DER SECURITY-IMPERATIV: DAS UNTERNEHMENSWACHSTUM IN DER APPLICATION ECONOMY SICHERN >>

Im Auftrag von ca technologies

COLEMAN PARKES RESEARCH

Inhalt

HINWEIS ZUR NUTZUNG DIESES INTERAKTIVEN PDFS

Die Interaktivität auf Tablets und Smartphones ist je nach PDF-Reader unterschiedlich. Manche interaktiven Funktionen sind bei der Anzeige des PDF-Dokuments als E-Mail-Vorschau möglicherweise nicht verfügbar. Wir empfehlen Adobe Acrobat Reader.

START (erste Seite)	INHALT	ZURÜCK eine Seite	VOR eine Seite

Kurzfassung

Die Application Economy hat das Gesicht der IT Security verändert. Die Trennlinie zwischen Innen und Außen des Unternehmens hat sich so gut wie aufgelöst. Der Netzwerkperimeter ist heute nicht bloß verschoben, sondern zersplittert. Die neue Grenze der Security liegt an allen Stellen, an denen auf das Netzwerk zugegriffen wird.

Aber das ist nicht das einzige Problem. Kunden, Mitarbeiter und Partner erwarten mittlerweile, jederzeit nahtlos zugreifen zu können – über jedes Gerät und jede Plattform.

Die traditionellen IT-Security-Strategien haben in dieser komplexen Konstellation ausgedient. Unternehmen müssen hochgradig verteilte Identitäten aus unterschiedlichen Quellen authentifizieren und zugleich eine einwandfreie User Experience gewährleisten können. Das Gleichgewicht zwischen robustem Schutz und Anwenderzufriedenheit ist schwer zu halten, sodass ein neuer, identitätsbasierter Security-Ansatz nötig geworden ist. Dieser Ansatz muss Kontext, Verhaltensanalysen und weitere prognostische Konzepte nutzen, um für eine überzeugende Customer Experience zu sorgen und zugleich Identitäten und Daten zu schützen.

Schließlich können Sie mit identitätsbasierter Security außerdem die vertrauenswürdigen digitalen Beziehungen mit Ihren Kunden aufbauen, die in der Application Economy der größte Trumpf Ihres Unternehmens sind.

Vor diesem Hintergrund gab CA Technologies bei Coleman Parkes Research eine Umfrage unter 1.770 leitenden Business- und IT-Führungskräften in Auftrag, darunter mehr als 100 CSOs und CISOs. Sie wurden zu ihren IT Security Practices und der Einführung zentraler Elemente einer identitätsbasierten Security befragt.

So ließ sich ermitteln, was fortgeschrittene Anwender identitätsbasierter Security anders machen und wie sich dies auf ihre Unternehmen auswirkt.

Die Ergebnisse legen eindeutig einen Business Case für ein neues Modell der digitalen Security nahe, das den Erfordernissen der Application Economy gerecht wird und echte Verbesserungen bedeutet, die sich im Unternehmensergebnis niederschlagen.

Mit identitätsbasierter Security können Sie die vertrauenswürdigen digitalen Beziehungen mit Ihren Kunden aufbauen, die in der Application Economy der größte Trumpf Ihres Unternehmens sind.

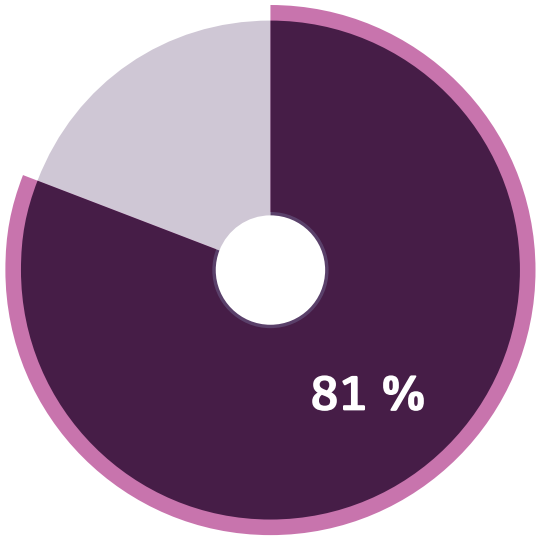
Unsere Analyse ergab Folgendes:

- **81 %** der Unternehmen gaben an, dass Security reibungslos funktionieren muss, damit Anwender nicht mit umständlichen Security-Anforderungen belästigt werden.
- **82 %** gaben an, dass identitätsbasierte Security für ihr Unternehmen entscheidend ist. Es können jedoch **nur 25 %** als fortgeschrittene Anwender identitätsbasierter Security-Ansätze eingeordnet werden.
- Doppelt so viele fortgeschrittene Anwender identitätsbasierter Security (**41 %**) wie Basisanwender (**21 %**) konnten einen Rückgang bei den Datenschutzverletzungen beobachten.
- **91 %** der fortgeschrittenen Anwender identitätsbasierter Security konnten Verbesserungen bei der digitalen Reichweite verzeichnen, **87 %** bei der Customer Experience und **87 %** bei der Kundenbindung.
- Fortgeschrittene Anwender identitätsbasierter Security konnten zudem quantifizierbare Unternehmensergebnisse beobachten:
  - **47 %**ige Verbesserung des Unternehmenswachstums
  - **50 %**ige Verbesserung der Mitarbeiterproduktivität
  - **45 %**ige Verbesserung der Kundenzufriedenheit

„Security ist der wichtigste Faktor unserer digitalen Entwicklung.“

Technologieleiter, US-Behörde

81 % der Unternehmen gaben an, dass Security reibungslos funktionieren muss, damit Anwender nicht mit umständlichen Security-Anforderungen belästigt werden.



Einführung: Die neue Grenze

Die digitale Revolution hat die Zielmarken der IT Security versetzt – und tut dies auch weiterhin. Sie hat eine Welt aus unterschiedlichsten Kanälen, Plattformen und Geräten erschaffen. Kunden, Partner und Mitarbeiter sind in dieser Welt ständig verfügbar – und erwarten dasselbe von Ihnen.

Kunden setzen in der Application Economy heute zügige Downloads, schnellen Zugriff, eine nahtlose Experience und zuverlässigen Schutz voraus. Sie wandern ab, wenn Ihre Security für sie zur Bremse wird oder Sie ihre Daten nicht schützen können.

Der alte Netzwerkperimeter hat sich aufgelöst. Anwender greifen uhrzeit-, tages- und standortunabhängig über beliebige Geräte und Plattformen auf Ihr Netzwerk zu. Die Anwenderidentität – und nicht die Firewall – markiert heute die Grenze für den Datenschutz.

Erfolgreich zu sein, setzt eine Vertrauensbeziehung zwischen Anwendern und Unternehmen in beide Richtungen voraus.

In diesem Klima muss die Security stärker identitätsbasiert verstanden und die Anwenderidentität in den Mittelpunkt gestellt werden. Identitätsbasierte Security nutzt Kontext, Verhaltensanalysen und weitere prognostische Security-Konzepte, die sicherstellen, dass Anwender tatsächlich die Personen sind, die sie zu sein behaupten. So können sie überall und jederzeit über das gewünschte Gerät sicher auf die Daten Ihres Unternehmens zugreifen.

„Die Security ist ein Haupthindernis bei der Erfüllung des Kundenanspruchs nach hohem Tempo.“

IT-Leiter, US-Gemeindeverband

Anwender greifen uhrzeit-, tages- und standortunabhängig über beliebige Geräte und Plattformen auf Ihr Netzwerk zu.

Identitätsbasierte Security ist jedoch mehr als nur eine wirksame Möglichkeit, Daten zu schützen. Richtig umgesetzt, ist sie außerdem ein nützlicher Business Enabler. Sie versetzt Sie in die Lage, neue Services schneller bereitzustellen. Sie kann Kundenbindung und Kundentreue festigen – beide basieren auf Vertrauen. Denn in der digitalen Welt ist die Security der zentrale Vertrauensfaktor.

„Die identitätsbasierte Security wird sich als zentraler Security-Ansatz für Telekommunikationsunternehmen etablieren.“

Marketingleiter, europäischer Telekommunikationsanbieter

Im Rahmen unserer Recherchen zur Unternehmenstransformation im digitalen Zeitalter haben wir Initiativen zur Einführung eines stärker identitätsbasierten Security-Konzepts untersucht. Wir haben Senior-Business-, -IT- und Security-Führungskräfte zu folgenden Aspekten befragt:

- ihre Wahrnehmung der Security als Katalysator für Unternehmenschancen
- wesentliche Leistungsindikatoren zur Bewertung des Einflusses der IT Security und beobachtete Ergebnisse
- Einführung identitätsbasierter Security als Voraussetzung für die Application Economy
- Grad des Einflusses der fortgeschrittenen Nutzung identitätsbasierter Security auf die Unternehmensperformance

In diesem Bericht stellen wir die Ergebnisse vor. Wir beleuchten, wie Unternehmen ihre IT Security weiterentwickeln können, um in der Application Economy Performance, Wettbewerbsfähigkeit und Wachstum zu verbessern.

Identitätsbasierte Security ist mehr als nur eine wirksame Möglichkeit, Daten zu schützen. Richtig umgesetzt, ist sie außerdem ein nützlicher Business Enabler.

01 Die Security-Lage in der Application Economy

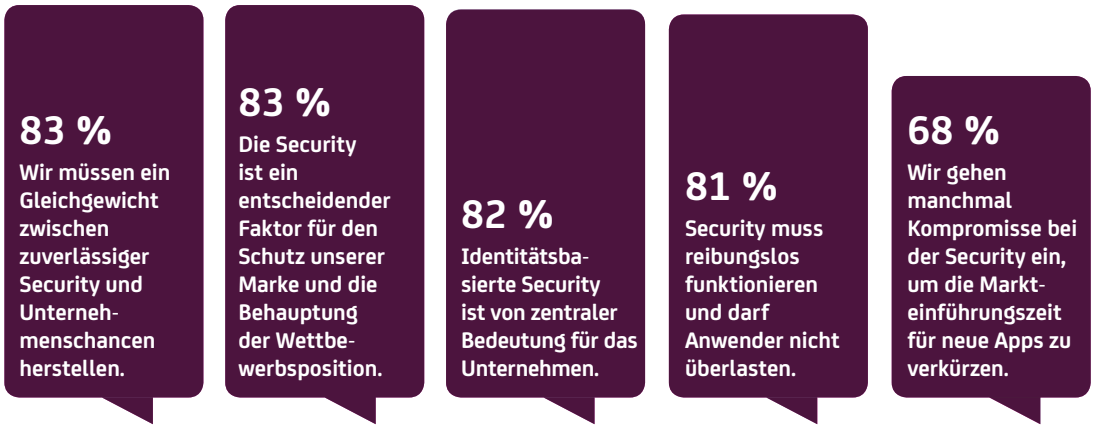
Unsere Recherchen weisen darauf hin, dass Unternehmen um die Funktion wissen, die die Security in der Geschäftsumgebung der Gegenwart spielen kann. Nach wie vor werden die traditionellen Security-Ziele verfolgt, darunter der Schutz vor Verstößen und die Einhaltung von Vorschriften. Zugleich sahen die Befragten die Security jedoch als Chance zum Ausbau der Unternehmenstätigkeit und zur Verbesserung der Wettbewerbsposition in der Application Economy.

Mehr als vier Fünftel der Befragten gaben an, dass Unternehmen mit der Security in der Lage sind, neue Chancen zu eröffnen, den Wettbewerbsvorteil auszubauen und Mitarbeitern und Kunden den mittlerweile vorausgesetzten schnellen, unkomplizierten und uhrzeit- und tagesunabhängigen Zugriff zu gewähren (siehe Abb. 1).

Dies schlägt sich in den wesentlichen Leistungsindikatoren nieder, anhand derer der Einfluss der IT Security bewertet wurde. Externe Messdaten zur Unternehmensperformance wie digitale Reichweite, Customer Experience und Kundenzufriedenheit werden mit ebenso hoher – oder sogar höherer – Wahrscheinlichkeit genutzt wie traditionelle Security-Kennzahlen wie Verstöße und nicht bestandene Compliance Audits (siehe Abb. 2).

Mehr als vier Fünftel der Befragten gaben an, dass Unternehmen mit der Security in der Lage sind, neue Chancen zu eröffnen, den Wettbewerbsvorteil auszubauen und Mitarbeitern und Kunden den mittlerweile vorausgesetzten schnellen, unkomplizierten und uhrzeit- und tagesunabhängigen Zugriff zu gewähren.

ABB. 1 DIE APPLICATION ECONOMY MACHT EINE NEUE ROLLE DER SECURITY ALS BUSINESS ENABLER ERFORDERLICH.



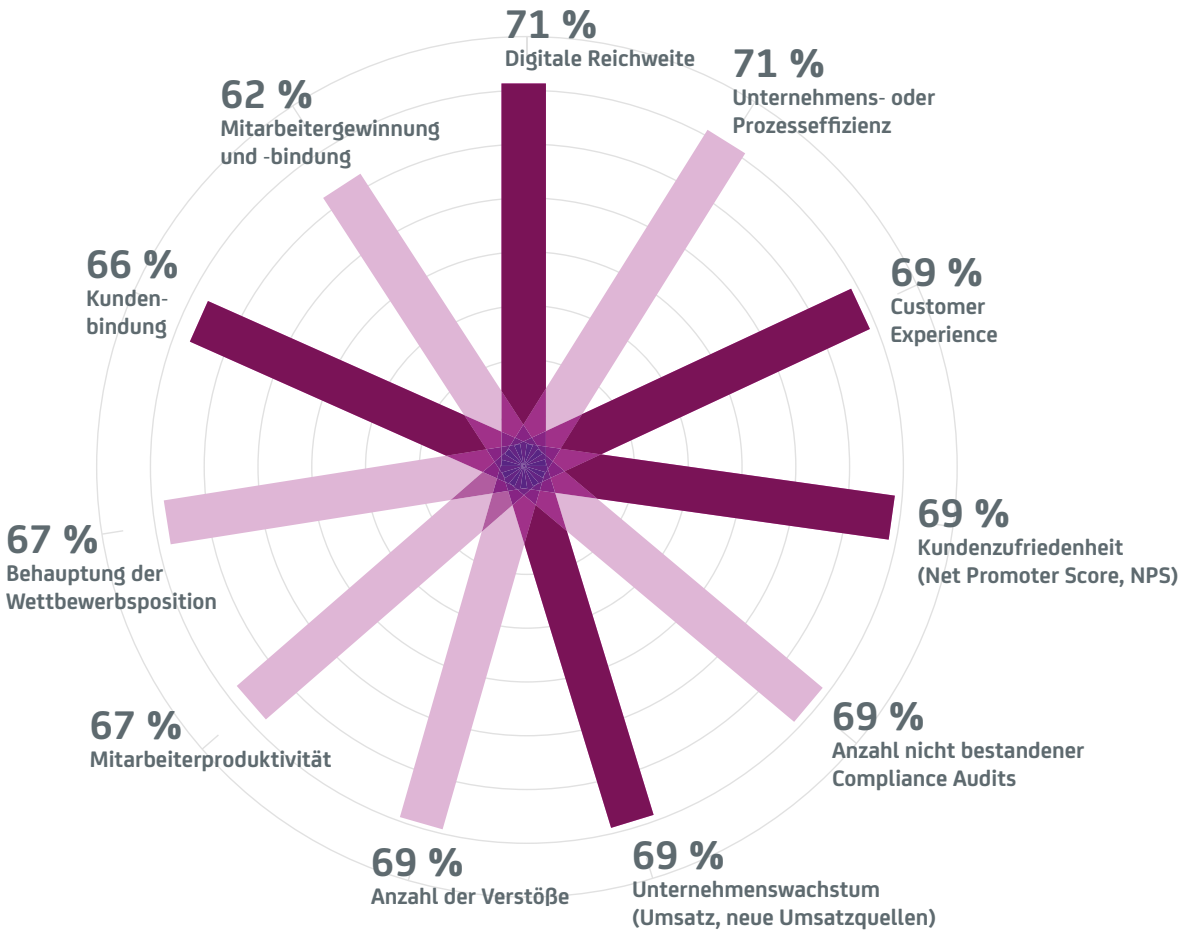
„Es gibt ein Tauziehen zwischen zuverlässiger Security und Kunden- und Mitarbeiterschnittstellen.“

IT-Leiter, US-Gemeindeverband

Die IT Security gilt in Unternehmen ganz klar als entscheidender Business Enabler und als Möglichkeit, Daten zu schützen. Viele Unternehmen nehmen unter dem Druck der Application Economy jedoch Abkürzungen. Bedenkliche 68 % gaben zu, Abstriche bei der Security zu machen, um Apps schneller auf den Markt zu bringen.

Der Security in der Application Economy nicht oberste Priorität einzuräumen, stellt ein enormes Risiko dar. Identitäten und Zugriff für Tausende von Apps, Services und Geräten zu verwalten, erfordert einen wesentlich stärker entwickelten Ansatz für den Schutz von Identitäten und Daten als bisher.

ABB. 2 EXTERNE UNTERNEHMENSMESSDATEN ZÄHLEN ZU DEN WICHTIGSTEN LEISTUNGSINDIKATOREN ZUR MESSUNG DES EINFLUSSES DER IT SECURITY.



02 Ein neuer Security-Ansatz

Das Problem in der Application Economy besteht darin, hochgradig verteilte Identitäten aus einem breiten Spektrum an Quellen wie Anwendungen, Systeme, Cloud und Social-Media-Plattformen zu überprüfen.

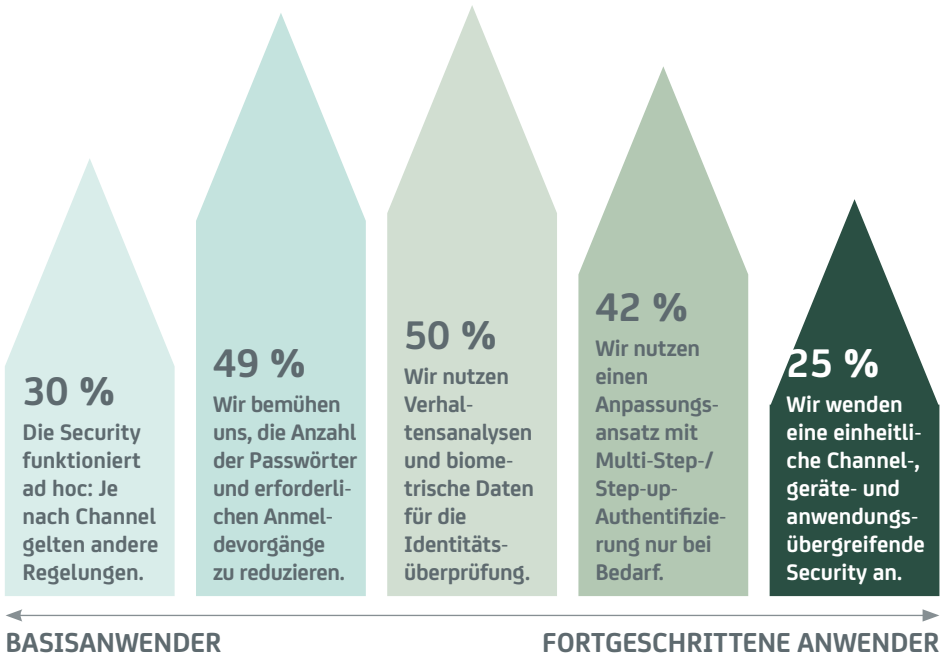
Dieser Vorgang muss für Anwender unbemerkt ablaufen. Kunden verlangen ausfallsichere Security und zugleich eine reibungslose Experience. Umständliche, uneinheitliche Registrierungs- und Authentifizierungsprozesse vertreiben Kunden schnell und behindern den Aufbau vertrauenswürdiger digitaler Beziehungen.

Mit identitätsbasierter Security sorgen Sie dafür, dass Ihre Security Practices sich nicht negativ auf die generelle User Experience auswirken. Zudem müssen Sie anpassungsfähigere IAM-Kontrollen (Identity and Access Management) einführen und Datenschutzverletzungen stärker proaktiv und prognostisch ausgerichtet aufdecken und verhindern.

Wir haben ein Reifemodell zur Bewertung der Einführung und aktuellen Nutzung dreier zentraler Elemente der identitätsbasierten Security aufgestellt:

1. **Customer Experience** (siehe Abb. 3). Einheitliche Channel-übergreifende Security-Ansätze mit Verhaltensanalysen und Anpassungsmöglichkeiten machen die Security weniger aufdringlich. Nur ein Viertel der Unternehmen nutzt einheitliche Channel-, geräte- und anwendungsübergreifende Security, um eine überzeugende User Experience zu gewährleisten. Eine Minderheit (42 %) wendet einen Anpassungsansatz an, die Hälfte nutzt Verhaltensanalysen.

ABB. 3 EINHEITLICHE, CHANNEL-ÜBERGREIFENDE SECURITY-ANSÄTZE VERBESSERN DIE CUSTOMER EXPERIENCE, WERDEN ABER NUR SELTEN ANGEWENDET.



„Die Security muss anwenderfreundlicher werden, ohne Abstriche bei der Zuverlässigkeit zu machen. Der Schlüssel liegt darin zu ermitteln, ob ein Anwender ein Kunde, ein Mitarbeiter oder ein Hacker ist, Kunden- und Mitarbeiterdaten zu schützen und sicherzustellen, dass Transaktionen nicht beeinträchtigt werden.“

VP Technology & Compliance, US-Bankinstitut

2. **Identity and Access Management** (siehe Abb. 4). Identitätsbasierte Security setzt zudem einen anpassungsfähigeren Ansatz für IAM-Kontrollen voraus. Nahezu 70 % nutzen zentrale, automatisierte IAM-Kontrollen, aber nur eines von zehn Unternehmen kann sie risikoabhängig anpassen.

„Das Identity and Access Management wird in Zukunft der Dreh- und Angelpunkt der Security sein.“

Marketingleiter, europäischer Telekommunikationsanbieter

3. **Erkennung von Verstößen** (siehe Abb. 5). Proaktive, prognostische Prozesse können die Fähigkeit von Unternehmen, Datenschutzverletzungen zu erkennen und zu verhindern, erheblich verbessern. Nur 37 % nutzen jedoch Analysen, um Datenschutzverletzungen proaktiv zu erkennen und zu verhindern, und weniger als die Hälfte davon (16 %) kann das Risiko von Sicherheitsverstößen vor ihrem Eintreten prognostizieren.

Nach der Befragung der Teilnehmer zu diesen drei Elementen identitätsbasierter Security wurden die Antworten mit Punkten bewertet. Wir stuften die Unternehmen anhand der Ergebnisse als fortgeschrittene Anwender, Basisanwender und Teilanwender identitätsbasierter Security ein.

Nur 25 % der Unternehmen stellten sich als fortgeschrittene Anwender heraus. Der mit Abstand größte Anteil (64 %) entfällt auf die Basisanwender, während nur gut ein Zehntel (11 %) identitätsbasierte Funktionen teilweise oder gar nicht nutzt.

ABB. 4 ANPASSUNGSFÄHIGE KONTROLLEN BEIM IDENTITY AND ACCESS MANAGEMENT VERBESSERN DIE IDENTITÄTSBASIERTE SECURITY, WERDEN JEDOCH BISHER WENIG GENUTZT.

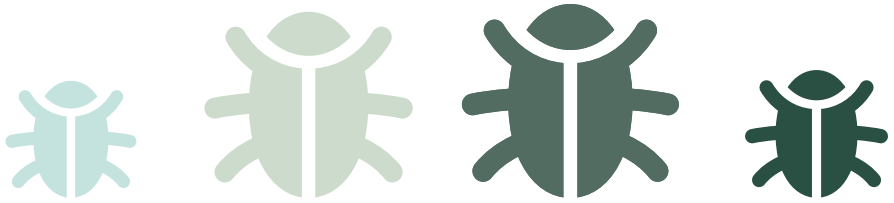
20 %
Überwiegend manuelle Kontrollen

69 %
Überwiegend zentrale und automatische Kontrollen

11 %
Anpassungsfähige Kontrollen in Abhängigkeit der Risiken

BASISANWENDER — **FORTGESCHRITTENE ANWENDER**

ABB. 5 MIT PROAKTIVEN UND PROGNOSTISCHEN ANALYSEN LASSEN SICH DATENSCHUTZVERLETZUNGEN ERKENNEN UND VERHINDERN, ABER SIE WERDEN SELTEN GENUTZT.



13 %
Nur gelegentliche Überprüfung von Aktivitätsberichten

34 %
Einige Analysen mit intelligenten Berichten und Warnungen

37 %
Proaktiv: gründliche Analysen mit Echtzeitreaktion auf Ereignisse und Vorfälle

16 %
Prognostisch: Antizipation von Risiken vor dem Eintreten von Verstößen

BASISANWENDER — **FORTGESCHRITTENE ANWENDER**

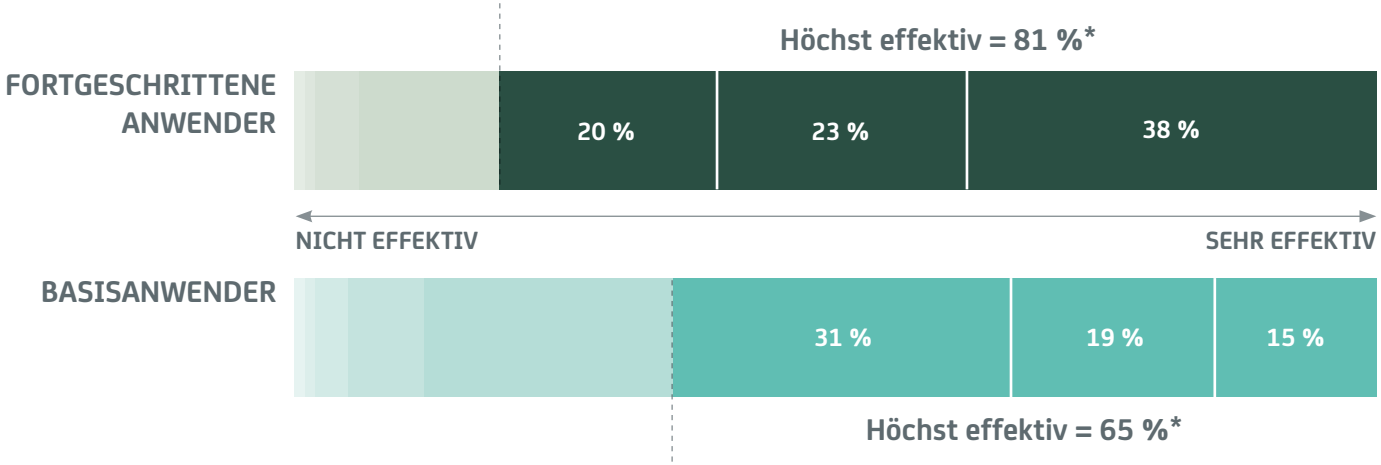
03 Der erhebliche Einfluss identitätsbasierter Security auf Unternehmen

Im nächsten Analyseschritt wurde die Korrelation zwischen der fortgeschrittenen Anwendung identitätsbasierter Security und Unternehmensergebnissen untersucht. Dazu verglichen wir die Unternehmensperformance von fortgeschrittenen Anwendern und Basisanwendern.

Die Analyse ergab, dass fortgeschrittene Anwender identitätsbasierter Security mit sehr viel höherer Wahrscheinlichkeit der Ansicht sind, dass die Security ihre Wettbewerbsposition verbessert. 81 % gaben an, dass dies ein Ergebnis der Security-Strategie ist, gegenüber 65 % der Basisanwender (siehe Abb. 6).

Fortgeschrittene Anwender ordneten zudem allen Security-Zielen, nach denen gefragt wurde, eine wesentlich höhere Priorität zu (siehe Seite 8). Insbesondere ist die Wahrscheinlichkeit, dass sie die Security für neue Unternehmensinitiativen und den Beziehungsaufbau nutzen, sehr viel höher als bei den Basisanwendern (55 % bzw. 34 %).

ABB. 6 MIT FORTGESCHRITTENER IDENTITÄTSBASIERTER SECURITY LÄSST SICH DIE WETTBEWERBSPOSITION BESSER BEHAUPTEN.

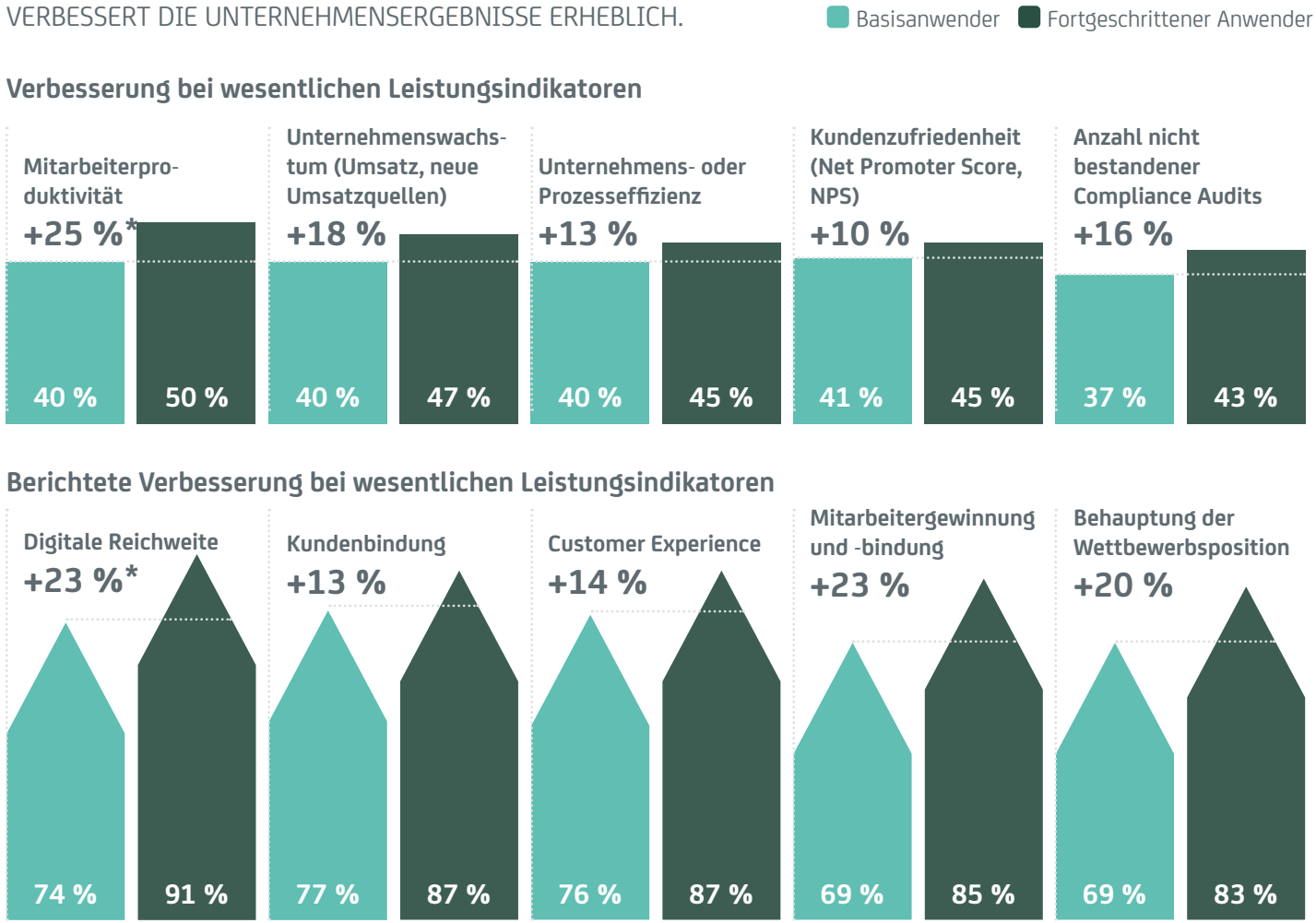


* Die besten 3 Prozentwerte von 10, wobei 10 sehr effektiv und 1 nicht effektiv ist

Beim Einfluss der IT Security auf die wesentlichen Leistungsindikatoren, die zu ihrer Bewertung herangezogen wurden, sieht es ähnlich aus. Fortgeschrittene Anwender identitätsbasierter Security verwiesen auf deutlichere Verbesserungen bei allen Unternehmens- und Security-Kennzahlen, nach denen wir fragten.

Die Differenz zwischen fortgeschrittenen Anwendern und Basisanwendern lag zwischen 10 % und 25 % (siehe Abb. 7). Beispielsweise gaben 87 % der fortgeschrittenen Anwender erhebliche Verbesserungen der Customer Experience an, gegenüber 76 % der Basisanwender. Ein noch größerer Einfluss ist bei der Mitarbeitergewinnung und -bindung zu verzeichnen: 85 % der fortgeschrittenen Anwender gaben eine Verbesserung an, gegenüber 69 % der Basisanwender.

ABB. 7 DER SCHRITT VON GRUNDLEGENDER ZU FORTGESCHRITTENER IDENTITÄTSBASIERTER SECURITY VERBESSERT DIE UNTERNEHMENSERGEBNISSE ERHEBLICH.



* Verbesserung wesentlicher Leistungsindikatoren bei Entwicklung von Basisanwender zu fortgeschrittenem Anwender in Prozent

Beim Datenschutz gab zwar rund ein Drittel nach wie vor einen Zuwachs bei den Security-Verstößen an, aber es ist bezeichnend, dass eine gesunkene Anzahl erkannter Datenschutzverletzungen bei den fortgeschrittenen Anwendern fast doppelt so wahrscheinlich wie bei den Basisanwendern ist. Zwei Fünftel (41 %) der fortgeschrittenen Anwender erzielten dieses Ergebnis trotz der zunehmend schwierigen Security-Lage im vergangenen Jahr. Dem steht weniger als ein Viertel (21 %) der Basisanwender gegenüber (siehe Abb. 8).

Die Business Impact Scorecard der digitalen Transformation

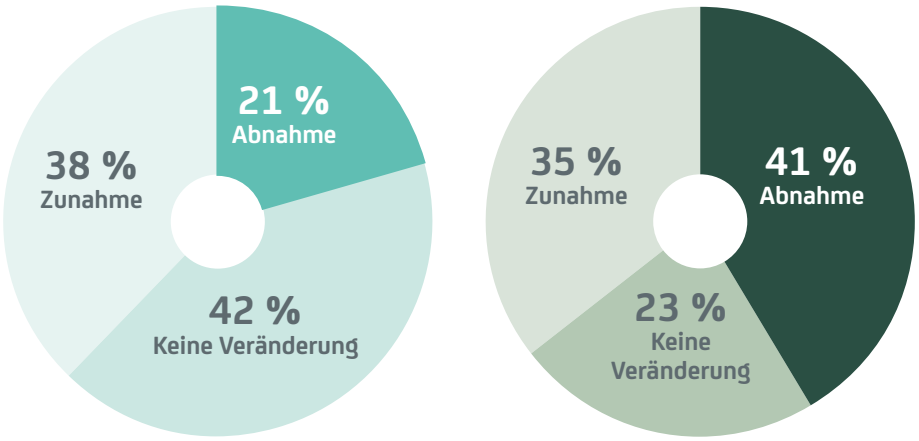
Wir bewerteten außerdem den Einfluss identitätsbasierter Security auf die Initiativen der Teilnehmer zur digitalen Transformation.

Dazu verwendeten wir die Business Impact Scorecard der digitalen Transformation, die wir im Rahmen unserer Recherchen zu Unternehmensinitiativen der digitalen Transformation ausgearbeitet haben.

Die Scorecard bewertet die Gesamtwirkung digitaler Unternehmensinitiativen anhand von 14 wesentlichen Leistungsindikatoren, die über eine erfolgreiche Transformation entscheiden.

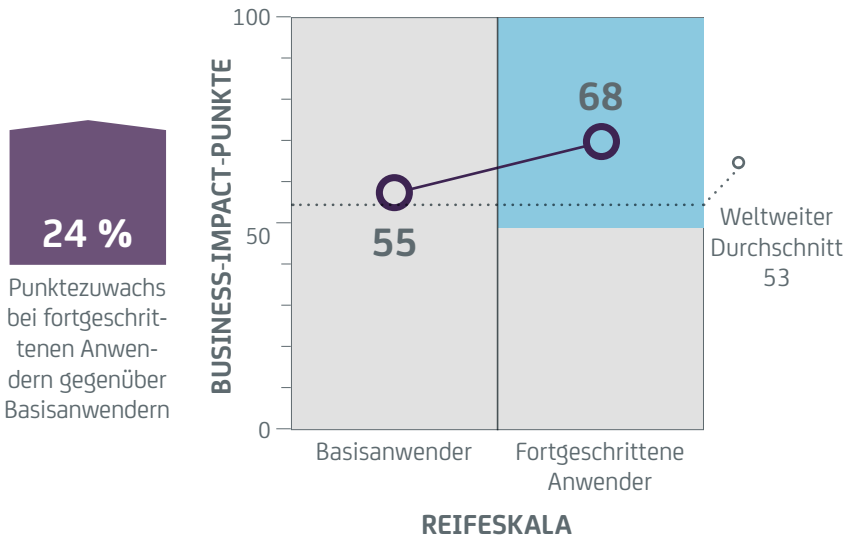
Wir verglichen die Scorecard-Ergebnisse für fortgeschrittene Anwender und Basisanwender identitätsbasierter Security. Die durchschnittliche Wertung für fortgeschrittene Anwender lag bei 68 von 100, gegenüber nur 55 für Basisanwender. Das entspricht einer 24%igen Steigerung (siehe Abb. 9).

ABB. 8 DER SCHRITT VON GRUNDLEGENDER ZU FORTGESCHRITTENER IDENTITÄTSBASIERTER SECURITY REDUZIERT DATENSCHUTZVERLETZUNGEN.



Anteil der Unternehmen, die einen Zuwachs, keine Veränderung oder eine Abnahme bei den Datenschutzverletzungen angaben
(Aufgrund von Rundung ergeben die Prozentanteile nicht 100.)

ABB. 9 DIE FORTGESCHRITTENE NUTZUNG IDENTITÄTSBASIERTER SECURITY VERBESSERT DIE UNTERNEHMENSERGEBNISSE BEI DER DIGITALEN TRANSFORMATION.



04 Erfahrungen fortgeschrittener Anwender identitätsbasierter Security

Die Botschaft ist klar: Fortgeschrittene Anwender identitätsbasierter Security erzielen in allen Bereichen einen höheren Nutzen für das Unternehmen. Was also machen sie bei der Security anders, damit diese so viel effektiver ist?

Zuallererst nehmen sie die IT Security wesentlich ernster: 81 % investieren gegenüber 55 % der Basisanwender mehr in die Vorbeugung von Verstößen. Zudem ist es unwahrscheinlicher, dass sie Abkürzungen nehmen: 58 % der fortgeschrittenen Anwender gehen Kompromisse bei der Security ein, um Anwendungen schneller auf den Markt zu bringen, bei den Basisanwendern sind es 70 %.

Zudem ist es wahrscheinlicher, dass sie auf sogenannte „DevSecOps“ zurückgreifen. Die Mehrheit der fortgeschrittenen Anwender identitätsbasierter Security (54 %) nutzt diese Practice, gegenüber 33 % der Basisanwender.

DevSecOps ist in der Application Economy von entscheidender Bedeutung. Ist Ihr Unternehmen von digitalen Technologien abhängig, können Sie die Security nicht erst hinterher an Ihre Anwendungen anheften. Ähnlich wie bei DevOps, wo IT Operations frühzeitig in den Lösungsentwicklungszyklus eingebunden wird, integriert DevSecOps die Security früher in den Entwicklungsprozess. So ist sichergestellt, dass die Security von Grund auf in digitale Anwendungen integriert ist.

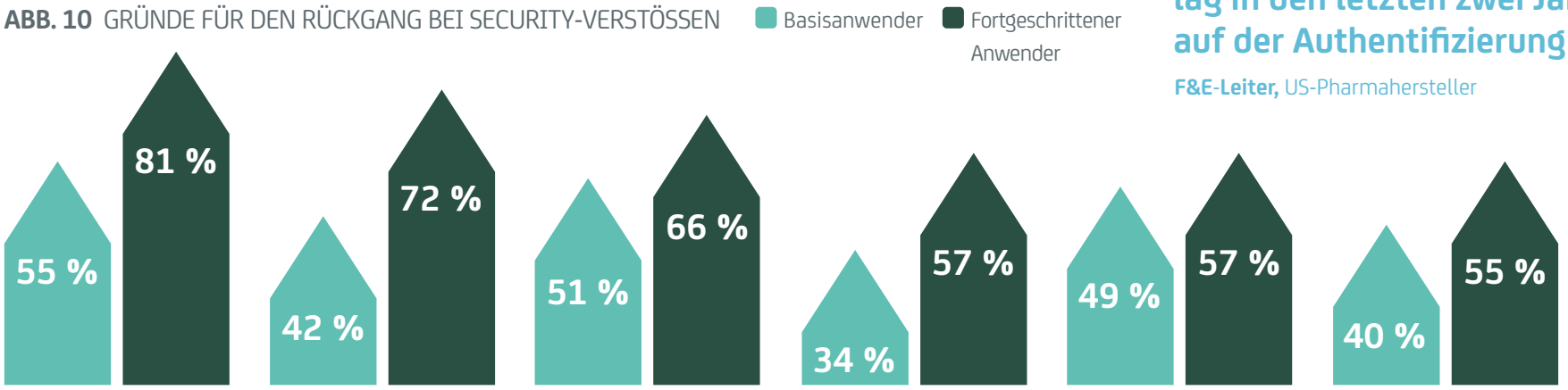
Schließlich ist es auch wahrscheinlicher, dass fortgeschrittene Anwender den Ansatz zur Vorbeugung gegen Verstöße an die Gegebenheiten der Application Economy anpassen (siehe Abb. 10).

Sehr viel höher ist auch die Wahrscheinlichkeit, dass sie spezielle Security für Mobile Devices und Apps (72 % gegenüber 42 %) implementieren, Security Practices neu konfigurieren, um Hochrisikobereiche wie privilegierte Identitäten zu schützen (57 % gegenüber 34 %), sichere Step-up-Authentifizierung bereitstellen (66 % gegenüber 51 %) und das Unternehmen umstrukturieren, um die Security-Verantwortlichkeiten zu unterstützen (55 % gegenüber 40 %).

„Unser größtes Security-Problem ist der Fernzugriff, der mittlerweile gang und gäbe ist. Der Schwerpunkt der IT Security lag in den letzten zwei Jahren auf der Authentifizierung.“

F&E-Leiter, US-Pharmahersteller

ABB. 10 GRÜNDE FÜR DEN RÜCKGANG BEI SECURITY-VERSTÖSSEN



05 Effektive identitätsbasierte Security – eine Roadmap

Unsere Studie legt einen deutlichen Business Case für die Einführung identitätsbasierter Security-Ansätze nahe. Aber wo können Sie beginnen? Wie können Sie diesen Ansatz für Ihr Unternehmen nutzen? Und wie sorgen Sie dafür, dass Performance und Wachstum gesteigert werden?

Unsere Erfahrung hat gezeigt, dass die folgenden Aktionen über den Erfolg der Implementierung identitätsbasierter Security entscheiden:

1. **Definieren Sie die Identität als Perimeter.** Heute markieren die Anwender die Security-Grenze, und sie greifen überall und jederzeit auf Ihr Netzwerk zu. Sie müssen wissen, dass diese Anwender tatsächlich die Personen sind, als die sie sich ausgeben, und dass sie nur auf die Informationen und Services zugreifen können, auf die sie zugreifen können sollen. Das bedeutet risikobasierte Authentifizierung plus analysebasierte Ansätze der Identitätsprüfung.
2. **Betrachten Sie die Security als Business Enabler.** In der Application Economy ist die Security nicht nur dazu da, um Risiken zu senken, sondern auch, um das Unternehmenswachstum anzukurbeln. Unsere Recherchen haben gezeigt, dass ein identitätsbasierter Ansatz eine Reihe von Vorteilen mit sich bringt, die das Unternehmensergebnis verbessern. Integrieren Sie daher Indikatoren für die Unternehmensperformance in den Rahmen zur Security-Bewertung.
3. **Legen Sie den Schwerpunkt auf den Aufbau vertrauenswürdiger digitaler Beziehungen**. Ihre größten Trümpfe sind die digitalen Beziehungen, die Sie mit jedem einzelnen Kunden aufbauen. Sie müssen sich darauf verlassen können, dass Sie ihre Bedürfnisse bei der Interaktion mit Ihrem Unternehmen kennen und ihre Identitäten und Daten so nahtlos wie möglich schützen.
4. **Schützen Sie Experiences und nicht nur Daten**. Security muss robust sein, aber auch reibungslos funktionieren. Kunden verlangen nach optimierten Interaktionen und makellosen Experiences, und jede Störung vertreibt sie. Das heißt, dass Sie Zugriff per Single Sign-On, Self-Service-Funktionen und einheitliche, aber flexible Authentifizierungsmechanismen anbieten müssen, während sich Anwender durch Anwendungen und Geräte bewegen.
5. **Wenden Sie einen anpassungsfähigen IAM-Ansatz an**. Unsere Recherchen zeigen, dass fortgeschrittene Anwender identitätsbasierter Security IAM-Kontrollen nutzen, die sich unkompliziert je nach Risiko anpassen lassen. Das verbessert die User Experience erheblich.
6. **Gehen Sie proaktiv und prognostisch vor**. Mit erweiterten Analysen können Sie Security-Risiken proaktiv vorbeugen, statt im Dauerbetrieb „Brände zu löschen“. Zudem bringen Sie die Security einen weiteren Schritt voran: Sie sind so in der Lage, Vorgänge zu erkennen, entsprechend zu reagieren und die Security-Prozesse anzupassen, um dem Risiko von Verstößen vor deren Eintreten vorzubeugen.
7. **Opfern Sie die Security nicht dem Tempo**. In der Application Economy herrscht ein erhöhter Druck, neue Apps schnell auf den Markt zu bringen. Es ist jedoch wichtiger als je zuvor, dass die Security von Grund auf integriert ist, damit nicht am Ende Abstriche nötig sind. Nutzen Sie möglichst einen DevSecOps-Ansatz, der sicherstellt, dass sämtliche Security-Aspekte früh in der Entwicklung abgedeckt sind.

Weitere Informationen

Forschungsmethodik

CA Technologies beauftragte Coleman Parkes Research, Führungskräfte zu Umfang und Auswirkungen der Maßnahmen für die digitale Transformation in ihren Unternehmen zu befragen.

Wir befragten 1.770 Senior-Business- und IT-Entscheidungsträger (darunter 106 CSOs/CISOs) in Großunternehmen in 21 Ländern in Amerika, EMEA und im Asien-Pazifik-Raum und Japan (APJ). Die Jahresumsätze der befragten Unternehmen beliefen sich auf mehr als 1 Mrd. USD (bzw. 0,5 Mrd. USD in bestimmten kleineren Volkswirtschaften).

Länder der Teilnehmer:

Amerika	**EMEA**	**Asien/Pazifik und Japan**
Brasilien	Deutschland	Australien
USA	Frankreich	China
	Großbritannien	Hongkong
	Italien	Indien
	Niederlande	Indonesien
	Schweden	Japan
	Schweiz	Korea
	Spanien	Malaysia
	Südafrika	Singapur
		Thailand

Branchen der Teilnehmer:

- Automobilbranche
- Bankwesen und Finanzdienstleistungen
- Einzelhandel
- Energie- und sonstige Versorgung
- Fertigung
- Gesundheitswesen
- Medien und Unterhaltung
- Nationaler öffentlicher Sektor
- Telekommunikation
- Transport und Logistik

Die Untersuchung und die Analyse wurden im Mai und Juni 2016 durchgeführt.

Über CA Technologies

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht in allen Branchen und in allen Unternehmen im Mittelpunkt. Von der Planung über die Entwicklung bis hin zu Management und Security arbeitet CA Technologies weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, neu zu gestalten – ob mobil, in der privaten oder öffentlichen Cloud oder in verteilten Systemen oder Mainframe-Umgebungen. www.ca.com/de

Informationen zu Coleman Parkes Research

Coleman Parkes Research ist auf die Rekrutierung und Befragung hochrangiger Interviewpartner aus unterschiedlich globalen Märkten, vertikalen Branchen und Funktionsbereichen spezialisiert, die ein breites Kundenspektrum abdecken. Wir bieten alles von Thought-Leadership-Forschung für PR- und Marketingkampagnen bis hin zu Analysen von Gewinn-/Verlustchancen, Testing von Produktbotschaften und Tiefeninterviews mit Führungskräften. Coleman Parkes Research arbeitet gemeinsam mit Kunden an der Formulierung bewährter Strategien, die auf Basis individueller Anforderungen und zentraler Hypothesen Markterkenntnisse liefern. colemanparkes.com/

Informationen zu Grist

Text- und Kreativservices. Grist ist eine preisgekrönte B2B-Thought-Leadership- und Content-Marketingagentur, die die digitale Zukunft fest im Blick hat und deren redaktioneller Hintergrund von The Economist und der Financial Times stammt. www.gristonline.com