

DATEN IN GANZ EUROPA BEDROHT

DATENSCHUTZVERLETZUNGEN WERDEN IM ZUGE DER DIGITALEN TRANSFORMATION UND DER DARAUS RESULTIERENDEN AUSWEITUNG DER BEDROHUNGSLANDSCHAFTEN HÄUFIGER UND SCHMERZHAFTE FOLGEN EINES VERSAGENS BEIM SCHUTZ DER DATEN NEHMEN ZU.

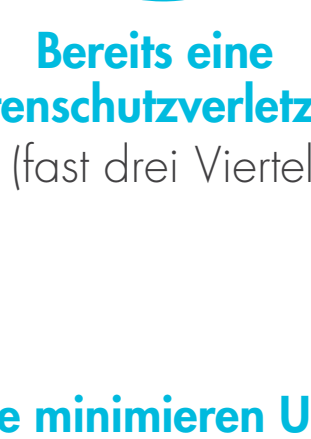
„UM ES DEUTLICH ZU MACHEN: WIE WIR DIE DINGE SEIT JAHRZEHNEN HANDHABEN, FUNKTIONIERT HEUTE NICHT MEHR: DIE WICHTIGSTE FRAGE, DIE SICH DIE IT UND FÜHRUNGSKRÄFTE DIESBEZÜGLICH STELLEN MÜSSEN, LAUTET: WAS MUSS GETAN WERDEN, UM DIE DATENSCHUTZVERLETZUNGEN ZU STOPPEN?“

— Garrett Bekker, 451 Research Principal Analyst, Informationssicherheit

In 8 Ländern wurden mehr als 1.200 Führungskräfte aus dem Bereich IT-Sicherheit befragt, darunter jeweils 100 in Großbritannien, Deutschland, Schweden und den Niederlanden

DATENSCHUTZVERLETZUNGEN SIND HEUTE AN DER TAGESORDNUNG

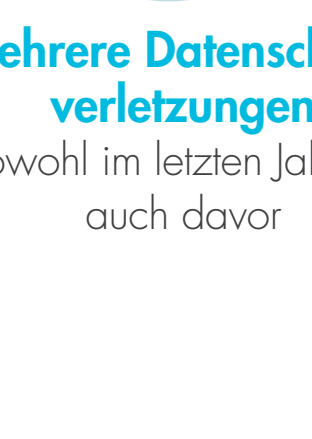
Eine Flut von Datenschutzverletzungen überschwemmt Europa. Nur wenige Unternehmen bleiben verschont und die Einführung der DSGVO erhöht die sich daraus ergebenden Risiken für Organisationen.



Bereits eine **Datenschutzverletzung** (fast drei Viertel)



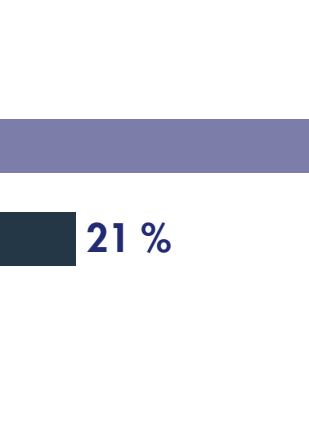
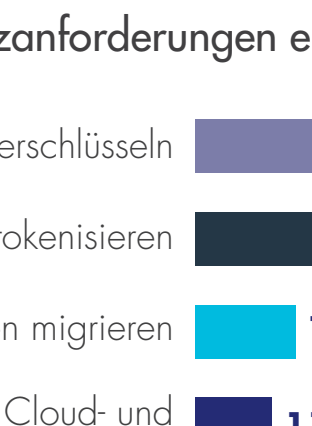
Datenschutzverletzung im letzten Jahr



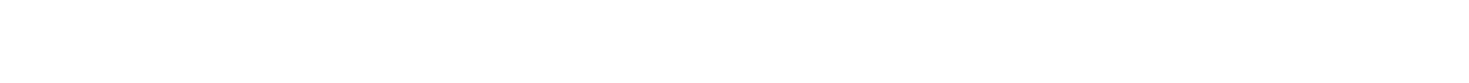
Mehrere Datenschutzverletzungen sowohl im letzten Jahr als auch davor

Wie minimieren Unternehmen diese Risiken?

Erhöhung der Ausgaben für IT-Sicherheit



Datenschutzanforderungen erfüllen



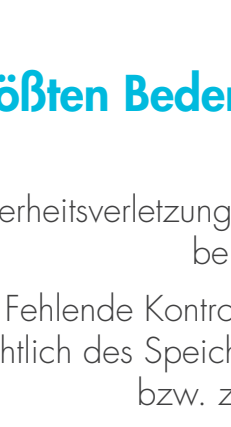
DIGITALE TRANSFORMATION ERWEITERT DATENBEDROHUNGSLANDSCHAFT



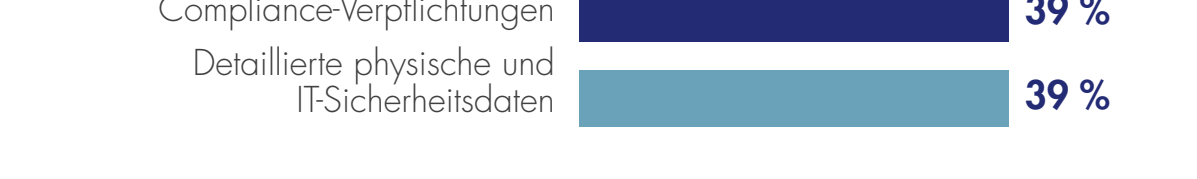
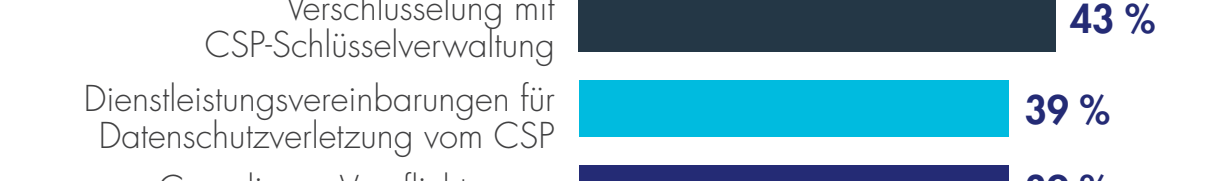
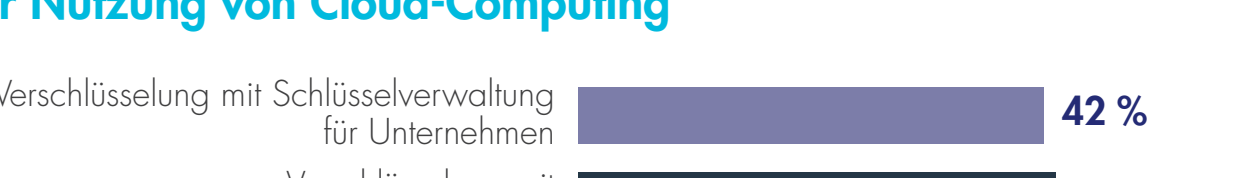
99 % nutzen digitale Transformations-technologien für **sensiblen Daten**

(Cloud, Big Data, IoT, Container, Blockchain oder mobile Zahlungen)

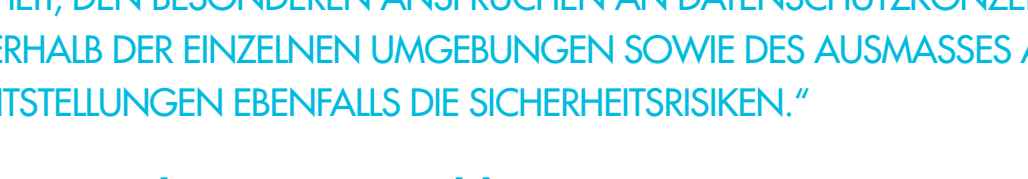
Hohe Multi-Cloud-Nutzung birgt zusätzliche Risiken



Die größten Bedenken hinsichtlich Cloud-Computing



Erforderliche IT-Sicherheits-Tools zur Ausweitung der Nutzung von Cloud-Computing



„DA UNTERNEHMEN ZUNEHMEND MIT MEHREREN CLOUD-ANBIETERN ARBEITEN, IST ES ZU EINEM ENORMEN POTENZIELLEN PROBLEM GEWORDEN, WER DIE KONTROLLE ÜBER DIE KRYPTOGRAPHISCHEN SCHLÜSSEL HAT – INSBESONDERE FÜR DIEJENIGEN, DIE SYSTEMEIGENE VERSCHLÜSSELUNGSDIENSTE NUTZEN.“

— Garrett Bekker, 451 Research Principal Analyst, Informationssicherheit

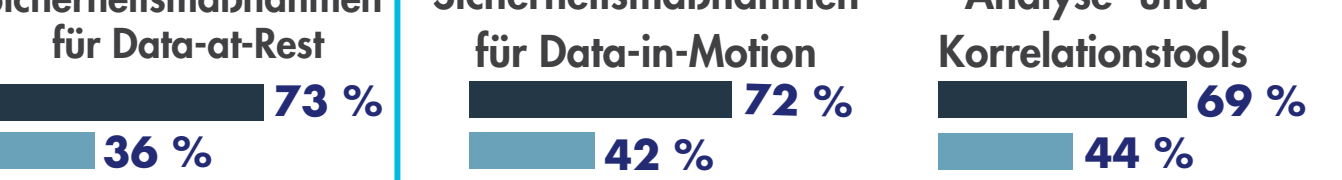
DIGITALE TRANSFORMATION ERHÖHT RISIKEN

„DER ALLGEMEINE EINSATZ VON CLOUD- UND SAAS-ANWENDUNGEN, BIG-DATA-IMPLEMENTIERUNGEN, IOT, CONTAINERN, MOBILLEN ZAHLUNGEN UND BLOCKCHAIN-TECHNOLOGIEN ERHÖHT AUFGRUND DER RELATIVEN NEUHEIT, DEN BESONDEREN ANSPRÜCHEN AN DATENSCHUTZKONZEPTE INNERHALB DER EINZELNEN UMGEBUNGEN SOWIE DES AUSMASSES AN BEREITSTELLUNGEN EBENFALLS DIE SICHERHEITSRISIKEN.“

Hohe Verwendung von sensiblen Daten in digitalen Transformationstechnologien

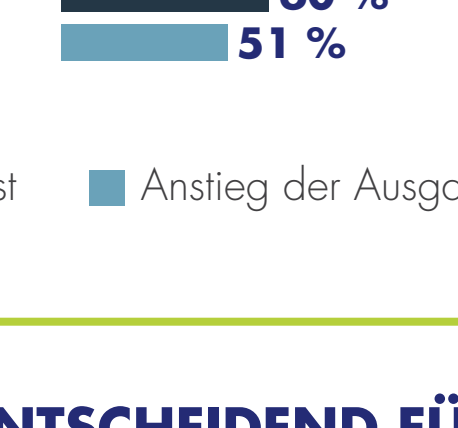


Prozentsatz der Befragten, die angaben, dass Ihre Unternehmen sensible Daten mit diesen Technologien verwenden.



Maschinelles Lernen – Vorteil oder Bedrohung?

Befragte sind der Ansicht, dass beides zutreffend sein kann

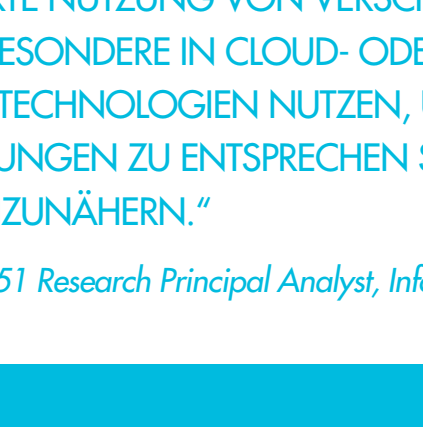


VIELE INVESTIEREN IHR GELD NICHT DORT, WO IHRE DATEN SIND

„OBWOHL SICHERHEITSMASSNAHMEN FÜR ENDPUNKTE UND MOBILE GERÄTE DAS SCHLUSSLICHT IN SACHEN EFFEKTIVITÄT BILDEN, LIEGEN SIE 2018 BEI DEN AUSGABENPRIORITÄTEN MIT 51 % GANZ VORNE, WÄHREND DATA-AT-REST-SICHERHEIT – DIE ALS BESONDERS EFFEKTIV BEWERTET WURDE – IN DEN AUSGABENPLÄNEN HINTEN ANSTEHT (36 %).“

— Garrett Bekker, 451 Research Principal Analyst, Informationssicherheit

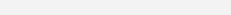
Die Befragten gaben an, dass ihre Unternehmen die Ausgaben für die effektivsten Tools zum Schutz von Daten am geringsten steigern



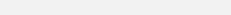
■ Als sehr oder äußerst effektiv bewertet ■ Anstieg der Ausgaben

VERSCHLÜSSELUNG IST ENTSCHEIDEND FÜR DIE LÖSUNG VON DATENSICHERHEITSPROBLEMEN

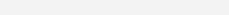
Verschlüsselung fördert digitale Transformation und traditionelle Datensicherheit



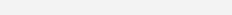
Container: Verfügbarkeit von Verschlüsselung fördert die Annahme



IoT: Sichere Authentifizierung (eine Verschlüsselungstechnologie) ist das wichtigste Tool für häufigeren Einsatz von IoT



Cloud: Datenverschlüsselung ist das wichtigste Tool für mehr Cloud-Nutzung



Big Data: Das wichtigste Tool für den Einsatz von Big Data – Fähigkeit, verschlüsselte/tokenisierte Daten zu analysieren

Verschlüsselung ist das wichtigste Tool, um weltweite Datenschutzrichtlinien wie die DSGVO zu erfüllen

der Befragten setzen Datenbank- und Dateiverschlüsselung jetzt ein

„UNTERNEHMEN SOLLTEN DIE VERMEHRTE NUTZUNG VON VERSCHLÜSSELUNG UND BYOK IN BETRACHT ZIEHEN – INSBESONDERE IN CLOUD- ODER SONSTIGEN UMGEBUNGEN, DIE FORTSCHRITTLICHE TECHNOLOGIEN NUTZEN, UM STEIGENDEN COMPLIANCE-ANFORDERUNGEN ZU ENTSPRECHEN SOWIE SICH DEN BEST PRACTICES DER BRANCHE ANZUNÄHERN.“

— Garrett Bekker, 451 Research Principal Analyst, Informationssicherheit

ÜBER THALES ESECURITY

Thales eSecurity ist führender Anbieter von fortschrittlichen Datensicherheitslösungen und -services, die überall dort Vertrauen schaffen, wo Daten erstellt, geteilt oder gespeichert werden. Wir stellen durch Verschlüsselung, Zugriffssteuerung, Datenaudit-Protokollierung, PKI sowie Zahlungstechnologien sicher, dass die Daten, die Unternehmen und Regierungsbehörden gehören, sowohl gesichert als auch vertraulich behandelt werden, und zwar im Unternehmen selbst, in der Cloud, in Rechenzentren oder Big-Data-Umgebungen, ohne dabei die Unternehmensprozesse einzuschränken.

LADEN SIE HIER DEN REPORT HERUNTER

FOLGEN SIE UNS:

