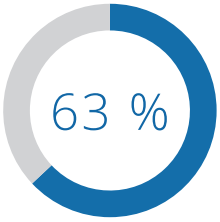
CYBER SECURITY IN DEUTSCHLAND 2020+

Sichere IT für sicheres Business

IDC ANALYZE THE FUTURE

OKTOBER 2020
GESPONSERT VON TREND MICRO



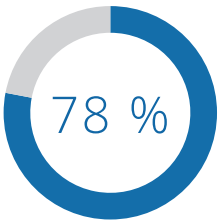
63 Prozent der Unternehmen betonen, dass die aktuellen Cyber-Risiken eine veränderte Security-Architektur erfordern.

IT-SICHERHEIT GERÄT WEITER UNTER DRUCK

Die IT-Sicherheitslage in Deutschland ist nach wie vor angespannt. Der maßgebliche Grund dafür ist, dass sich die wachsende Komplexität der IT-Landschaften, die Agilität und Masse der Cyber-Attacken sowie die steigenden Compliance-Anforderungen mit den implementierten, aber vielfach unzulänglichen IT-Security-Ressourcen immer schwerer beherrschen lassen.

COVID-19 und die damit verbundene Abwanderung zahlloser Mitarbeiter in die Homeoffices war und ist ein weiterer Prüfstein für die Qualität der Abwehr- und Reaktionsfähigkeit der Unternehmen in Bezug auf industrieübergreifende Ereignisse von globaler Reichweite. Dabei liegt es auf der Hand, dass umfassende IT-Security kritischer für den wirtschaftlichen Erfolg jedes Unternehmens und jeder Organisation wird.

Die Aufgaben für die Security-Entscheider und die Mitarbeiter in den Security-Abteilungen werden nicht weniger, eher mehr. Aus diesem Grund ist es empfehlenswert, dass Sie Ihre Sicherheitsarchitektur, Ihre Lösungen und Prozesse noch einmal auf den Prüfstand stellen. Bereits mit wenigen gezielten Schritten können Sie überprüfen, wo Sie stehen und welche Schritte erforderlich sind für eine bessere IT-Security.



78 Prozent der befragten Unternehmen wurden bereits mit Sicherheitsvorfällen konfrontiert.

HANDELN SIE, UND ZWAR JETZT, UM IHR UNTERNEHMEN SICHERER UND REAKTIONSSCHNELLER ZU MACHEN

Lösungen für IT-Sicherheit existieren in allen Unternehmen. Vorrangig in kleinen und mittleren Unternehmen vertrauen allerdings noch deutlich zu viele Verantwortliche auf „Bordlösungen“ und Standardeinstellungen. Das ist hochriskant. Unsere aktuelle Erhebung zeigt, dass 78 Prozent der Unternehmen bereits mit Sicherheitsvorfällen konfrontiert wurden. Diese Zahl belegt, dass signifikanter Verbesserungsbedarf besteht.

Das Ziel von Angriffen ist immer ein wirtschaftlicher Schaden in den Zielunternehmen. Hierzu zählen finanzielle Einbußen, der Verlust von geistigem Eigentum, Rufschädigung oder Kundenverlust. Selbst dann, wenn die IT ruht und die Daten nicht verfügbar sind, hat das direkte finanzielle Auswirkungen auf Ihr Unternehmen.

Worauf kommt es also an? IDC empfiehlt, eine ganzheitliche Sicht auf die Security zu entwickeln und Security-Lösungen und -Services gezielt einzusetzen. Mehr Lösungen garantieren nicht immer mehr Sicherheit. Maximale Widerstandsfähigkeit Ihrer Organisation erreichen Sie durch einen strategischen Blick und operative Maßnahmen, die Ihnen gestatten, Attacken im Vorfeld abzuwehren, erfolgreiche Angriffe rasch einzudämmen und zeitnah auf die Lage vor dem Angriff zurückzukehren.

IDC hat im August 2020 eine primäre Marktbefragung durchgeführt, um detaillierte Einblicke in die aktuellen Umsetzungspläne, Herausforderungen und Erfolgsfaktoren in puncto Cyber Security zu erhalten. Anhand eines strukturierten Fragebogens wurden branchenübergreifend 210 Organisationen in Deutschland mit mehr als 100 Mitarbeitern befragt. Der vorliegende Executive Brief bietet IT-Security- und Fachbereichsentscheidern auf Basis der Studien-Highlights Best Practices und Empfehlungen für die Optimierung der Cyber Security in ihrem Unternehmen.

Abbildung 1: Top-5-Sicherheitsrisiken 2020

N = 210 Unternehmen; Mehrfachnennungen; Abbildung gekürzt

FÜNF RATSCHLÄGE FÜR EINE UMFASSENDE CYBER SECURITY

Die folgenden fünf Ratschläge sollen Ihnen Anregungen und Impulse vermitteln, um die Transparenz und Wirksamkeit Ihrer Security-Landschaft zu erhöhen, um einzelne Maßnahmen zu priorisieren und um die Cyber Security insgesamt zu stärken.

Ratschlag 1: Mit Ad-hoc-Maßnahmen erzielen Sie schnelle Erfolge und sind bereit, die nächsten Schritte zu gehen

Cyber Security startet mit einer umfassenden Bestandsaufnahme. Diese muss unbedingt alle IT-Systeme und Geräte berücksichtigen. Wir stellen immer wieder fest, dass der Wartung und der Systempflege häufig nicht die erforderliche Aufmerksamkeit geschenkt wird. Planmäßig durchgeführte Maßnahmen wie das regelmäßige Einspielen von Updates und Patches sind zwingend notwendige Schritte zur Erhöhung der IT-Sicherheit. Wenn IT-Security-Verantwortliche und Systemadministratoren die Aufgaben klar abgrenzen und ihre Umsetzung kontinuierlich überprüfen, engen sie den Spielraum von Hackern deutlich ein. Handeln Sie sofort, wenn Schwachstellen in Lösungen bekannt werden und der Hersteller Patches bereitstellt. Verzögerungen sind sehr riskant und gefährden Ihr Unternehmen. 15 Prozent der befragten Entscheider gaben an, dass Angreifer über eine ungepatchte bekannte Schwachstelle in ihr Unternehmen eindringen konnten. Hier besteht also eine reale Gefahr für jede Organisation.

