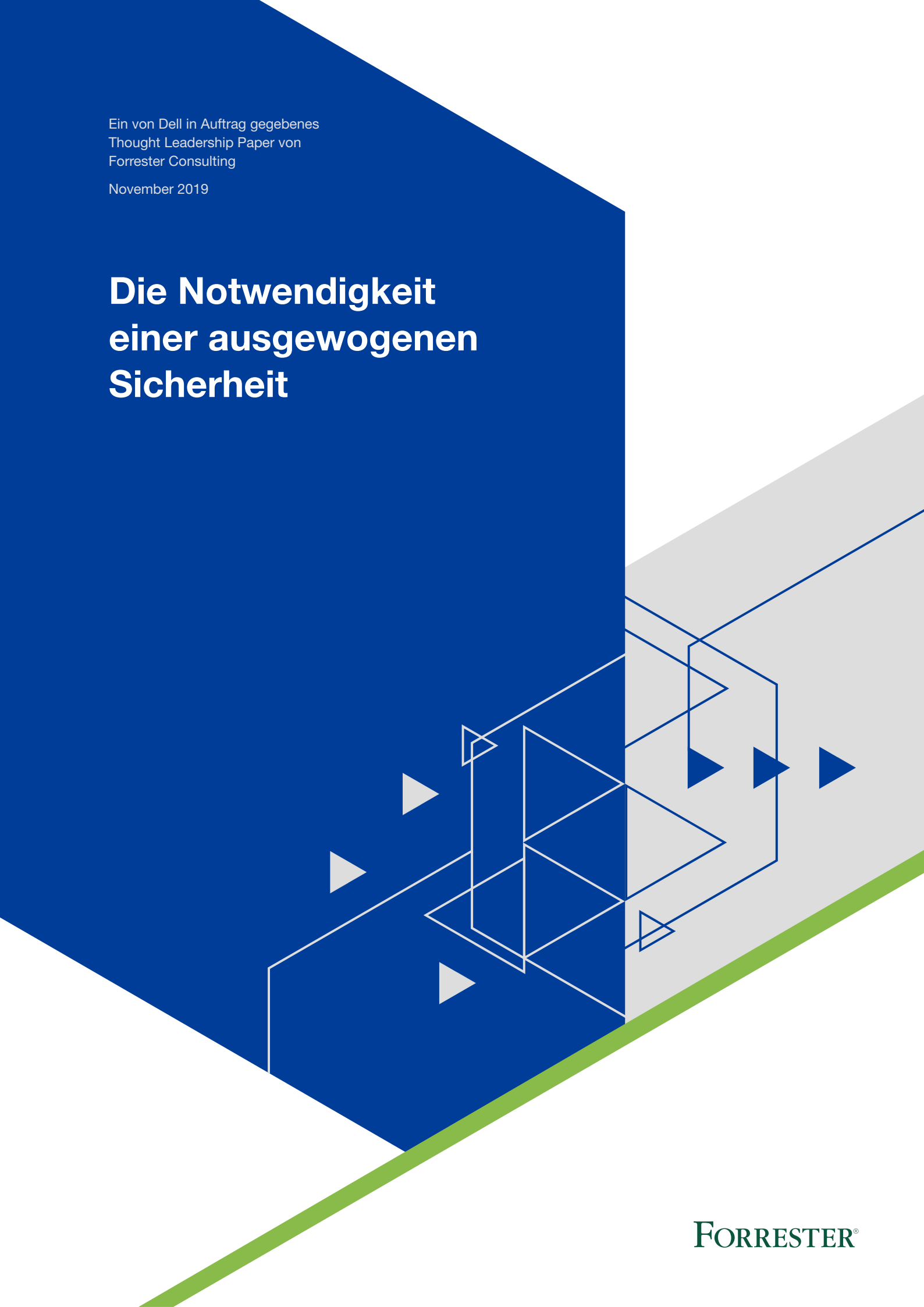
Ein von Dell in Auftrag gegebenes
Thought Leadership Paper von
Forrester Consulting

November 2019

Die Notwendigkeit einer ausgewogenen Sicherheit



FORRESTER®

Inhaltsverzeichnis

Projektleiter:
Tarun Avasthy,
Market Impact Consultant

Forschungsbeitrag:
Infrastructure & Operations
Research Group von Forrester

ÜBER FORRESTER CONSULTING

Forrester Consulting bietet unabhängige und objektive forschungsbasierte Beratung, um Führungskräften zu helfen, in ihren Unternehmen erfolgreich zu sein. Die Beratungsdienstleistungen von Forrester reichen von kurzen Strategiesitzungen bis hin zu kundenspezifischen Projekten und bringen Sie in direkten Kontakt mit Forschungsanalysten, die ihre Fachkenntnis auf Ihre spezifischen geschäftlichen Herausforderungen anwenden. Weitere Informationen finden Sie unter forrester.com/consulting.

FORRESTER®

Zusammenfassung

Ausgewogene Sicherheit bedeutet, dass Unternehmen dazu übergehen müssen, Datenschutz und Datensicherheit nicht mehr als Complianceanforderungen zu behandeln, sondern sich für Datenschutz einzusetzen und die Technologiefähigkeiten zu nutzen, um die Marke von der Konkurrenz abzuheben. Jeder Fehltritt mit oder Änderungen an der IT-Infrastruktur kann und wird die Komplexität verschärfen und genau aus diesem Grund ist die Entwicklung einer ausgewogenen Sicherheitsstrategie so wichtig. Eine ausgewogene Sicherheitsstrategie negiert die Komplexität, indem sie mit dem Tempo des technologischen Wandels sowie den Umwälzungen in der Branche und der sich ständig weiter entwickelnden Compliance Schritt hält.

Dell hat Forrester Consulting im März 2019 mit der Bewertung aufkommender Sicherheitstrends und -technologien für den Schutz und die Unterstützung von Mitarbeitern beauftragt. Unsere Studie ergab, dass sich die Mitarbeiterproduktivität verbessert, wenn Mitarbeiter unterstützt und gleichzeitig Sicherheitsprotokolle befolgt werden. Forrester hat eine Onlineumfrage unter 887 leitenden Geschäfts- und IT-Entscheidungsträgern durchgeführt, um dieses Thema zu untersuchen.

WICHTIGE ERKENNTNISSE

- **Sich ständig weiter entwickelnde Bedrohungen zwingen mittelständische Unternehmen, eher proaktiv als reaktiv zu agieren.** Angesichts der zahlreichen, regelmäßig in den Nachrichten öffentlich gemachten Sicherheitsverletzungen und/oder Cyberangriffe müssen mittelständische Unternehmen ihren Sicherheitsansatz überdenken.
- **Ausgaben für Sicherheit allein werden keine Patentlösung sein.** Mittelständische Unternehmen müssen sich auf eine Kultur der Förderung, die kontinuierliche Weiterentwicklung von Kompetenzen für Mitarbeiter und – vielleicht der wichtigste Punkt – eine solide und robuste Sicherheitsinfrastruktur konzentrieren.
- **Restriktive IT-Policies führen dazu, dass Mitarbeiter die Best Practices für die IT-Sicherheit umgehen, um ihre Arbeit zu erledigen.** Vorschriften am Arbeitsplatz zu umgehen, ist nicht weiter ungewöhnlich, aber wenn IT-Policies komplett vermieden werden, um die Arbeit erledigen zu können, ist das einfach nur riskant.

Unternehmen benötigen eine ausgewogene Sicherheit, um die Mitarbeitererfahrung und Betriebseffizienz zu verbessern

Eine vielfältige Technologielandschaft und sich ändernde Arbeitsstile bei Mitarbeitern haben die Tür zu einer Fülle an Risiken geöffnet, die die allgemeine Sicherheitslage eines Unternehmens und seinen Ruf gefährden. Eine robuste, ausgewogene Sicherheitsinfrastruktur sorgt für eine maximale und geschützte Unternehmensperformance. Unterdessen wächst die Bedeutung der Mitarbeitererfahrung (Employee Experience, EX) als geschäftliche Initiative, da immer mehr Unternehmen daran interessiert sind, eine Strategie rund um die Mitarbeitererfahrung zu entwickeln, die Reibungen reduziert und es Mitarbeitern ermöglicht, ihre wichtigsten Aufgaben auf effiziente Weise zu erledigen.

Ausgaben für Technologie allein werden nicht dazu beitragen, die Mitarbeitererfahrung zu verbessern. Unternehmen, insbesondere mittelständische Unternehmen, müssen auch in den Aufbau einer Kultur der Mitarbeiterförderung, der kontinuierlichen Weiterentwicklung von Kompetenzen und der robusten Sicherheit investieren, um Risiken zu managen und gleichzeitig die Unternehmensperformance zu unterstützen. Für eine großartige Mitarbeitererfahrung benötigen Unternehmen einen ausgewogenen Sicherheitsansatz in drei wichtigen Bereichen (siehe Abbildung 1):

- **Steigerung der Mitarbeiterproduktivität.** Der geschäftige Arbeitsplatz von heute stellt intensive kognitive Anforderungen an Mitarbeiter. Aus diesem Grund ist die Unterstützung von Mitarbeitern, damit diese ihre Arbeit meistern können, ein wesentlicher Teil einer guten Mitarbeitererfahrung. Viele Sicherheitsmaßnahmen bewirken jedoch das Gegenteil und unterbrechen ihre Produktivität. Vor diesem Hintergrund möchten mittelständische Unternehmen die Produktivität ihrer Mitarbeiter in den nächsten 12 Monaten verbessern (88 %). Angesichts der Weiterentwicklung der Technologie gaben die Befragten auch an, dass sie die Mitarbeiterbindung und -weiterbildung verbessern werden (79 %), um sicherzustellen, dass die Talentlücken so klein wie möglich bleiben.
- **Verstärkung der Informationssicherheit.** Damit Mitarbeiter erfolgreich sein können, benötigen sie auch einen ungehinderten Zugang zu den Informationen, die für ihre Aufgaben erforderlich sind – unabhängig davon, wo sie arbeiten und welche Geräte sie verwenden, um ihre Arbeit zu erledigen. Unternehmen unterliegen jedoch einem Sperrfeuer von unterschiedlichen Arten von Cyberangriffen und Ereignissen, die den Geschäftsbetrieb unterbrechen und sensible Daten gefährden können – ganz gleich, ob es sich um personenbezogene Daten von Kunden/Mitarbeitern oder um sensible Unternehmensinformationen handelt. Darüber hinaus bedeuten Bedenken wie Drittanbieterrisiken und Lieferkettensicherheit, dass Unternehmen ihre Sicht auf die Risiken für das Unternehmen über die eigene Umgebung hinaus ausweiten müssen. Es überrascht nicht, dass 86 % der Unternehmen sagten, dass sie die Informationssicherheit priorisieren werden.
- **Verbesserung der Betriebseffizienz.** Sicherheitsteams, die den Geschäftsbetrieb unterstützen, müssen einen wesentlich konsistenteren Prozess für ihren Betrieb einrichten und sich darum bemühen, ihren Sicherheitsansatz proaktiv statt reaktiv zu gestalten. Mittelständische Unternehmen müssen über einen standardmäßigen Abhakansatz hinausgehen, bei dem Sicherheitsmaßnahmen hauptsächlich auf Complianceanforderungen basieren, und zu einem eher strategisch orientierten und risikobasierten Sicherheitsansatz übergehen. Dies erfordert Prozesse zur Unterstützung von Risikoinformationen, Bedrohungserkennung und -reaktion, Risikobewertung und Unternehmensstabilität, um das Versprechen der Projektausführung und -bereitstellung zu erfüllen (83 %).

Mittelständische Unternehmen sollten in den Aufbau einer Kultur der Mitarbeiterförderung, der kontinuierlichen Qualifizierung und der Bemühung um eine robuste Sicherheitsinfrastruktur investieren.

FORRESTER®

Abbildung 1

„Welche der folgenden technologiebezogenen Initiativen wird in den nächsten 12 Monaten in Ihrer Abteilung oder Division priorisiert?“

Basis: 887 Unternehmens- und IT-Entscheidungsträger, die an der Entscheidungsfindung für Laptops, Computer und andere Geräte beteiligt sind
Quelle: Eine von Forrester Consulting im Auftrag von Dell durchgeführte Studie, September 2019

Zunehmende Bedrohungen und IT-Komplexität sind ständige Herausforderungen

Angesichts konkurrierender Prioritäten, neu aufkommender Technologien und neuer behördlicher Auflagen sind Sicherheitsmanager beauftragt, kontinuierliche Abwehrmaßnahmen zu entwickeln und sicherzustellen, dass Angreifer nicht erfolgreich sind. Als wir jedoch die Umfrageteilnehmer nach ihren größten Sicherheitsherausforderungen fragten, stellten wir Folgendes fest (siehe Abbildung 2):

