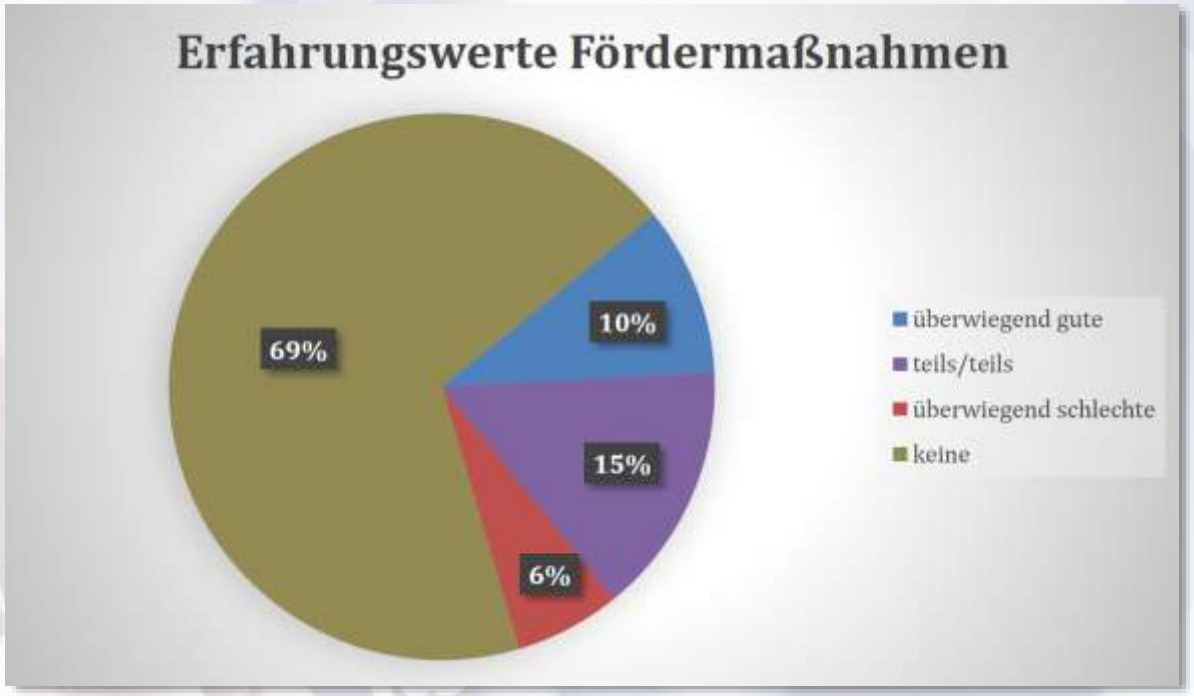
Erkenntnisse: Budget für IT-Sicherheit in KMU



Spezielle IT-Sicherheitsbudgets in der Jahres-Budgetplanung der KMU. Quelle: Studie, Abbildung 53

- Über die Hälfte: max. 10 % der IT-Ausgaben speziell für IT-Sicherheit
- Bei über 76 %: Anteil der Ausgaben für externe IT-Dienstleister im Verhältnis zum IT-Budget bei 1 bis 30 %
- Wahrscheinlich hohe Kosten für die Heranziehung auswärtiger IT-Services werden gescheut

Erkenntnisse: Öffentliche Förderung von KMU



Erfahrungswerte der KMU zu staatlichen bzw. öffentlichen Fördermaßnahmen. Quelle: Studie, Abbildung 63

- Erwartungshaltung an öffentlich Hand seitens der KMU groß
- Nur durchwachsene Erfahrungswerte mit Förderprogrammen
- Zweifel an Visibilität und Akzeptanz

Handlungsempfehlungen

Handlungsfeld 1: Lagebild und Risikomanagement

Empfehlung 1.1	*Lagebild und Informationen*
Ziel	✓ Ganzheitliches Bild der Bedrohungslandschaft für KMU → Problem: Handlungslähmung durch Informationsflutung
Maßnahmen	❖ Zeitreihendaten müssen geführt werden ❖ Austausch zwischen Akteuren, um Bedürfnisse der KMU zu eruieren und digitale Bedrohungsinformationen aufzubereiten

Handlungsfeld 1: Lagebild und Risikomanagement

Empfehlung 1.2	*Risikomanagement und -tools*
Ziel	✓ Bedrohungsanalysen/Risikobewertungen ✓ Risikotools und Risikoprofile → Priorisierte Berücksichtigung/Befähigung zur Anwendung/an KMU-Belange ausgerichtet
Maßnahmen	❖ Informationen zu Risikomanagement, -tools und zu Risikoprofilen ❖ Befähigung zur verbesserten Selbsteinschätzung der Bedrohungen und IT-Sicherheitsrisiken in den KMU muss gestärkt werden

