THALES 451 Research

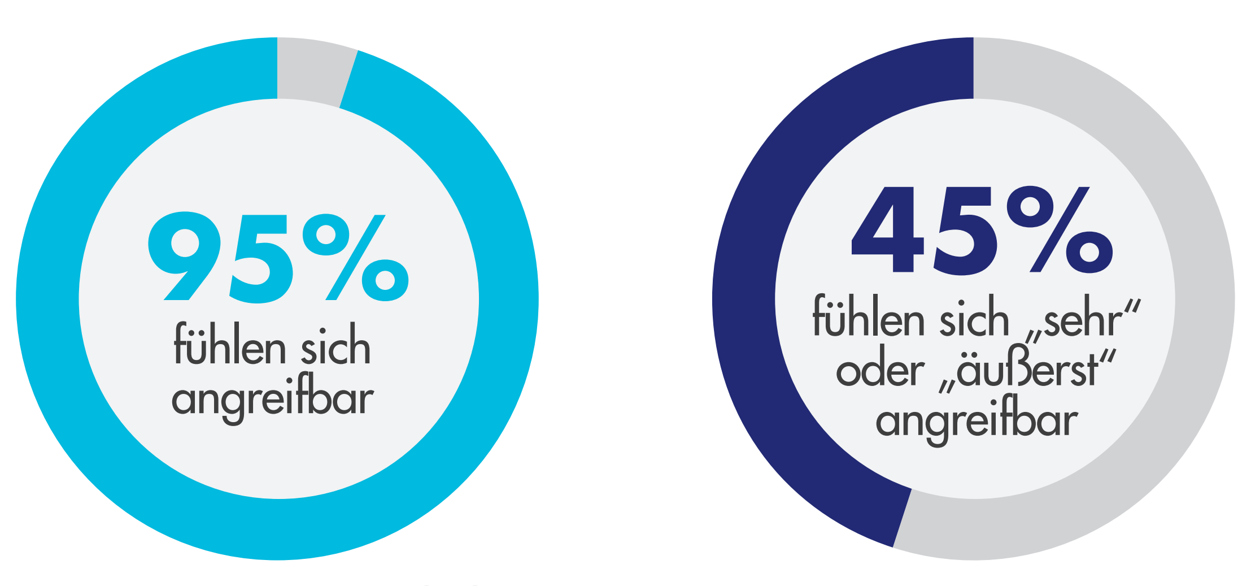
IT-SICHERHEITS-BEDROHUNGEN IN DEUTSCHLAND 2017

VORBEREITUNG AUF DIE DSGVO (GDPR)

> „Angesichts der bevorstehenden Auswirkungen der Datenschutz-Grundverordnung (DSGVO/GDPR) herrscht bei den deutschen Umfrageteilnehmern der Eindruck vor, dass sie in stärkerem Mass von Datenschutzregelungen betroffen sind, als ihre Kollegen in anderen Ländern. Nur 19 Prozent der Befragten gaben an, dass ihre Organisation nicht von Bestimmungen zu Datenschutz bzw. Datenhoheit betroffen sind (weltweit niedrigster Wert).“
>
> *– Garrett Bekker, Principal Analyst, Information Security bei 451 Research*