Wie gut ist Ihr Überblick über Ihre Security-Landschaft und Ihre Security-Prozesse? Es ist wichtig, Transparenz über alle vorhandenen Lösungen und deren Wirksamkeit, deren Zusammenspiel, aber auch über die Lücken in der Security-Landschaft zu haben.

Eine weitere Herausforderung liegt im „Appliance- und Lösungs-Wirrwarr“. Da für jede neue Bedrohung ein neues Produkt angeboten und angeschafft wird, sind schwerfällige und unüberschaubare Sicherheitsarchitekturen entstanden. Neue Lösungsansätze sind also zwingend erforderlich. Genau dafür benötigen Sie eine umfassende Transparenz, um die nächsten Schritte sauber planen zu können.

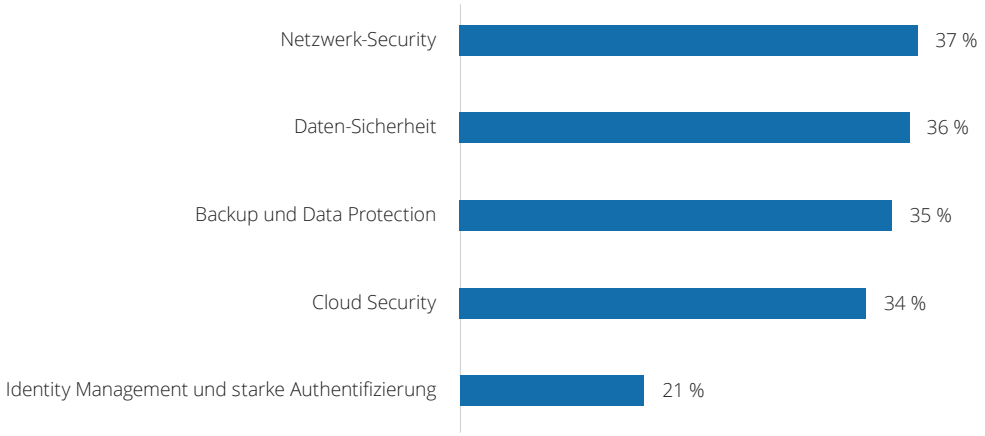
Zwei weitere Punkte zählen ebenfalls zu den Ad-hoc-Maßnahmen. Ändern Sie Werkseinstellungen und wählen Sie starke Passwörter. Unveränderte Standardeinstellungen sind für Angreifer ein leichtes Spiel. Zudem sollten Sie nach wie vor Awareness-Maßnahmen bei den Endanwendern in den Fachbereichen durchführen. Einfache Passwörter, Phishing und Social Engineering sind nach wie vor erfolgreiche Einfall-Tore für Angreifer. Bei Phishing und Social Engineering haben Angreifer ihre Methoden perfektioniert und damit das Erkennen dieser Attacken deutlich erschwert. Aber auch Awareness-Schaffung bei Entscheidern und im Management sind weiterhin erforderlich, denn die Unternehmensführung und leitende Angestellte haben einen wesentlichen Einfluss auf die Security-Kultur und -Akzeptanz in jedem Unternehmen.

Ratschlag 2: Adressieren Sie die relevanten Themen: Netzwerk-Security, Daten-Sicherheit, Data Protection, Cloud Security und Identity Management

Keine Frage, jeder Unternehmensbereich muss geschützt werden. Allerdings zeigt sich, dass folgende Themen für die Entscheider eine besondere Relevanz haben. Das sind Netzwerk-Security, Daten-Sicherheit, Data Protection, Cloud Security und Identity Management. Warum stehen genau diese Themen im Mittelpunkt? Dafür ist eine Reihe von Entwicklungen maßgeblich:

Mit einer Nennung von 37 Prozent führt Netzwerk-Security die Liste der wichtigsten Themen für das Jahr 2020 an. Aus Sicht von IDC war es längst überfällig, dass das Netzwerk und seine Absicherung stärker in den Blickwinkel der IT-Entscheider rücken. Über Netze läuft der gesamte interne und externe Traffic jedes Unternehmens. Mit wachsenden Datenmengen und immer extremeren Anforderungen an Applikationen und Services bleiben Netzwerke nicht nur ein kritischer Bestandteil jeglicher IT-Infrastruktur, sondern rücken immer mehr in den Vordergrund.

Abbildung 2: Was sind für Ihre Organisation die Top-3-Security-Bereiche?



N = 210 Unternehmen; drei Nennungen möglich; Abbildung gekürzt

Die Abhängigkeit der Unternehmen von Daten ist gleichzeitig eine Abhängigkeit von ihren Netzwerken. Netzwerkausfälle müssen daher dringend verhindert und die Integrität der versendeten Daten geschützt werden. Das rückt das Netzwerkmanagement und insbesondere die Netzwerkautomatisierung in den Fokus. Die effiziente und kostengünstige Anbindung von Niederlassungen mit SD-WAN sowie weitere neue Technologien weisen jedem Netzwerk eine tragende Rolle in Informations- und Telekommunikationstechnologie zu und fordern ein umfassendes Update der Netzwerk-Security und der Security-Architektur in den Unternehmen. Mit COVID-19 und Remote Work werden diese Anforderungen noch einmal unterstrichen.

Daten-Sicherheit hat immer die Vertraulichkeit, die Integrität und die Verfügbarkeit der Daten zum Ziel. Mit einer Nennung von 36 Prozent verzeichnet Daten-Sicherheit die zweithäufigste Nennung. Data Loss Prevention zählt zu den zentralen Ansätzen zur Verbesserung der Daten-Sicherheit. Ein umfassendes Rechte-Management, die Verschlüsselung der Daten, die Datenklassifizierung sowie ein Monitoring der Datenbewegungen und eine umfassende Zugriffskontrolle unterstützen Sie bei der Daten-Sicherheit. Wie in den meisten Bereichen der IT-Sicherheit kommen auch hier analytische Ansätze für eine hohe Transparenz über alle Aktivitäten immer umfassender zum Einsatz. Grundsätzlich gilt: Daten-Sicherheit sollte immer einen End-to-End-Ansatz verfolgen.

