
accenture
STATE OF CYBER RESILIENCE
INNOVATION SCHÜTZT
SKALIEREN. SCHULEN. ZUSAMMENARBEITEN.
WIE SIE MEHR AUS CYBERSECURITY-INVESTITIONEN HERAUSHOLEN

VORWORT

Wie ernst nehmen Unternehmen das Thema Cybersicherheit? Und was können österreichische Unternehmen von Vorreitern lernen? In der vorliegenden Studie gehen wir diesen Fragen nach.

Accenture Security hat dazu 4.644 Cybersecurity-Verantwortliche aus Großunternehmen in 24 Branchen und 15 Ländern befragt. Wir haben untersucht, wie umfassend die Security-Pläne der Unternehmen sind und welche Schwerpunkte sie legen. Vor allem wollten wir wissen, welche Security-Investitionen besonders effektiv waren und welche sich gar nicht amortisiert haben. Daraus lassen sich klare Handlungsempfehlungen für Security-Entscheider ableiten.

Die Konsequenzen erfolgreicher Angriffe sind so weitreichend wie nie. Beispielsweise kann der Verlust von Kundendaten zu einem langfristigen Vertrauensverlust führen. Und wegen der inzwischen strengeren Datenschutzgesetzgebung drohen dabei hohe Strafzahlungen. Teilweise wurden bereits Geldstrafen in zweistelliger Millionenhöhe verhängt. Das Risiko ist also gestiegen und trotz höherer Investitionen in Sicherheitstechnologien ist nur jedes fünfte Unternehmen weltweit „resilient", also zukunftssicher aufgestellt.

Die Studie dokumentiert daher auch, wie sich Vorreiter in Sachen Cybersecurity von allen anderen unterscheiden. Wir zeigen, wie diese Unternehmen Angriffe schnell unterbinden und den Schaden begrenzen.

Was Sie tun können, um einer dieser Vorreiter zu werden? In dieser Studie finden Sie sicherlich einige Anregungen.

Viel Spaß beim Lesen!

GEORG SCHWONDRA
SECURITY LEAD
ACCENTURE ÖSTERREICH

georg.schwondra@accenture.com

„Perfekt durchgeplante Cyberangriffe im großen Stil sind heute an der Tagesordnung – und der dabei entstehende Schaden geht in die Milliarden. Jedem muss klar sein: Es geht bei Cybersecurity längst nicht mehr nur um die Sicherheit der IT-Systeme. Es geht um den Fortbestand ganzer Unternehmen."

NEUE RISIKEN, VERDECKTE GEFAHREN

Indirekte Cyberangriffe verbergen das wahre Ausmaß

Noch unmittelbar vor der Pandemie haben Strafverfolgungsbehörden weltweit in großem Stil cyberkriminelle Vereinigungen aufgedeckt und die Täter verhaftet. Dabei ist klar geworden, wie ausgereift und professionell die Angriffe inzwischen ablaufen. Die Hackergruppe, auf deren Konto die global verbreitete GozNym-Malware geht, versuchte beispielsweise allein mit ihren Angriffen auf US-Ziele 100 Millionen US-Dollar zu erbeuten. Dahinter steckt ein komplexes Netzwerk verteilt operierender Personen mit Zugang zu fortschrittlichen Technologien, von denen jeder Einzelne eine klar definierte Rolle erfüllt. Jeder Hacker arbeitet extrem spezialisiert und trägt jeweils einen kleinen Teil zum Angriff bei. Eine ganze Lieferkette ist entstanden – oder, wie das Technologiemagazin Wired es nannte: „ein Supermarkt der Cybercrime-Dienstleistungen".[1]

Ob finanziell motivierte Cyberkriminelle oder politisch motivierte Cyberspionage-Gruppierungen: Sie alle entwickeln sich permanent weiter und bedeuten für die Organisationen neue Risiken und verdeckte Gefahren. Darunter:

Jagd auf die Großen – Eine kleinere Zahl von Cyberangriffen richten sich gegen finanziell attraktive Organisationen.

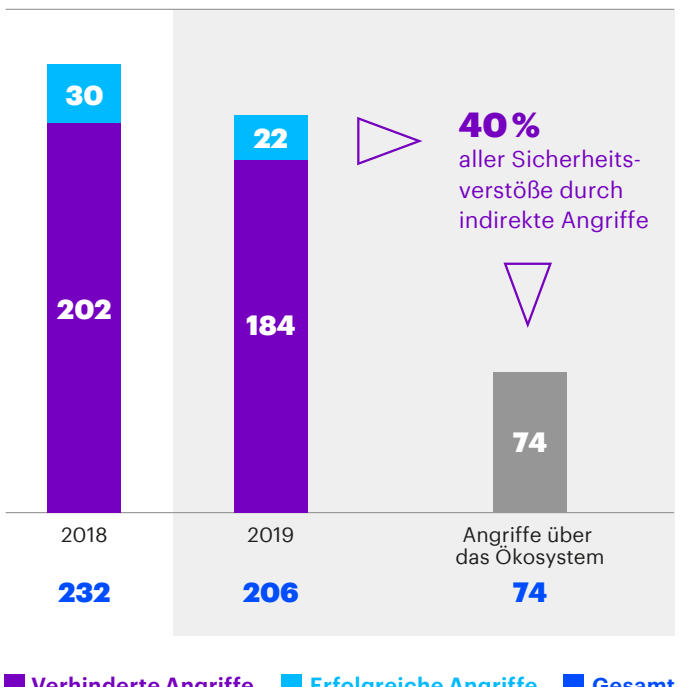
Regionale Angriffe – Spezialisiertes Wissen bezüglich lokaler Sprachen, Kulturen und Technologien wird genutzt, um die Erfolgschancen eines Angriffs zu erhöhen.

Indirekte Angriffe – Der Zugang zum Zielsystem erfolgt über Schwachstellen in der Lieferkette oder über Kompromisse innerhalb der Cloud- oder Managed-Services-Struktur einer Organisation.

Zwar wurden 2019 weltweit weniger Cyberangriffe gemeldet als noch im Jahr zuvor (im Schnitt pro Unternehmen 206 im Vergleich zu 232). Doch indirekte Angriffe stellen eine verdeckte Gefahr dar, die das wahre Ausmaß der Bedrohungslage verschleiern.

Inzwischen gehen 40 Prozent aller Sicherheitsverstöße auf Schwachpunkte in der Lieferkette oder im geschäftlichen Ökosystem eines Unternehmens zurück – Angriffe gegen die Partner dieses Unternehmens bleiben dabei verborgen. Geht man bei diesen Partnern vom gleichen Verhältnis zwischen erfolgreichen und abgewehrten Angriffen aus, landen wir bei einer Gesamtzahl von ca. 290 pro Unternehmen. Das wäre ein Anstieg von 25 Prozent gegenüber dem Vorjahr. Es ist zu vermuten, dass diese Zahlen in der aktuellen Situation ansteigen werden: Viele Partner innerhalb der Lieferkette priorisierten vor allem zu Beginn der Pandemie den Schutz ihrer Mitarbeiter und ihres Unternehmens an sich.

Abbildung 1: Die verborgene Gefahr indirekter Angriffe weltweit



[1] Global takedown shows the anatomy of a modern cybercriminal supply chain. Wired. 16. Mai 2019

SCHEITERNDE INVESTITIONEN

Trotz hoher Budgets für Security-Maßnahmen bleibt die Investitionsrendite oft hinter den Erwartungen zurück

Unternehmen investieren in immer mehr Technologien. Damit nimmt auch die Zahl der Cybersecurity-Lösungen zu. Doch die Rendite liegt im Schnitt bei gerade einmal 53 Prozent. Das mag auch daran liegen, dass die Tools zum Teil gar nicht getestet oder aber nur lückenhaft genutzt werden: Tatsächlich schalten Unternehmen nur bei einem Viertel ihrer Security-Lösungen eine Pilotphase vor und skalieren sie später organisationsübergreifend.

Wer sich mit Cybersecurity beschäftigt, sieht sich zudem einer Landschaft gegenüber, die sich permanent verändert. Security-Teams müssen in der Lage sein, mit Hackergruppen Schritt zu halten – und benötigen dafür neue Technologien. Mit der zunehmenden Zahl indirekter Angriffe müssen sich die Unternehmen zudem nicht mehr allein um den Schutz ihrer eigenen Güter kümmern, sondern verstärkt auch um den ihres gesamten Ökosystems. Unsere Studie zeigt: Im Durchschnitt werden nur 60 Prozent des geschäftlichen Netzwerks eines Unternehmens aktiv vor Cyberangriffen geschützt. Das ist ein Problem, wenn genau darüber 40 Prozent aller Angriffe stattfinden.

Viele Unternehmen scheitern also daran, mehr aus ihren Investitionen herauszuholen. Das wirkt sich auch auf den eigentlichen Schutzeffekt und die Reaktion auf Vorfälle aus. Unserer Studie zufolge werden durchschnittlich nur 59 Prozent aller Unternehmensgüter aktiv durch Cybersecurity-Programme abgesichert. Zudem dauert es bei mehr als der Hälfte aller Sicherheitsvorfälle (54 Prozent) über 16 Tage, bis ihre Folgen beseitigt sind. Bei einem Viertel von ihnen dauert es sogar länger als einen Monat.

GEZIELTE CYBERANGRIFFE

Im Rahmen dieser Studie haben wir gezielte Cyberangriffe untersucht. Diese können zum einen Netzwerk-Schutzmaßnahmen aushebeln und Schäden verursachen, zum anderen können dabei wertvolle Daten aus dem Unternehmen entwendet werden. Nicht zu den gezielten Angriffen gehört die Flut Hunderter bis Tausender spekulativer Angriffe, mit denen Unternehmen täglich zu tun haben.

DIE VORREITER DER CYBERSECURITY

Sie stoppen Angriffe häufiger und schneller – mit geringerem Schaden

Wie leistungsstark ist ein Unternehmen in Sachen Cybersecurity? Um Geschäftsleitung und Vorstand in das Thema einzubinden, müssen zur Zielgruppe passende Metriken aufgestellt werden. Wenn es hingegen darum geht, wie effektiv die Investitionen in Security-Technologien sind, braucht es direktere, sicherheitsbezogene Kennzahlen.

Ein wesentlicher Zweck einer Security-Lösung ist, die Widerstandsfähigkeit eines Unternehmens zu steigern. Das heißt: Sie muss Angriffe nicht nur verhindern, sondern es dem Unternehmen auch ermöglichen, sich schnell von Sicherheitsvorfällen zu erholen.

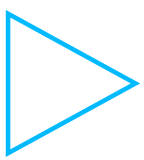
Manche der untersuchten Unternehmen erzielen mit ihren Investitionen in Cybersecurity-Technologien erheblich bessere Resultate als andere. Und zwar in praktisch allen Bereichen: Sie haben weniger Sicherheitsvorfälle, identifizieren diese schneller, haben deren Folgen nach kürzerer Zeit beseitigt und den Schaden dadurch minimiert.

EIGENSCHAFTEN DER VORREITER	VORREITER GLOBAL	REST GLOBAL
GERINGE ERFOLGSQUOTE Der Anteil jener Cyberangriffe, die zu einem Sicherheitsvorfall geführt haben.	**4 %**	**13 %**
SCHNELLE ERKENNUNG Der Anteil der Gruppe, die einen Sicherheitsvorfall in weniger als einem Tag erkennt.	**88 %**	**22 %**
SCHNELLE BESEITIGUNG Der Anteil der Gruppe, die alle Folgen eines Sicherheitsvorfalls in weniger als 15 Tagen beseitigt.	**96 %**	**36 %**
MINIMALER SCHADEN Der Anteil der Sicherheitsvorfälle, die keine oder nur geringe Auswirkungen haben.	**83 %**	**50 %**

WAS VORREITER ANDERS MACHEN

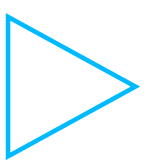
Sie skalieren häufiger, schulen mehr und arbeiten intensiver zusammen

VORREITER SKALIEREN HÄUFIGER



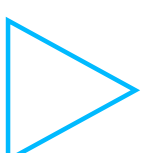
Unternehmen, die ihre Technologie-Investitionen am besten skalieren, wehren Angriffe viermal effektiver ab.

VORREITER SCHULEN MEHR



Unternehmen, die ihre Mitarbeiter am besten schulen, wehren Angriffe zweimal effektiver ab.

VORREITER ARBEITEN INTENSIVER ZUSAMMEN



Unternehmen, die am besten zusammenarbeiten, wehren Angriffe zweimal effektiver ab.

Von den 4.644 untersuchten Unternehmen scheinen 17 Prozent eine Art Erfolgsrezept entdeckt zu haben, das sie in puncto Security vom Rest abhebt. Diese Vorreiter schlagen andere Wege ein, um mehr aus ihren Investitionen in Cybersecurity-Technologien herauszuholen.

VORREITER SKALIEREN HÄUFIGER

Unternehmen, die ihre Technologie-Investitionen am besten skalieren, wehren Angriffe viermal effektiver ab

Sie stoppen Cyberangriffe effektiver

Wie schnell ein Unternehmen seine Cybersecurity-Investitionen organisationsweit skaliert, wirkt sich erheblich darauf aus, wie effektiv es Angriffe abwehren kann. Die am besten skalierenden Unternehmen schneiden viermal besser ab als der Rest der Befragten. Nur 5 Prozent der Angriffe resultierten bei ihnen in einem Sicherheitsvorfall – im Vergleich zu 21 Prozent bei allen anderen Unternehmen.

Sie spüren Sicherheitsvorfälle schneller auf

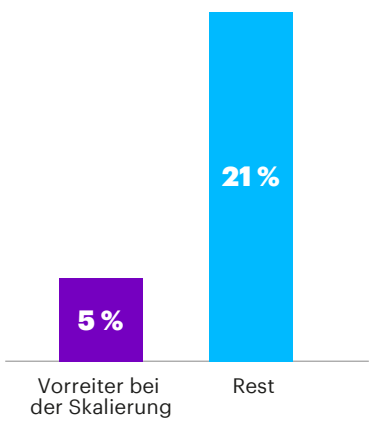
Die besten Skalierer verfügen zudem über die effektivsten Security-Teams. Diese Teams waren in der Lage, fast drei Viertel der Angriffe auf ihr Unternehmen zu entdecken. Die anderen Organisationen spürten nur die Hälfte der Angriffe auf.

Sie schützen mehr ihrer wichtigsten Güter

Skalierung ist ein wichtiger Faktor für die Reichweite einer Security-Initiative. Die besten Skalierer schützen mithilfe aktiver Maßnahmen drei Viertel ihrer wichtigsten Güter – von Daten bis zu technischen Anlagen. Alle anderen Unternehmen decken im Schnitt nur die Hälfte ihrer Güter ab.

Der Faktor Skalierung zeigt, wie effektiv Investitionen in neue Security-Technologien sein können. Allerdings nur dann, wenn sie auch unternehmensweit ausgerollt werden.

Abbildung 2: Anteil der Cyberangriffe, die zu einem Sicherheitsvorfall führen



Definition „Vorreiter bei der Skalierung“: 50 % oder mehr der Security-Tools gelangen von der Pilotphase in den umfassenden Rollout.

81 % **sagen, neue Cybersecurity-Tools vergrößern die Abdeckung ihrer Organisation mit Sicherheitsmaßnahmen**

VORREITER SCHULEN MEHR

Unternehmen, die ihre Mitarbeiter am besten schulen, wehren Angriffe zweimal effektiver ab

Sie stoppen Cyberangriffe effektiver

Tool-Einweisungen und Weiterbildungen bilden ein weiteres Feld, in dem die meisten Unternehmen noch großen Nachholbedarf haben. Im Rahmen der Studie haben wir gefragt, wie umfangreich Unternehmen entsprechende Trainings für Tools anbieten, die eine Schulung erfordern. Die Vorreiter schulten mehr als drei Viertel der Nutzer. Das Resultat: Nur 6 Prozent der Cyberangriffe führten zu einem Sicherheitsvorfall. Bei den anderen Unternehmen waren es durchschnittlich 11 Prozent.

Sie spüren Sicherheitsvorfälle schneller auf

Wer intensiver schult, entdeckt Sicherheitsvorfälle schneller. Vorreiter konnten 52 Prozent der Vorfälle in weniger als 24 Stunden aufspüren, beim Rest der Unternehmen waren es nur 32 Prozent.

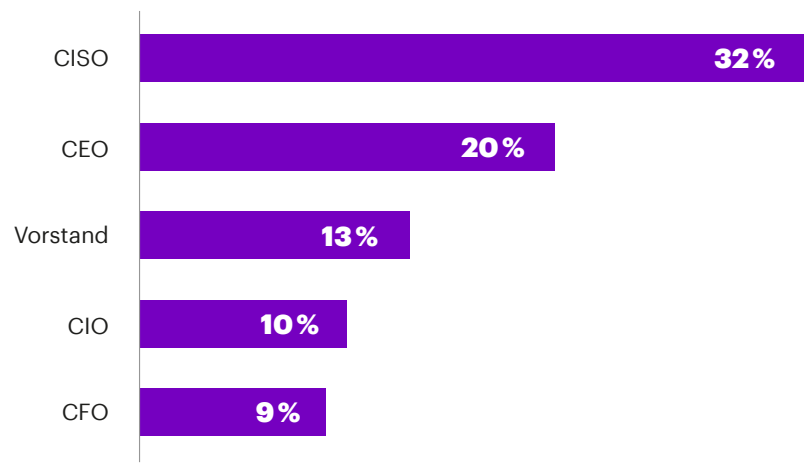
Sie schützen mehr ihrer wichtigsten Güter

Mit der Einführung neuer Tools werden Schulungen wichtiger. Nur so lässt sich der Nutzen der Lösungen ausschöpfen. Unternehmen, die das praktisch umsetzen, schützen im Schnitt 85 Prozent ihrer Organisation durch aktive Cybersecurity-Maßnahmen. Alle anderen decken durchschnittlich nur 56 Prozent ab.

Schulungen erhöhen die Effektivität von Security-Lösungen. Doch nicht jedes Unternehmen misst dem Training den nötigen Stellenwert bei, wenn es um die Verteilung von Security-Budgets geht.

Definition „Vorreiter bei Schulungen“: 75 % oder mehr der Anwender erhalten die nötigen Schulungen für ihre Cybersecurity-Tools.

Abbildung 3: Wer bewilligt das Budget für Schulungen?



VORREITER ARBEITEN INTENSIVER ZUSAMMEN

Unternehmen, die am besten zusammenarbeiten, wehren Angriffe zweimal effektiver ab

Sie stoppen Cyberangriffe effektiver

Unternehmen, die bei Cybersecurity-Maßnahmen verstärkt zusammenarbeiten, eröffnen sich mehrere Vorteile. Beispielsweise führen weniger Angriffe zu tatsächlichen Sicherheitsvorfällen – nämlich nur 6 Prozent bei jenen Unternehmen, die mindestens fünf verschiedene Methoden der Zusammenarbeit einsetzen. Beim Rest der Unternehmen sind 13 Prozent der Angriffe erfolgreich.

Sie schützen mehr ihrer wichtigsten Güter

Eine intensivere Zusammenarbeit führt zu einem erheblich besseren Schutz durch Cybersecurity-Maßnahmen – und zwar im gesamten Ökosystem. Die Vorreiter auf diesem Gebiet schützen 67 Prozent ihres Unternehmens aktiv, beim Rest sind es nur 58 Prozent.

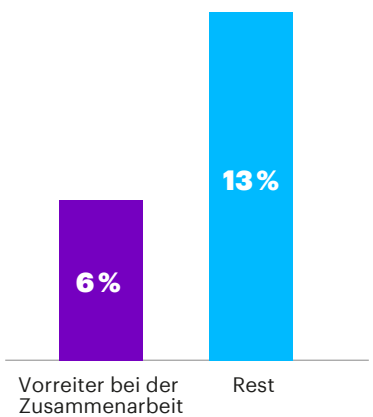
Sie halten regulatorische Vorgaben besser ein

Compliance-Maßgaben einzuhalten ist innerhalb der letzten Jahre aufwendiger geworden – und wichtiger. Denn mit Verordnungen wie der Datenschutz-Grundverordnung (DSGVO) sind nicht nur die Anforderungen hinsichtlich Audits gestiegen, sondern vor allem die drohenden Bußgelder. 54 Prozent der Vorreiter in Sachen Zusammenarbeit sagen, dass sie gerade durch ihren intensiveren Austausch die rechtlichen Vorgaben besser einhalten können. Beim Rest der Befragten sagen das nur 25 Prozent.

Der Faktor Zusammenarbeit führt zu einer höheren Rendite von Technologie-Investitionen. Die Auswirkungen eines Cyberangriffs lassen sich besser eindämmen und wichtige Güter im erweiterten Ökosystem besser schützen.

Definition „Vorreiter bei der Zusammenarbeit“: Sie nutzen mindestens fünf Methoden bei der Vernetzung strategischer Partner, der Sicherheits-Community, Konsortien und der internen Task-Force, um ein besseres Verständnis der Bedrohungslage zu gewinnen.

Abbildung 4: Anteil der Cyberangriffe, die zu einem Sicherheitsvorfall führen



79 % **halten die Zusammenarbeit mit anderen Unternehmen, staatlichen Behörden und der Sicherheits-Community im Kampf gegen Cyberangriffe für essenziell**

SO LOHNEN SICH DIE INVESTITIONEN

Beim Thema Cybersecurity gilt: Größere Investitionen bedeuten nicht automatisch auch eine bessere Leistung – und damit einen größeren Schutz. Zudem steigen die Kosten für Cybersicherheit an. Jede Investition muss daher einen größeren Wertbeitrag leisten als bislang.

In den vergangenen zwei Jahren hat sich das Kostenverhältnis stark verschoben. Topmanager und Vorstände müssen jetzt mehr denn je dafür sorgen, dass ihre Investitionen den jetzigen, aber auch den zukünftigen Schutz ihres Unternehmens gewährleisten.

Dabei hilft es, die erfolgreichen Strategien der Vorreiter zu verstehen. Diese investieren in Geschwindigkeit, setzen also auf Technologien, mit denen sie möglichst schnell die operative Cybersicherheit erhöhen können. Außerdem achten sie darauf, ihre bereits getätigten Security-Investitionen zu erhalten. Und schließlich legen sie großen Wert auf Skalierung, Schulungen und Zusammenarbeit. Mit diesen Vorgehensweisen lassen sich nicht nur die Security-Investitionen optimieren. Auch die Effektivität der Maßnahmen steigt.

Entscheider sollten sich jetzt folgende Fragen stellen:

1.

Gehen wir bei unseren Cybersecurity-Initiativen über die Pilotphase hinaus? Skalieren wir unsere Investitionen unternehmensweit und bis hin zu Lieferanten und Partnern in unserem Ökosystem?

2.

Bringen wir die Schulungs- und Weiterbildungsangebote für unsere Mitarbeiter regelmäßig auf den aktuellen Stand – immer mit Blick auf die bestehenden und geplanten Security-Tools und -Maßnahmen?

3.

Arbeiten wir eng mit strategischen Partnern, Security-Communities und -konsortien zusammen? Verfügen wir über eine interne Task-Force, die unser Gesamtverständnis der Bedrohungslage verbessert?

ÜBER DIESE STUDIE

Im Rahmen dieser Studie hat Accenture Security weltweit 4.644 Entscheider befragt. Das Ziel: ein umfassendes Lagebild darüber, wie Unternehmen das Thema Cybersecurity priorisieren, wie umfassend ihre Security-Pläne sind und wie sich ihre Security-Investitionen bezahlt machen. Die Entscheider gehören Unternehmen mit einem Jahresumsatz von mindestens 1 Milliarde US-Dollar an – aus 24 Branchen und 15 Ländern in Nord- und Südamerika, Europa und Asien.

Was ist Cyber-Resilienz?

Ein cyber-resilientes Unternehmen verfügt über fortschrittliche Cybersecurity-Maßnahmen und ist in der Lage, auch in kritischen Situationen den Geschäftsbetrieb aufrechtzuerhalten. Dafür nutzt es fluide Strategien, um schnell auf Bedrohungen zu reagieren, so den verursachten Schaden zu minimieren und weiterhin einsatzfähig zu bleiben. Ein cyber-resilientes Unternehmen kann innovative Angebote und Geschäftsmodelle auf sichere Weise einführen, das Vertrauen seiner Kunden stärken und selbstbewusst wachsen.

Über Accenture

Accenture ist ein weltweit führendes Beratungsunternehmen, das ein breites Portfolio von Dienstleistungen sowie digitale Expertise in den Bereichen Strategy & Consulting, Interactive, Technology und Operations anbietet. Wir setzen unsere umfassende Erfahrung und spezialisierten Fähigkeiten in mehr als 40 Branchen ein – gestützt auf das weltweit größte Netzwerk aus Centern für Advanced Technology und Intelligent Operations. Mit 513.000 Mitarbeitern, die für Kunden in über 120 Ländern tätig sind, treiben wir kontinuierlich Innovationen voran, um die Leistungsfähigkeit unserer Kunden zu stärken und für ihr Geschäft nachhaltig Mehrwert zu schaffen.

Besuchen Sie uns unter **www.accenture.at**

Über Accenture Security

Accenture Security hilft Unternehmen dabei, widerstandsfähig gegenüber Cyberangriffen zu werden, damit sie sich ganz auf Innovation und Wachstum konzentrieren können. Unterstützt von einem globalen Netzwerk von Cybersecurity-Einrichtungen und basierend auf einer tiefen Branchenerfahrung über Wertschöpfungsketten hinweg schützt Accenture seine Kunden durchgängig. Wir unterstützen in den Bereichen Strategie- und Risikomanagement, Cyberabwehr, digitales Identitätsmanagement, Anwendungssicherheit und Managed Security. So können sich unsere Kunden weltweit effektiv vor hoch entwickelten Bedrohungen schützen – und zwar vor bekannten wie vor unbekannten gleichermaßen.

Folgen Sie uns auf Twitter unter **@AccentureSecure**

Über Accenture Research

Accenture Research untersucht Trends und gibt auf der Basis klarer Daten aufschlussreiche Einblicke in die dringlichsten Themen global agierender Unternehmen. Unser Team von 300 Forschern und Analysten aus 20 Ländern kombiniert die Leistungsfähigkeit innovativer Forschungsmethoden mit umfassendem Branchenwissen und veröffentlicht jedes Jahr Hunderte von Berichten, Artikeln und Whitepaper. Unsere impulsorientierte Forschung – unterstützt durch firmeneigene Daten und Partnerschaften mit führenden Organisationen wie dem MIT und Harvard – gibt unseren Innovationen die Richtung vor und versetzt uns in die Lage, Theorien und neue Ideen in reale Lösungen für unsere Kunden zu verwandeln.

Besuchen Sie uns unter **www.accenture.com/research**

NEW.APPLIED.NOW