ISG Provider Lens™

Cybersecurity – Solutions and Services

Eine Untersuchung der Information Services Group Germany GmbH

Customized report courtesy of:

T · ·

QUADRANT REPORT | JULI 2022 | GERMANY

Inhaltsverzeichnis

Report autor: Frank Heuer

Aktuelle Krisen treiben den deutschen Markt für Cybersecurity

Die aktuell verstärkten Cyberbedrohungen im Rahmen des Ukraine-Konflikts sowie die raschen Umbrüche durch die COVID-Pandemie – und selbstverständlich auch der langfristige Trend hin zur Digitalisierung – haben in Deutschland zu vergrößerten Angriffsflächen für Cyberangriffe geführt, die entsprechender Gegenmaßnahmen bedürfen.

Im Rahmen der Digitalisierung werden Geschäftsprozesse zunehmend in die IT verlagert. Auch geistiges Eigentum der Unternehmen wird immer mehr digital dargestellt. Mit der steigenden Notwendigkeit, IT- und Kommunikationssysteme in Unternehmen zu schützen, hat sich IT-Sicherheit zur Unternehmenssicherheit gewandelt. Aktuell bedeutet die Corona-Krise auch weiterhin eine Herausforderung für die IT-Sicherheit, da mit der verstärkten Home-Office-Nutzung – und der dadurch bedingten externen Anbindung der Mitarbeiter – die IT-Systeme leichter angreifbar sind. Da auch nach dem Ende der Pandemie nicht zu erwarten ist, dass alle Arbeitsplätze wieder in die Unternehmen zurückverlagert werden, wird diese Herausforderung voraussichtlich langfristig bestehen.

Cyberkriminelle realisieren in immer kürzeren Abständen neue, raffiniertere und komplexere Methoden, um die Cyberverteidigungssysteme von Unternehmen und Behörden zu überwinden. In den letzten zwölf Monaten waren wieder einige spektakuläre Cyberattacken zu verzeichnen; aber auch nicht so prominente Angriffe – etwa durch

Cyberattacken überfordern zunehmend

Zusammenfassung

Ransomware – machen immer mehr Unternehmen zu schaffen. Entsprechend müssen die Cybersecurity-Maßnahmen lückenlos auf dem neuesten Stand sein. Damit sind immer mehr Unternehmen und Behörden nicht zuletzt durch den IT-Fachkräftemangel – speziell im Cybersecurity-Markt – überfordert. Somit wenden sich immer mehr IT-Verantwortliche und Führungskräfte an externe Dienstleister, zum Beispiel Anbieter von Managed Security Services. Diese sowie auch viele IT-Security-Produktanbieter setzen, um selbst mit den Bedrohungen mithalten zu können, verstärkt auf proaktive statt reaktive Methoden, die zum Beispiel auf künstlicher Intelligenz basieren.

Neben dem Eigenschutz des Unternehmens zwingen auch gesetzliche Regelungen, wie die Datenschutz-Grundverordnung (DSGVO) in der EU, Unternehmen dazu, stärkere Sicherheitsmaßnahmen umzusetzen, um Cyberattacken vorzubeugen. Gerade für mittelständische Unternehmen stellt dies immer noch eine große Herausforderung dar.

Der Mittelstand ist andererseits ein interessantes Marktsegment für Cybersecurity-Anbieter. Da Mittelständler insgesamt gesehen weniger ausgereifte IT-Sicherheitssysteme als Großunternehmen besitzen, aber durch die oben beschriebenen Faktoren zu Nachrüstungen gezwungen sind, haben sie einen großen Nachholbedarf und verzeichnen dementsprechend eine überdurchschnittlich stark wachsende Nachfrage nach Cybersecurity-Lösungen. Noch vorteilhafter für Anbieter ist eine ausgewogene Kundenstruktur aus Mittelstand und Großunternehmen, um auch von den großen Budgets der Large Accounts zu profitieren.

Trotz der großen Bedeutung von Cybersicherheit kämpfen IT-Verantwortliche oft mit der Aufgabe, Investitionen in IT-Sicherheit gegenüber Stakeholdern des Unternehmens zu legitimieren, besonders gegenüber dem CFO. Anders als bei anderen IT-Projekten ist es nicht immer möglich, die Rentabilität der Investitionen nachzuweisen, auch ist es nicht einfach, Bedrohungsrisiken zu quantifizieren. Allerdings haben auch immer mehr Führungskräfte erkannt, dass Cyberattacken zu massiven, unter Umständen existenziellen finanziellen und Imageschäden führen können. Somit gewinnt Cybersicherheit in Unternehmen an Bedeutung, und Führungskräfte werden verstärkt in das Cyberrisikomanagement eingebunden.

Auf der anderen Seite liegt das Problem oft nicht (allein) auf der technischen Seite; viele Angriffe werden durch unbedachtes Verhalten von Anwendern begünstigt, wie z.B. bei Trojaner- und Phishing-Angriffen. Neben einem zeitgemäßen IT-Sicherheitsequipment spielen daher Beratung und Nutzerschulungen weiterhin eine wichtige Rolle.

Identity & Access Management (Produkte)

IAM ist aktuell und auch in Zukunft ein besonders wichtiges Cybersecurity-Thema. Ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen ist die zunehmende Digitalisierung aller Bereiche, die dazu beiträgt, dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern auch Maschinen und bestimmte Unternehmensbereiche (Industrie 4.0).

Darüber hinaus nimmt die Anzahl der Benutzer, Geräte und Dienste stetig zu und damit auch die Anzahl von digitalen Identitäten, die zu verwalten sind. Ein weiterer Faktor ist die gestiegene Nutzung

des Home Offices in Folge der Pandemie. Viele Mitarbeiter greifen remote auf die Unternehmensressourcen zu, so dass die Regulierung und Kontrolle des Zugriffs auf Daten und Systeme noch wichtiger werden.

Data Leakage/Loss Prevention (Produkte)

Das Interesse in Deutschland an DLP-Lösungen hat in den letzten Jahren weiter deutlich zugenommen. Dazu tragen verschiedene Faktoren bei, welche die Sicherheit der Daten im Unternehmen berühren. So haben sich Daten und geistiges Eigentum zu immer wichtigeren und teilweise existentiell bedeutsamen Unternehmens-Assets entwickelt. Immer mehr Cyberkriminelle setzen an diesem Punkt an, um Informationen zu stehlen.

Auch die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar, da sie sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration entziehen.

Advanced Endpoint Threat Protection, Detection & Response (Produkte)

Zum Schutz der Endpoints in Unternehmen vor komplexer werdenden Bedrohungen sollen Lösungen für Advanced Endpoint Threat Protection, Detection & Response sorgen.

Im Gegensatz zu herkömmlichen Sicherheitslösungen – wie klassischen Anti-Viren-Lösungen – beruhen sie nicht auf Signaturen, sondern sind proaktiv gegen potenzielle Bedrohungen ausgerichtet, indem sie Verhaltensanalysen sowie Machine Learning beziehungsweise künstliche Intelligenz zur Anwendung bringen. Des Weiteren ist eine kontinuierliche Überwachung der Endpoints möglich.

Strategic Security Services

Neben den akuten Krisen (Ukraine-Konflikt und weiterhin die COVID-Pandemie) sind Unternehmen in Deutschland vor vielfältige Herausforderungen gestellt, welche die IT-Sicherheit und den Datenschutz betreffen. Die weiter zunehmende Gefährdungssituation bewirkt zusammen mit mangelnden Ressourcen ein zunehmendes Bedürfnis nach Orientierung.

Angesichts der immer intensiveren wie auch raffinierteren Cyberattacken sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. Hiervon sind schon lange nicht mehr nur die bekannten großen Unternehmen und Behörden betroffen, sondern zunehmend auch kleine und mittelgroße Firmen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin.

Unter dem besonders starken Fachkräftemangel hinsichtlich IT-Security haben gerade die mittelgroßen Unternehmen zu leiden. Der Mittelstand ist damit ein überdurchschnittlich wachsendes – und entsprechend zunehmend attraktives – Marktsegment.

Technical Security Services

Weiterhin sind Unternehmen und Behörden in Deutschland angesichts immer raffinierterer Cyberangriffe und des Fachkräftemangels immer häufiger darauf angewiesen, externe Dienstleister in Anspruch zu nehmen, um ihre IT-Security-Systeme auf dem laufenden Stand zu halten.

Auch unbedachtes Verhalten von Anwendern wird von Kriminellen verstärkt ausgenutzt, z.B. bei Trojaner- und Phishing-Angriffen; es sind auch immer mehr Ransomware-Angriffe zu beobachten. Neben einem zeitgemäßen

Security Equipment spielen daher auch Schulungen für die Anwender nach wie vor eine wichtige Rolle.

IT-Security-Projekte sind häufig anspruchsvoll und vielfältig angelegt. Daher sind hier insbesondere Dienstleister im Vorteil, die ein breites Leistungsspektrum an Technical Security Services aus einer Hand bieten.

Managed Security Services

Die immer raffinierteren, häufigeren, komplexeren und wandlungsfähigeren Cyberattacken – sowie die zusätzlichen Herausforderungen durch die aktuellen Krisen – fördern besonders auch die Nachfrage nach Managed Security Services. Knappe qualifizierte Ressourcen und das erforderliche stets aktuelle Spezialistenwissen rücken diese Dienstleistungen zusätzlich in den Fokus deutscher Unternehmen.

Große wie auch mittelständische Kunden wissen Security Operations Centers (SOCs) mit deutschem Standort aufgrund des wichtiger gewordenen Datenschutzaspektes zu schätzen. Für beide Zielgruppen sind darüber hinaus auch End-to-End Security Services, integrierte Lösungen aus IT- und zugehöriger Security-Lösungen sowie eine hohe Innovationskraft wichtig, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben.

Fachkräftemangel fördert die Nachfrage nach externen Dienstleistern

Anbieterpositionierung

Page 1 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Absolute Software	Not In	Contender	Not In	Not In	Not In	Not In
Accenture	Not In	Not In	Not In	Leader	Leader	Leader
Acronis	Not In	Product Challenger	Not In	Not In	Not In	Not In
Alice&Bob.Company	Not In	Not In	Not In	Product Challenger	Not In	Not In
All for One Group	Not In	Not In	Not In	Market Challenger	Contender	Not In
Atos	Leader	Not In	Not In	Leader	Leader	Leader
Axians	Not In	Not In	Not In	Leader	Leader	Leader

Anbieterpositionierung

Page 2 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
BAYOONET	Product Challenger	Not In	Not In	Not In	Not In	Not In
Bechtle	Not In	Not In	Not In	Leader	Market Challenger	Leader
Beta Systems	Product Challenger	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Not In	Contender	Not In	Not In	Not In
Blackberry (Cylance)	Not In	Not In	Contender	Not In	Not In	Not In
Brainloop	Not In	Product Challenger	Not In	Not In	Not In	Not In
Broadcom	Product Challenger	Leader	Leader	Not In	Not In	Not In

Anbieterpositionierung

Page 3 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
CANCOM	Not In	Not In	Not In	Leader	Market Challenger	Leader
Capgemini	Not In	Not In	Not In	Leader	Leader	Leader
CGI	Not In	Not In	Not In	Not In	Product Challenger	Contender
Check Point	Not In	Not In	Product Challenger	Not In	Not In	Not In
Cisco	Not In	Not In	Contender	Not In	Not In	Not In
Cognizant	Not In	Not In	Not In	Contender	Product Challenger	Contender
Computacenter	Not In	Not In	Not In	Leader	Leader	Product Challenger

Anbieterpositionierung

Page 4 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Controlware	Not In	Not In	Not In	Leader	Market Challenger	Leader
CoSoSys	Not In	Market Challenger	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Not In	Leader	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Not In	Product Challenger	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger
Deutsche Telekom	Not In	Not In	Not In	Leader	Leader	Leader

Anbieterpositionierung

Page 5 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
DIGITALL	Not In	Not In	Not In	Product Challenger	Not In	Not In
DriveLock	Not In	Leader	Market Challenger	Not In	Not In	Not In
DXC Technology	Not In	Not In	Not In	Leader	Product Challenger	Product Challenger
ESET	Not In	Not In	Contender	Not In	Not In	Not In
EY	Not In	Not In	Not In	Not In	Product Challenger	Not In
Fidelis Cybersecurity	Not In	Contender	Not In	Not In	Not In	Not In
Forcepoint	Not In	Leader	Not In	Not In	Not In	Not In

Anbieterpositionierung

Page 6 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In
Fortinet	Contender	Not In	Not In	Not In	Not In	Not In
GBS	Not In	Leader	Not In	Not In	Not In	Not In
Getronics	Not In	Not In	Not In	Not In	Not In	Contender
glueckkanja-gab	Not In	Not In	Not In	Not In	Not In	Product Challenger
Google	Not In	Contender	Not In	Not In	Not In	Not In
HCL	Not In	Not In	Not In	Product Challenger	Rising Star ★	Leader

Anbieterpositionierung

Page 7 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
HelpSystems	Not In	Leader	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Product Challenger	Leader	Leader	Leader
iC Consult	Not In	Not In	Not In	Contender	Not In	Not In
Ilantus Products	Product Challenger	Not In	Not In	Not In	Not In	Not In
indevis	Not In	Not In	Not In	Product Challenger	Not In	Not In
Infosys	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
itWatch	Not In	Product Challenger	Not In	Not In	Not In	Not In

Anbieterpositionierung

Page 8 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Kaspersky	Not In	Not In	Product Challenger	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Leader	Not In
Logicalis	Not In	Not In	Not In	Contender	Contender	Product Challenger
LTI	Not In	Not In	Not In	Not In	Not In	Product Challenger
Lumen	Not In	Not In	Not In	Not In	Not In	Product Challenger
Matrix42	Market Challenger	Leader	Not In	Not In	Not In	Not In
Micro Focus	Product Challenger	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Page 9 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Microsoft	Leader	Leader	Leader	Not In	Not In	Not In
Netskope	Not In	Product Challenger	Not In	Not In	Not In	Not In
NEVIS	Product Challenger	Not In	Not In	Not In	Not In	Not In
Nexus Group	Product Challenger	Not In	Not In	Not In	Not In	Not In
NTT	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
OGiTiX	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Okta	Leader	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Page 10 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Omada	Contender	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In	Not In
OpenText	Not In	Product Challenger	Not In	Not In	Not In	Not In
Oracle	Market Challenger	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Not In	Not In	Leader
Palo Alto Networks	Not In	Not In	Contender	Not In	Not In	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In

Anbieterpositionierung

Page 11 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Proofpoint	Not In	Market Challenger	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Not In	Leader	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In
SailPoint	Product Challenger	Not In	Not In	Not In	Not In	Not In
SAP	Market Challenger	Not In	Not In	Not In	Not In	Not In
Saviynt	Product Challenger	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Not In	Not In	Not In	Product Challenger	Not In

Anbieterpositionierung

Page 12 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
SentinelOne	Not In	Not In	Leader	Not In	Not In	Not In
Skyhigh	Not In	Product Challenger	Not In	Not In	Not In	Not In
Solarwinds	Contender	Not In	Not In	Not In	Not In	Not In
Sophos	Not In	Not In	Leader	Not In	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger
suresecure	Not In	Not In	Not In	Rising Star ★	Not In	Not In
Syntax	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger

Anbieterpositionierung

Page 13 of 14

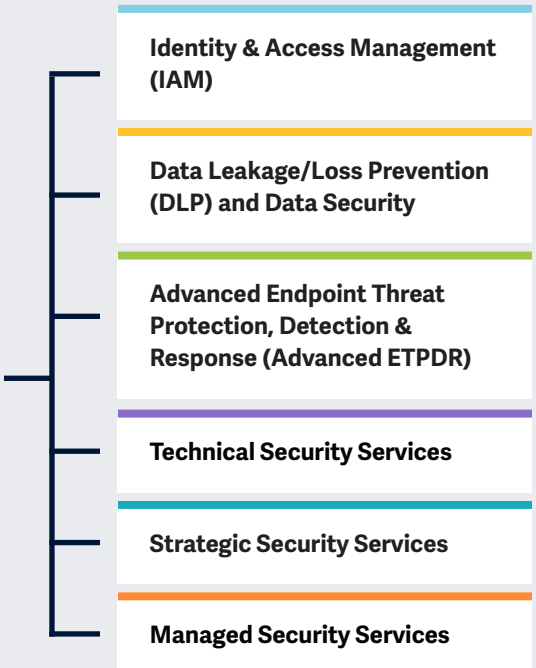
	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
TCS	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Thales	Contender	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Rising Star ★	Not In	Not In	Not In
Trend Micro	Not In	Leader	Leader	Not In	Not In	Not In
Trustwave	Not In	Not In	Not In	Not In	Not In	Product Challenger
Unisys	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger

Anbieterpositionierung

Page 14 of 14

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services
Varonis	Not In	Product Challenger	Not In	Not In	Not In	Not In
Verizon	Not In	Not In	Not In	Not In	Contender	Product Challenger
VMware Carbon Black	Not In	Not In	Leader	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Leader	Rising Star ★
Zensar	Not In	Not In	Not In	Contender	Contender	Contender
Zscaler	Not In	Product Challenger	Not In	Not In	Not In	Not In

Diese Studie konzentriert sich auf das, was ISG im Jahr 2022 für Cybersecurity Solutions and Services als besonders wichtig erachtet.