Data Protection gehört aus Sicht von IDC klar in den Security Life Cycle. Ransomware-Attacken haben die Aufmerksamkeit gegenüber Data Protection deutlich gesteigert. Mehr als ein Drittel der Befragten zählt auch aus diesem Grund das Thema Data Protection zu ihren Top-3-Themen. Data Protection umfasst eine Reihe von Lösungen, die on-premises oder in der Cloud bereitgestellt werden. Ein Cloud Backup in einer physisch getrennten Lokation ermöglicht Ihnen ein schnelles Wiederherstellen der Ausgangslage, etwa nach einer Ransomware-Attacke, indem Sie auf saubere Kopien oder Snapshots zurückgreifen können. Im Zuge von COVID-19 sehen wir zudem einen deutlichen Trend zu Data Protection as a Service. Aus Business-Perspektive und als Element eines Business-Continuity-Plans muss Data Protection eine kontinuierliche Aufgabe sein.

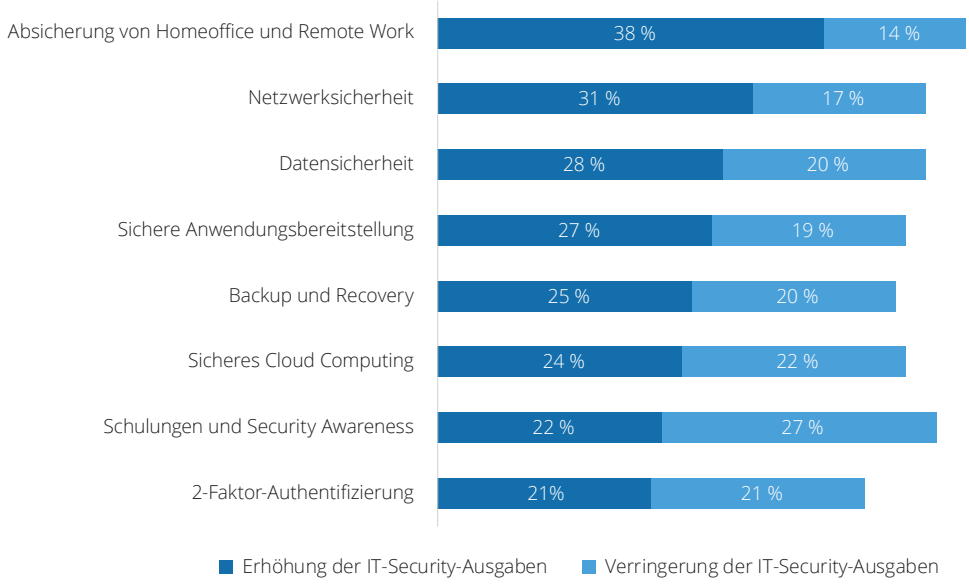
Die Cloud entwickelt sich immer stärker zum integralen Bestandteil der IT-Landschaft. Aus diesem Grund müssen sich Unternehmen deutlich stärker als bisher auf Cloud Security konzentrieren. Die Absicherung der Private Cloud und die Nutzung von Public Cloud Services ist für viele Unternehmen Tagesgeschäft. Mit hybriden Clouds und Multi Clouds steigen sowohl die Zahl der potenziellen Angriffspunkte als auch die Anzahl der Personen und Identitäten, die gemeinsam an einer Aufgabe arbeiten oder in einem Ökosystem miteinander agieren. Das erfordert eine hohe Robustheit der Lösungen, um potenziellen Angreifern wenig Raum zu lassen bzw. sofort reagieren zu können.

Der hohe Stellenwert von Access und Identity Management wurde gerade bei der Cloud Security erwähnt. Die Erstellung und aktive Verwaltung der Rollen und Berechtigungen während des gesamten Identity Life Cycle, die Validierung von Identitäten sowie das Provisioning und die Überwachung der Zugriffe auf Dienste und Daten ermöglichen Ihrem Unternehmen sichere Abläufe in der IT und den Geschäftsprozessen. Klare Identitäten sind die Basis, um als vertrauenswürdiger Partner in digitalen Ökosystemen akzeptiert zu werden. Das gilt ebenso im Umkehrschluss. Denn selbstverständlich müssen Ihre Vertragspartner vertrauenswürdig sein.

Ratschlag 3: Agieren Sie operativ und strategisch – „The New Normal“

COVID-19 hat sehr plastisch gezeigt, dass viele Unternehmen nicht auf plötzlich auftretende externe Großlagen vorbereitet sind. Das gilt sowohl für ihre Fähigkeit, auf die Veränderungen im Tagesgeschäft zu reagieren, als auch für Konzepte mit langfristiger Auswirkung. COVID-19 hat in vielen Unternehmen zunächst zu einer starken Verunsicherung und dann zu einer Neubewertung der IT-Projekte geführt. COVID-19 stellt nach wie vor für die meisten von uns einen großen Unsicherheitsfaktor dar. Die wirtschaftliche Unsicherheit wird auch in den kommenden Monaten fortbestehen und in vielen Organisationen Kosteneinsparungen, Anpassungen und die Optimierung von Prozessen zur Folge haben. Der Fokus liegt auf kurzfristig orientierten und operativ angelegten Aktivitäten. IT-Sicherheit darf hier nicht zu kurz kommen. Das ist auch nicht der Fall, das zeigt der IDC Research deutlich. IT-Security zählt zu den „Gewinnern“ der aktuellen Situation. Für die Absicherung von Homeoffice und Remote Work haben 38 Prozent der Befragten ihre Budgets erhöht. Hierzu zählen Ausgaben für die bessere Absicherung der Endgeräte und Investitionen für Data Protection. 31 Prozent der Befragten wollen mehr für Netzwerksicherheit ausgeben. Dringliche Investitionen in Backup und Recovery, sicheres Cloud Computing und stärkeres Identity und Access Management stehen weiterhin aus und müssen aus IDC Sicht kurzfristig adressiert werden.

Abbildung 3: Wie haben sich aufgrund von COVID-19 die IT-Security-Ausgaben Ihres Unternehmens in folgenden Bereichen geändert?