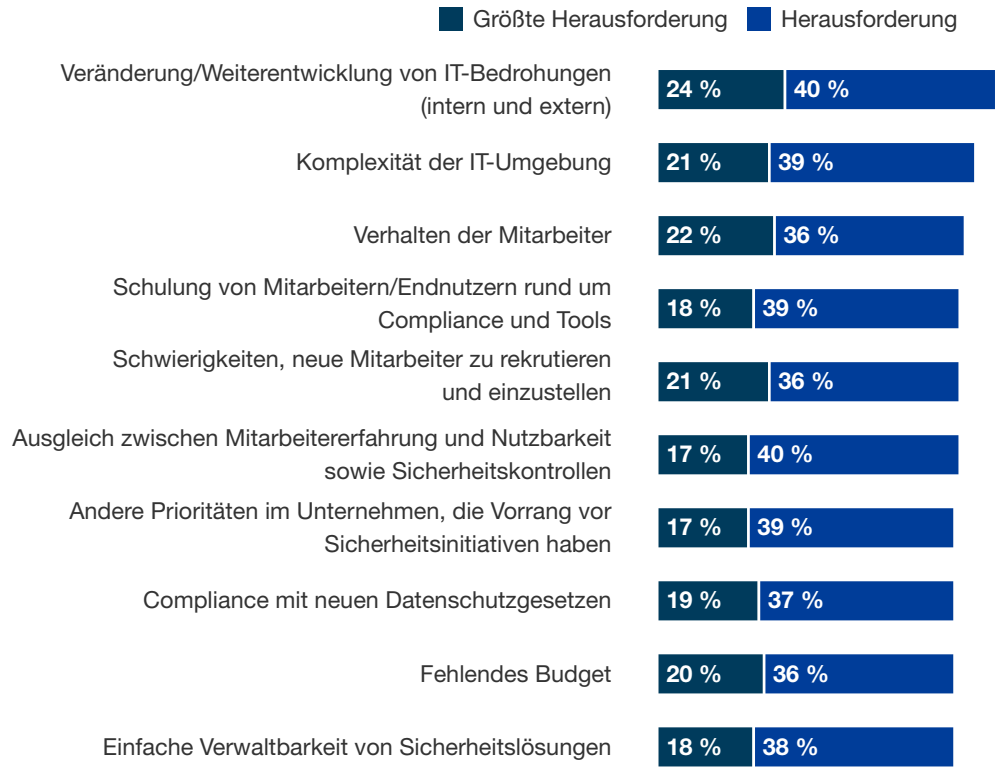
› **Die sich ständig weiter entwickelnden Bedrohungen sorgen dafür, dass mittelständische Unternehmen ständig auf der Hut sind und sich immer wieder auf den neuesten Stand bringen müssen.** Die IT muss über eine robuste, anpassbare Strategie verfügen, um Reibungsfläche für Angreifer zu schaffen. 65 % Unternehmen stehen vor Problemen mit der sich wandelnden Natur heutiger Sicherheitsangriffe. Wenn Führungskräfte innerhalb des Unternehmens die neuesten Berichte über Cyberangriffe und Ereignisse in den Nachrichten sehen, fragen sie sich, ob das auch in ihrem Unternehmen passieren kann. Sinnvoll ist, das Warum und Wie (oder Warum nicht, je nach Umgebung und Kontrollen) zu bewerten und zu kommunizieren. Lassen Sie jedoch nicht zu, dass dieser reaktive Ansatz Ihrer allgemeinen Sicherheitsstrategie zugrunde liegt.

FORRESTER®

› **IT-Komplexität führt zu erhöhten Risiken und größeren Herausforderungen beim IT-Management.** Fehltritte mit oder Änderungen an der IT-Infrastruktur können und werden die Komplexität verschärfen und genau aus diesem Grund ist die Entwicklung einer robusten Sicherheitsstrategie so wichtig. Eine Sicherheitsstrategie, die mit technologischen Veränderungen, Branchenumwälzungen und sich ändernden Vorschriften und Complianceanforderungen Schritt halten kann, wird als Katalysator für positive Veränderungen dienen. Eine Strategie, die es Ihnen ermöglicht, von Anfang an Sicherheit zu schaffen, sollte gegenüber einer erst im Nachhinein aufgesetzten Sicherheitsstrategie vorgezogen werden. Gleiches gilt für eine Strategie, in deren Mittelpunkt die Konsolidierung der Anzahl der Sicherheitsprodukte in Ihrer Umgebung steht, um ein einfacheres IT-Management zu unterstützen. Derzeit betrachten 60 % der Umfrageteilnehmer die Komplexität ihrer IT-Umgebung als Bedrohung für ihr Unternehmen.

Abbildung 2

„Vor welchen der folgenden Herausforderungen steht Ihr Unternehmen in Bezug auf die IT-Sicherheit?“



Basis: 887 Unternehmens- und IT-Entscheidungsträger, die an der Entscheidungsfindung für Laptops, Computer und andere Geräte beteiligt sind
Quelle: Eine von Forrester Consulting im Auftrag von Dell durchgeführte Studie, September 2019

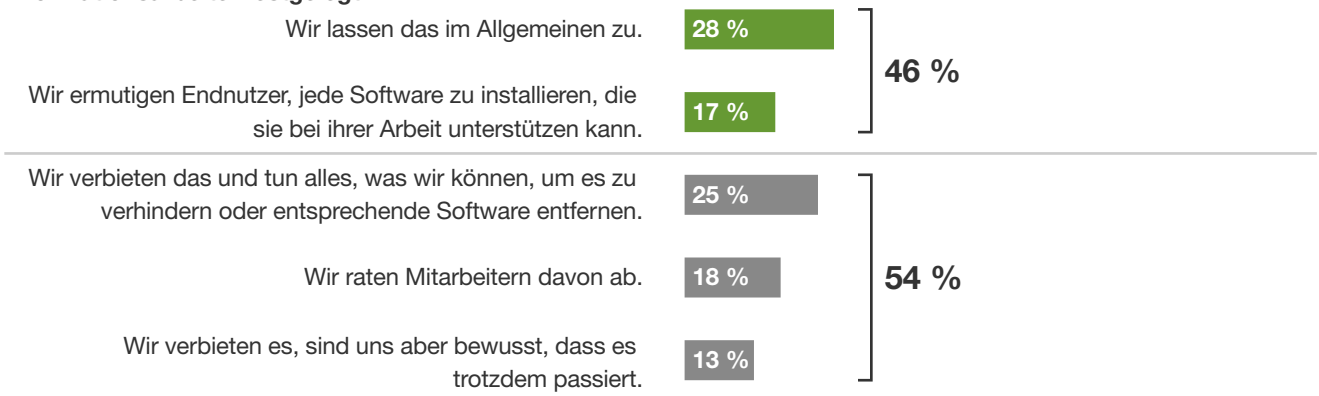
WENN MITARBEITER SICH NICHT UNTERSTÜTZT FÜHLEN, WERDEN SIE IT-POLICIES UMGEHEN

Mitarbeiter entscheiden sich für den Weg des geringsten Widerstands, um ihre Arbeit zu erledigen. Wenn Mitarbeiter dafür eigene Software/Anwendungen installieren möchten, sagen 54 % der Befragten aus mittelständischen Unternehmen, dass sie verhindern, davon abraten oder verbieten, dass Mitarbeiter dies tun. Sie wissen jedoch, dass es dennoch passiert. Mitarbeiter müssen das Gefühl haben, dass sie vom Unternehmen unterstützt werden (siehe Abbildung 3).