UNTERNEHMEN FÜHLEN SICH ANGREIFBAR UND ERHÖHEN IT-SICHERHEITSBUDGET, DOCH ZAHL DER SICHERHEITSVORFÄLLE IST RÜCKLÄUFIG

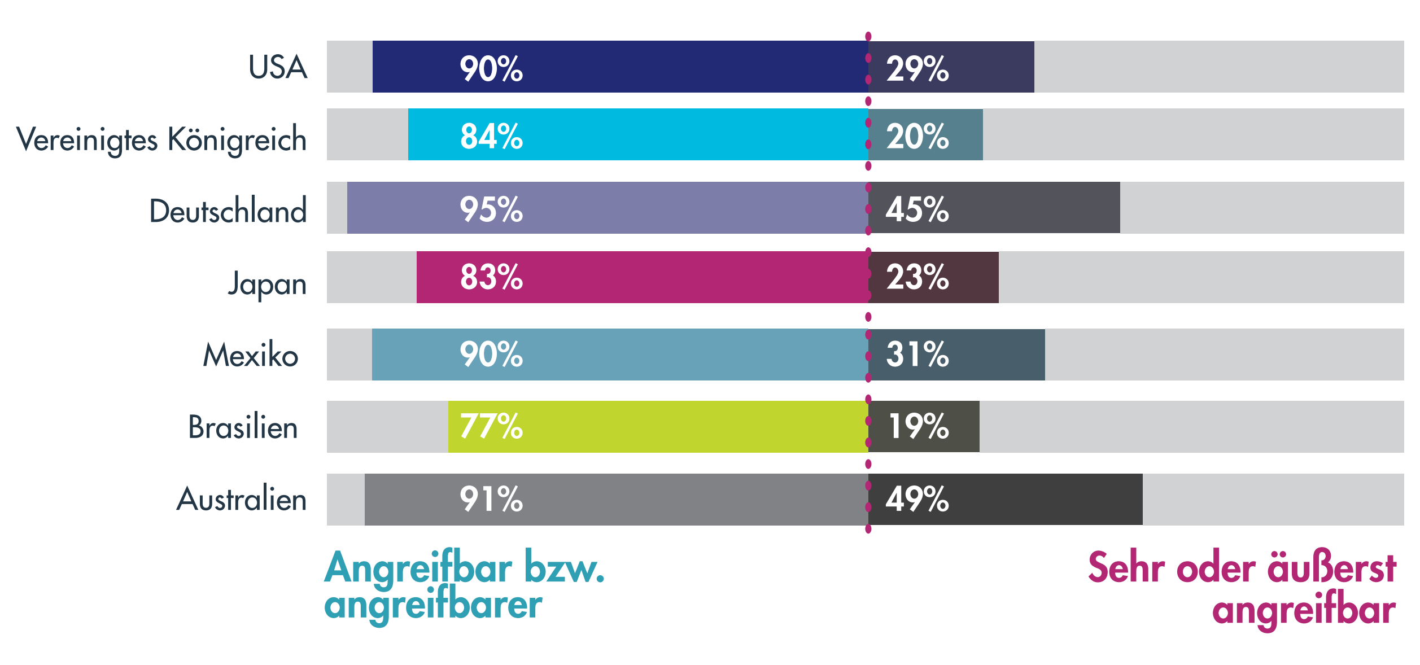
Sie fühlen sich angreifbarer als ihre Kollegen in anderen Ländern:



Dieser Prozentsatz ist höher als in allen anderen Regionen

Im Vergleich zu **91%** im vergangenen Jahr

Im Vergleich zu **40%** im vergangenen Jahr



Erhöhung des IT-Sicherheitsbudgets zur Abwehr von Bedrohungen

Zahl der Datensicherheitsvorfälle geht allmählich zurück

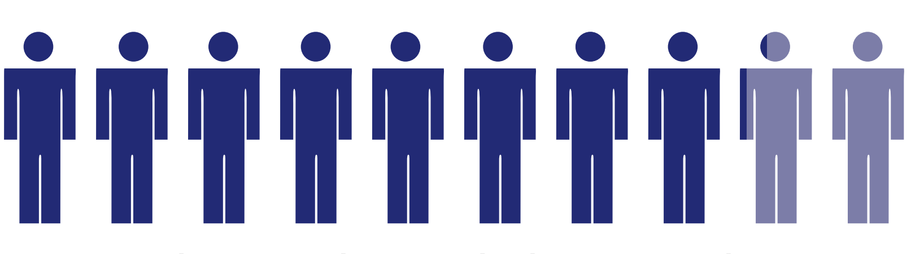
Im Vergleich zu **37%** laut unserem Bericht von 2016

9% wurden letztes Jahr und davor Opfer eines Sicherheitsvorfalls

---

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Deutschen Unternehmen drohen bei Nichteinhaltung der DSGVO drastische Geldbußen (bis zu 4 Prozent des weltweiten Umsatzes)



81% sind von Gesetzen zu Datenschutz und Datenhoheit, wie der DSGVO, betroffen

Compliance und Best Practices, beide im Hinblick auf die DSGVO sehr wichtig, haben bei den IT-Sicherheitsausgaben 2017 oberste Priorität

Wie hoch ist das Risiko eines Sicherheitsvorfalls? Für größere deutsche Unternehmen sehr hoch:

(1 von 4) werden jedes Jahr Opfer eines Sicherheitsvorfalls

haben schon einmal gegen Compliance-Anforderungen verstoßen oder waren Opfer eines Sicherheitsvorfalls.

> „Die Compliance-Anforderungen sind jetzt schon hoch, werden aber mit dem Inkrafttreten der DSGVO ab Mai 2018 noch viel strenger.“
>
> *—Garrett Bekker, Principal Analyst, Information Security bei 451 Research*

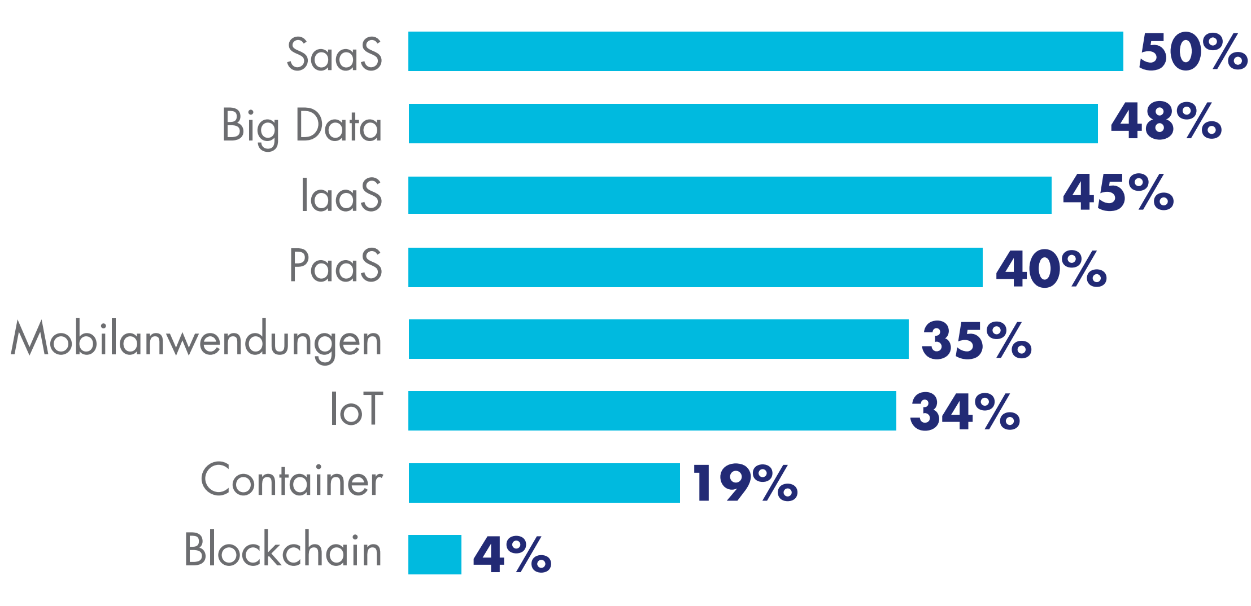
EINSATZ NEUER TECHNOLOGIEN VERSCHÄRFT DAS PROBLEM ZUSÄTZLICH

> „Die Cloud, Big Data, das Internet der Dinge (IoT) und zunehmend auch Container-Technologien erfreuen sich steigender Beliebtheit und könnten die Grundregeln der Sicherheit, nach denen Unternehmen traditionell funktionieren, außer Kraft setzen.“
>
> *—Garrett Bekker, Principal Analyst, Information Security bei 451 Research*

96% speichern oder verarbeiten vertrauliche Daten in neuen Umgebungen.

66% setzen in diesen Umgebungen keine Sicherheitslösungen zum Schutz vertraulicher Daten ein.