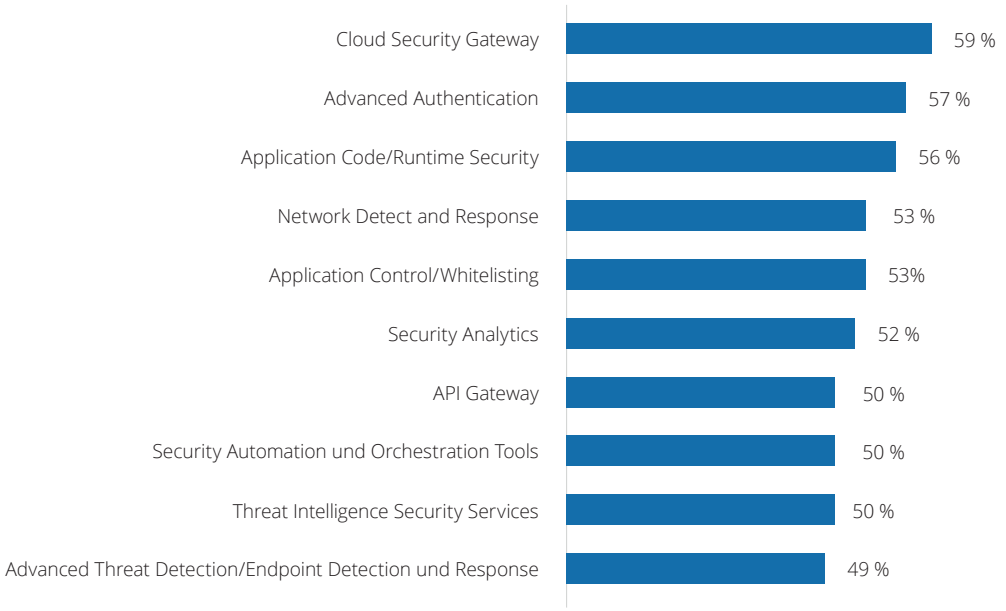
N = 210 Unternehmen; Mehrfachnennungen; Abbildung gekürzt

Arbeiten Sie also an Lösungskonzepten, die weg von Business as Usual führen und Unternehmen fit machen für die anstehenden Herausforderungen. Die Zeichen stehen aktuell gut dafür, dass Sie in der Unternehmensleitung auf Offenheit gegenüber IT-Security stoßen, wenn Sie das Thema als wirtschaftlich notwendig positionieren. Wir erwarten weiter sinkende IT-Budgets. IT-Security bewegt sich also mit Blick auf finanzielle Ressourcen in einem herausfordernden Umfeld. Aber die Chancen sind hoch, sich in diesem Umfeld zu behaupten und zu verbessern. Dafür ist es notwendig, Ad-hoc-Schritte, operative Tätigkeiten und strategische Maßnahmen in einen Gesamtkontext zu stellen.

Ratschlag 4: Forcieren Sie Automatisierung und Integration und nutzen Sie gezielt Cyber Security Tools

69 Prozent der Befragten sehen in einer umfassenden Automatisierung der Security-Prozesse aufgrund der wachsenden Cyberrisiken einen erforderlichen Schritt zur Stärkung der Sicherheit. Die Automatisierung ist ohne Zweifel einer der Schlüssel für eine erfolgreiche Cyber Security, denn die Masse der Angriffe erzwingt schnelle Reaktionen oder, was noch wichtiger ist, vorbeugende Maßnahmen (Detect & Respond). Zwar zeigt sich, dass Unternehmen damit begonnen haben, ihre IT-Security-Abläufe zu automatisieren, allerdings in vielen Fällen nur punktuell. Ein wichtiger Treiber für die Automatisierung und die Integration ist die Nutzung von Cyber-Security-Lösungen. Aus Sicht von IDC ist die Durchdringungsrate noch viel zu gering. Scheuen Sie sich nicht, diese modernen und mitunter komplexen Tools einzusetzen. Ihr Nutzen beim Aufspüren und Bekämpfen von Advanced Threats ist signifikant. Wenn Sie intern keine Spezialisten für diese Tools einsetzen können oder wollen, dann stehen Ihnen Dienstleister oder Managed Security Services zur Verfügung.

Abbildung 4: Welche der folgenden Cyber Security Tools nutzt Ihr Unternehmen derzeit?



N = 210 Unternehmen; Mehrfachnennungen; Abbildung gekürzt

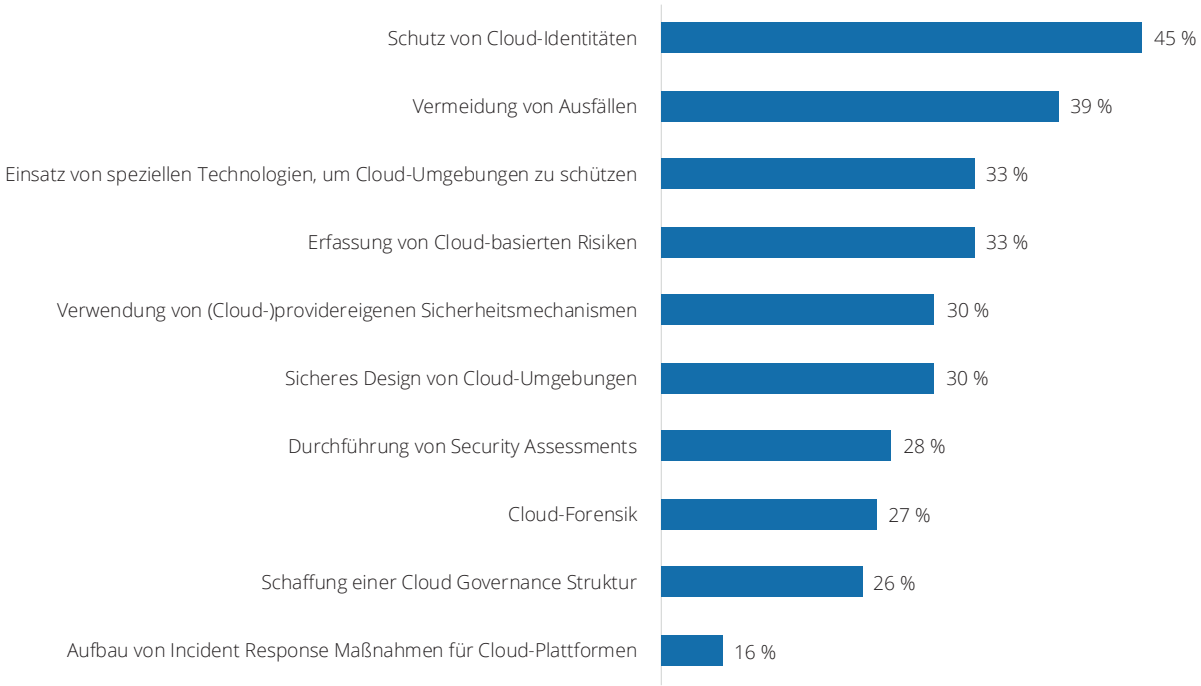
Für **23 Prozent** sind fehlende Security-Spezialisten eine ernsthafte Hürde für höhere IT-Sicherheit.

Die Automatisierung einzelner Prozesse über verschiedene Security-Domains hinweg braucht Integration. Die Integration von verschiedenen Security-Lösungen ist seit Jahren eine Dauerbaustelle in den Unternehmen, an der die IT-Security-Industrie aufgrund geringer Integrationsfähigkeit der Lösungen ihren Anteil hat. Nun kommt aber langsam Bewegung in die Sache. 49 Prozent der Befragten nutzen derzeit Lösungen zur engeren Verzahnung der Komponenten eines Anbieters. Jeweils 42 Prozent korrelieren Security-Lösungen mit Netzwerk-Management-Lösungen und integrierten Lösungen Dritter auf Basis eines Kommunikations-Layers. Diese Ansätze unterstreichen das Streben nach proaktivem Schutz, nach Monitoring und Transparenz als wichtige Voraussetzung für reaktionsschnelles Handeln. Analytische Ansätze und KI-basierte Funktionalitäten bieten hier einen deutlichen Mehrwert. Analytics und KI sind seit vielen Jahren „Built-in"-Funktionalitäten in Lösungen und Services. Ohne solche leistungsstarken Funktionen können die riesigen anfallenden Datenmengen gar nicht mehr bearbeitet werden. Automatisierung und Integration helfen zudem, den Mangel an qualifizierten Mitarbeitern – eine permanente Herausforderung – abzumildern und in Ansätzen zu kompensieren. Somit erfüllen Automatisierung und Integration mehrere Aufgaben: die Optimierung der Lösungslandschaft, die Beschleunigung unterschiedlicher Prozesse, die Stärkung einer proaktiven Vorgehensweise und die Entschärfung kritischer Personalengpässe.

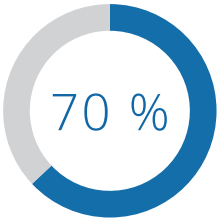
Ratschlag 5: Positionieren Sie Cloud Security als ein wesentliches Element von Cyber Security

Die wachsende Bedeutung von Cloud-Architekturen, Cloud Services, Cloud-Technologie und Cloud-native Modellen und Vorgehensweisen machen sehr klar deutlich, dass Cloud Security einen zentralen Stellenwert für Cyber Security hat. Aus diesem Grund ist es folgerichtig, der Cloud Security besondere Aufmerksamkeit zu widmen und Cloud Security fokussiert zu betrachten. Cloud Security umfasst Schutz- und Abwehrmaßnahmen, die auch in den weiteren Bereichen der Informationstechnologie zum Einsatz kommen. Allerdings sind einige Besonderheiten zu beachten. Hierzu zählen die Integration von Cloud Services aus unterschiedlichen Quellen und ein sehr hoher Automatisierungsgrad aller Abläufe und Prozesse.

Abbildung 5: Was gehört für Sie zu Cloud Security?



N = 210 Unternehmen



70 Prozent der Befragten betonen, dass hybride Clouds und Multi Clouds eine angepasste Security-Architektur erfordern.

Die Integration und die Automatisierung sind ein echter Mehrwert der Cloud. Die Zahl der potenziellen Angriffspunkte aber auch die Anzahl der Personen und Identitäten, die in Ökosystemen – auf der Basis von hybriden Clouds oder Multi-Clouds – agieren, stellen an die Security-Architektur vor allen aufgrund der immensen Komplexität besonders hohe Anforderungen. Das ist umso wichtiger, da in der Cloud IT und Business enger zusammenrücken. In der frühzeitigen Integration von IT-Security zeigt die Befragung der Entscheider noch deutliche Lücken. In gerade einmal 36 Prozent der Unternehmen ist die IT-Sicherheit in die Planung, Initiierung und Bewertung aller neuen Initiativen eingebunden. Das ist deutlich zu wenig. Prüfen Sie genau, wo Ihr Unternehmen hier steht. Mit dem Terminus „Shift Left" ist eine Bezeichnung etabliert, die diesen Ansatz der Einbeziehung von Security von Anfang an auf den Punkt bringt. Wie dringlich „Shift Left" ist, zeigt sich sehr klar in Cloud-nativen Umgebungen, die nach DevOps-Methoden arbeiten. Weitere Studien von IDC etwa zeigen, dass nur in 35 Prozent der Unternehmen Security in DevOps-Prozessen abgebildet und Security-Teams aktiv in die App-Entwicklung einbezogen werden. Das gilt wohlgemerkt für Unternehmen, die DevOps-Methoden nutzen.

Cloud Security erhöht die Anforderungen an Governance signifikant; Transparenz und Integration über die Security Tools sind zentrale Enabler für eine umfassende Cloud Security. Sensibilisieren Sie alle Stakeholder in Ihrem Unternehmen für einen Perspektiv- und Paradigmenwechsel bei der Bewertung und Umsetzung von IT-Security in Business-Initiativen auf Basis der Cloud.

FAZIT UND AUSBLICK

IT-Sicherheit erhält nach wie vor nicht die Aufmerksamkeit zur Absicherung der Betriebsabläufe, die erforderlich ist. Zwar sind ein Basisschutz und Standard-Security-Lösungen in allen Organisationen vorhanden. Das allein reicht aber immer weniger dafür aus, der Vielzahl und der Intensität der Angriffe zu begegnen und die Ausgangslage nach erfolgreichen Attacken wiederherzustellen.

Die aktuelle Anforderung besteht für die meisten Unternehmen explizit darin, ihre IT-Security-Strategie auf den Prüfstand zu stellen, um neue Technologien und Lösungsansätze, digitales Business und neue Formen der Zusammenarbeit zwischen unterschiedlichen Marktteilnehmern umfassend abzusichern und die Agilität und Widerstandsfähigkeit ihrer Organisation gegenüber unerwarteten Vorkommnissen zu erhöhen.

Cyber Security ist eng mit der digitalen Transformation verbunden. Aus diesem Grund ist es für Sie wichtig, auch diejenigen Stakeholder anzusprechen, die Innovationen evaluieren und umsetzen. Das ist eine dringliche Aufgabe, da die IT-Bereiche und die Fachbereiche der IT-Security nach wie vor einen untergeordneten Stellenwert beimessen.

Integration, Automatisierung und eine kontinuierliche Optimierung von Security-Prozessen über alle IT-Domains und Business-Domains hinweg sind dabei der Schlüssel zum Erfolg. Daran müssen Sie gemeinsam mit Ihren Anbietern und Partnern arbeiten. Allerdings bedeuten mehr Tools und Lösungen nicht zwangsläufig mehr Sicherheit. Es geht darum, die neuralgischen Punkte abzusichern. Das Netzwerk, die Cloud, Endpoints, Identitäten und Daten sind dabei Punkte, auf die Sie sich unbedingt konzentrieren müssen.

Die meisten Unternehmen in Deutschland haben die Herausforderungen nach IDC Einschätzungen erkannt, müssen aber weitere grundlegende Schritte gehen, um für die Herausforderungen, die da kommen, gewappnet zu sein.

EMPFEHLUNGEN VON ANWENDERN FÜR ANWENDER

Die Befragungsteilnehmer wurden gebeten, anderen Entscheidungsträgern ihre Best Practices im Kontext Cyber Security mitzuteilen. Einige der Antworten sind nachfolgend ungefiltert wiedergegeben. Auf eine Kommentierung wird hier bewusst verzichtet, um einen authentischen Eindruck zu vermitteln.

„Ein einheitliches Bedrohungsmanagementsystem kann die Integration ausgewählter Sicherheitsprodukte automatisieren und wichtige Funktionen der Sicherheitsoperationen beschleunigen: Erkennung, Untersuchung, Behebung."

„Für uns sind drei Aspekte wichtig: Mitarbeiter besser schulen! Aktuelle Firmware und Patches aufspielen! Bessere Abstimmung in den Abteilungen!"

„Cloud-Sicherheit steht für unser Unternehmen an erster Stelle."

„Security muss von Anfang an umgesetzt werden."

„Alle Schwachstellen in der IT müssen abgedeckt werden."

„Die Transparenz über alle Systeme und Anwendungen ist die Voraussetzung dafür, alles gut absichern zu können."

„Die Komplexität der Security ist viel zu hoch."

„Die Geschäftsführung muss den Wert der IT-Sicherheit besser verstehen."

„Wir brauchen häufig zu lange, um auf neue Risiken einzugehen. Hier müssen wir schneller werden."

„Für die neuen Anforderungen müssen Unternehmen Cyber-Security-Experten einstellen."

METHODIK

IDC hat im August 2020 eine primäre Marktbefragung durchgeführt, um detaillierte Einblicke in die aktuellen Umsetzungspläne, Herausforderungen und Erfolgsfaktoren in puncto Cyber Security zu erhalten. Anhand eines strukturierten Fragebogens wurden branchenübergreifend 210 Organisationen in Deutschland mit mehr als 100 Mitarbeitern befragt.

Die nachfolgenden Informationen wurden von Tend Micro zur Verfügung gestellt. Für diese Angaben übernimmt IDC keine Gewähr.

COMPUTACENTER AG & CO. OHG & TREND MICRO DEUTSCHLAND GMBH

Fallstudie: Unternehmen im Finanzsektor

TREND MICRO™ Securing Your Connected World

WWW.TRENDMICRO.COM/DE_DE/BUSINESS/PRODUCTS/HYBRID-CLOUD.HTML

Computacenter

WWW.COMPUTACENTER.COM/DE

ANFORDERUNGEN DES KUNDEN

Der Kunde möchte im Rahmen seiner digitalen Transformation die Anwendungsentwicklung zukünftig mit agilen Methoden und hohem Automatisierungsgrad in mehreren dedizierten Cloud-Umgebungen durchführen. Er beauftragt Computacenter daher mit Architekturentwicklung, Implementierung und Betrieb einer geeigneten Container-Umgebung. Um nicht von einem Cloud-Anbieter abhängig zu sein, soll die Umgebung als Multi-Cloud Deployment realisiert werden.

Da das Unternehmen im Finanzsektor tätig ist, unterliegt es bei der Datennutzung strengen Regularien und muss anspruchsvolle Security-Vorgaben erfüllen. Im Bereich Cloud Security herrscht beim Kunden zudem noch Unsicherheit hinsichtlich der Tools, die zur Erreichung von Sicherheit und Compliance eingesetzt werden sollten. Ebenso ist die Verschiebung der Verantwortlichkeiten weg von klassischen Silo-Strukturen hin zu eigenverantwortlichen Teams eine organisatorische Herausforderung für das Unternehmen.

LEISTUNGEN VON COMPUTACENTER

Mit Unterstützung von Computacenter entwickelt und baut der Kunde Container-Plattformen in mehreren Cloud-Umgebungen auf. Hierbei profitiert das Unternehmen von den Stärken von Computacenter, die besonders in den Bereichen Architektur und Implementierung von Multi-Cloud-Umgebungen und Container-Plattformen, Integration unterschiedlicher Lösungen und Anbieter sowie deren Automatisierung liegen.

Computacenter designt und implementiert eine umfassende Red-Hat-OpenShift-Umgebung. Die Bereitstellung der OpenShift-Komponenten erfolgt dabei entsprechend den Kundenvorgaben bei mehreren Cloud-Anbietern. In diesem Fall fiel die Entscheidung auf AWS, Microsoft Azure und Google Cloud. Da die Sicherheit der Cluster maßgeblich durch die zugrundeliegende Cloud-Infrastruktur beeinflusst wird, berät Computacenter ebenfalls beim Design der Cloud-Umgebungen.

Zudem entwickelt Computacenter gemeinsam mit dem Kunden ein Cloud- und Container-spezifisches Governance-Modell, welches die effiziente, Compliance-konforme und regulatorisch adäquate Nutzung der Umgebungen gewährleistet. Dabei dienen die bereits bestehenden Policies des Unternehmens als Grundlage. Regulatorische Anforderungen werden ebenso berücksichtigt wie die Anforderungen und Arbeitsweisen der Anwender.

Die Beratung erfolgt dabei nach einem bewährten Vorgehen in fünf Schritten:

- Review der bestehenden Policies
- Implementierung von Cloud-spezifischen Guardrails
- Cloud Risk Assessments für zu migrierende Anwendungen
- Threat Modeling für fortlaufende Software-Entwicklung
- Continuous Control Monitoring mittels Posture-Management-Lösung

Das Vorgehensmodell beinhaltet ebenfalls die Entwicklung von Policies für Container-Umgebungen. Diese unterscheiden sich von den Vorgaben für Cloud-Umgebungen, da die Nutzer Freiraum zur Entwicklung neuer Anwendungen benötigen. Zudem müssen die Vorgaben mit der Schnelllebigkeit von Containern in Einklang sein und dürfen dem hohen Automatisierungsgrad von Container-Plattformen und CI/CD-Pipelines nicht entgegenstehen.

LEISTUNGEN VON TREND MICRO

Zur Absicherung der Bereitstellungs-Cluster kommt Trend Micro Cloud One zum Einsatz, wobei die Multi- und Hybrid-Cloud-Fähigkeit der Lösung ausschlaggebend ist. Diese kann in AWS, Microsoft Azure, Google Cloud und On-Premise eingesetzt werden, wobei das Management zentral über eine einzelne Cloud-basierte Konsole geschieht. Die Lösung wurde zudem unter Berücksichtigung der relevanten Regelwerke entwickelt (u. a. PCI DSS), sodass mit ihr auch anspruchsvolle Compliance-Anforderungen erfüllt werden können.

Bei Cloud One handelt es sich um eine Cloud-native Sicherheitsplattform mit zentralem Management für ein umfassendes Portfolio von Sicherheitsfunktionen. Mit ihr können Unternehmen bestehende Anwendungen in die Cloud migrieren, neue Cloud-native Applikationen ausrollen und die Betriebsabläufe in der Cloud optimieren, während sie umfassende Compliance sicherstellen. Cloud One bietet unter anderem flexible, automatisierte Bereitstellung und verbrauchsabhängige Abrechnung. Somit ist die Lösung genauso skalierbar wie die Cloud-Instanz, die sie schützt.

Mit Trend Micro XDR stehen zudem Funktionen zur Verfügung, mit denen interne und externe Sicherheits-Teams Cyberangriffe über die komplette IT-Infrastruktur hinweg erkennen und beseitigen können, einschließlich Cloud-Workloads, Servern, Netzwerken, Endpunkten und E-Mails.

MEHRWERTE FÜR DEN KUNDEN

- Bewährtes Vorgehensmodell für Cloud- und Container-Security gewährleistet Sicherheit.
- Expertise etablierter Anbieter schafft Vertrauen.
- Posture-Management-Lösung ermöglicht beständige Überwachung und Sicherstellung von Sicherheit und Compliance.
- Flexible Lösung ermöglicht Skalierbarkeit über verschiedene Cloud- und Datacenter-Infrastrukturen hinweg – auch für zukünftige Projekte.

Interview mit Richard Werner, Trend Micro & Hauke Moritz, Computacenter

CYBER-SECURITY IN DEUTSCHLAND 2020+

Anlässlich der Vorstellung der Ergebnisse der Studie „Cyber-Security in Deutschland 2020+ " sprach IDC mit Richard Werner, Business Consultant, Trend Micro & Hauke Moritz, Lead Consultant – Secure Cloud Usage, Computacenter

IDC: Sie sprechen tagtäglich mit Ihren Kunden über Risiken und deren Vermeidung, Minimierung bzw. Abwehr. Welche Risiken betrachten Ihre Kunden als besonders kritisch?

Hauke Moritz: Eine der größten Befürchtungen ist, Innovationsthemen zu verschlafen und dem stetig wachsenden Verlangen des Marktes und der eigenen Mitarbeiter nach digitalen Angeboten nicht gerecht zu werden. Digitalisierung bringt viele neue Technologien mit sich, angefangen bei den großen Hyperscalern über Container und Orchestratoren bis hin zu Tools zur Bereitstellung solcher Umgebungen. Die Vielzahl an Tools lässt Raum für Fehlkonfigurationen, die von Angreifern ausgenutzt werden können. Deshalb sind ihre Erkennung und Beseitigung sicher eine der größten Herausforderungen für unsere Kunden.

Ebenso, die eingesetzten Komponenten immer aktuell zu halten und damit softwarebasierten Schwachstellen entgegenzuwirken. Dabei kann man schon in der Designphase eklatante Fehler machen. Zudem ist Automatisierung das Kernelement moderner Software-Entwicklung und Bereitstellung. Sicherheitslösungen müssen deshalb in der Lage sein, sich ständig ändernde Infrastrukturen und Anwendungen genauso effektiv zu schützen wie bisher.

Richard Werner: Die Problematik von Fehlkonfigurationen zeigt, dass der menschliche Fehler noch immer die größte Sicherheitsproblematik ist, der sich Unternehmen stellen müssen – auch in der Cloud. Hier agieren vor allem Fachleute für bestimmte Bereiche, wie Software-Entwickler oder Administratoren, die das Thema IT-Security oft nur als Zusatzaufgabe erhalten. Daraus entstehen zwei Herausforderungen: Zum einen wird Sicherheit als lästige Pflicht so einfach gehalten wie möglich. Zum anderen passieren oft simple, vermeidbare Fehler durch schiere Unkenntnis. Kommt es dann zu einem Vorfall, ist es nicht nur schwierig, die Auswirkungen in ihrer Gänze zu umfassen, sondern auch darzustellen, dass das Unternehmen ein adäquates Risikomanagement betrieben hat.

IDC: Transparenz, die Automatisierung von Abläufen und Prozessen sowie proaktives Handeln gelten als Erfolgsschlüssel. Warum tun sich viele Unternehmen so schwer damit?

Richard Werner: Bisher ist der Grund meist die Vielfalt der eingesetzten Security-Technologien verschiedener Hersteller. Es ist oft schon schwierig, unterschiedliche Datenquellen miteinander zu verbinden und daraus Rückschlüsse über Zusammenhänge zu ziehen. Fast unmöglich ist es, dann noch adäquate Gegenmaßnahmen zu unternehmen, wenn unterschiedliche Lösungen nicht miteinander koordiniert werden können. Gerade der Wechsel in die Cloud bietet die Chance, aus früheren Fehlern zu lernen und auf automatisierte, übergreifende Werkzeuge zu setzen, die zentral von der IT-Security-Abteilung gesteuert werden. Leider ist dies noch immer zu selten der Fall.

Hauke Moritz: Verschärft wird diese Problematik noch durch den Fachkräftemangel – gerade im Cloud- und Security-Bereich: Dieser bremst Unternehmen in ihrem Vorankommen, sodass sie digitale Angebote nicht mit der gewünschten Geschwindigkeit entwickeln können. Viele lassen dann die Sicherheit außer Acht, um vermeintlich schneller voranzukommen.

Gleichzeitig ist das auch ein kulturelles Thema: Unternehmen haben einen enormen Bedarf an Architekten, die sowohl technisch hochqualifiziert sind als auch mit Menschen umgehen können. Bei der Entwicklung digitaler Angebote sind viele Fachbereiche involviert, die bisher nicht zusammengearbeitet haben. Somit stoßen auch unterschiedliche Erwartungshaltungen, Wissensstände und Vorgehensweisen aufeinander, die erstmal in Einklang gebracht werden müssen.

IDC: Was sind aus Ihrer Sicht die wichtigsten drei Erfolgsfaktoren, die Unternehmen unbedingt berücksichtigen müssen, um den Fachabteilungen jederzeit sichere IT-Ressourcen bereitstellen zu können?

Hauke Moritz: Erstens die Risiken bei der Bereitstellung von digitalen Angeboten kennen und verstehen – auch im Kontext von Services und Applikationen, die direkt von den großen Public Cloud Providern angeboten werden. Zweitens die Anpassung der organisatorischen Sicherheit an Cloud-Plattformen und die Integration in umfassende Cyber Defense Center und ihre Prozesse. Und drittens

ein hoher Automatisierungsgrad von Infrastruktur und Security – gerade für erfolgreiche Incident Detection and Response.

Richard Werner: Security wird nur dann nicht als Belastung empfunden, wenn sie sich erstens in die Aufgaben der Fachabteilungen integriert, zweitens diese bei der Ausführung ihrer Tätigkeiten nicht einschränkt und drittens die nötige Logistik minimiert, um Sicherheit zu erreichen. Gerade die Cloud mit ihrem klaren Fokus auf Automatisierung bietet hierfür optimale Voraussetzungen.

IDC: Mit welchen Angeboten unterstützen Sie IT-Organisationen und Fachentscheider in den Unternehmen im Detail?

Richard Werner: Trend Micro bietet Lösungen, die Security-Informationen konsolidieren und Security-Aufgaben automatisieren. In der Cloud sind die Sicherheitsfunktionen auf die darunter liegenden Cloud-Angebote ausgerichtet und können deshalb automatisiert in derselben Art und Weise genutzt werden wie der Cloud-Service selbst. Dadurch gelingt eine optimale Integration in die Arbeitsbereiche der Fachabteilungen, während die IT-Security den nötigen Überblick erhält, um Sicherheit und Compliance des Unternehmens zu gewährleisten.

Hauke Moritz: Computacenter stellt Architekten bereit, die sowohl technisch als auch organisatorisch in der Lage sind, die Entwicklung von sicheren digitalen Angeboten und die notwendige Infrastruktur zu unterstützen. Dazu wird ein umfangreiches Framework verwendet, welches unter anderem Cloud- und DevSecOps-Governance adressiert, also die Anpassung von Richtlinien und Trainings. Zudem unterstützen wir organisatorisch, indem wir beispielsweise die Anwendungsentwicklung sowie das Design und die Bereitstellung von Infrastrukturen begleiten und die Wahrung der Security sicherstellen. Zuletzt begleiten wir unsere Kunden natürlich auch mit technischen Maßnahmen, wie der Auswahl und Implementierung von Sicherheitslösungen, der Anbindung von Cloud-Plattformen an bestehende Security-Infrastrukturen und der Automatisierung von Incident-Response-Maßnahmen.

IDC: Werfen wir einen Blick voraus: Wie wird eine erfolgreiche IT-Security-Landschaft in den nächsten zwei bis drei Jahren idealerweise aussehen?

Hauke Moritz: Je einfacher ein System oder eine Umgebung, desto leichter ist sie zu schützen. In den kommenden Jahren werden wir deshalb eine Reduktion der Anzahl an Security-Herstellern sehen. Dabei werden diejenigen überleben, die in der Lage sind, möglichst viele Sicherheitsfunktionen zu vereinen und ein vollständiges Sicherheitslagebild auf Knopfdruck zu liefern. Hersteller, die bereits heute einen plattformbasierten Ansatz fahren, sind daher auf einem guten Weg, dürfen jetzt aber nicht nachlassen. Schlüsselelemente sind die Automatisierung sowie eine umfassende Integration in andere Komponenten. Interessant sind dabei vor allem automatisierbare Schnittstellen und Konzepte, um Services und Lösungen von einer Cloud in eine andere oder in ein Multicloud-Szenario zu überführen – speziell um die Abhängigkeit von einem einzelnen Hyperscaler zu vermeiden und flexibel zu bleiben.

Richard Werner: Da sind wir ja auf dem besten Weg! Ich denke auch, dass die IT-Security noch stärker zu einer zentralen Funktion wird, die konsolidiert und vor allem die Anzahl der eingesetzten Tools und Hersteller minimiert. Die Aufgabe, das Unternehmen in seinem Erfolg abzusichern, wird bestehen bleiben. Allerdings wird die Erwartungshaltung dahin gehen, dies ohne Verbote oder Einschränkungen moderner Technologien zu erfüllen. Hierfür benötigt die IT-Sicherheit ihrerseits Flexibilität und strategischen Weitblick.

Richard Werner
Business Consultant, Trend Micro

Hauke Moritz
Lead Consultant – Secure Cloud Usage, Computacenter

IDC CENTRAL EUROPE GMBH

Hanauer Landstr. 182 D
60314 Frankfurt • Germany
T: +49 69 90502-0
F: +49 69 90502-100
E: info_ce@idc.com
www.idc.de

IDC ANALYZE THE FUTURE