Simplified Illustration Source: ISG 2022

Definition

Unternehmen setzen neue Technologien ein, um die digitale Transformation voranzutreiben, wettbewerbsfähig zu bleiben und den sich ständig ändernden Anforderungen der Endbenutzer gerecht werden zu können. Diese Entwicklung wurde durch die COVID-19-Pandemie noch beschleunigt, denn dadurch wurde verstärkt auf Telearbeit, Cloud-Anwendungen und andere digitale Technologien gesetzt, um wirtschaftlich überleben und wachsen zu können. Die zunehmende Verbreitung dieser Technologien sowie neue Tools, die für mehr Effizienz und Geschwindigkeit sorgen, haben zu einer immer größeren Angriffsfläche geführt. Ransomware, Advanced Persistent Threats und Phishing-Angriffe stellten sich 2022 als die schlimmsten Cyber-Bedrohungen heraus. Angesichts der immer vielfältigeren und komplexen Cyberangriffe ist die Cybersicherheit nicht nur für Unternehmen, sondern auch für Regierungsbehörden zu einer Priorität geworden, um den Schutz der Wirtschaft, Industrie und Bürger zu gewährleisten.

Im Zuge dieser sich ständig verändernden Bedrohungslandschaft muss ein detaillierter und umfassender Ansatz für die Cybersicherheit zum Schutz des Unternehmens verfolgt werden, und zwar mit einer Kombination aus Sicherheitsprodukten und -services aus Bereichen wie Identity & Access Management (IAM), Data Leakage/Loss Prevention (DLP) sowie Datensicherheit und Managed Security Services (MSS), um so ein robustes, sicheres Framework aufzubauen und potenzielle Risiken zu mindern.

Neben dem erforderlichen Selbstschutz haben Verordnungen wie die Datenschutz-Grundverordnung (DSGVO) in Europa und weitere regionale Compliance-Vorgaben

Unternehmen dazu gezwungen, robuste Schutzmaßnahmen zu implementieren, um Cyberangriffe abwehren zu können. Auch in anderen Ländern wie Brasilien und Australien gibt es ähnliche Gesetze, die Anwender vor Cyberbedrohungen schützen sollen.

Cybersicherheit ist für CISOs in Unternehmen zu einem wichtigen Tätigkeitsbereich geworden; dennoch haben IT-Führungskräfte oft Schwierigkeiten, Sicherheitsinvestitionen zu verargumentieren, da es nicht immer möglich ist, den ROI zu messen und aufzuzeigen sowie die mit Bedrohungen verbundenen Risiken zu quantifizieren. Die Ausgereiftheit der verfügbaren Technologien, die Schwierigkeiten bei der Erkennung und Behebung von Schwachstellen und die mangelnde Sensibilisierung der Endbenutzer bereiten Unternehmen und ihren Führungskräfte weiterhin Kopfzerbrechen.

Andererseits bedeutet der Einsatz angemessener Sicherheitstools nicht, dass ein Unternehmen gegen Schwachstellen immun ist; der Faktor Mensch ist und bleibt das schwächste Glied in der Sicherheits-Kette, das von Angreifern durch Cyberbedrohungen wie Trojaner- und Phishing-Angriffe entsprechend ausgenutzt wird. Ein zu geringes Sicherheitsbewusstsein der Endanwender kann zu gezielten Angriffen wie Advanced Persistent Threats (APTs) und Ransomware führen, die den guten Ruf des Unternehmens beeinträchtigen, Daten- und finanzielle Verluste verursachen und zu Betriebsausfällen führen. Daher werden Benutzerschulungen, Risikobewertungen und Beratungsdienste weiterhin eine Schlüsselrolle bei der Gewährleistung der Sicherheit der unternehmensweiten Informations- und Kommunikationstechnologie (IKT)-Infrastruktur spielen.

Umfang des Berichts

In dieser ISG Provider Lens™ Quadrantenstudie betrachtet ISG die folgenden 6 Quadranten: Identity & Access Management (IAM), Data Leakage/ Loss Prevention (DLP), Advanced Endpoint Threat Protection, Detection & Response, Strategic Security Services, Technical Security Services und Managed Security Services.

Diese ISG Provider Lens™ Studie bietet IT-Entscheidern:

- Transparente Darstellung der Stärken und Schwächen der relevanten Provider/Softwarehersteller
- Eine differenzierte Positionierung der Anbieter nach Segmenten
- Fokus auf den regionalen Markt

Die Studie dient als Grundlage für wichtige Entscheidungen in Bezug auf Positionierung, Schlüsselbeziehungen und Go-to-Market-Überlegungen. ISG-Berater und Unternehmenskunden nutzen die Informationen aus diesen Berichten auch, um ihre bestehenden Anbieterbeziehungen und potenzielle Engagements zu bewerten.

Anbieterklassifizierungen

Die Anbieterposition spiegelt die Eignung von IT-Dienstleistern/ Softwareanbietern für ein definiertes Marktsegment (Quadrant) wider. Ohne weitere Zusätze gilt die Position immer für alle Unternehmensgrößenklassen und Branchen. Sind die Anforderungen der Unternehmenskunden an die IT-Leistungen unterschiedlich und ist das Spektrum der im lokalen Markt agierenden IT-Anbieter ausreichend groß, erfolgt eine weitere Differenzierung der IT-Anbieter nach Leistung entsprechend der Zielgruppe für Produkte und Dienstleistungen. Dabei berücksichtigt ISG entweder die Branchenanforderungen oder die Anzahl der Mitarbeiter sowie die Unternehmensstrukturen der Kunden und positioniert die IT-Anbieter entsprechend ihrem Schwerpunkt. Im Ergebnis differenziert ISG diese ggf. in zwei Kundenzielgruppen, die wie folgt definiert sind:

- **Midmarket:** Unternehmen mit 100 bis 4.999 Mitarbeitern oder einem Umsatz zwischen US$ 20 Millionen und US$ 999 Millionen mit Hauptsitz in dem jeweiligen Land, in der Regel in Privatbesitz.
- **Large Accounts:** Multinationale Unternehmen mit mehr als 5.000 Mitarbeitern oder einem Umsatz von über 1 Milliarde US-Dollar, mit weltweiten Aktivitäten und global verteilten Entscheidungsstrukturen.

Die ISG Provider Lens™ Quadranten werden anhand einer Bewertungsmatrix erstellt, die vier Segmente (Leader, Product & Market Challenger und Contender) enthält, und die Anbieter werden entsprechend positioniert. Jeder ISG Provider Lens-Quadrant kann einen oder mehrere Dienstleister enthalten, von denen ISG das Potenzial sieht, in den Leader-Quadranten aufzusteigen. Diese Art von Anbieter kann als Rising Star eingestuft werden.

Anzahl der Anbieter in jedem Quadranten: Die ISG bewertet und positioniert die relevantesten Anbieter entsprechend dem Umfang des Berichts für jeden Quadranten und begrenzt die maximale Anzahl der Anbieter pro Quadrant auf 25 (Ausnahmen sind möglich).

Anbieterklassifizierungen: Quadrantenzuordnung

Product Challenger:
Die Product Challenger decken mit ihren Produkten und Services die Anforderungen der Unternehmen überdurchschnittlich gut ab, können aber in den verschiedenen Kategorien der Marktbearbeitung nicht die gleichen Ressourcen und Stärken vorweisen wie die als Leader positionierten Anbieter. Häufig liegt dies in der Größe des Anbieters oder dem schwachen „Footprint" im jeweiligen Zielsegment begründet.

Leader:
Die als Leader eingeordneten Anbieter verfügen über ein hoch attraktives Produkt- und Serviceangebot sowie eine ausgeprägt starke Markt- und Wettbewerbsposition und erfüllen daher alle Voraussetzungen für eine erfolgreiche Marktbearbeitung. Sie sind als strategische Taktgeber und Meinungsführer anzusehen. Darüber hinaus sind sie ein Garant für Innovationskraft und Stabilität.

Contender:
Unternehmen, die als Contender positioniert sind, mangelt es bisher noch an ausgereiften Produkten und Services bzw. einer ausreichenden Tiefe und Breite des Offerings. Anbieter in diesem Bereich sind häufig auch Generalisten oder auch Nischenanbieter.

Market Challenger:
Market Challenger verfügen naturgemäß über eine hohe Wettbewerbsstärke, haben allerdings auf der Portfolio Seite noch ausgeprägtes Verbesserungspotenzial und liegen hier klar hinter den Unternehmen, die als „Leader" positioniert sind. Häufig sind es etablierte Anbieter, die Trends aufgrund ihrer Größe und der damit einhergehenden Unternehmensstruktur nicht schnell genug aufgreifen und in puncto Portfolioattraktivität deshalb Optimierungspotentiale vorweisen.

Anbieterklassifizierungen: Kategorien

★ Rising Stars
Ein solches Unternehmen kann zum Zeitpunkt der Auszeichnung ein vielversprechendes Portfolio bzw. die erforderliche Markterfahrung inkl. der notwendigen Roadmap mit adäquater Ausrichtung an den wichtigen Markttrends bzw. Kundenanforderungen vorweisen. Zudem verfügt das Unternehmen über ein ausgezeichnetes Management mit Verständnis für den lokalen Markt. Dieses Prädikat erhalten daher nur Anbieter oder Dienstleister, die in den letzten zwölf Monaten extreme Fortschritte hinsichtlich der gesteckten Zielerreichung verzeichnet haben und dank ihres überdurchschnittlichen Impacts und ihrer Innovationskraft auf dem besten Weg sind, innerhalb von 12-24 Monaten zu den Top-Anbietern zu gehören.

Not in
Diese Anbieter konnten aus einem oder mehreren Gründen nicht in den jeweiligen Quadranten positioniert werden: ISG konnte nicht genug Informationen für eine Positionierung einholen, das Unternehmen bietet nicht die entsprechend relevanten Services bzw. Lösungen, die für die einzelnen Quadranten definiert wurden, oder das Unternehmen konnte aufgrund seines Marktanteils, der Leistungsfähigkeit, der Kundenzahl oder anderer Größenmetriken mit den anderen Mitbewerbern im jeweiligen Quadranten nicht direkt verglichen werden. Eine „Nicht-Aufnahme" bedeutet weder, dass der Anbieter diese Leistungen oder Lösungen nicht bereitstellt noch soll damit etwas anderes ausgesagt werden.

Identity and Access Management (IAM)

Wer sollte dieses Kapitel lesen?

Dieser Bericht ist für Unternehmen aller Branchen in Deutschland relevant. Hier werden die Lösungen von Anbietern bewertet, die IAM-Lösungen anbieten.

Im Rahmen dieses Quadranten wird insbesondere die aktuelle Marktpositionierung von Anbieter von Identity & Access Management (IAM-) Lösungen untersucht, die mit ihren Angeboten Sicherheitsbedrohungen für Unternehmen in Deutschland reduzieren, und auch darauf eingegangen, wie die einzelnen Anbieter die wichtigsten Herausforderungen angehen.

In Deutschland sind Sicherheitslösungen vor allem in den Branchen Finanzdienstleistungen und verarbeitende Industrie sowie im öffentlichen Sektor im Einsatz. Unternehmen bevorzugen IAM-Anbieter, die eine adaptive Zugriffskontrolle, eine kontextabhängige Zugriffskontrolle und eine Zero-Trust-Architektur ermöglichen.

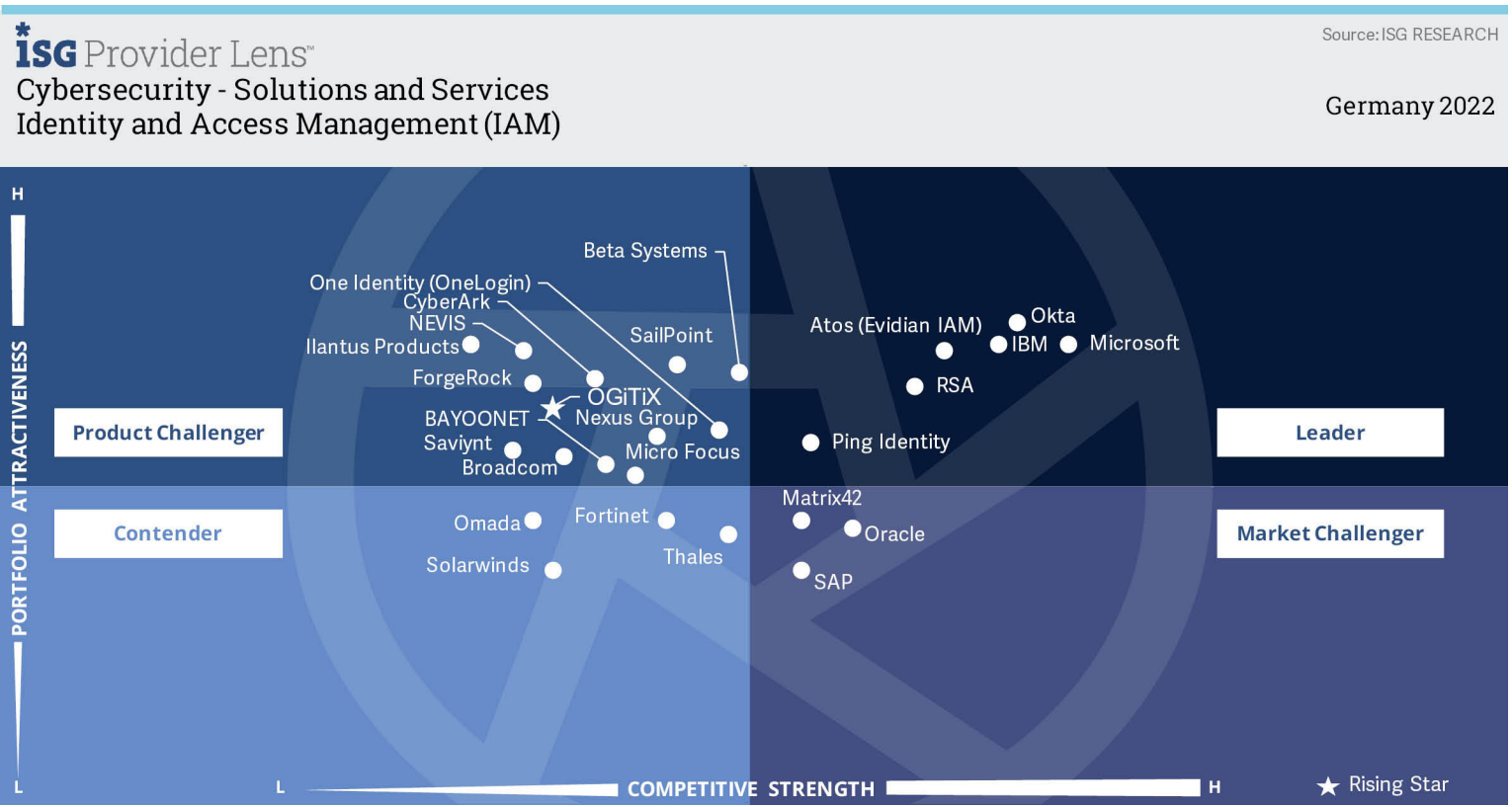
Bei vielen Unternehmen wurde die Cloud-Migration durch die COVID-19-Pandemie beschleunigt, da die Zahl der Remote-Mitarbeiter über Nacht drastisch anstieg. Da die Mitarbeiter Zugriff von außerhalb des herkömmlichen Netzwerks benötigten, waren viele Unternehmen, die auf lokale IAM-Systeme angewiesen waren, gezwungen, cloud-basierte Optionen in Betracht zu ziehen. Um die geforderten modernen Arbeitsplätze bieten zu können, wenden sich Unternehmen verstärkt über die Cloud gemanagten IAM-Funktionen zu, die die Bereitstellung von Produkten erfordern, die über mehrere Cloud-Installationen hinweg funktionieren.

Unternehmen implementieren Zero-Trust-Verfahren und -Richtlinien, die in IAM integriert sind, um nicht nur Benutzerverifizierung, sondern auch eine kontinuierliche Überprüfung von Maschinen- und Anwendungsidentitäten zu ermöglichen.

Verantwortliche für die Informationssicherheit (CISOs) erfahren aus diesem Bericht, wie Anbieter von IAM-Lösungen die erheblichen Herausforderungen im Zusammenhang mit der Einhaltung von Vorschriften und der Sicherheit bewältigen und gleichzeitig eine nahtlose Erfahrung für Unternehmenskunden gewährleisten.

Strategieverantwortliche werden in diesem Bericht über die Möglichkeiten von Lösungsanbietern informiert, durch die sie die sich entwickelnden neuen Kundenanforderungen besser adressieren und sich so einen Wettbewerbsvorteil verschaffen können.

Daten- und Datenschutzbeauftragten vermittelt dieser Bericht ein besseres Verständnis der Angebote von Anbietern im Hinblick auf den Informations- und Datenschutz, die Information Governance, die Datenqualität und das Data Lifecycle Management.



Dieser Quadrant bewertet die **relevantesten IAM-Anbieter** in Deutschland. Nicht einbezogen sind Anbieter, die keine eigene Software anbieten beziehungsweise betreiben. Zu den wichtigsten Themen gehören Single-Sign-On **(SSO)** und **Multifaktor**-Authentifizierung, wobei die **passwortlose** Authentifizierung immer bedeutender wird.

Frank Heuer

Definition

IAM-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Services für die sichere Verwaltung von Benutzeridentitäten und -geräten in Unternehmen Dieser Quadrant umfasst auch Software-as-a-Service-Angebote auf Basis von proprietärer Software. Reine Dienstleister, die keine IAM-Produkte (On-Premise oder in der Cloud) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert. Entsprechend der individuellen Unternehmensanforderungen können diese Lösungen auf verschiedene Arten bereitgestellt werden, z.B. vor Ort oder in der Cloud (vom Kunden verwaltet), auf Basis eines as-a-Service-Modells oder in Form einer kombinierten Lösung.

IAM-Lösungen dienen der Erfassung, Aufzeichnung und Verwaltung von Benutzeridentitäten und zugehörigen Zugriffsrechten sowie dem spezialisierten Zugriff auf kritische Assets, einschließlich Privileged Access Management (PAM). Sie stellen sicher, dass die Zugriffsrechte entsprechend den definierten Richtlinien gewährt werden. Um mit bestehenden und neuen Anforderungen aus der Anwendungswelt umgehen zu können, werden IAM-Lösungen im Rahmen von Management Suites zunehmend in sichere Mechanismen, Frameworks und Automatisierung (z.B. der Risikobewertung) eingebunden, um Nutzer- und Attacken-Profiling in Echtzeit durchführen zu können. Von den Lösungsanbietern werden zudem weitere Funktionalitäten im Zusammenhang mit Social Media und mobilen Anwendungen erwartet, um deren Sicherheitsbedarfe abzudecken, die über web- und kontextbezogenes Berechtigungsmanagement hinausgehen. Auch das Machine Identity Management (MIM), also die Verwaltung von Maschinenidentitäten, ist hier mit berücksichtigt.

Zulassungskriterien

1. Die Lösung sollte in Kombination vor Ort, in der Cloud, als Identity as a Service (IDaaS) und einem verwalteten Modell eines Drittanbieters eingesetzt werden können.
2. Authentifizierungs-Unterstützung anhand einer Kombination von Single-Sign-On (SSO), Multifaktor-Authentifizierung (MFA) sowie risiko- und kontextbasierten Modellen
3. Unterstützung von rollenbasiertem Zugriff und Privileged Access Management (PAM)
4. Zugriffsmanagement für eine oder mehrere Unternehmensanforderungen wie Cloud, Endpunkte, mobile Geräte, Anwendungsprogrammierschnittstellen (APIs) und Webanwendungen.
5. Unterstützung von einem oder mehreren älteren und neueren IAM-Standards, einschließlich, aber nicht nur, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust und SCIM
6. Sicherer Zugriff durch eine oder mehrere der folgenden Möglichkeiten: Directory-Lösungen, Dashboard- oder Self-Service-Management und Lifecycle Management (Migration, Synchronisierung und Replizierung)

Beobachtungen

IAM ist derzeit und zukünftig ein besonders wichtiges Cybersecurity-Thema. Ein wesentlicher Grund für die steigende Nachfrage nach IAM-Lösungen ist die zunehmende Digitalisierung aller Bereiche, die dazu beiträgt, dass nicht nur Benutzer und deren Identitäten zu schützen sind, sondern auch Maschinen und bestimmte Unternehmensbereiche (Industrie 4.0). Zudem nimmt die Anzahl zu verwaltender digitaler Identitäten stetig zu. Ein weiterer Faktor ist der Umzug vieler Mitarbeiter in das Home Office. Durch vermehrte Remote- und mobile Zugriffe auf die Unternehmensressourcen wird die Regulierung und Kontrolle des Zugriffs zunehmend wichtig. Dies resultiert auch in nochmals höheren Sicherheits- bei gleichzeitig höheren Komfortanforderungen. Daher gewinnen Themen wie intuitive Schnittstellen, passwortlose Authentifizierung sowie der Einsatz von Biometrie und künstlicher Intelligenz an Bedeutung.

Darüber hinaus werden Unternehmensanwendungen und -daten immer mehr in die Cloud migriert. Dies erfordert IAM-Lösungen, die auch Cloudanwendungen absichern können.

Wie im Softwaremarkt insgesamt ist auch hinsichtlich IAM-Lösungen eine Verschiebung vom On-Premise-Betrieb in die Cloud festzustellen. Die meisten Anbieter haben sich darauf eingestellt und bieten sowohl den On-Premise- als auch den Cloudbetrieb (Identity as a Service) an. Auch reine Cloudanbieter treten immer häufiger auf, allen voran der US-amerikanische Anbieter Okta. Auf der anderen Seite profilieren sich Anbieter im Markt, die die On-Premises-Delivery betonen, wie der neue Rising Star OGiTiX. Ein Grund dafür ist, dass bestimmte Unternehmen keine Cloudlösungen nutzen können, zum Beispiel im Gesundheitswesen.

Neben der Identifizierung eines neuen Rising Stars war anbieterseitig die Übernahme von One Login durch OneIdentity die markanteste Entwicklung im IAM-Markt.

Von den 97 Anbietern, die in dieser Studie bewertet wurden, konnten sich 26 für diesen Quadranten qualifizieren. Dabei erreichten sechs eine Position als Leader, ein Anbieter – OGiTiX - wurde als Rising Star identifiziert.

Atos

Atos – Atos bietet seine Produkte für Identity & Access Management unter dem Namen „Evidian" an. Atos ist ein innovativer Anbieter mit einem vielseitigen IAM-Portfolio und ist darüber hinaus in der Lage, seinen Kunden große Flexibilität bei der Wahl der Betriebsform ihrer Lösungen zu bieten.

IBM

IBM – IBM bietet seine Produkte für Identity & Access Management unter dem Namen „IBM Security Verify Access" an. IBM kann im Markt für Identity & Access-Management von seinem breiten Leistungsspektrum und seiner großen Marktpräsenz profitieren und punktet darüber hinaus mit starker Performance und einer hohen Integrationsfähigkeit.

Microsoft

Microsoft – Das Angebot von Microsoft für Identity & Access Management wird unter anderem durch „Azure Active Directory" repräsentiert. Microsoft baut seine Position im Markt für Identity- & Access-Management-Lösungen geschickt mit Hilfe von bewährten

Marketingrezepten, aber auch mit technologischen Verbesserungen des Produktes aus.

Okta

Okta – Okta hat sich auf Identity & Access-Management-Lösungen aus der Cloud spezialisiert. Der rein cloudbasierte Ansatz von Okta ermöglicht seinen Kunden einen leichten Einstieg in IAM-Lösungen. Auch aufgrund dieses Vorteils baut Okta seine Position im deutschen Markt für Identity & Access Management immer weiter aus.

Ping Identity

Ping Identity – Zum Portfolio von Ping Identity für Identity & Access Management zählen die cloudbasierenden Angebote PingOne MFA und PingOne Verify. Ping Identity bietet eine innovative IAM-Lösung an, die vielseitig einsetzbar ist. Auch aufgrund dieser Merkmale ist Ping Identity auch in Deutschland zunehmend erfolgreich.

RSA

RSA – RSA bietet sein Portfolio für Identity & Access Management unter dem Namen „RSA SecurID Suite“ an und erleichtert mit seinem Identity- & Access-Management-Angebot die Implementierung und das Management der IAM-Lösung. Die Kunden von RSA profitieren von der hohen Leistungsfähigkeit der IAM-Lösung.

OGiTiX

OGiTiX – OGiTiX ist der „Rising Star“ unter den Anbietern von Identity- & Access-Management-Lösungen in Deutschland. OGiTiX bietet sein Produktportfolio für IAM unter dem Namen „OGiTiX unimate“ an. Die Lösung von OGiTiX kann dank der integrierten Low-Code-Plattform mit den zukünftigen Kundenanforderungen wachsen und angepasst werden.

Data Leakage/Loss Prevention (DLP) and Data Security

Wer sollte dieses Kapitel lesen?

Dieser Bericht ist für Unternehmen aller Branchen in Deutschland relevant. Hier werden die Lösungen von Anbietern bewertet, die DLP-Lösungen anbieten.

Im Rahmen dieses Quadranten wird insbesondere die aktuelle Marktpositionierung von Anbietern von Data Leakage/Loss Prevention (DLP) und Datensicherheits-Lösungen untersucht, die mit ihren Angeboten Sicherheitsbedrohungen für Unternehmen in Deutschland reduzieren, und auch darauf eingegangen, wie die einzelnen Anbieter die wichtigsten Herausforderungen angehen.

Der rasche Wechsel zur Remote-Arbeit während der Pandemie beschleunigte die Einführung von Cloud-Diensten, da die Unternehmensverantwortlichen Schwierigkeiten damit hatten, die neue Nachfrage nach dezentralisierten Arbeitskräften zu befriedigen. Unternehmen aller Größenordnungen investieren auch weiterhin stark in DLP-Lösungen, um ihre Daten zu schützen und die Einhaltung von Vorschriften zu gewährleisten.

Es herrschen Bedenken hinsichtlich gezielter Cyberangriffe, Trends der digitalen Transformation und der Datenschutzgesetze. Immer mehr Datenschutzverletzungen in Deutschland, Compliance- und regulatorische Anforderungen sowie eine Verschiebung der Nachfrage in Richtung Public und Private Clouds erhöhen die Nachfrage nach DLP-Lösungen.

Verantwortliche für die Informationssicherheit (CISOs) erfahren aus diesem Bericht, wie Anbieter von DLP-Lösungen die erheblichen Herausforderungen im Zusammenhang mit der Einhaltung von Vorschriften und der Sicherheit bewältigen und gleichzeitig eine nahtlose Erfahrung für Unternehmenskunden gewährleisten.

Unternehmensleiter (CEOs) werden in diesem Bericht über die enormen Möglichkeiten von Lösungsanbietern informiert, durch die sie die sich entwickelnden neuen Kundenanforderungen besser adressieren und sich so einen Wettbewerbsvorteil verschaffen können.

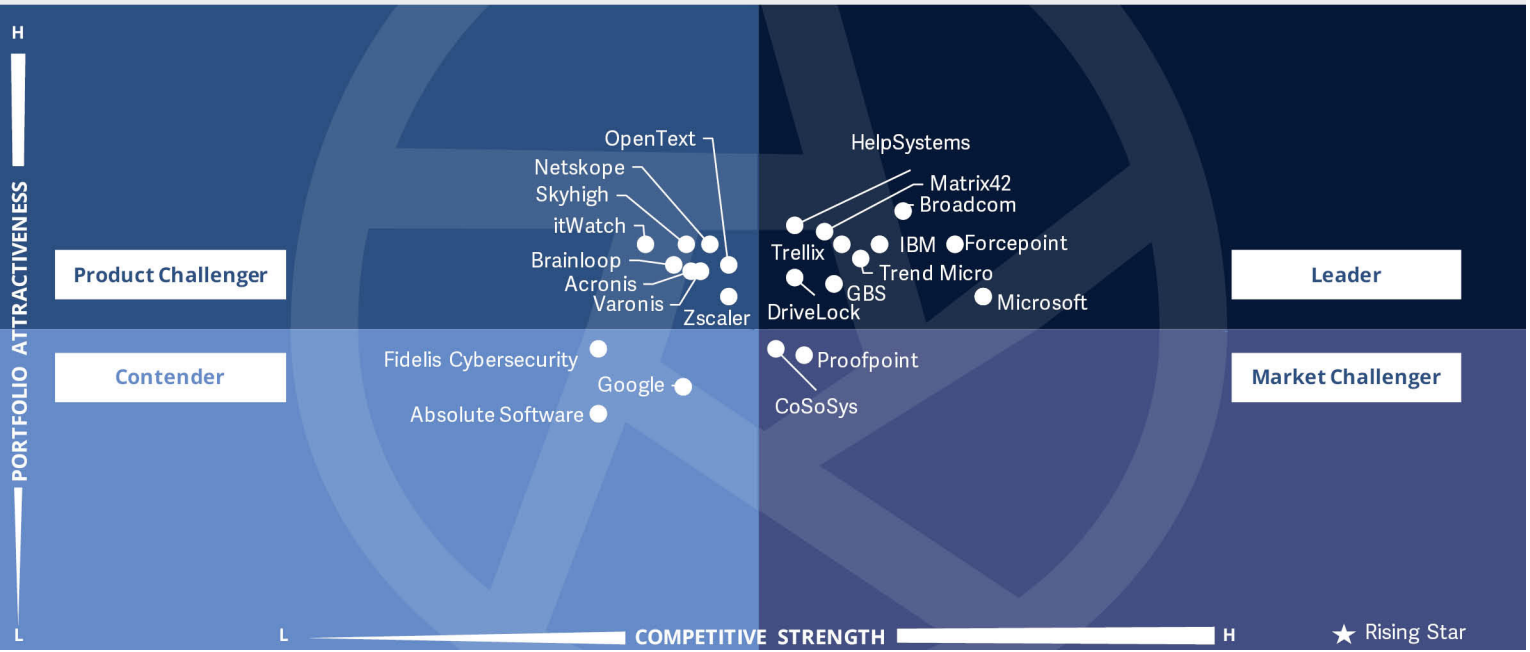
Daten- und Datenschutzbeauftragten vermittelt dieser Bericht ein besseres Verständnis der Angebote von Anbietern im Hinblick auf den Informations- und Datenschutz, die Information Governance, die Datenqualität und das Data Lifecycle Management.

ISG Provider Lens™

Cybersecurity - Solutions and Services
Data Leakage/Loss Prevention (DLP) and Data Security

Source: ISG RESEARCH

Germany 2022



Dieser Quadrant bewertet die **relevantesten DLP-Anbieter** in Deutschland. Nicht einbezogen sind Anbieter, die keine eigene Software anbieten beziehungsweise betreiben. Die Relevanz des **Schutzes von Daten** und **geistigem Eigentum** tragen zur Bedeutung des Marktes bei.

Frank Heuer

Definition

DLP-Vendoren und -Lösungsanbieter offerieren proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch Software-as-a-Service-Angebote auf Basis von proprietärer Software. Reine Dienstleister, die keine DLP-Produkte (on-premise oder cloudbasiert) auf Basis eigenentwickelter Software anbieten, werden hier nicht analysiert. DLP-Lösungen sind Angebote, die sensible Daten identifizieren und überwachen können, den Zugriff nur für autorisierte Benutzer ermöglichen und Datenverluste verhindern. Die Lösungen der Anbieter in diesem Markt bestehen aus einer Kombination von Produkten, die Transparenz und Kontrolle über sensible Daten in Cloud-Anwendungen, Endpunkten, im Netzwerk und auf anderen Geräten gewährleisten.

Sie gewinnen erheblich an Bedeutung, da es für Unternehmen immer schwieriger wird, Datenbewegungen und -übertragungen zu kontrollieren. Die Zahl der Geräte, einschließlich der Mobilgeräte, die zur Datenspeicherung genutzt werden, nimmt in Unternehmen zu. Sie sind meistens mit einer Internetverbindung ausgestattet und können Daten senden und empfangen, ohne diese über ein zentrales Internet-Gateway zu leiten. Datensicherheitslösungen schützen Daten vor unberechtigtem Zugriff, Offenlegung oder Diebstahl.

Zulassungskriterien

1. DLP-Angebot auf Basis von proprietärer Software und nicht auf Basis von Software von Drittanbietern
2. DLP-Unterstützung über eine beliebige Architektur wie Cloud, Netzwerk, Speicher oder Endpunkt
3. Schutz von sensiblen Daten, egal ob es sich dabei um strukturierte oder unstrukturierte Daten, Text- oder Binärdaten handelt
4. Grundlegender Management-Support verfügbar, einschließlich, aber nicht nur Reporting, Richtlinienkontrolle, Installation und Wartung sowie erweiterte Funktionen zur Erkennung von Bedrohungen
5. Fähigkeit, sensible Daten zu erkennen, Richtlinien durchzusetzen, den Datenverkehr zu überwachen und die Daten-Compliance zu verbessern

Beobachtungen

Zum gewachsenen Interesse an DLP-Lösungen tragen verschiedene Faktoren bei, welche die Sicherheit der Daten im Unternehmen berühren. So haben sich Daten und geistiges Eigentum zu immer wichtigeren und teilweise existentiell bedeutsamen Unternehmens-Assets entwickelt.

Auch die zunehmende geschäftliche Nutzung privater Endgeräte stellt eine besondere Herausforderung hinsichtlich des Schutzes vor unerwünschten Datenabflüssen dar, da sie sich oftmals der Konfiguration und Kontrolle durch die betriebliche Administration entziehen und teilweise auch aus rechtlichen Gründen nicht umfassend betrieblich überwacht werden dürfen. DLP-Lösungen müssen diese Einschränkungen bei der Kontrolle berücksichtigen, ohne betriebliche Sicherheitslücken zuzulassen. Mit der Datenschutz-Grundverordnung hat die Bedeutung des Datenschutzes in Unternehmen – und damit auch der DLP-Lösungen – weiter zugenommen.

Die enorm wachsende Menge an Daten im Unternehmen macht leistungsfähige DLP-Lösungen erforderlich, die die Daten schnell aufspüren, klassifizieren und entsprechend ihrem Schutzbedarf vor unerlaubten Aktionen wie Kopieren oder Verschieben schützen. Cloudspeicherlösungen und Cloud Apps führen dazu, dass Daten bei der Verarbeitung unter Umständen ungewollt das Firmennetzwerk verlassen. Dabei besteht auch die Gefahr, dass betriebliche Daten in private Cloudspeicherdienste übertragen werden. Soziale Netzwerke und andere Social-Media-Plattformen eröffnen neue Kommunikationskanäle, über die Daten abfließen können; hinzu kommen die Risiken durch Datentransfers via E-Mail. Aber nicht nur ungewollt können Daten durch das Verschulden von internen Akteuren abfließen; auch vor ungetreuem Verhalten interner Beteiligter müssen sich Unternehmen schützen können.

Anbieterseitig waren zwei Unternehmenszusammenschlüsse die markanteste Entwicklung: HelpSystems übernahm Digital Guardian, Trellix wurde 2021 durch die Fusion des Unternehmenskundengeschäftes von McAfee mit FireEye gegründet.

Von den 97 Anbietern, die in dieser Studie bewertet wurden, konnten sich 23 für diesen Quadranten qualifizieren. Dabei erreichten zehn eine Position als Leader.

Broadcom

Broadcom – Mit seiner umfangreichen und innovativen Lösung kann sich Broadcom als Spitzenreiter im deutschen Markt für Data-Leakage/-Data-Loss-Produkte positionieren. Dabei ist unter anderem die Leistungsfähigkeit und Flexibilität der Lösung für Broadcom und seine Kunden von Vorteil. Des Weiteren unterstützt Broadcom seine Kunden durch Zentralisierung und Vereinheitlichung.

DriveLock

DriveLock – DriveLock punktet mit seiner Vertrauenswürdigkeit als Anbieter von Data-Leakage- & Data-Loss-Produkten und erwirbt sich dieses Vertrauen im Markt mit den Devisen „Made in Germany" und „No Backdoor". DriveLock zeichnet sich darüber hinaus hinsichtlich seiner DLP-Lösung durch einen konsequenten Einsatz von Machine-Learning-Algorithmen aus.

Forcepoint

Forcepoint – Forcepoint entlastet seine Kunden besonders effektiv bei Data-Leakage- & Data-Loss-Themen, hilft den Anwendern dabei schnell und

entlastet sie zudem hinsichtlich ihrer Herausforderungen in Bezug auf die Sicherung vor Datenverlusten. Forcepoint gelingt dies mit seinem Angebot an fortschrittliche Lösungen.

GBS

GBS – GBS ist in diesem Jahr die Rückkehr in den Kreis der führenden Anbieter von Data-Leakage- & Data-Loss-Produkten gelungen. Neben den verstärkten Aktivitäten von GBS für eine erhöhte Präsenz im deutschen Markt tragen auch die ausgefeilte Technik und das Vier-Augen-Prinzip zu diesem Erfolg bei.

HelpSystems

HelpSystems – HelpSystems hat sich mit der Übernahme von Digital Guardian im deutschen Markt für Data-Leakage- & Data-Loss-Lösungen umfangreich verstärkt und ist somit in der Lage, seine Kunden mit proaktiver Datenklassifizierung, fortschrittlichen Analyse- und Reporting Services sowie einfacher Integration umfassend zu unterstützen.

IBM

IBM – IBM ist in der Lage, eine hohe Marktpräsenz in Deutschland mit einer zukunftsweisenden Data-Loss-/ Data-Leakage-Prevention-Lösung zu vereinen und punktet dabei mit der kompetenten Verknüpfung von Data Loss & Data Leakage Prevention mit Technologien für künstliche Intelligenz. Die Lösung von IBM deckt darüber hinaus ein universelles Einsatzspektrum ab und ist flexibel anwendbar.

Matrix42

Matrix42 – Matrix42 bietet eine anwenderfreundliche und effiziente Data-Loss- & Data-Leakage-Prevention-Lösung an, die über ein sehr breites Funktionsspektrum verfügt. Matrix42 bewirkt mit anwenderfreundlich geringen Beeinträchtigungen eine hohe Akzeptanz bei den Endusern – und fördert damit auch den erfolgreichen Einsatz der Lösung in Unternehmen.

Microsoft

Microsoft – Mit geschicktem Marketing und Unterstützung beim Datenschutz gelingt es Microsoft, seine Position im deutschen Markt für Data-Loss- & Data-Leakage-Prevention-Lösungen weiter auszubauen. Aber nicht nur mit Hilfe von Integration und Bundling etabliert sich Microsoft hierzulande immer mehr, sondern auch mit überzeugenden Leistungsmerkmalen.

Trellix

Trellix – Trellix gelingt es, als neu geformtes Unternehmen als Leader im deutschen Markt für Data-Loss- & Data-Leakage-Prevention-Produkte zu starten. Dank des übernommenen Unternehmens McAfee ist das Vertriebsnetz in Deutschland sehr dicht. Darüber hinaus ist Trellix im Hinblick auf die Delivery durch seine starke lokale und internationale Präsenz sehr vielseitig aufgestellt.

Trend Micro

Trend Micro – Seinen Erfolg im deutschen Markt für Data-Loss- & Data-Leakage-Prevention-Produkte hat Trend Micro insbesondere der Integrierbarkeit sowie der einfachen Einführung und Anwendung seiner DLP-Lösung zu verdanken. Trend Micro setzt mit seinen Schulungsfunktionen zudem an einem wichtiger Faktor für die Datensicherheit an, dem Anwender.

Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)

Wer sollte dieses Kapitel lesen?

Dieser Bericht ist für Unternehmen aller Branchen in Deutschland relevant. Hier werden Anbieter von Produkten für Advanced Endpoint Threat Protection, Detection and Response bewertet.

Im Rahmen dieses Quadranten wird insbesondere die aktuelle Marktpositionierung von Anbietern dargelegt, die Advanced Endpoint Threat Protection, Detection & Response Produkte für deutsche Unternehmenskunden offerieren, und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen.

Endgeräte sind eine häufige Schwachstelle, über die Angriffe in das Netzwerk gelangen können. Mit fortschrittlicher Endpunktsicherheit können Unternehmen Angriffspunkte abriegeln und so einen wertvollen Schutz bieten.

Bei der Erkennung von Endpunkt-Bedrohungen werden Echtzeitüberwachung, automatische Reaktionen und Analysefunktionen miteinander kombiniert, um Angriffe verhindern zu können. Technologien wie KI, maschinelles Lernen, Sicherheitsanalysen und Echtzeit-Bedrohungsinformationen (Threat Intelligence) helfen, potenzielle und komplexe Bedrohungen besser zu erkennen.

Deutschland betrachtet Cybersicherheit als eine Priorität und hat Strategien zur Sicherung der Gesellschaft, der Unternehmen und der Behörden entwickelt, um einen digitalen Schutzraum für die Öffentlichkeit zu schaffen. Diverse politische Maßnahmen und Programme, die die Einführung der neuesten Technologien und Netzwerke unterstützen, haben die deutsche Cybersicherheitslandschaft gestärkt und die Einführung fortschrittlicher Sicherheitslösungen ermöglicht.

Verantwortliche für die Informationssicherheit (CISOs) sollten diesen Bericht lesen, da er einen breiteren Überblick über die neuesten Trends im Security-Markt bietet. Ebenso gewinnen sie dadurch ein umfassendes Verständnis der unmittelbaren Bedrohungen und der zu ihrer Bekämpfung erforderlichen Security-Fähigkeiten und werden bei strategischen Geschäftsentscheidungen zur Lösung bestehender Sicherheitsprobleme unterstützt.

Chief Technology Officers (CTOs) werden in diesem Bericht über die neuesten für sie relevanten Trends informiert und können so mit der sich verändernden Sicherheitslandschaft Schritt halten. Neben der Festlegung strategischer Ziele und der Entwicklung von Sicherheitsplattformen im Einklang mit den Marktanforderungen können CTOs ihre Wettbewerbsvorteile verbessern.

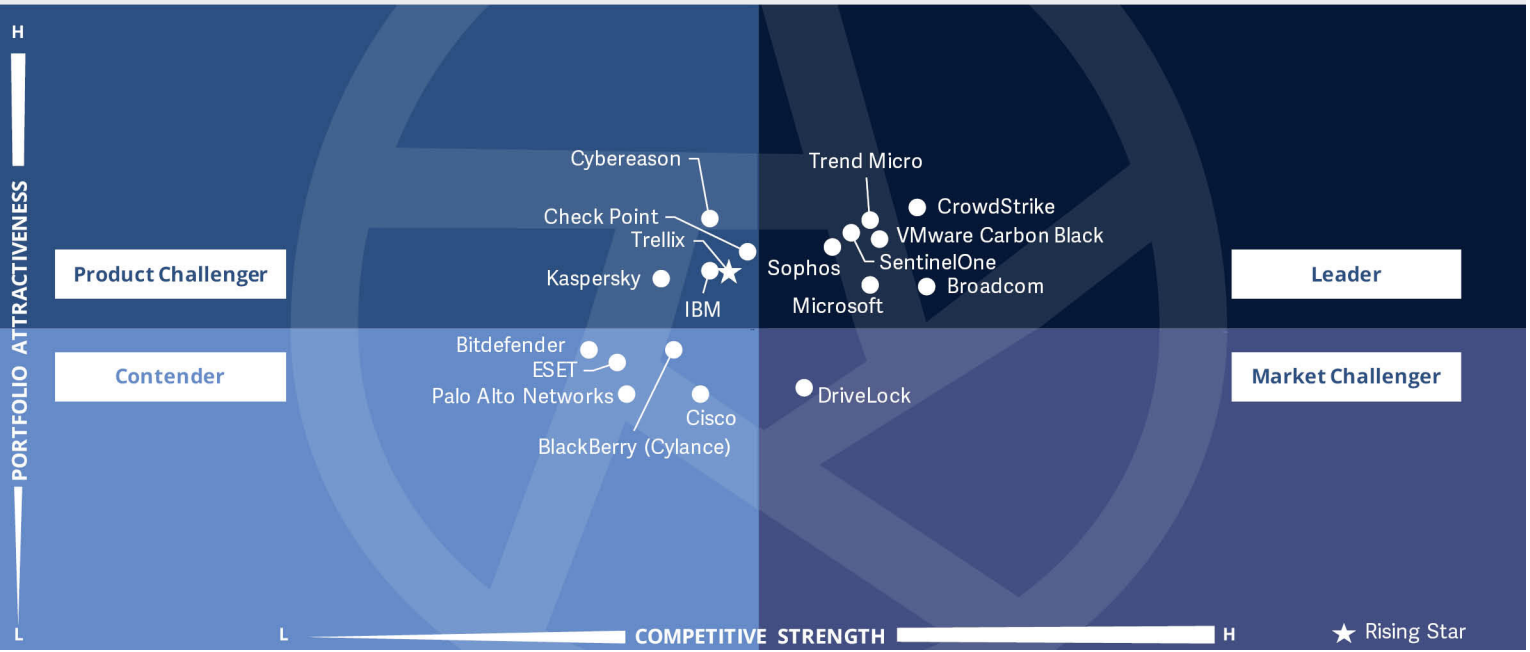
Strategieverantwortliche gewinnen mit diesem Bericht Einblicke in die relative Positionierung und die Fähigkeiten der Anbieter von fortschrittlichen Endpoint-Lösungen in Deutschland; sie erhalten Unterstützung beim Aufsetzen einer Sicherheits-Vision und -Strategie und bei der Entscheidungsfindung in Bezug auf Kooperationen, Partnerschaften und Kostensenkungsinitiativen.

ISG Provider Lens™

Cybersecurity - Solutions and Services
Advanced Endpoint Threat Protection Detection and Response (Advanced ETPDR)

Source: ISG RESEARCH

Germany 2022



Im Rahmen dieses Quadranten werden die **relevantesten Anbieter von Advanced Endpoint Threat Protection, Detection & Response** in Deutschland bewertet. Unberücksichtigt sind Anbieter, die keine eigene Software anbieten beziehungsweise betreiben. **Künstliche Intelligenz** und **Automatisierung** helfen, vor komplexer werdenden Bedrohungen zu schützen.

Frank Heuer

Definition

Anbieter von Advanced- ETPDR-Produkten und -Lösungen offerieren eigenentwickelte, proprietäre Software und zugehörige Dienstleistungen. Dieser Quadrant umfasst auch Software-as-a-Service-Angebote auf Basis von proprietärer Software. Reine Dienstleister, die kein auf eigenentwickelter Software basierendes Advanced- ETPDR-Produkt (vor Ort oder in der Cloud) anbieten, werden hier nicht analysiert. Im Rahmen dieses Quadranten werden Anbiete bewertet, die Produkte für die kontinuierliche Überwachung und vollständige Transparenz aller Endpunkte bieten und hochentwickelte Bedrohungen analysieren, verhindern und darauf reagieren können. Endpunkt-Sicherheitslösungen, die Secure Access Service Edge (SASE) integrieren, werden hier ebenfalls berücksichtigt. Für ISG umfasst die Endpunktsicherheit auch den entsprechenden Schutz von OT-Lösungen (Operational Technology).

Diese Lösungen gehen über einen reinen signaturbasierten Schutz hinaus und beinhalten auch den Schutz vor Risiken wie Ransomware, Advanced Persistent Threats (APTs) und Malware; zu diesem Zweck werden Vorfälle über alle Endpunkte hinweg untersucht. Die Lösung sollte in der Lage sein, den gefährdeten Endpunkt zu isolieren und die notwendigen Korrekturmaßnahmen/ Reparaturen durchzuführen. Solche Lösungen bestehen aus einer Datenbank, in der die vom Netzwerk und den Endpunkten gesammelten Informationen aggregiert, analysiert und untersucht werden, und dem Agenten, der im Host-System residiert und die Überwachungs- und Reporting-Funktionen für die Vorfälle bereitstellt.

Zulassungskriterien

1. Umfassende und vollständige Abdeckung und Visibilität aller Endpunkte im Netzwerk
2. Nachweisliche effektive Abwehr von komplexen Bedrohungen wie Advanced Persistent Threats, Ransomware und Malware
3. Nutzung und Analyse von Bedrohungsdaten sowie Echtzeit-Einblicke in Bedrohungen, die von den Endpunkten ausgehen
4. Automatische Reaktionsfunktionen, unter anderem das Löschen bösartiger Dateien, Sandboxing, das Beenden verdächtiger Prozesse, das Isolieren infizierter Endpunkte und das Sperren verdächtiger Konten

Beobachtungen

Cyberangriffe nehmen in Deutschland sowohl in ihrer Quantität als auch besonders hinsichtlich ihrer Gefährlichkeit immer weiter zu. Zudem wandeln sich die Attacken immer schneller. Des Weiteren trägt der Ukraine-Konflikt zu einer gewachsenen Bedrohungswahrnehmung bei. Lösungen für Advanced Endpoint Threat Protection, Detection & Response sollen Unternehmen vor diesen komplexer werdenden Bedrohungen schützen.

Herkömmliche Sicherheitslösungen – wie klassische Anti-Viren-Lösungen – sind im immer dynamischer werden Bedrohungsumfeld zunehmend überfordert, da sie auf Signaturen beruhen. Lösungen für Advanced Endpoint Threat Protection, Detection & Response hingegen sind proaktiv gegen potenzielle Bedrohungen ausgerichtet, da sie Verhaltensanalysen und Machine Learning beziehungsweise künstliche Intelligenz zur Anwendung bringen. Des Weiteren ermöglichen diese fortschrittlichen Sicherheitslösungen eine kontinuierliche Überwachung der Endpoints.

Nicht nur die Entwicklung auf der Angreiferseite führt zu einer zunehmenden Nachfrage nach Lösungen für Advanced Endpoint Threat Protection, Detection & Response, sondern – speziell in jüngster Zeit – auch die veränderte Situation der Anwenderunternehmen und ihrer Mitarbeiter. Die zunehmende Nutzung von Clouddaten und -anwendungen ist bereits seit mehreren Jahren ein zu beobachtender Trend. Gerade durch die Pandemie hat sich diese Entwicklung verstärkt – viele Mitarbeiter arbeiten inzwischen von zu Hause aus und damit außerhalb der gesicherten Unternehmenssysteme. Damit hat sich die Bedrohungslage zusätzlich verschärft. Dementsprechend interessieren sich immer mehr Unternehmen für proaktiv und umfassender schützende Advanced-Endpoint-Threat-Protection-, Detection- & Response-Lösungen.

Anbieterseitig war ein Unternehmenszusammenschluss die markanteste Entwicklung: Trellix wurde 2021 durch die Fusion des Unternehmenskundengeschäftes von McAfee mit FireEye gegründet und konnte sich als Rising Star positionieren.

Von den 97 Anbietern, die in dieser Studie bewertet wurden, konnten sich 18 für diesen Quadranten qualifizieren. Dabei erreichten sieben eine Position als Leader, ein Anbieter – Trellix – wurde als Rising Star identifiziert.

Broadcom

Broadcom – Broadcom überzeugt mit flexiblen Schutzmaßnahmen seiner Lösungen für Advanced Endpoint Threat Protection, Detection & Response, die auf die individuellen Anforderungen seiner Kunden eingehen. Das Portfolio von Broadcom ist sehr umfangreich, und die Lösungen decken ein breites Spektrum an Endpoints ab.

CrowdStrike

CrowdStrike – CrowdStrike offeriert seinen Kunden ein leistungsfähiges Angebot im Markt für Advanced Endpoint Threat Protection, Detection & Response und hat sich damit einen guten Namen im Markt erworben. Das Bereitstellungsmodell von CrowdStrike ist zeitgemäß. Zudem bietet die Lösung zahlreiche Leistungsmerkmale.

Microsoft

Microsoft – Microsofts Erfolg im Markt basiert unter anderem auf einer bewährten Strategie und versteht es, seine Präsenz im Softwaremarkt auch im Markt für Advanced Endpoint Threat Protection, Detection & Response zu nutzen. Microsofts Erfolg basiert aber nicht nur auf geschicktem Marketing, sondern auch auf dem sehr breiten Funktionsspektrum.

SentinelOne

SentinelOne – SentinelOne überzeugt mit einer aktuellen Lösung für Advanced Endpoint Threat Protection, Detection & Response. Die Lösung von SentinelOne lässt sich einfach bereitstellen, hat ein zeitgemäßes Design und bietet dadurch effektiven Schutz. SentinelOne bietet seinen Kunden große Flexibilität; zudem überzeugt der Support von SentinelOne die Kunden.

Sophos

Sophos – Sophos überzeugt nicht nur seine bestehenden Kunden mit dem integrierten Management seiner Security-Lösungen auch für Endpoints. Sophos unterstützt seine Kunden mit künstlicher Intelligenz. Das Portfolio ist zudem sehr umfangreich und wartet mit vielseitigen Funktionen auf. Darüber hinaus bietet Sophos erweiterte Funktionen für seinen Managed Service an.

Trend Micro

Trend Micro – Trend Micro bietet seinen Kunden eine sehr umfassende Lösung für Advanced Endpoint Threat Protection, Detection & Response. Auch die Anwender von Legacy-Lösungen werden von Trend Micro optimal unterstützt. Über sein umfangreiches Partnernetzwerk verfügt der Anbieter in Deutschland über eine große Marktreichweite.

VMware Carbon Black

VMware Carbon Black – VMware Carbon Black kann eine sehr leistungsfähige und zugleich benutzerfreundliche Lösung vorweisen, dies sich sehr gut für das Threat Hunting eignet. VMware Carbon Black hat im Zuge der Weiterentwicklung seiner Lösung den Schutz von Cloud Workloads ausgebaut. Die Managementkonsole zeichnet sich durch hohe Leistungsfähigkeit aus.

Trellix

Trellix – Trellix ist der Rising Star im deutschen Markt für Advanced Endpoint Threat Protection, Detection & Response, unter anderem auch weil das Portfolio auf den neuesten Stand gebracht wurde. Die Lösung ist darüber hinaus kundenfreundlich, und Trellix bietet seinen Kunden auch umfassende Unterstützung.

Technical Security Services

Wer sollte dieses Kapitel lesen?

Dieser Bericht ist für Unternehmen aller Branchen in Deutschland relevant. Hier werden Anbieter bewertet, die sich nicht ausschließlich auf ihre jeweiligen proprietären Cybersecurity-Produkte konzentrieren, sondern Produkte oder Lösungen anderer Anbieter implementieren und integrieren können.

Im Rahmen dieses Quadranten wird die aktuelle Marktpositionierung von Anbietern dargelegt, die Implementierungs- und Integrations-Services für Security-Produkte und -Lösungen in Deutschland offerieren, und auch aufgezeigt, wie die einzelnen Anbieter die wichtigen Herausforderungen in dieser Region angehen.

Mithilfe der von den Anbietern offerierten Dienste können sich Unternehmen auf die Abwehr von Angriffen vorbereiten und schnell auf Bedrohungen reagieren, die ihre sensiblen Daten gefährden.

Angesichts des drastischen Anstiegs von Cyberbedrohungen ist die Nachfrage nach technischen Sicherheitsdienstleistungen in Deutschland hoch. Jeder Unternehmenskunde hat jedoch seine eigenen Prioritäten in Bezug auf Sicherheit, Skalierbarkeit etc.

Im Laufe des letzten Jahres ist in Deutschland die Nachfrage nach Security Services gestiegen, da sich die Angriffsfläche aufgrund der Digitalisierung insgesamt schnell ausweitet. Es sind kostengünstige Sicherheitsdienste gefragt, die sich in die vorhandenen Systeme integrieren lassen. Unternehmen in der Region suchen auch nach hochqualifizierten, spezialisierten Services, die Flexibilität und Sicherheit garantieren, um die Kunden- und Mitarbeitererfahrung zu verbessern.

Verantwortliche für die Informationssicherheit (CISOs) sollten diesen Bericht lesen, da die Vorstandsebene gefordert ist, im Zuge der digitalen Transformation ein Gleichgewicht zwischen Datensicherheit, Kundenerfahrung und Datenschutz zu finden. Der Bericht vermittelt ein umfassendes Verständnis der führenden Dienstleister im Markt, die IT-Sicherheitslösungen integrieren, um ihnen dabei zu helfen, dieses Ziel zu erreichen.

Strategieverantwortliche gewinnen durch diesen Bericht ein besseres Verständnis der relativen Positionierung und Fähigkeiten von Dienstleistern, mit denen sie gemeinsam eine effektive Cybersecurity-Lösung entwickeln können. Der Bericht vermittelt zudem nützliche Informationen für die Implementierung einer Sicherheitslösung.

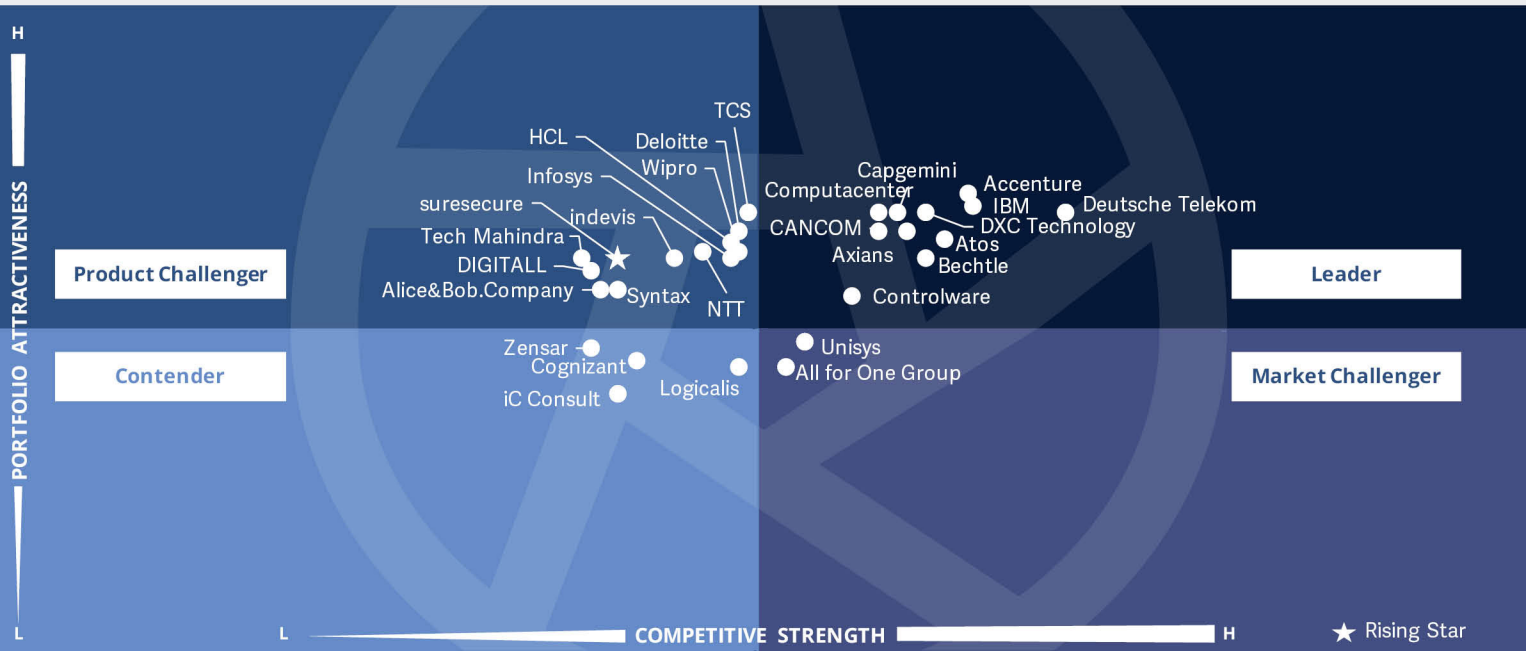
Security-Analysten erfahren aus diesem Bericht, wie Anbieter die Sicherheits- und Datenschutzvorgaben in Deutschland einhalten; sie bleiben so über die kommenden Markttrends auf dem Laufenden.

ISG Provider Lens™

Cybersecurity - Solutions and Services
Technical Security Services

Source: ISG RESEARCH

Germany 2022



Dieser Quadrant bewertet die **relevantesten Dienstleister für technische Security Services** in Deutschland. Unberücksichtigt sind Anbieter, die ihre Leistungen nur auf eigene Produkte beziehen. **Externe Dienstleister** werden immer wichtiger, um IT-Security-Systeme **auf dem Laufenden** zu halten.

Frank Heuer

Definition

Technical Security Services umfassen Integration, Wartung und Support von IT- wie auch OT (Operational Technology) Sicherheitsprodukten oder -lösungen. Auch DevSecOps-Dienste werden hier berücksichtigt. Sie adressieren alle Sicherheitsprodukte, einschließlich Antivirus, Cloud- und Rechenzentrumssicherheit, IAM, DLP, Netzwerksicherheit, Endpunktsicherheit, Unified Threat Management (UTM), OT Security, SASE und weitere Angebote. In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf ihre jeweiligen proprietären Produkte konzentrieren und Produkte oder Lösungen anderer Anbieter implementieren und integrieren können.

Zulassungskriterien

1. Nachweisliche Erfahrung mit der Implementierung von Cybersecurity-Lösungen für Unternehmen im jeweiligen Land
2. Autorisierung durch Sicherheitstechnologie-Anbieter (Hardware und Software) für den Vertrieb und die Unterstützung von Sicherheitslösungen
3. Experten mit Zertifizierungen (von Herstellern, Verbänden und Organisationen, staatlichen Stellen), die in der Lage sind, Sicherheitstechnologien zu unterstützen

Beobachtungen

Weiterhin fordern die immer intensiveren wie auch raffinierteren, komplexeren und ständig neuen Cyberattacken die Unternehmen in Deutschland heraus. Aktuell wird dies durch die wahrgenommene Bedrohungslage im Zuge des Ukraine-Konfliktes und weiterhin die Corona-Krise angefacht.

Die Situation wird immer noch durch den Mangel an Cybersecurity-Experten erschwert. Daher sind Firmen immer häufiger darauf angewiesen, externe Dienstleister in Anspruch zu nehmen.

Mittelständische Unternehmen zeigen nach wie vor besonderen Nachholbedarf, da sie besonders häufig unter dem IT-Fachkräftemangel, Überforderung oder mangelndem Kapital leiden. Die zunehmenden, komplexeren Sicherheitsbedrohungen und die verschärften gesetzlichen Regelungen bewegen diese Firmen jedoch immer häufiger zum Handeln, wofür in vielen Fällen externe Unterstützung erforderlich ist. Mittelständler wissen dabei häufig die lokale Präsenz der Dienstleister für kurze Wege und unkomplizierte, schnelle Unterstützung zu schätzen.

IT-Security-Projekte sind häufig anspruchsvoll und vielfältig angelegt. Daher sind Dienstleister im Vorteil, die umfangreiche Technical Security Services aus einer Hand bieten. Dabei können auch Dienstleister profitieren, die mit renommierten Technologieanbietern kooperieren und deren Mitarbeiter zahlreiche hochwertige Zertifizierungen vorweisen können.

Um darüber hinaus im anspruchsvollen Markt für Großkunden erfolgreich zu sein, müssen die Anbieter große, auch internationale Erfahrung und Teams präsentieren können.

Aus den oben beschriebenen Gründen nehmen auch mittelständische Firmen Security Services zunehmend in Anspruch. Anbieter mit einer ausgewogenen Kundenstruktur aus Großkunden und mittelständischen Unternehmen profitieren sowohl von den umfangreichen Budgets der Großkunden als auch vom überdurchschnittlichen Nachfragewachstum der Mittelständler.

Zudem sind Dienstleister im Vorteil, die ihren Kunden End-to-End-Sicherheitsdienstleistungen und auch zugehörige IT-Lösungen aus einem Guss anbieten können.

Von den 97 Anbietern, die in dieser Studie bewertet wurden, konnten sich 29 für diesen Quadranten qualifizieren. Dabei erreichten elf eine Position als Leader, ein Anbieter – suresecure – wurde als Rising Star identifiziert.

accenture

Accenture – Die Security Automation Factory von Accenture unterstützt bei der Transformation von prozess- und ressourcenintensiven Aufgaben mit Hilfe von Robotic Process Automation. Accenture deckt bereits ein sehr umfangreiches Themen- wie auch Leistungsspektrum hinsichtlich der Umsetzung von IT-Security-Projekten ab und arbeitet mit zahlreichen renommierten Anbietern von Cybersecurity-Produkten zusammen.

Atos

Atos – Atos ist mit den Anforderungen und gesetzlichen Regelungen im Zusammenhang mit Security-Projekten vertraut und unterstützt seine Kunden bei der Einhaltung dieser Vorgaben. Atos verfolgt einen ganzheitlichen Cybersecurity-Ansatz,

der auch die Geschäftsrelevanz der Sicherheitsdienstleistungen betont, und kann ein großes Security-Team vorweisen.

Axians – Axians unterhält Partnerschaften mit zahlreichen renommierten Cybersecurity-Technologieanbietern. Die technischen IT-Sicherheitsdienstleistungen von Axians lassen bei den Kunden keine Wünsche offen und adressieren ein sehr breites Spektrum. Axians kann mehrere namhafte Referenzkunden vorweisen und hat gleichzeitig einen starken Fokus auf mittelständische Unternehmen.

Bechtle

Bechtle – Bechtle zeigt hierzulande große lokale Präsenz und ist in Deutschland mit zahlreichen Standorten vertreten. Bechtle ist ein profilierter Anbieter von Technical Security Services für das dynamisch wachsende Marktsegment der mittelständischen Unternehmen und kann zudem in Deutschland eine der größten Mannschaften für IT-Sicherheit vorweisen.

CANCOM

CANCOM – Die Technical Security Services von CANCOM decken sowohl ein umfangreiches Themen- als auch Leistungsspektrum hinsichtlich der Umsetzung von Projekten für Cybersecurity ab. Hinsichtlich seiner Technical Security Services hat CANCOM einen starken Fokus auf mittelständische Unternehmen – eine Zielgruppe mit besonderem Wachstumspotenzial.

Capgemini – Capgemini ist ein Security-Dienstleister, der Thought Leadership vorweisen kann. Capgemini ist in der Lage, im Rahmen der Cybersecurity-Projekte für seine Kunden fortschrittliche Technologien wie Security Automation und künstliche Intelligenz einzusetzen und kann zudem ein großes weltweites Spezialistenteam für Technical Security Services vorweisen.

Computacenter

Computacenter – Das Dienstleistungsspektrum von Computacenter hinsichtlich Technical Security Services ist sehr breit aufgestellt. Computacenter unterhält im Rahmen seiner technischen Security-Dienstleistungen Beziehungen zu zahlreichen großen IT-Sicherheitsherstellern sowie vielen kleineren und aufstrebenden Anbietern. In den vergangenen zwölf Monaten hat Computacenter zahlreiche Auszeichnungen von führenden Technologiepartnern erhalten.

Controlware

Controlware – Mit seiner deutschen Herkunft ist Controlware insbesondere im Schwerpunktsegment des gehobenen Mittelstands, der lokal präsenten Dienstleistern besonderes Vertrauen entgegenbringt, gut aufgestellt. Das Angebot von Controlware für technische IT-Sicherheitsdienstleistungen ist bedarfsgerecht modular aufgebaut. Es steht zudem ein umfangreiches Expertenteam für die technischen IT-Security-Leistungen zur Verfügung.

Deutsche Telekom

Deutsche Telekom – Die Deutsche Telekom bietet Ihren Kunden lückenlose Technical Security Services, die ein komplettes Spektrum an Themen abdecken. Das Expertenteam für Cybersecurity ist sehr groß. Mit „Security

made in Germany" kann die Deutsche Telekom speziell bei mittelständischen Kunden punkten.

DXC

DXC – Das Portfolio von DXC beinhaltet integrierte Lösungen aus Cybersecurity und verbundener IT-Technologie. Die globale Präsenz und die globalen Ressourcen von DXC sind umfangreich – DXC ist mit seinen Experten für Cybersecurity in etwa 70 Ländern vertreten. Trotz umfangreicher Manpower entwickelt DXC die Themen Automatisierung und Blueprints für eine größere Agilität weiter.

IBM

IBM – IBM ist ein erfahrener und erfolgreicher Cybersecurity-Technologieanbieter und besitzt somit ein tiefes Verständnis von IT-Security-Lösungen, für die technische Services angeboten werden. IBM ist im deutschen Markt mit einem der breitesten Portfolios für IT Security Services vertreten und setzt zudem auf einen kollaborativen Informationsaustausch seiner zahlreichen Kunden.

sure[secure]

suresecure – suresecure ist der „Rising Star" für Technical Security Services in Deutschland, denn suresecure entwickelt sich sehr dynamisch und kann auf eine bemerkenswerte Entwicklungsgeschichte zurückschauen. suresecure hat sich ambitioniert das Ziel gesetzt, ein Qualitätsführer im Markt für Cybersecurity Services zu werden.

Leader

"Die Deutsche Telekom überzeugt mit umfangreichen Leistungen und großer Manpower."

Frank Heuer

Deutsche Telekom

Überblick

Telekom Security wurde Anfang 2017 als Geschäftseinheit innerhalb von T-Systems gegründet – und zum 1. Juli 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" (nachfolgend „Deutsche Telekom") innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom Security mehr als 1.600 Mitarbeiter. Der Hauptsitz befindet sich in Bonn. Neben Managed Security Services und Strategic Security Services werden auch Technical Services angeboten.

Stärken

Das Expertenteam der Deutschen Telekom für Cybersecurity ist sehr groß: Deutsche Telekom Security beschäftigt das größte Spezialistenteam für Cybersecurity in Deutschland.

Es werden komplette Security Services und integrierte Lösungen aus einer Hand offeriert: Die Deutsche Telekom bietet ihren Kunden lückenlose Technical Security Services, die ein komplettes Spektrum an Themen abdecken. Neben Technical Security Services werden auch Strategic Security Services und Managed Security Services aus einer Hand angeboten, so dass der gesamte Lifecycle eines Security-Projektes aus einem Guss möglich ist. Darüber hinaus ermöglicht die Deutsche Telekom aufgrund der generellen IT-Kompetenz auch IT-Lösungen mit damit verbundener Cybersecurity. Hervorzuheben ist insbesondere auch die spezielle Kompetenz der Deutschen Telekom hinsichtlich der Kombination von IT-Security und TK-Security.

Ein weiterer Pluspunkt ist die lokale Erbringung der Technical Security Services: Mit „Security made in Germany" kann die Deutsche Telekom speziell bei mittelständischen Kunden punkten.

Herausforderungen

Ein weiterer Ausbau der globalen Präsenz ist erwägenswert: Die Deutsche Telekom ist inzwischen auf drei Kontinenten vertreten, gemessen an anderen herausragenden führenden Anbietern ist die internationale Präsenz aber noch ausbaufähig.

Strategic Security Services

Wer sollte dieses Kapitel lesen?

Dieser Bericht ist für Unternehmen aller Branchen in Deutschland relevant, um die Dienste von Cybersecurity-Beratern bewerten zu können.

Im Rahmen dieses Quadranten wird insbesondere die aktuelle Marktpositionierung von Strategic Security Service Providern untersucht, die mit ihren Leistungen Sicherheitsbedrohungen für Unternehmen in Deutschland reduzieren, und auch darauf eingegangen, wie die einzelnen Anbieter die wichtigsten Herausforderungen angehen.

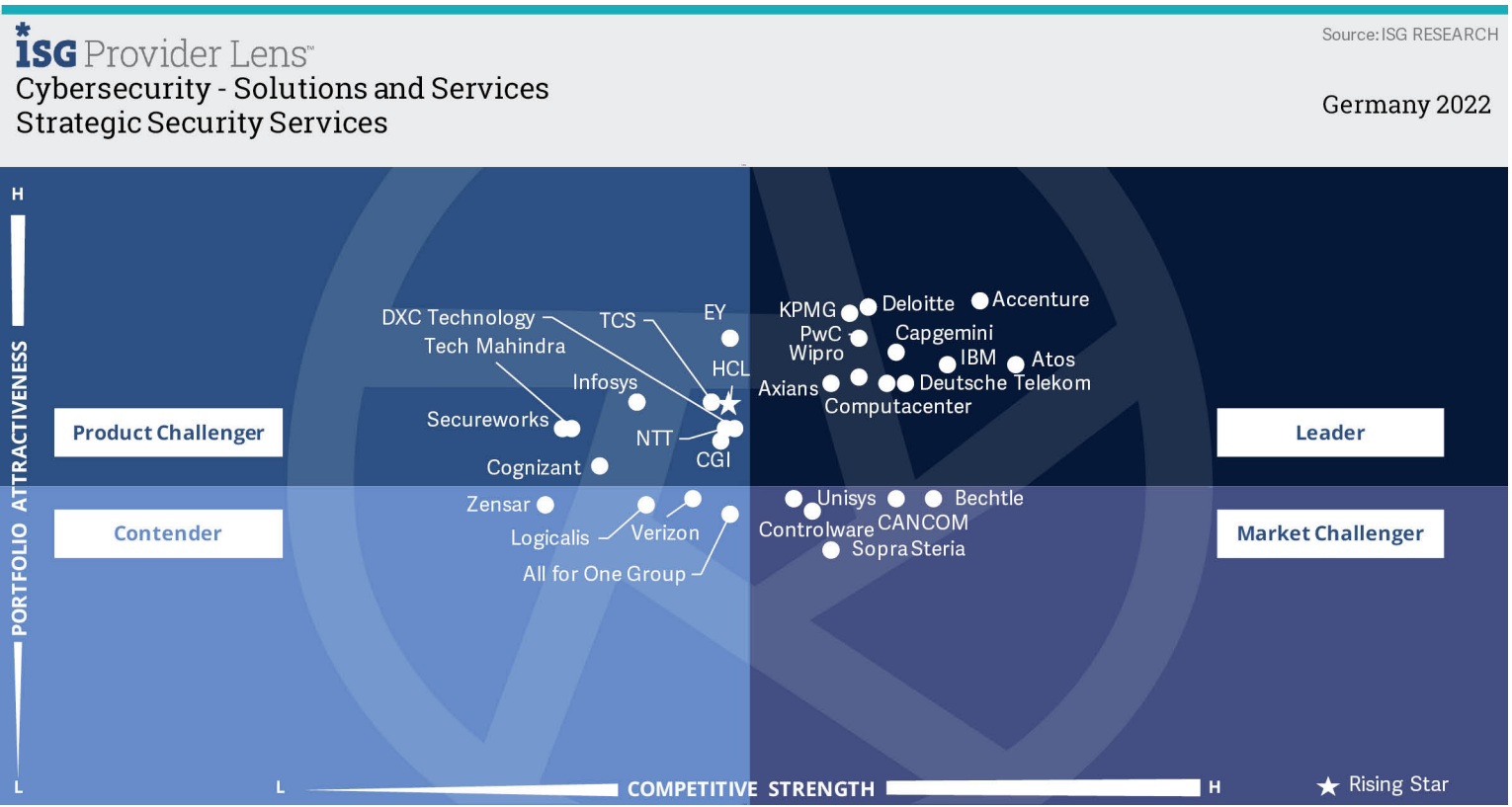
Angriffen vorzubeugen ist wichtiger, als auf sie zu reagieren. Daher sind Dienstleister mit fortschrittlichen Fähigkeiten, qualifizierten Ressourcen und einer globalen Präsenz gefragt.

Deutsche Unternehmen suchen nach strategischen Sicherheitsdienstleistungen, die eine Cybersicherheits-Strategie, Beratung zur Einhaltung von Vorschriften, Sicherheitsarchitekturen, Frameworks und Bewertungen umfassen. Kunden erwarten einen Pool an vielfältig qualifizierten Mitarbeitern, nachweisliche Erfahrung und technik- sowie branchenübergreifende Skalierungsmöglichkeiten. Zudem sind Anbieter gefragt, die einen Secure-by-Design-Ansatz für die digitale Transformation verfolgen und im Bereich der Cybersicherheit auf entsprechendes geistiges Eigentum und Patente zurückgreifen können.

Verantwortliche für die Informationssicherheit (CISOs) sollten diesen Bericht lesen, da er einen breiteren Überblick über die neuesten Trends im Security-Markt bietet. Ebenso gewinnen sie dadurch ein umfassendes Verständnis der unmittelbaren Bedrohungen und der zu ihrer Bekämpfung erforderlichen Security-Fähigkeiten und werden bei strategischen Geschäftsentscheidungen zur Lösung bestehender Sicherheitsprobleme unterstützt.

Chief Technology Officers (CTOs) werden in diesem Bericht über die neuesten für sie relevanten Trends informiert und können so mit der sich verändernden Sicherheitslandschaft Schritt halten. Neben der Festlegung strategischer Ziele und der Entwicklung von Sicherheitsplattformen im Einklang mit den Marktanforderungen können CTOs ihre Wettbewerbsvorteile verbessern.

Strategieverantwortliche gewinnen mit diesem Bericht Einblicke in die relative Positionierung und die Fähigkeiten der Anbieter von Strategic Security Services in Deutschland; sie erhalten Unterstützung beim Aufsetzen einer Sicherheits-Vision und -Strategie und bei der Entscheidungsfindung in Bezug auf Kooperationen, Partnerschaften und Kostensenkungsinitiativen.



Dieser Quadrant bewertet die **relevantesten Cybersecurity-Berater** in Deutschland. Nicht einbezogen sind Anbieter, die ihre Leistungen nur auf ihre eigenen Produkte beziehen. Angesichts **zunehmender Cyberbedrohungen** suchen Unternehmen vermehrt nach externer **Unterstützung und Orientierung**.

Frank Heuer

Definition

Strategic Security Services umfassen in erster Linie die Beratung für IT- und OT-Sicherheit. Die in diesem Quadranten abgedeckten Services beinhalten Sicherheitsaudits, Compliance- und Risikoberatung, Sicherheitsbewertungen, Beratung zur Architektur von Sicherheitslösungen sowie Aufklärung und Schulungen. Diese Services dienen der Bewertung des Sicherheitsreifegrads sowie der Risikolage und der Definition einer auf die individuellen Anforderungen zugeschnittenen Cybersicherheits-Strategie für Unternehmen. In diesem Quadranten werden Dienstleister untersucht, die sich nicht ausschließlich auf eigene Produkte oder Lösungen konzentrieren. Die hier analysierten Dienste decken alle Sicherheitstechnologien ab, insbesondere auch OT-Sicherheit und SASE.

Zulassungskriterien

1. Nachweis von Leistungen in Bereichen der Strategic Security Services wie Evaluierung, Assessments, Anbieterauswahl, Architekturberatung und Risikoberatung
2. Angebot von mindestens einem der oben genannten Strategic Security Services im jeweiligen Land
3. Die Durchführung von Sicherheitsberatungen unter Verwendung von Frameworks ist von Vorteil.
4. Kein ausschließlicher Fokus auf proprietäre Produkte oder Lösungen

Beobachtungen

Die weiter zunehmende Gefährdungssituation – aktuell auch durch den Ukraine-Konflikt angefacht – bewirkt zusammen mit mangelnden Ressourcen ein zunehmendes Bedürfnis nach Orientierung hinsichtlich Cybersicherheit.

Angesichts der immer intensiveren wie auch raffinierteren Cyberattacken sind Unternehmen gefordert, ihre IT-Systeme vor Schaden zu bewahren. Hiervon sind schon lange nicht mehr nur die bekannten großen Unternehmen und Behörden betroffen, sondern zunehmend auch kleine und mittelgroße Firmen. Gleichzeitig erschwert der Mangel an IT-Fachkräften diese Situation auch weiterhin. Unter dem besonders starken Fachkräftemangel hinsichtlich IT-Security haben gerade die mittelgroßen Unternehmen zu leiden.

Darüber hinaus sind die gesetzlichen Anforderungen, speziell durch die Datenschutz-Grundverordnung (DSGVO), für viele Firmen eine große Herausforderung.

Diese Faktoren bewirken, dass Unternehmen zunehmend externe Unterstützung benötigen. Am Anfang steht hierbei häufig die Beratung. Über diese grundsätzliche Entwicklung hinaus sorgen auch die Corona-Krise und die Bedrohungswahrnehmung infolge des Ukraine-Konflikts für zusätzlichen Beratungsbedarf.

Großunternehmen zählen weiterhin zu den wichtigsten Nachfragern von Strategic Security Services. Aus den oben beschriebenen Gründen nehmen auch mittelständische Firmen diese Leistungen zunehmend in Anspruch. Anbieter mit einer ausgewogenen Kundenstruktur aus Großkunden und mittelständischen Unternehmen profitieren sowohl von den umfangreichen Budgets der Großkunden als auch vom überdurchschnittlichen Nachfragewachstum der Mittelständler.

Des Weiteren sind Dienstleister, die ihren Kunden neben Sicherheitsberatung auch -Umsetzung und -Betrieb anbieten können, damit die Strategie bruchlos in die Tat umgesetzt werden kann, im Vorteil, ebenso wie Provider, die neben der Security-Beratung auch zugehörige IT-Lösungen aus einem Guss anbieten können.

Von den 97 Anbietern, die in dieser Studie bewertet wurden, konnten sich 30 für diesen Quadranten qualifizieren. Dabei erreichten elf eine Position als Leader, ein Anbieter – HCL – wurde als Rising Star identifiziert.

accenture

Accenture – Die Berater von Accenture zeichnen sich durch große Kompetenz und Erfahrung aus – einer der Gründe dafür, dass sie Zugang zur Vorstandsebene haben. Das Serviceportfolio ist sehr breit und wird systematisch weiterentwickelt. Auch insgesamt wächst die Cybersecurity-Beratungseinheit von Accenture außerordentlich stark.

Atos

Atos – Der Ansatz von Atos in der Cybersecurity-Beratung ist ganzheitlich ausgeprägt. Atos ist in der Lage, im Rahmen seiner Security-Beratung bei seinen (potenziellen) Kunden Vertrauen durch zahlreiche Zertifizierungen zu schaffen und kann darüber hinaus eine umfangreiche globale Security Consulting Community vorweisen.

Axians – Axians kann im deutschen Markt für Cybersecurity Consulting mit pragmatischen, zielgerichteten Lösungen speziell bei mittelständischen Unternehmen punkten. Axians entwickelt sein Portfolio darüber hinaus dynamisch weiter. Die ständig wachsende Nachfrage der mittelständischen Unternehmen nach Security-Beratung – durch die zunehmende Bedrohungslage bei gleichzeitig knappen Ressourcen – kommt Axians zugute.

Capgemini – Das Beratungsspektrum von Capgemini zum Thema Cybersecurity ist sehr umfangreich und wird weiter engagiert ausgebaut. Capgemini profiliert sich des Weiterem mit seinem erfahrenen Beraterteam. Sie verstehen sich nicht nur auf die Theorie, sondern auch auf die praktische Umsetzung der Empfehlungen.

Computacenter

Computacenter – Computacenter kann sich als strategischer Partner mit einem ganzheitlichen Security-Ansatz und Verständnis für die Infrastruktur- und Geschäftsanforderungen der Kunden positionieren. Das Beratungsportfolio und die dabei adressierbaren Security-Themen sind sehr umfangreich. Computacenter ist nicht nur ein leistungsfähiger Cybersecurity-Berater, sondern insbesondere sehr kompetent in der technischen Umsetzung von IT-Security-Projekten.

Deloitte

Deloitte – Deloitte kann eine starke globale Präsenz vorweisen und besitzt im Rahmen der Security-Beratung ein tiefes Verständnis auch für die speziellen Businessbedürfnisse seiner Kunden in Deutschland. Deloitte bietet darüber hinaus umfangreiche Beratungsleistungen für die Cybersecurity-Herausforderungen seiner Kunden an.

Deutsche Telekom

Deutsche Telekom – Die Deutsche Telekom bietet ihren Kunden End-to-End-Dienstleistungen aus einer Hand – also nicht nur die Beratung, sondern auch die zugehörige Umsetzung und den Betrieb von Sicherheitslösungen. Die Deutsche Telekom besitzt zudem Expertise auch für anspruchsvolle Umgebungen und verfügt über langjährige zertifizierte Cybersecurity-Kompetenz.

IBM

IBM – Das Portfolio von IBM für die Beratung im Bereich Cybersecurity ist umfassend, integriert und innovativ. Das Security Consulting von IBM fußt auf tiefen technischen Insights, die auch aus der Erfahrung von IBM als Security-Produktanbieter resultieren. IBM pflegt einen engen Kontakt zu seinen Kunden.

KPMG

KPMG – KPMG vermag es, in seiner Beratung zu Cybersecurity-Themen geschickt Business- und technisches Verständnis miteinander zu verbinden. Die Berater von KPMG besitzen im Rahmen der Sicherheitsberatung auch hohe strategische Kompetenz. Darüber hinaus zeichnen sie sich durch gute Zusammenarbeit mit den Kunden aus.

PwC

PwC – Seine verschiedenen Fähigkeiten setzt PwC im Rahmen seiner Cybersecurity-Beratungsmandate geschickt ein und überzeugt in der Beratung mit seinem Kompetenzspektrum. PwC verfolgt einen nachhaltigen Ansatz und versetzt die Kunden in die Lage, selbst auf Vorfälle und Krisen reagieren können. PwC ermöglicht seinen Kunden globale Delivery.

Wipro – Wipro offeriert ein umfangreiches Portfolio für die Beratung hinsichtlich Cybersecurity und besitzt großes technisches Fachwissen, welches in die Cybersicherheitsberatung einfließt. Bei der Preisgestaltung ist interessant, dass Wipro bereit ist, kundenorientiert ein Risiko einzugehen, indem auch ergebnisorientierte Preismodelle angeboten werden.

HCL – HCL ist der Rising Star unter den Anbietern von Strategic Security Services in Deutschland. HCL offeriert ein umfangreiches Portfolio und baut es weiter aus, ebenso wie die Präsenz im deutschen Markt für Cybersicherheit. Des Weiteren ist HCL bereit, bei seinen Preismodellen kundenorientiert ein Risiko einzugehen.

Leader

"Der Deutschen Telekom gelingt der Sprung unter die führenden Berater für Cyber Security Services."

Frank Heuer

Deutsche Telekom

Überblick

Telekom Security wurde Anfang 2017 als Geschäftseinheit innerhalb von T-Systems gegründet – und zum 1. Juli 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" (nachfolgend „Deutsche Telekom") innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom Security mehr als 1.600 Mitarbeiter. Der Hauptsitz befindet sich in Bonn. Neben Managed Security Services und Technical Security Services werden auch Strategic Security Services angeboten.

Stärken

Die Deutsche Telekom ermöglicht End-to-End-Dienstleistungen: Die Deutsche Telekom ist nicht nur ein leistungsfähiger Cybersecurity-Berater, sondern insbesondere ein renommierter Anbieter von Managed Security Services, zudem sehr kompetent in der technischen Umsetzung von IT-Security-Projekten und somit in der Lage, die eigenen Empfehlungen auch bruchlos und in einem Guss in die Praxis umzusetzen.

Die Deutsche Telekom besitzt Expertise auch für anspruchsvolle Umgebungen: Die Deutsche Telekom ist Spezialist für die Sicherheit kritischer nationaler Infrastrukturen. Darüber hinaus verfügen die Security-Berater der Deutschen Telekom über Expertise hinsichtlich der speziellen Bedingungen regulierter Branchen.

Die Deutsche Telekom hat langjährige zertifizierte Cybersecurity-Kompetenz: Die Deutsche Telekom kann auf über 25 Jahre Sicherheits- und Projektexpertise zurückgreifen und konnte eine der größten Datenbanken für Threat Intelligence aufbauen. Die Mitarbeiter der Deutsche Telekom sind hoch zertifizierte Berater.

Herausforderungen

Die stärkere Betonung einzelner Aspekte in der Beratung könnte sich lohnen: Die Deutsche Telekom adressiert in ihrer Beratung schwerpunktmäßig zahlreiche wichtige Themen. Themen wie z.B. die Strategieberatung und die Anbieterauswahl könnten jedoch etwas stärker betont werden, um sich ein größeres Marktpotenzial zu erschließen.

Managed Security Services

Wer sollte dieses Kapitel lesen?

Dieser Bericht ist für Unternehmen aller Branchen in Deutschland relevant, um die Dienste von Anbietern von Managed Security Services bewerten zu können.

Im Rahmen dieses Quadranten wird insbesondere die aktuelle Marktpositionierung von Managed Security Service Providern untersucht, die mit ihren Leistungen Sicherheitsbedrohungen für Unternehmen in Deutschland reduzieren, und auch darauf eingegangen, wie die einzelnen Anbieter die wichtigsten Herausforderungen angehen.

Sicherheitsfragen sind für Unternehmen ein wichtiges Anliegen. Angesichts des häufigen Auftretens neuer Bedrohungen müssen sie intelligentere Methoden zur Verbesserung und Verwaltung von Sicherheitsbelangen implementieren. Derzeit werden die neuesten Sicherheitstrends auf dem Markt genutzt, um die Effizienz und Effektivität zu steigern und gleichzeitig alle Risiken zu mindern.

Der Markt für Managed Security Services in Deutschland wird durch die zunehmende Nutzung von SASE und Zero-Trust-Netzwerken in Reaktion auf die wachsende Zahl von Cyber-Bedrohungen angetrieben. Im Laufe des letzten Jahres ist die Nachfrage nach IoT/OT-Sicherheit und Security Operations Centers (SOCs) als Service bei Unternehmen gestiegen, da sich die Angriffsfläche mit der Digitalisierung insgesamt rasant ausweitet.

Verantwortliche für die Informationssicherheit (CISOs) sollten diesen Bericht lesen, da er einen breiteren Überblick über die neuesten Trends im Security-Markt bietet. Ebenso gewinnen sie dadurch ein umfassendes Verständnis der unmittelbaren Bedrohungen und der zu ihrer Bekämpfung erforderlichen Security-Fähigkeiten und werden bei strategischen Geschäftsentscheidungen zur Lösung bestehender Sicherheitsprobleme unterstützt.

Chief Technology Officers (CTOs) werden in diesem Bericht über die neuesten für sie relevanten Trends informiert und können so mit der sich verändernden Sicherheitslandschaft dem Schritt halten. Neben der Festlegung strategischer Ziele und der Entwicklung von Sicherheitsplattformen im Einklang mit den Marktanforderungen können CTOs ihre Wettbewerbsvorteile verbessern.

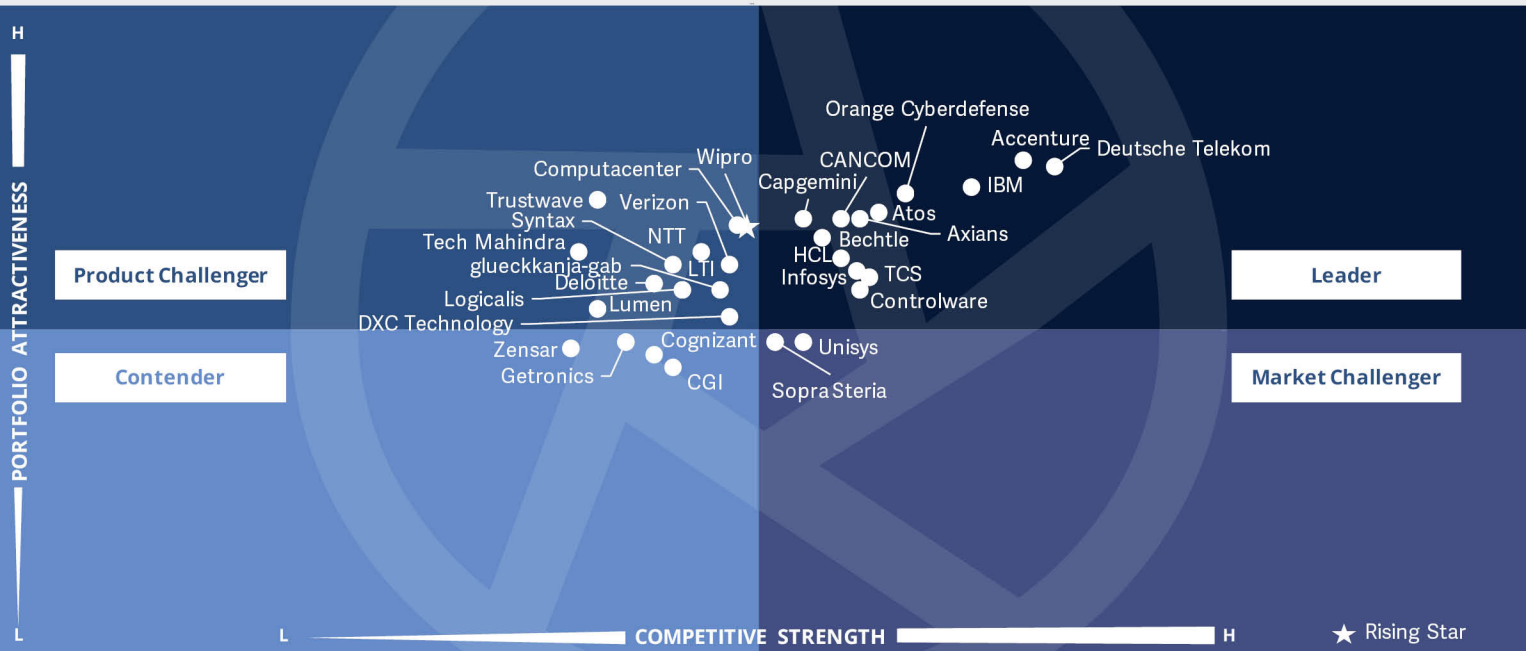
Strategieverantwortliche gewinnen mit diesem Bericht Einblicke in die relative Positionierung und die Fähigkeiten der Anbieter von Managed Security Services in Deutschland. Er hilft dem jeweiligen Unternehmen, eine Sicherheits-Vision und -Strategie aufzusetzen und unterstützt die Entscheidungsfindung in Bezug auf Kooperationen, Partnerschaften und Kostensenkungsinitiativen.

ISG Provider Lens™

Cybersecurity - Solutions and Services
Managed Security Services

Source: ISG RESEARCH

Germany 2022



Dieser Quadrant bewertet die **relevantesten Dienstleister für Managed Security Services** in Deutschland. Unberücksichtigt sind Anbieter, die ihre Leistungen nur auf eigene Produkte beziehen. Der externe Betrieb durch **Security Operations Centers** ist eine **zunehmend gefragte** Leistung.

Frank Heuer

Definition

Unter Managed Security Services fallen Betrieb und Management von IT- und OT-Sicherheitsinfrastrukturen für einen oder mehrere Kunden durch ein Security Operations Center (SOC). Dieser Quadrant untersucht Dienstleister, die sich nicht ausschließlich auf proprietäre Produkte konzentrieren, sondern Best-of-Breed-Sicherheitstools verwalten und betreiben können. Sie kümmern sich um den gesamten Security Incident Lifecycle, von der Identifizierung bis zur Lösung von Problemen.

Zulassungskriterien

1. Zu den typischen Dienstleistungen gehören Sicherheitsüberwachung, Verhaltensanalyse, Erkennung von unbefugten Zugriffen, Beratung zu Präventionsmaßnahmen, Penetrationstests, Firewall-Betrieb, Anti-Virus-Betrieb, Identity & Access Management (IAM)-Betriebsservice, Data Leakage/Loss Prevention (DLP)-Betrieb und alle anderen Betriebsservices, um einen kontinuierlichen Echtzeitschutz zu bieten, ohne die Leistungsfähigkeit des Unternehmens zu beeinträchtigen. Insbesondere ist auch Secure Access Service Edge (SASE) mit berücksichtigt.
2. Angebot von Sicherheitsdiensten wie Erkennung und Vorbeugung, Security Information & Event (SIEM) sowie Sicherheitsberatung und Audits, per Fernzugriff oder vor Ort beim Kunden
3. Vorhandene Akkreditierungen von Anbietern von Sicherheitstools
4. SOCs sind idealerweise im Besitz und unter der Leitung des Anbieters und nicht überwiegend von Partnern.
5. Zertifizierte Mitarbeiter, z.B. Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) und Global Information Assurance Certification (GIAC)

Beobachtungen

Die immer raffinierteren, häufigeren, komplexeren und wandlungsfähigeren Cyberattacken – sowie die zusätzlichen Herausforderungen durch die Pandemie und den Ukraine-Konflikt – fördern besonders auch die Nachfrage nach Managed Security Services. Knappe qualifizierte Ressourcen und das erforderliche stets aktuelle Spezialistenwissen rücken diese Dienstleistungen zusätzlich in den Fokus deutscher Unternehmen.

Im Segment der großen Unternehmen spielen aufgrund der häufig internationalen Präsenz dieser Large Accounts global verteilte Security Operations Centers (SOCs) eine besondere Rolle. Aber auch SOCs mit deutschem Standort wissen Großunternehmen aufgrund des wichtiger gewordenen Datenschutzaspektes – im Zuge unternehmensinterner Compliance oder gesetzlicher Regelungen – zu schätzen.

Aber gerade auch mittelständische Unternehmen – die noch stärker als die Großunternehmen vom Cybersecurity-Fachkräftemangel betroffen sind – sind immer mehr auf die Unterstützung externer Dienstleister angewiesen, um diese wachsenden Herausforderungen zu meistern. So interessiert sich inzwischen auch der Mittelstand zunehmend für Managed Security Services, mit denen die Kunden umfassend beim Handling der Security-Systeme entlastet werden. Für diese Zielgruppe sind SOCs in Deutschland ein Pluspunkt. Auch deutschsprachige Ansprechpartner spielen für diese Kundengruppe eine wichtige Rolle.

Darüber hinaus wird von den Managed-Security-Services-Anbietern eine hohe Innovationskraft erwartet, um im Wettlauf mit den Cyberkriminellen stets die Nase vorn zu haben. Hierzu zählt unter anderem die Erweiterung der SOCs in Richtung Cyber Defense Centers, indem den immer komplexeren Bedrohungen auch mit künstlicher Intelligenz und Automatisierung begegnet wird. Da auch Cyberkriminelle sich zunehmend künstlicher Intelligenz bedienen, sind Cyber Fusion Centers als Ergänzung zu den bestehenden SOCs entstanden, um den Bereich des Cyber Security Managements zielgerichtet und zukunftsgerecht auszubauen.

Von den 97 Anbietern, die in dieser Studie bewertet wurden, konnten sich 32 für diesen Quadranten qualifizieren. Dabei erreichten dreizehn eine Position als Leader, ein Anbieter – Wipro – wurde als Rising Star identifiziert.

accenture

Accenture – Accenture offeriert seinen Kunden ein sehr umfangreiches Spektrum an Leistungsmerkmalen und ist in der Lage, sämtliche IT-Security-Themen aus einer Hand abzudecken. Mit hohem Wachstum weitet Accenture seine Marktpräsenz, Leistungsfähigkeit und Reichweite stetig aus und kommt den Anforderungen seiner oft global aktiven Großkunden durch die eigene internationale Präsenz sehr gut entgegen.

Atos

Atos – Deutschland zählt zu den SOC-Standorten von Atos, was auch für viele Großunternehmen interessant ist. Sowohl die abgedeckten Themen als auch die Leistungen der Managed Security Services adressieren ein breites Spektrum. Die Multi-Vector Detection von Atos kombiniert Informationen

aus verschiedenen Quellen für bessere Möglichkeiten zur Erkennung von Bedrohungen.

Axians – Axians bietet im Rahmen seiner Managed Security Services ein breites Spektrum an Services und gemanagten Security-Themen an. Für besonders gefährdete Daten und Systeme bietet das globale Cyber Defence Center von Axians ein erhöhtes Maß an Sicherheit und flexible Lösungen. Axians betreibt Security Operations Centers unter anderem auch in Deutschland.

Bechtle

Bechtle – Bechtles Managed Security Services decken ein breites Spektrum an Leistungen und gemanagten Security-Technologien ab. Zudem sind sie auch modular anpassungsfähig. Neben verschiedenen anderen Ländern betreibt Bechtle auch ein dediziertes Security Operations Center in Deutschland mit deutschsprachigem Support und besitzt eine ausgewogene Kundenstruktur aus Groß- und Mittelstandskunden.

CANCOM

CANCOM – Das Managed Security Services Portfolio von CANCOM deckt ein breites Spektrum an gemanagten Technologien ab und bietet zahlreiche Leistungen. CANCOM betreibt unter anderem in Deutschland ein dediziertes Security Operations Center und hat hinsichtlich seiner Managed Security Services einen starken Fokus auf mittelständische Unternehmen, eine Zielgruppe mit besonderem Wachstumspotenzial.

Capgemini – Capgemini bietet im Rahmen seiner Managed Security Services vielfältige Dienstleistungen an, die ein breites Spektrum gemanagter Security-Themen adressieren. Speziell auch gemessen an der Anzahl der Bestandskunden stellt Capgemini in Deutschland ein großes Expertenteam für Managed Security Services bereit und ist auf mehreren Kontinenten mit Security Operations Centers vertreten.

Controlware

Controlware – Speziell auch gemessen an der Anzahl der Kunden unterhält Controlware in Deutschland ein großes Expertenteam für seine Managed Security Services und offeriert seinen Kunden modulare, individualisierbare Managed Security Services. Controlware hat hinsichtlich seiner Managed Security Services einen starken Fokus auf mittelständische Unternehmen.

Deutsche Telekom

Deutsche Telekom – Die Deutsche Telekom betreibt Managed Security Services unter anderem in Deutschland und unterhält hierzulande zudem ein äußerst großes Team für Managed Security Services. Um auch zukünftig ein leistungsfähiges Portfolio anbieten zu können, entwickelt die Deutsche Telekom ihr bereits sehr umfassendes Angebot kontinuierlich weiter.

HCL – Allein in Deutschland betreibt HCL drei dedizierte Security Operations Centers. Auch personell ist HCL hinsichtlich seiner Managed Security Services in Deutschland stark aufgestellt. Das Portfolio deckt viele Leistungen ab

und bezieht ein umfangreiches Spektrum an Technologien für Cybersecurity ein. So ist HCL in Deutschland zunehmend erfolgreich.

IBM

IBM – IBM ist im Markt mit einem der breitesten Portfolios für IT Security Services vertreten. Die Managed Security Services von IBM basieren auf der leistungsstarken, hauseigenen QRadar-Technologie. Das weltweite Netzwerk aus Security Operations Centers ermöglicht einen globalen Betrieb. IBM zählt zu den weltweit bekanntesten Anbietern von Managed Security Services.

Infosys – Die Leistungen von Infosys im Rahmen der Managed Security Services lassen keine Wünsche offen. Darüber hinaus ist Infosys auch personell hinsichtlich seiner Managed Security Services in Deutschland stark aufgestellt und unterstützt seine Kunden darüber hinaus dabei, ihre Cybersicherheitsreife kontinuierlich zu verbessern.

Orange Cyberdefense

Orange Cyberdefense – Orange Cyberdefense ist weltweit mit Security Operations Centers vertreten und ermöglicht so einen globalen Betrieb der Cybersecurity-Lösungen. Auch Deutschland zählt zu den Staaten, in denen Orange Cyberdefense Security Operations Center betreibt. Die Managed Security Services decken ein sehr breites Spektrum an Technologien ab.

TCS – Die Managed Security Services von TCS ermöglichen den Betrieb sämtlicher Cybersecurity-Technologien, inklusive OT-Sicherheit. Sowohl in absoluter Zahl als auch gemessen an der Anzahl der Kunden unterhält TCS in Deutschland ein großes Team und ist auf mehreren Kontinenten mit zahlreichen Security Operations Centers vertreten, unter anderem in Deutschland.

Wipro – Wipro ist der „Rising Star" für Managed Security Services in Deutschland. Der Anbieter hat stark in Akquisitionen und Partnerschaften investiert und konnte außerdem seine Kundenzahl in Deutschland in den letzten zwölf Monaten deutlich steigern. Die Leistungen von Wipro im Rahmen der Managed Security Services lassen keine Wünsche offen.

Leader

"Die Deutsche Telekom baut ihre Managed Security Services made in Germany umfangreich aus."

Frank Heuer

Deutsche Telekom

Überblick

Telekom Security wurde Anfang 2017 als Geschäftseinheit innerhalb von T-Systems gegründet – und zum 1. Juli 2020 in eine eigene rechtliche Einheit, die „Deutsche Telekom Security GmbH" (nachfolgend „Deutsche Telekom") innerhalb des Deutsche Telekom-Konzerns umgewandelt. Weltweit beschäftigt Deutsche Telekom Security mehr als 1.600 Mitarbeiter. Der Hauptsitz befindet sich in Bonn. Neben Technical Security Services und Strategic Security Services werden auch Managed Services angeboten.

Stärken

Die Deutsche Telekom bietet „Security made in Germany": Die Deutsche Telekom betreibt Managed Security Services unter anderem in Deutschland, was besonders von vielen Mittelstandskunden geschätzt wird. Der Anbieter verfügt über Europas größtes integriertes Cyber Defense und Security Operations Center und unterhält in Deutschland vier dedizierte Security Operations Center. Mit „Security made in Germany" kann die Deutsche Telekom speziell angesichts der Datenschutzdiskussion – und besonders in der Zielgruppe des Mittelstandes – punkten.

Die umfangreichen Managed Security Services werden weiter ausgebaut: Um auch zukünftig ein leistungsfähiges Portfolio anbieten zu können, entwickelt die Deutsche Telekom ihr bereits sehr umfassendes Angebot kontinuierlich weiter und plant weitere umfangreiche Ergänzungen des Portfolios – die Roadmap zählt zahlreiche Vorhaben auf.

Die Deutsche Telekom kann ein umfangreiches Expertenteam für ihre Managed Security Services vorweisen: Die Deutsche Telekom unterhält in Deutschland ein äußerst großes Team für Managed Security Services.

Herausforderungen

Der Anteil der Mittelstandskunden ist ausbaufähig: Im Gegensatz zu den meisten Wettbewerbern kann die Deutsche Telekom spezielle Kompetenzen hinsichtlich des Mittelstandes vorweisen. Dennoch liegt der Schwerpunkt der Managed Security Services weiterhin noch auf Großkunden, weniger auf dem Mittelstandssegment, dessen Nachfrage überdurchschnittlich wächst.

Anhang

Die Marktforschungsstudie „ISG Provider Lens™ 2022 – Cybersecurity – Solutions and Services" analysiert die entsprechenden Softwareanbieter/ Dienstleister im deutschen Markt auf Basis eines mehrstufigen Marktforschungs- und Analyseprozesses und positioniert diese Anbieter auf Basis der ISG Research-Methodik.

Lead Author:
Frank Heuer

Editor:
Maria Müller

Research Analyst:
Monica K

Data Analyst:
Rajesh Chillappagari

Consultant Advisor:
Roger Albrecht

Project Manager:
Ridam Bhattacharjee

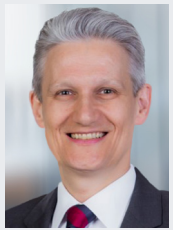
Information Services Group übernimmt die alleinige Verantwortung für diesen Bericht. Soweit nicht anders angegeben, wurden sämtliche Inhalte, u.a. Abbildungen, Marktforschungsdaten, Schlussfolgerungen, Aussagen und Stellungnahmen im Rahmen dieses Berichtes von Information Services Group, Inc. entwickelt und sind Alleineigentum von Information Services Group Inc.

Die in diesem Bericht vorgestellten Marktforschungs- und Analysedaten umfassen Research-Informationen aus dem ISG Provider Lens™ Programm sowie aus kontinuierlich laufenden ISG Research-Programmen, Gesprächen mit ISG-Advisors, Briefings mit Dienstleistern und Analysen von öffentlich verfügbaren Marktinformationen aus unterschiedlichen Quellen. Die für diesen Bericht erhobenen Daten und Informationen, entsprechen nach Ansicht von ISG sowohl für Anbieter, die aktiv teilgenommen haben, als auch für Anbieter, die nicht teilgenommen haben, dem aktuellen Stand vom Juni 2022. Zwischenzeitliche Fusionen und Akquisitionen und die damit zusammenhängenden Veränderungen sind in diesem Bericht nicht berücksichtigt.

Falls nicht anders angegeben, sind alle Umsätze in US-Dollar (USD) angegeben.

Dabei wurde die Studie in folgende Schritte gegliedert:

1. Definition des Marktes für Cybersecurity – Solutions and Services
2. Fragebogenbasierte Studien über Dienstleister/Anbieter und zu allen Trendthemen
3. Interaktive Gespräche mit Dienstleistern/Anbietern über ihre Leistungen und Use Cases
4. Nutzung der ISG-internen Datenbanken sowie des Know-hows und der Erfahrung der ISG Advisors (soweit möglich)
5. Nutzung der Star of Excellence CX-Daten
6. Detaillierte Analyse und Evaluierung von Services und entsprechenden Dokumentationen auf Basis der von den Anbietern zur Verfügung gestellten Daten und Zahlen sowie anderer Quellen
7. Auswertung auf Basis der folgenden Kriterien:
   * Strategie & Vision
   * Technologische Innovationen
   * Markenbekanntheitsgrad und Marktpräsenz
   * Vertriebs- und Partnerlandschaft
   * Breite und Tiefe des Service-Angebots
   * CX und Empfehlung



Autor

Frank Heuer
Principal Analyst

Frank Heuer ist Principal Analyst bei ISG Germany. Sein Schwerpunkt liegt auf den Themen Cyber Security, Digital Workspace, Communication, Social Business & Collaboration sowie Cloud Computing.

Zu seinen Aufgabengebieten gehört vor allem die Beratung von ICT-Anbietern zum strategischen und operativen Marketing sowie Vertrieb. Herr Heuer ist als Sprecher bei Konferenzen und Webcasts zu seinen Themenschwerpunkten im Einsatz und Mitglied des IDG-Expertennetzwerks. Herr Heuer ist seit 1999 als Analyst und Berater im IT-Markt aktiv.

Research Analyst

Monica K
Research Specialist

Monica K. ist eine Forschungsspezialistin und Digitalexpertin bei ISG. Sie unterstützt und ist Co-Autorin von Provider Lens™-Studien zum Internet der Dinge (IoT), zur digitalen Unternehmenstransformation, zu Blockchain, Enterprise Application as a Service und zur Cybersicherheit. Sie hat Inhalte für die oben genannten Provider Lens™-Studien sowie Inhalte aus Unternehmensperspektive erstellt und ist Autorin des globalen zusammenfassenden Berichts. Monica K. verfügt über mehr als 8 Jahre Erfahrung und Fachwissen in den Bereichen Technologie, Wirtschaft und Marktforschung für ISG-Kunden. Bevor sie zu ISG kam, arbeitete Monica K. für ein Forschungsunternehmen, das sich auf Technologien wie IoT und Produktentwicklung sowie auf Anbieterprofile und Talent Intelligence spezialisiert hat. Sie war auch für die Durchführung von End-to-End-Forschungsprojekten und die Zusammenarbeit mit internen Stakeholdern bei verschiedenen Beratungsprojekten verantwortlich.

IPL-Produktverantwortlicher

Jan Erik Aase

Partner und globaler Leiter – ISG Provider Lens™

Herr Aase verfügt über umfangreiche Erfahrung in der Implementierung und Erforschung der Dienstleistungsintegration und des Managements von IT- und Geschäftsprozessen. Mit mehr als 35 Jahren Erfahrung ist er hochqualifiziert in der Analyse von Trends und Methoden der Vendor Governance, der Identifizierung von Ineffizienzen in aktuellen Prozessen und der Beratung der Branche. Jan Erik hat Erfahrungen auf allen vier Seiten des Sourcing- und Vendor-Governance-Lebenszyklus - als Kunde, als Branchenanalyst, als Dienstleister und als Berater. Als Research Director, Principal Analyst und Global Leader des ISG Provider Lens™ Programms ist er in der Lage, den aktuellen Stand der Branche zu beurteilen und darüber zu berichten sowie Empfehlungen für Unternehmen und Service-Provider- Kunden auszusprechen.

ISG Provider Lens™

Die ISG Provider Lens™ Quadranten-Reports bieten Bewertungen von Dienstleistern und kombinieren als einzige Studien dieser Art datengestützte Forschung und Marktanalysen mit praktischen Erfahrungen und Beobachtungen, gestützt auf das globale ISG-Beraterteam. Unternehmen erhalten eine Fülle detaillierter Daten und Marktanalysen, die ihnen bei der Auswahl geeigneter Sourcing-Partner helfen; die ISG-Berater wiederum nutzen die Berichte, um ihre Marktkenntnisse zu validieren und Empfehlungen für die Unternehmenskunden von ISG abzugeben. Die Studien decken derzeit Provider mit Angeboten in mehreren Regionen weltweit ab. Weitere Informationen über die ISG Provider Lens Studien finden Sie auf dieser Webseite.

ISG Research™

Das ISG Research™ Angebot umfasst Research-Subskriptionsservices, Beratungs - Services und Executive Event Services mit Fokus auf Markttrends und disruptive Technologien im Unternehmensumfeld. ISG Research™ zeigt Unternehmen auf, wie sie ein schnelleres Wachstum und einen höheren Mehrwert erzielen können.

Weitere Informationen zu den ISG Research™ Subskriptions-Services sind erhältlich unter contact@isg-one.com, Tel.+49 (0) 561-50697524 oder auf unserer Website unter research.isg-one.com

ISG

ISG (Information Services Group) (Nasdaq: III) ist ein führendes, globales Marktforschungs- und Beratungsunternehmen im Informationstechnologie-Segment. Als zuverlässiger Geschäftspartner für über 800 Kunden, darunter über 75 der 100 weltweit größten Unternehmen, unterstützt ISG Unternehmen, öffentliche Organisationen sowie Service- und Technologie-Anbieter dabei, Operational Excellence und schnelleres Wachstum zu erzielen. Der Fokus des Unternehmens liegt auf Services im Kontext der digitalen Transformation, inklusive Automatisierung, Cloud und Daten-Analytik, des Weiteren auf Sourcing-Beratung, Managed Governance und Risk Services, Services für den Netzwerkbetrieb, Strategie- und -Betriebs-Design, Change Management sowie Marktforschung und Analysen in den Bereichen neuer Technologien. 2006 gegründet, beschäftigt ISG mit Sitz in Stamford, Connecticut, über 1.300 mit der Digitalisierung vertraute Experten und ist in mehr als 20 Ländern tätig. Das globale Team von ISG ist bekannt für sein innovatives Denken, seine geschätzte Stimme im Markt, tiefgehende Branchen- und Technologie-Expertise sowie weltweit führende Marktforschungs- und Analyse-Ressourcen, die auf den umfangreichsten Marktdaten der Branche basieren. Weitere Informationen unter www.isg-one.com.

ISG Provider Lens™

JULI 2022

REPORT: CYBERSECURITY — SOLUTIONS AND SERVICES