Handlungsfeld 2: Informationsaustausch und Wissenstransfer

Empfehlung 2.1	*Ansprechstelle für Erste Hilfe*
Ziel	✓ Ergänzend zu Zentren/Transferstellen: Notfall-Hotlines ✓ Zusammen mit Etablierung von Standards zu Servicequalität ✓ Prävention ✓ → Staatliche Stellen können Hilfestellung bei Bedarfsermittlung der IT-Sicherheit leisten ✓ → Konkrete Maßnahmen sind aber von der Privatwirtschaft umzusetzen ✓ Schadensbegrenzung/Eindämmung ✓ → Aufklärung durch BSI oder z.B. Digitalagenturen der Länder ✓ → Umsetzung ist eine private Aufgabe und schließt IT-Dienstleister, die nah an KMU dran sind, unbedingt ein
Maßnahmen	❖ Verstärkter Aufbau einer Notfall-Hotline mit zentraler Erreichbarkeit & Vermittlung von regionalen IT-Sicherheitsdienstleistern ❖ Erweiterung bestehender Serviceangebote bei Transferstellen, Mittelstandszentren, IHKn etc. ❖ Erarbeitung von Qualitätsstandards für Notfall-Hotlines (für Service und Personal)

Handlungsfeld 3: Fachkräfte und Personalressourcen

Empfehlung 3.1	*IT-Sicherheitswissen von Führungs- & Fachkräften*
Ziel	✓ Anzahl der MA & Führungskräfte mit IT-Sicherheitskenntnissen in KMU erhöhen ✓ Qualifikation & die Sensibilisierung der verantwortlichen Mitarbeiter weiter erhöhen
Maßnahmen	❖ Verstärkte Informationen zu Aufgaben von IT-Sicherheitsleitlinien & der Rolle der GF für die IT-Sicherheit im Unternehmen ❖ Verstärkte Schulungsangebote zur Rolle der GF für IT-Sicherheit ❖ Verpflichtende Beratung in IT-Sicherheitsfragen auf Geschäftsleitungsebene bei Inanspruchnahme von Förderprogrammen zur Digitalisierung, Bundesweite Vernetzung und Ausbau der Awareness-Angeboten für KMU

Handlungsfeld 4: Förderung

Empfehlung 4.1	*Förderung von IT-Sicherheitsmaßnahmen und Investitionen*
Ziel	✓ Die für die Umsetzung notwendigen Investitionen, z.B. in Hard- und Software, und die erforderlichen technischen Maßnahmen sollten stärker berücksichtigt werden → Umsetzung der IT-Sicherheitsmaßnahmen könnte erleichtert/externe Effekte kompensiert werden
Maßnahmen	❖ Verstärkte Förderung der Umsetzung geeigneter IT-Sicherheitsmaßnahmen einschließlich der Investitionen für Hard- und Software ❖ Prüfung der Anpassung weiterer Instrumente, z.B. AfA-Tabellen (Verkürzung Abschreibungszeiten)

Handlungsfeld 4: Förderung

Empfehlung 4.2	*Kompetenzen im Bereich Förderprogramme*
Ziel	✓ Beratung der KMU-Kunden durch IT-Dienstleister bzgl. Fördermöglichkeiten ✓ Unterstützung der Kunden bei der Beantragung der Fördermaßnahmen ✓ Erleichterung der Antragsstellung für KMU & Etablierung einer Interessenskonvergenz
Maßnahmen	❖ Beratungsbefähigung der IT-Dienstleister in das notwendige Know-how zur Leistungserbringung ❖ Unterstützung der IT-Dienstleister bei der Durchführung der Beratungsleistung → Über staatliche Stellen, die IHKn oder Berufsverbände

Handlungsfeld 5: Qualität und Standards

Empfehlung 5.2	*Qualitätskriterien und -standards*
Ziel	✓ Erleichterung der Suche nach geeigneten Dienstleistern und Serviceangeboten für KMU → Die nach den definierten Qualitätskriterien arbeiten
Maßnahmen	❖ Prüfung existierender Standards (z.B. BSI-GS, ISO 27001, VdS 10000)/Personenzertifizierungen ❖ Analyse der Hemmnisse zur weiteren Verbreitung der existierenden Angebote ❖ Schaffung von Anbieterverzeichnissen mit definierten und nachprüfbaren Qualitätskriterien ❖ Transparente Darstellung und weitere Vernetzung von Sachverständigen und Personenregistern

Handlungsfeld 5: Qualität und Standards

Empfehlung 5.4	*Serviceangebote und Pakete durch IT-Dienstleister*
Ziel	✓ Unterstützung der KMU bei der Steigerung des IT-Sicherheitsniveaus durch komplette Servicepakete-/plattformen ✓ Servicepakete sollten nicht nur als individuelle Beratungen angeboten werden sondern im Sinne der Übernahme und des Managen von IT-Servicepaketen
Maßnahmen	❖ Prüfung bereits existierender Serviceangebote für mehr IT-Sicherheit für KMU ❖ Klärung der Hemmnisse bei der weiteren Etablierung dieser Services ❖ Vernetzung von Serviceanbietern mit IT-Dienstleistern für Kundengruppe der KMU ❖ Weitere Vernetzung von Serviceanbietern mit Netzwerken und Transferstellen

Handlungsempfehlungen

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Informationen unter it-security@m-und-h.de oder www.m-und-h.de/it-security

Jonas Schubert, 26.10.2022