Sie müssen ihre Arbeit auf eine Art und Weise erledigen können, die ihre Produktivität nicht unterbricht, und Sicherheitspersonal muss sicherstellen, dass das Unternehmen geschützt ist. 58 % der Befragten berichten, dass Mitarbeiter manchmal IT-Policies umgehen, um ihre Aufgaben zu erledigen, und damit das Unternehmen gefährden. Aus diesem Grund ist es wichtig, Mitarbeitererfahrung und Nutzbarkeit mit Sicherheitskontrollen abzuwägen – für 57 % ist dies aber weiterhin eine Herausforderung. Wenn Unternehmen die Effektivität ihres Sicherheitsprogramms nicht messen können (52 %), befinden sie sich in einem nie enden wollenden Rennen und die Ziellinie – unser goldener Torbogen einer ausgewogenen Sicherheitsstrategie – liegt stets weiter direkt hinter dem nächsten Hügel.

Abbildung 3

„Welche Policy hat Ihre IT-Abteilung für die Nutzung/Installation eigener Software durch einen typischen Informationsarbeiter festgelegt?“



Basis: 887 Unternehmens- und IT-Entscheidungsträger, die an der Entscheidungsfindung für Laptops, Computer und andere Geräte beteiligt sind
Quelle: Eine von Forrester Consulting im Auftrag von Dell durchgeführte Studie, September 2019

Ihre Sicherheitsinfrastruktur muss sich mit den Zeiten weiterentwickeln

Die Idee eines Unternehmensperimeters ist heute sonderbar und veraltet. Mitarbeiter arbeiten an verschiedenen Standorten und benötigen von überall aus Zugriff auf Informationen. Der Verbrauchermarkt beeinflusst, wie Mitarbeiter in einer Unternehmensumgebung mit welchen Geräten arbeiten. Ein digitales Unternehmen hat keinen Perimeter. Heute kann sich Ihr Unternehmen auf die Cloud erstrecken, mobile Mitarbeiter unterstützen und physische Umgebungen mit Konnektivität über Sensoren und andere mit dem Internet verbundene Geräte digitalisieren. Es gibt eine zunehmende Permutation der Möglichkeiten, mit denen einerseits Mitarbeiter sensible Daten offenlegen können und andererseits Angreifer Ihre Umgebung und Ihre Daten gefährden können. In der heutigen Arbeits- und Bedrohungsumgebung müssen Sicherheitsstrategie und -architektur sich weiterentwickeln, um datenzentriert und in einem Zero-Trust-Ansatz für die Sicherheit verwurzelt zu sein.

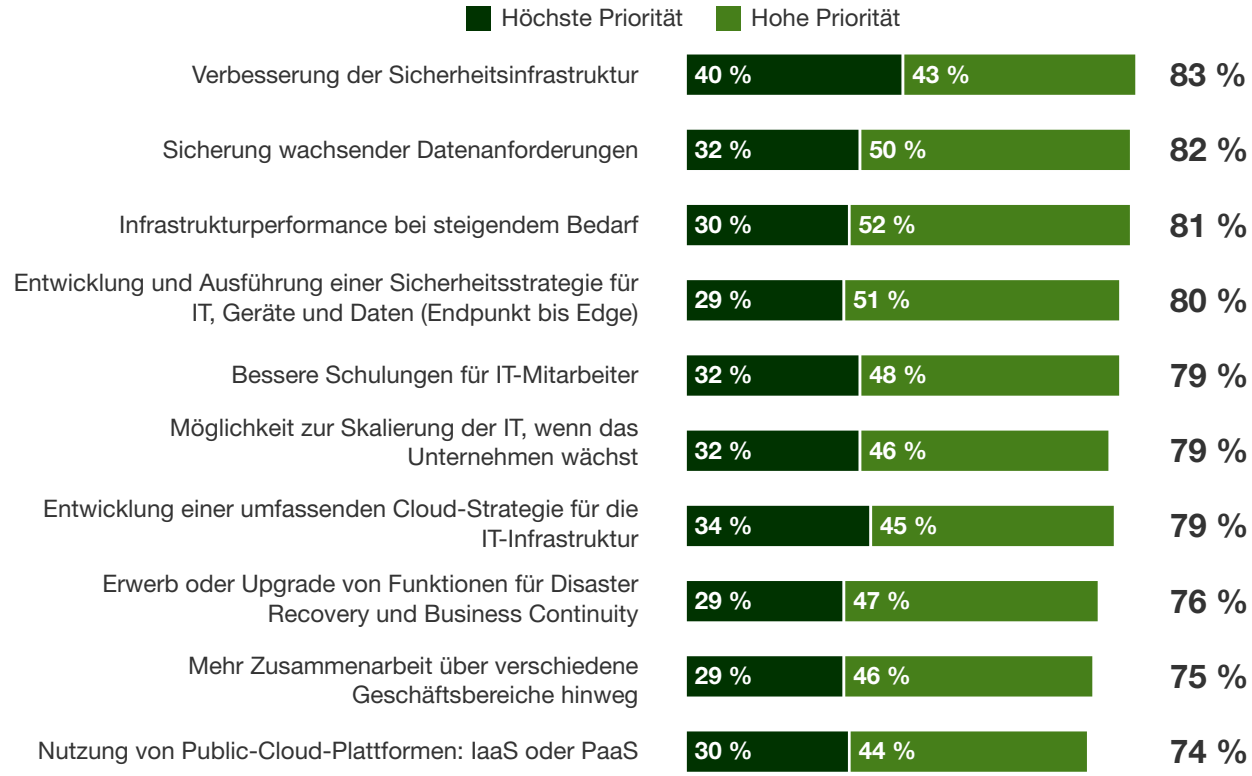
Zero Trust ist ein konzeptionelles und architektonisches Modell für die Art und Weise, in der Sicherheitsteams Netzwerke in sichere Mikroperimeter umgestalten, Verschleierung nutzen, um die Datensicherheit zu verstärken, Risiken begrenzen, die mit übermäßigen Nutzerrechten verbunden sind, sowie Analysen und Automatisierung, um die Sicherheitserkennung und -reaktion deutlich zu verbessern. Dieser Ansatz trägt zu einer drastischen Verbesserung der Datensicherheit bei. Viele Unternehmen nutzen heute bereits einen Zero-Trust-Ansatz. Die Umfrageteilnehmer identifizierten die folgenden Infrastrukturprioritäten, die auf die Bereitschaft für Zero Trust hindeuten (siehe Abbildung 4):

- **Schulung von Endnutzern zur Verbesserung der Praktiken für eine sichere Datenverarbeitung.** Um Zugang zu geistigem Eigentum zu erlangen, richten sich Angreifer an Mitarbeiter und Contractors. Am Arbeitsplatz nutzen Mitarbeiter vernetzte Geräte, die mit Cloud-Services in unternehmenseigenen Systemen/Netzwerken interagieren, aber anderswo – sei es unterwegs, zu Hause oder in öffentlichen Bereichen wie Flughäfen und Cafés – müssen Mitarbeiter immer noch auf vertrauliche Informationen und Daten von privaten Geräten zugreifen, die nicht so gut geschützt sind wie die unternehmenseigenen Systeme/Netzwerke. Die Notwendigkeit, dass Mitarbeiter verantwortungsvoll und mit sicheren Verfahren mit Daten umgehen müssen, wird nicht unbedingt verständlich und effektiv vermittelt.
- **Schulung der IT-Mitarbeiter zur Minimierung von Risiken.** Die kontinuierliche Weiterentwicklung der Kompetenzen von IT-Mitarbeitern ist wichtig, um sicherzustellen, dass die Personen, die für Technologie- und Sicherheitsinfrastrukturen verantwortlich sind, über aktuelle Best Practices informiert sind. Das Verständnis der sich ändernden Technologieoptionen und der sich ständig weiter entwickelnden Risiko- und Bedrohungslandschaft ist notwendig, um das IT-Team für Erfolg zu positionieren. Daher gaben 79 % der Befragten an, dass sie Schulungen der IT-Mitarbeiter verbessern werden. Das sind in zweierlei Hinsicht gute Nachrichten: 1) wird sichergestellt, dass die IT-Mitarbeiter mit ihren Kompetenzen und Ansätzen auf dem neuesten Stand sind und 2) werden Bemühungen der Mitarbeiterbindung in einer Zeit unterstützt, in der die Nachfrage nach Talenten hoch ist.

› **Überprüfen der Sicherheitsstrategie.** Unternehmen sind sich zunehmend bewusst, dass die Einhaltung von Complianceanforderungen nicht ausreicht, um eine robuste Sicherheit aufzubauen. Businesspartner von Drittanbietern werden als Voraussetzung für die Zusammenarbeit Nachweise verlangen, dass eine starke Sicherheits- und Risikomanagementpraxis vorliegt. Eine zukunftsorientierte Strategie unterstützt die Bemühungen eines Unternehmens, ein robustes Sicherheitsprogramm zu entwickeln und Bereiche zu antizipieren, in denen Kompetenzen zur Behebung von Problemen auf der Grundlage geschäftlicher Prioritäten verbessert oder neu eingebracht werden müssen. 80 % der Befragten gaben an, dass sie die Notwendigkeit der Entwicklung und Ausführung einer Sicherheitsstrategie für IT, Geräte und Daten priorisieren.

Abbildung 4

„Welche der folgenden Initiativen werden in Ihrem Unternehmen in den nächsten 12 Monaten wahrscheinlich die höchsten Prioritäten im Bereich IT-Infrastruktur haben?“



Basis: 887 Unternehmens- und IT-Entscheidungsträger, die an der Entscheidungsfindung für Laptops, Computer und andere Geräte beteiligt sind
Quelle: Eine von Forrester Consulting im Auftrag von Dell durchgeführte Studie, September 2019

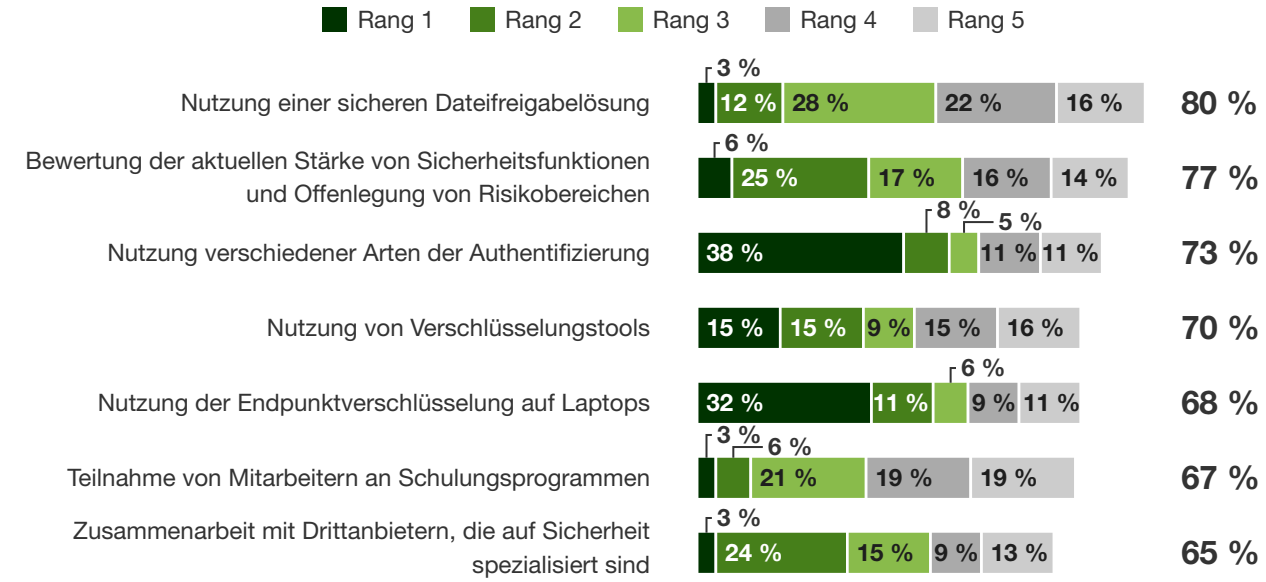
TAKTIKEN ZUR VERBESSERUNG DER SICHERHEIT

Im digitalen Zeitalter sind Cyberbedrohungen allgegenwärtig und Verstöße schaffen es fast täglich in Schlagzeilen, was Unternehmen ihren Ruf, ihr Kapital sowie zukünftiges Wachstum und weitere Expansion kostet. Anders gesagt: Die Sicherheit des Nettogewinns eines Unternehmens hängt von den Technologien ab, die die Daten sichern, d. h. die fundamentale Währung des digitalen Geschäfts. Datenschutzverletzungen sind eine bedauerliche Tatsache des Lebens. 50 % der globalen Entscheidungsträger im Bereich Netzwerksicherheit gaben an, dass ihr Unternehmen im vergangenen Jahr mindestens eine Sicherheitsverletzung erlitten hat, die sie bemerkt, und diese Zahl steigt bei Befragten aus großen Unternehmen auf 55 %. Vor diesem Hintergrund haben Unternehmen berichtet, welche Elemente der Sicherheit sie verbessern möchten (siehe Abbildung 5):

- **Sichere Dateifreigaben zur Unterstützung der Zusammenarbeit unter Mitarbeitern.** Technologie und Mitarbeiter spielen beide eine wichtige Rolle, wenn es darum geht, die Zusammenarbeit von Unternehmen zu unterstützen und so einen langfristigen wirtschaftlichen Wert zu schaffen. 80 % der Befragten gaben an, dass sie eine sichere Lösung für Dateifreigaben verwenden werden, um ihre Sicherheitsfunktionen zu verbessern. Dies sollte jedoch nicht nur innerhalb der vier Wände des Büros verwendet werden, da Homeoffice-Mitarbeiter und alle, die beruflich unterwegs sind, bei Bedarf ebenfalls auf Dateien zugreifen und diese gemeinsam nutzen können müssen.
- **Authentifizierung zur Unterstützung des sicheren Mitarbeiterzugriffs auf Daten.** In der einfachsten Form sorgen Authentifizierungslösungen dafür, Angreifer fernzuhalten und legitime Nutzer zuzulassen. Angesichts der zahlreichen Datenschutzverletzungen auf der ganzen Welt steht die Durchsetzung von Kontrollen ganz oben auf der Tagesordnung. 73 % der Befragten gaben an, dass sie verschiedene Authentifizierungsarten verwenden werden, und 38 % der Befragten stuften die Authentifizierung als vorrangige strategische Anstrengung ein, die sie zur Verbesserung der Sicherheit durchführen würden. Diese Prozesse sollten jedoch weder die Mitarbeiterproduktivität beeinträchtigen noch der Erledigung von Aufgaben im Weg stehen. Eine reibungslose Erfahrung bei der Authentifizierung von Nutzern macht einen großen Unterschied.
- **Verschlüsselung zur Kontrolle der Daten und Erfüllung der Complianceanforderungen.** 73 % der Befragten gaben an, dass sie Verschlüsselungstools einsetzen würden, während 68 % speziell auf die Endpunktverschlüsselung für Mitarbeiterlaptops (vollständige Festplattenverschlüsselung) hinwiesen, die sie als wichtigen Faktor zur Verbesserung der Sicherheit erachten. In einer Welt, in der Mitarbeiter ein Gerät nur allzu schnell verlieren oder regelmäßig Geräte gestohlen werden, ist dies eine umsichtige Entscheidung. Die Verschlüsselung von Daten im Ruhezustand ist ebenfalls in vielen Varianten möglich und Unternehmen können diese gemäß ihren Anforderungen auswählen, d. h. vollständige Festplatte, Dateiebene, Datenträger, E-Mails, Anwendungs-/Bereichsebene, transparente/Datenbankverschlüsselung.
- **Sicherheitsbewertung zum Verstehen der aktuellen Sicherheitsreife.** Während die meisten Sicherheitsteams eine Vielzahl von Kontrollen und Standards implementiert haben, um die Sicherheit ihres Unternehmens zu gewährleisten, sind viele nicht in der Lage, objektiv zu ermitteln, wo Sicherheitslücken bestehen. Sie können nur schwer bestimmen, ob sie alle wichtigen Probleme behoben haben oder ob ein Teil der Best Practices nicht befolgt wird. 77 % der Befragten sind sich dessen bewusst und möchten die Sicherheit verbessern, indem sie präzise Korrekturpläne entwickeln, um sicherzustellen, dass alle Komponenten den gewünschten Funktionsstatus erreichen.

Abbildung 5

„Was möchten Sie tun, um die Sicherheit zu verbessern?“



Basis: 887 Unternehmens- und IT-Entscheidungsträger, die an der Entscheidungsfindung für Laptops, Computer und andere Geräte beteiligt sind
Quelle: Eine von Forrester Consulting im Auftrag von Dell durchgeführte Studie, September 2019

Eine ausgewogene Sicherheit kommt Mitarbeitern und dem Unternehmen zugute

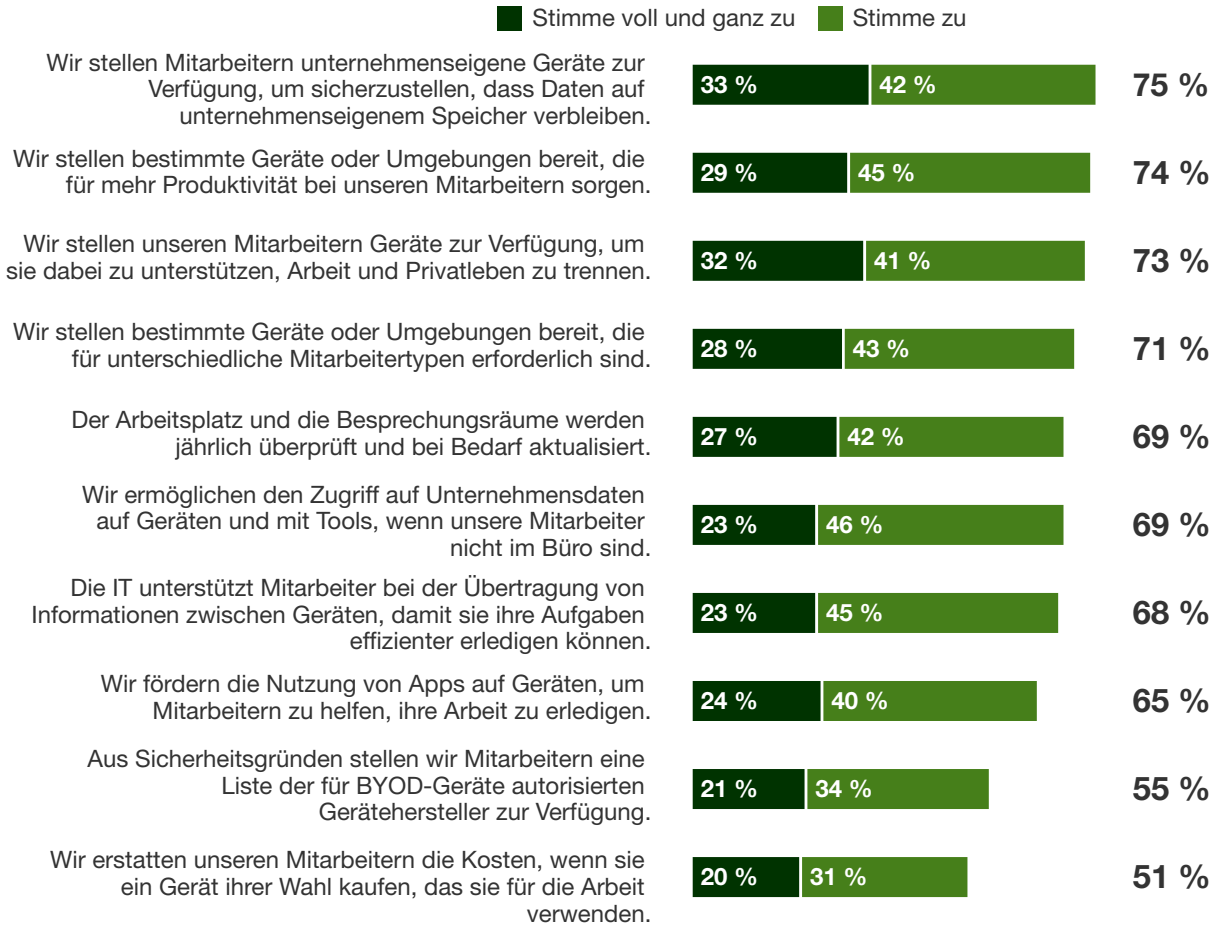
Sicherheitsmaßnahmen werden es einem Unternehmen ermöglichen, sicherer zu sein, anstatt den Fortschritt mit Herausforderungen zu verschleiern, eine höhere Umsatzgenerierung zu verfolgen. Um das Unternehmen von Hindernissen zu befreien, müssen Entscheidungsträger einen mitarbeiterzentrierten und risikoorientierten Ansatz verfolgen, wenn sie die Sicherheitserfahrung entwickeln. Wenn Sie ein ausgewogenes Verhältnis zwischen einer hervorragenden Mitarbeitererfahrung und hoher Sicherheit bieten, können Sie Folgendes erreichen (siehe Abbildung 6):

- **Remotearbeitsmöglichkeiten zur Unterstützung von Produktivität und Wettbewerbsvorteil.** Ganz gleich, ob Mitarbeiter eine bessere Unterstützung für ihre Work-Life-Balance fordern oder Ihr Unternehmen die beste Person für einen Job unabhängig von der Nähe zu einem Büro finden möchte – eine Unterstützung für Remotearbeitsplätze ist ein Wettbewerbsvorteil bei der Einstellung und Bindung von Talenten. Technologie hilft, Remotearbeitsplätze zu ermöglichen, und Sicherheit ist eine wichtige Grundlage dafür, wie Ihr Unternehmen Remotearbeit auf sichere Weise unterstützen kann. 69 % der Befragten gaben an, dass sie den Zugriff auf Unternehmensdaten auf Geräten ermöglichen, wenn Mitarbeiter außerhalb des Büros arbeiten.
- **Fördern der Zusammenarbeit zum Voranbringen von Innovationen.** Mitarbeiter möchten Erfahrungen teilen und letztendlich Dateien und Ideen mit Kollegen austauschen. Sowohl die Vernetzung zwischen Mitarbeitern als auch die Tools zur Vereinfachung dieser Vernetzung sind Voraussetzungen, um eine Umgebung – oder Kultur – der Innovation zu unterstützen, insbesondere bei einer verteilten Belegschaft, in der Mitarbeiter nicht immer persönlich in einem Büro mit ihren Fachkollegen in Kontakt stehen. Für den Moment sagen 49 % der Befragten, dass sie Schwierigkeiten haben, Mitarbeitern eine einfache und sichere gemeinsame Nutzung von Daten zu ermöglichen. Es gibt noch Spielraum für Verbesserungen, um Vorteile zu erzielen.

› **Verbessern der Kundenerfahrung und Reduzierung der Mitarbeiterfluktuation.** Die Verbesserung der Zufriedenheit von Mitarbeitern durch bessere Mitarbeitererfahrungen führt zu zufriedenen Kunden, die einen besseren Support und bessere Interaktionen mit ihren Mitarbeitern genießen. Zufriedene Mitarbeiter treffen mit größerer Wahrscheinlichkeit die richtigen Entscheidungen, die Ihren Kunden gerecht werden.[1] Eine Studie hat ergeben, dass Unternehmen mit zufriedenen Mitarbeitern eine 81 % höhere Kundenzufriedenheit und eine halb so hohe Mitarbeiterfluktuation verzeichnen konnten.[2]

Abbildung 6

„Welche Maßnahmen hat Ihr Unternehmen ergriffen, um Remote- oder flexible Arbeit zu ermöglichen?“



Basis: 887 Unternehmens- und IT-Entscheidungsträger, die an der Entscheidungsfindung für Laptops, Computer und andere Geräte beteiligt sind
Quelle: Eine von Forrester Consulting im Auftrag von Dell durchgeführte Studie, September 2019

Wichtige Empfehlungen

Investitionen in Ihre Sicherheitsinfrastruktur und -kontrollen sind eine wichtige Komponente Ihres Sicherheitsprogramms. Allerdings sind Technologieinvestitionen allein unzureichend. Bestimmen Sie das richtige Maß einer ausgewogenen Sicherheit für Ihr Unternehmen, basierend auf Ihren spezifischen Anforderungen und Ihrer Risikotoleranz.

Befolgen Sie heute noch vier Schritte, um Ihr Unternehmen für Erfolg bei der Erzielung eines angemessenen Gleichgewichts zwischen Sicherheit und Mitarbeitererfahrung zu positionieren:

Bewerten Sie Ihren aktuellen Status der Sicherheitsreife. Der Prozess, bei dem die Bewertung selbst durchgeführt wird, kann auch Sichtbarkeit in Verfahren oder Prozesse bieten, die unternehmensbezogenes Wissen sind. Da einige dieser Verfahren/Prozesse undokumentiert sind, wird es im weiteren Verlauf wichtig sein, die Details zutage zu bringen, falls wichtige Teammitglieder in den Ruhestand gehen oder das Unternehmen verlassen. Eine Bewertung bietet einen Überblick über die vorhandenen Sicherheitskontrollen, -prozesse und -kontrollmaßnahmen Ihres Unternehmens, sodass Sie Bereiche ermitteln können, in denen potenzielle Lücken vorhanden sind, die geschlossen werden müssen. Diese Bewertung ist hilfreich, um Anleitungen für Ihren weiteren Weg zu erhalten und zu erfahren, worauf Sie sich warum konzentrieren müssen.

Identifizieren Sie, was sensible Daten sind, warum und wo sich diese befinden. Dazu gehört das Verständnis dafür, welche Daten durch Complianceanforderungen reguliert sind und welchen Wert die Daten für Ihr Unternehmen insgesamt bieten. Mit Sicherheitskontrollen und entsprechenden Überlegungen zur Datenverarbeitung sorgt ein Verständnis Ihrer Daten auch für eine Grundlage zur Unterstützung des Datenschutzes und der ethischen Nutzung personenbezogener Daten. Durch eine klarere Sicht und ein besseres Verständnis Ihrer Daten können Sie besser bestimmen, was erforderlich ist, um sie zu schützen und angemessen zu nutzen.

Ermitteln Sie die Risikotoleranz Ihres Unternehmens. Bestimmungen mögen zwar bestimmte Aktionen und Aktivitäten vorgeben, aber die Arten und das Maß an Kontrollen, die Ihr Unternehmen implementiert, hängen von Ihrem Maß an Risikotoleranz ab. Verstehen Sie die Risiken für Ihre Daten und Ihres Unternehmens und treffen Sie risikobasierte Entscheidungen für Sicherheitskontrollen, um die Anforderungen und die Produktivität Ihrer Mitarbeiter auszugleichen.

Bewerten Sie, wie Mitarbeiter arbeiten und ihre Arbeit erledigen. Ordnen Sie zu, an welchen Stellen Sicherheitskontrollen die Arbeitserfahrung der Mitarbeiter beeinträchtigen und welche Auswirkungen dies auf ihren Arbeitstag und ihre Produktivität hat. Unterschiedliche Profile der Mitarbeiter – von den Rollen, in denen sie sich befinden, bis hin zu den Daten, auf die sie zugreifen können, um ihre Aufgaben zu erledigen – wirken sich ebenfalls auf ihre Technologieanforderungen, die Risiken, denen sie möglicherweise ausgesetzt sind, und die Arten von Sicherheitskontrollen aus, die Sie implementieren müssen, um diese Risiken zu minimieren. Implementieren Sie nur die erforderlichen Sicherheitskontrollen, statt solche, die zu unnötigen Reibungen führen.

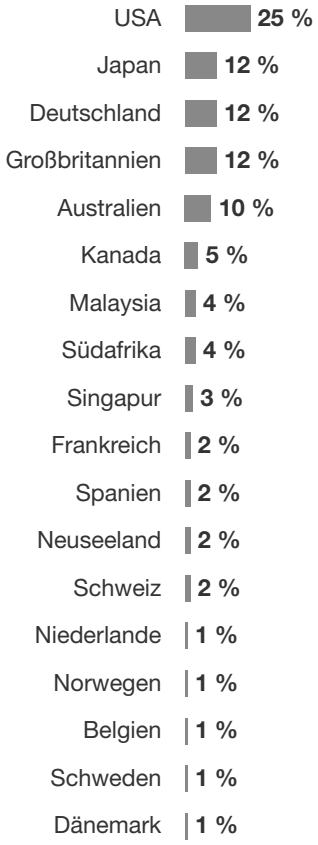
FORRESTER®

Anhang A: Methodik

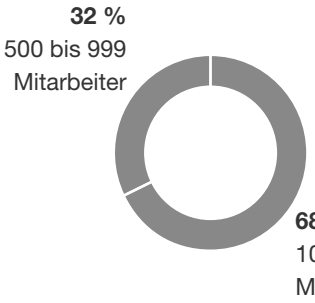
In dieser Studie hat Forrester eine Onlineumfrage unter 887 Unternehmens- und IT-Führungskräften in verschiedenen Branchen auf dem Markt durchgeführt. Die Fragen, die den Teilnehmern gestellt wurden, drehten sich darum, wie sich ihre Ausgaben für Sicherheit geändert haben, welche Faktoren ihre Sicherheitsstrategie beeinflussen, welche Herausforderungen rund um Compliance und die Einhaltung von Bestimmungen bestehen und wie die Zukunft der Sicherheit für ihr Unternehmen aussehen wird. Die Studie begann im März 2019 und das Thought Leadership Paper wurde im August 2019 abgeschlossen.

Anhang B: Demografie

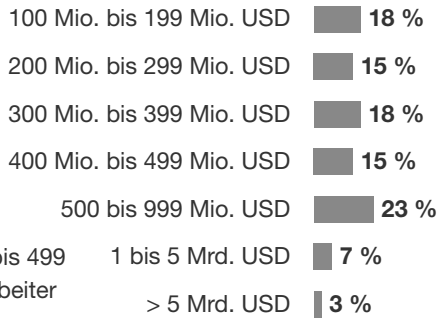
„In welchem Land befinden Sie sich?“



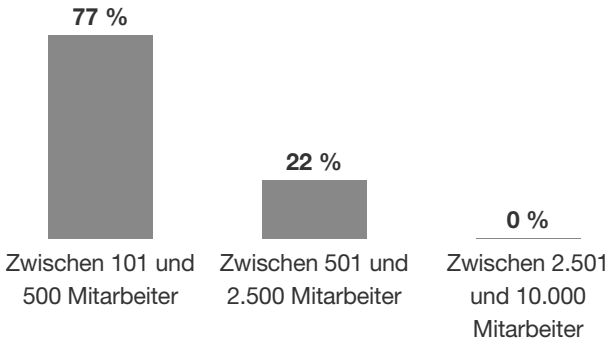
„Wie viele Mitarbeiter arbeiten Ihrer Schätzung nach weltweit für Ihr Unternehmen/Ihre Organisation?“



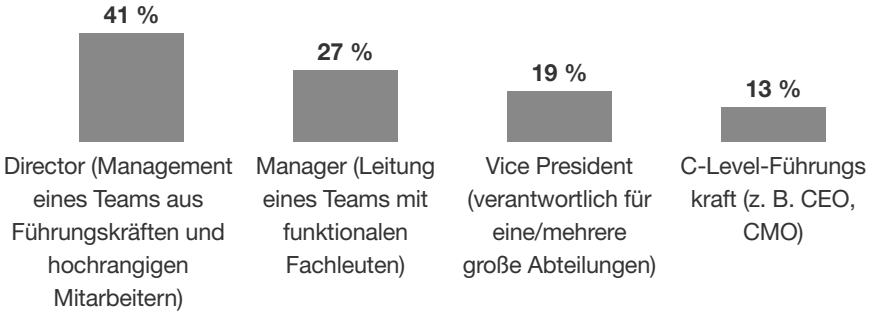
„Wie hoch ist Ihrer Schätzung nach der Jahresumsatz Ihres Unternehmens (in USD)?“ (N = 861)



„Wie viele Mitarbeiter oder Mitglieder der Belegschaft Ihres Unternehmens sind direkt von den Kaufentscheidungen für Technologie und Services betroffen, die Sie am meisten beeinflussen?“



„Welcher Titel beschreibt Ihre Position in Ihrem Unternehmen am besten?“



Basis: 887 Unternehmens- und IT-Entscheidungsträger, die an der Entscheidungsfindung für Laptops, Computer und andere Geräte beteiligt sind
Quelle: Eine von Forrester Consulting im Auftrag von Dell durchgeführte Studie, März 2019

FORRESTER®

Anhang C

FUSSNOTEN

[1] Quelle: „Transform The Employee Experience To Drive Business Performance“, Forrester Research, Inc., 12. Februar 2018.

[2] Quelle: James K. Harter, Frank L. Schmidt und Theodore L. Hayes, „Business-Unit-Level Relationship Between Employee Satisfaction, Employee Engagement, and Business Outcomes: A Meta-Analysis“, Journal of Applied Psychology, April 2002 (http://www.factorhappiness.at/downloads/quellen/s17_harter.pdf).