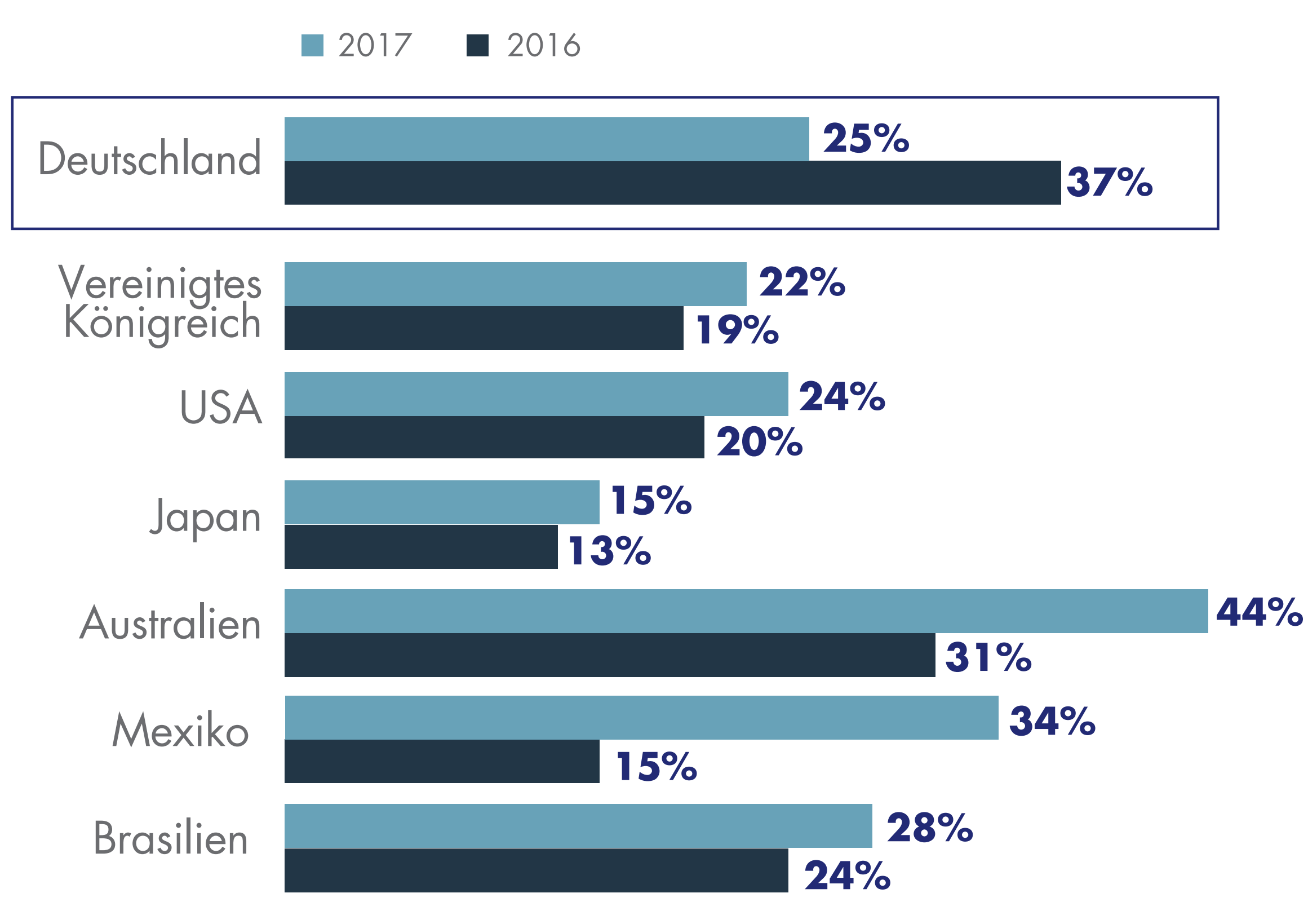
Einsatz neuer Technologien im Zusammenhang mit vertraulichen Daten in deutschen Unternehmen:



DIE GUTE NACHRICHT

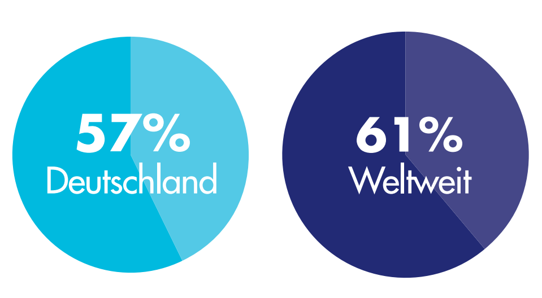
Deutsche Unternehmen fallen im Jahresvergleich weniger Datensicherheitsvorfällen zum Opfer, was in diesem Jahr keinem anderen Land gelungen ist

Sicherheitsvorfälle im vergangenen Jahr



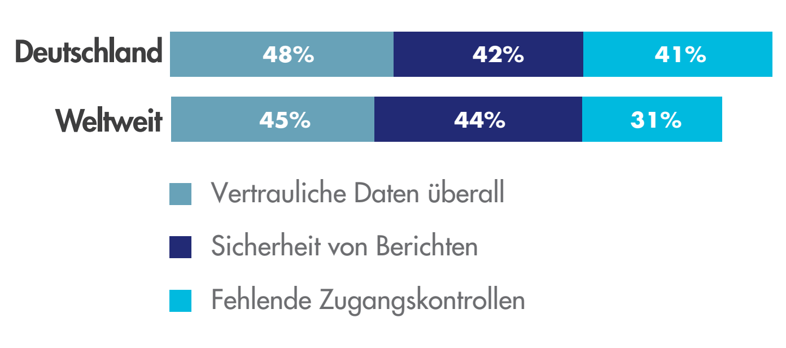
Einsicht, dass Verschlüsselung den digitalen Wandel und den Einsatz neuer Technologien ermöglicht

Cloud
Verschlüsselung ermöglicht eine verstärkte Nutzung der Cloud

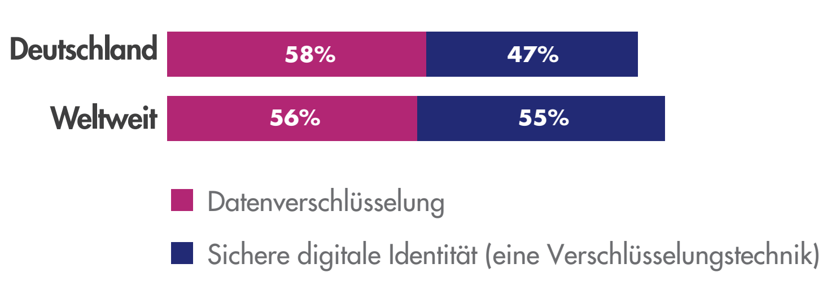


Datenverschlüsselung in der Cloud

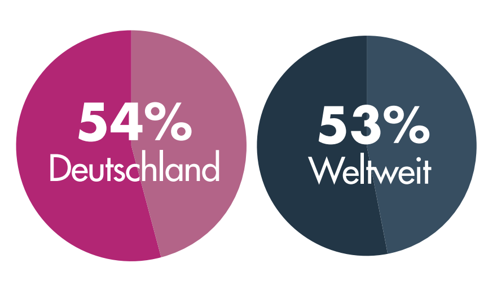
Big Data
Verschlüsselung löst die größten Sicherheitsprobleme



IoT
Die Technologien, die für einen verstärkten Einsatz am wichtigsten sind:



Container
Ein verstärkter Einsatz setzt Verschlüsselung als wichtigsten Kontrollmechanismus voraus



ES GIBT NOCH VIEL ZU TUN

1 NEUE SCHWERPUNKTE BEI IT-SICHERHEITS-LÖSUNGEN SETZEN

Traditionelle IT-Sicherheitsmodelle sind auf Cloud und SaaS nicht anwendbar: Datensicherheit in Form von Verschlüsselung und umgebungsübergreifenden Zugriffskontrollen ist erforderlich

Lösungen und Plattformen, die als Service zur Verfügung gestellt werden und Automatisierungsoptionen bieten, sind kostengünstiger und unkomplizierter und werden daher bevorzugt

2 DATEN AUSFINDIG MACHEN UND KLASSIFIZIEREN

Verschaffen Sie sich einen besseren Überblick über die Speicherorte vertraulicher Daten, insbesondere in Cloud-, Big-Data-, Container- und IoT-Umgebungen

3 COMPLIANCE NICHT NUR ALS BÜROKRATISCHE HÜRDE SEHEN

Setzen Sie unabhängig von Compliance-Anforderungen verstärkt auf Verschlüsselung und BYOK, insbesondere für die Cloud und andere neue Technologien

4 VERSCHLÜSSELUNG UND ZUGRIFFSKONTROLLE

Verschlüsselung darf nicht mehr nur auf Laptops und Desktop-PCs beschränkt sein

Rechenzentrum: Verschlüsselung und Zugriffskontrolle auf Datei- und Anwendungsebene

Cloud: Verschlüsselung und lokale Schlüsselverwaltung, BYOK als Voraussetzung für den sicheren Einsatz von SaaS, PaaS und IaaS

Big Data: Verschlüsselung und Zugriffskontrolle innerhalb der Umgebung

Container: Verschlüsselung und Kontrolle des Datenzugriffs innerhalb der Container und an deren Speicherorten

IoT: Sichere Gerätekennungen und Authentifizierung, Verschlüsselung von Data at Rest auf Geräten und in Back-End-Systemen und von Data in Motion, um Sicherheitsbedrohungen zu reduzieren

ZUM HERUNTERLADEN DES REPORTS KLICKEN

FOLGEN SIE UNS: