451 Research

Vormetric
A Thales company

VORMETRIC REPORT– IT SICHERHEITS-BEDROHUNGEN 2016

#2016DataThreat

INHALTSVERZEICHNIS

OUR SPONSORS

EINLEITUNG

In den vergangenen Jahren fielen Organisationen rund um den Globus einer scheinbar endlosen Kette von Sicherheitsvorfällen zum Opfer, die auch große Beachtung in den Medien fanden. Seither ist der Schutz sensibler Daten nicht mehr nur unter Sicherheitsexperten, sondern auch in der breiten Öffentlichkeit ein viel diskutiertes Thema. Nur mehr wenige Personen vertrauen darauf, dass Organisationen ausreichende Maßnahmen unternehmen, um die Sicherheit ihrer digital gespeicherten personenbezogenen Daten zu gewährleisten.

Es vergeht kaum eine Woche, in der nicht von einem weiteren verheerenden Sicherheitsvorfall berichtet wird. Laut der gemeinnützigen Organisation Privacy Rights Clearinghouse wurden im Jahr 2015 doppelt so viele Datensätze bei Sicherheitsvorfällen offengelegt wie 2014. Und das obwohl Organisationen jedes Jahr insgesamt mehrere Milliarden für unterschiedliche Formen der Cyber-Sicherheit ausgeben und Risikokapitalgeber fürstliche Summen in Startup-Unternehmen investieren, die neue Sicherheitsangebote anpreisen.

Doch in den vergangenen zwölf Monaten wurden wir schmerzlich daran erinnert, dass Datenbedrohungen nicht nur von bösartigen oder unvorsichtigen Insidern ausgehen. Viele der verheerendsten Attacken der jüngsten Vergangenheit gingen nicht allein von Insidern, sondern von unterschiedlichen externen Akteuren aus, darunter Cyber-Kriminelle, Staatsregierungen, Hacktivisten und Cyber-Terroristen. Sie verwenden häufig gestohlene Zugangsdaten, um sich als Insider auszugeben und alle möglichen wertvollen Daten wie personenbezogene, Gesundheits- und Finanzdaten sowie geistiges Eigentum zu entwenden. Da die Grenze zwischen „Insidern" und „Outsidern" zunehmend verschwimmt, schließt der Bericht zu Datenbedrohungen 2016 von Vormetric nun alle Arten von Bedrohungen für sensible Daten ein. Er stellt dar, welche Bedrohungen für Organisationen heute die größten Risiken darstellen, welche Maßnahmen sie dagegen ergreifen und was sie tun können, um sich besser gegen eine immer größere Anzahl von Widersachern zu schützen.

Diese Sonderausgabe des Berichts zu Datenbedrohungen 2016 ist auf den europäischen Markt, insbesondere Deutschland und das Vereinigte Königreich, zugeschnitten. Es werden sowohl Gemeinsamkeiten mit der globalen Ausgabe des Berichts als auch wichtige Unterschiede zu den USA und anderen Regionen wie Australien, Brasilien, Mexiko und Japan aufgezeigt.

ALTE SICHERHEITSGEWOHNHEITEN LASSEN SICH NUR SCHWER ABLEGEN

Insgesamt lieferten unsere weltweiten Umfragen eine Mixtur aus guten und weniger guten Ergebnissen, die deutlich machten, dass Sicherheitsexperten in vielerlei Hinsicht wie Generäle sind, die mit alten Waffen gegen neue Feinde kämpfen. Laut Schätzungen des IT-Marktforschungs- und Beratungsunternehmens 451 Research geben Organisationen jährlich fast 35 Milliarden Euro für Informationssicherheits-Produkte aus, wobei der Löwenanteil in veraltete Sicherheitstechnologien wie Firewalls, Antiviren- und Intrusion-Prevention-Software investiert wird. Gleichzeitig verstärkt sich die Häufigkeit und Schwere von Sicherheitsvorfällen kontinuierlich. Es besteht eindeutig nach wie vor eine Diskrepanz zwischen den Produkten, für die Unternehmen den Großteil ihres Sicherheitsbudgets ausgeben, und den Maßnahmen, die für den Schutz sensibler Daten wirklich nötig wären.

So zeigen beispielsweise die Ergebnisse unseres globalen Berichts 2016, dass gerne Geld für Dinge ausgegeben wird, die in der Vergangenheit funktioniert haben (oder auch nicht), wie Netzwerk- und Endgeräte-Sicherheitssoftware. Dies gilt auch für das Vereinigte Königreich, wo das Budget für die nächsten zwölf Monate am deutlichsten im Bereich Netzwerksicherheit erhöht wurde (42 Prozent). In puncto Effektivität belegten dort Netzwerksicherheitsprodukte zusammen mit Schutzmaßnahmen für „Data in Motion" den dritten Platz (69 Prozent), während „Data at Rest" auf dem ersten Platz landete (75 Prozent). Dabei war das Vereinigte Königreich das einzige Land, in dem die Sicherheit für „Data at Rest" als effektivste Maßnahme für den Schutz sensibler Daten eingestuft wurde. Leider zeigt sich der britische Optimismus im Hinblick auf die Datensicherheit noch nicht bei den Ausgaben: Bei der Budgetplanung für die kommenden zwölf Monate wurden Schutzmaßnahmen für „Data at Rest" eher hinten angestellt (34 Prozent). Nur Abwehrmaßnahmen für „Data in Motion" wurde eine noch niedrigere Priorität eingeräumt (30 Prozent). Wie in den meisten Regionen lösten auch im Vereinigten Königreich die Themen Komplexität, Personalmangel und Leistungsprobleme die größten Bedenken aus, wenn es um die Einführung von Datensicherheitsstrategien geht. Darauf wird weiter unten im Detail eingegangen.

In Deutschland hingegen wurden Netzwerksicherheitsprodukte als effektivste Datensicherheitsmaßnahme eingestuft: 81 Prozent der Befragten bewerteten Netzwerksicherheit für den Schutz sensibler Daten als „sehr" oder „äußerst" effektiv. Sicherheitsmaßnahmen für „Data at Rest" fielen dagegen auf den dritten Platz (68 Prozent). Bei der Budgetplanung schafften es Netzwerksicherheitsprodukte nur auf den vierten Platz: Lediglich 35 Prozent der deutschen Umfrageteilnehmer planen, ihre Ausgaben in diesem Bereich in den kommenden zwölf Monaten zu erhöhen – eines der weltweit niedrigsten Ergebnisse in diesem Punkt. Die Aussichten für Datensicherheitsausgaben sind in Deutschland jedoch deutlich besser. Während die Sicherheit von „Data at Rest" bei der Budgetplanung in vielen Regionen relativ weit hinten angestellt wurde, belegte die Kategorie in Deutschland den zweiten Platz (37 Prozent).

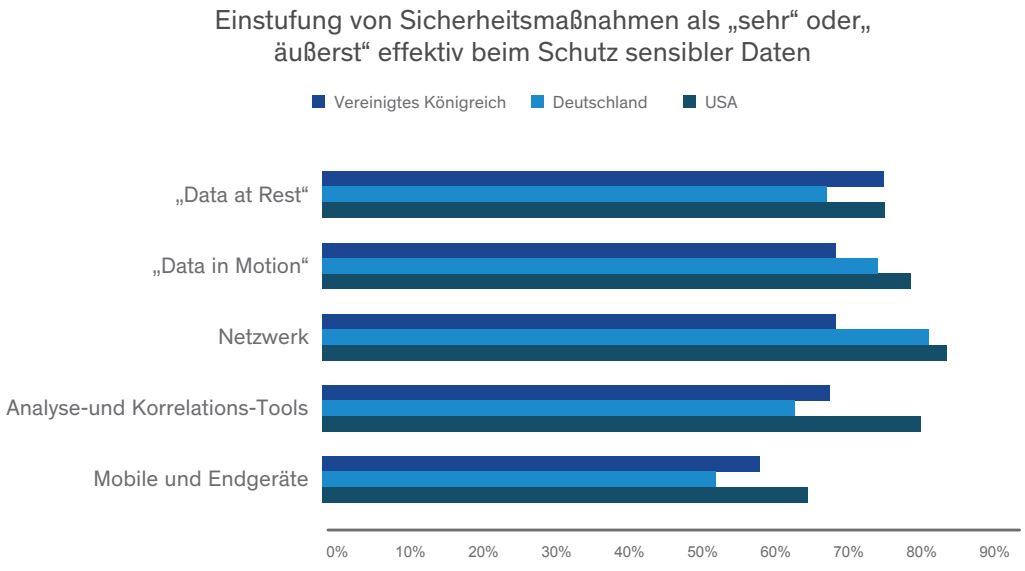

Diagramm 1: Einstufung von Sicherheitsmaßnahmen als „sehr" oder „äußerst" effektiv beim Schutz sensibler Daten

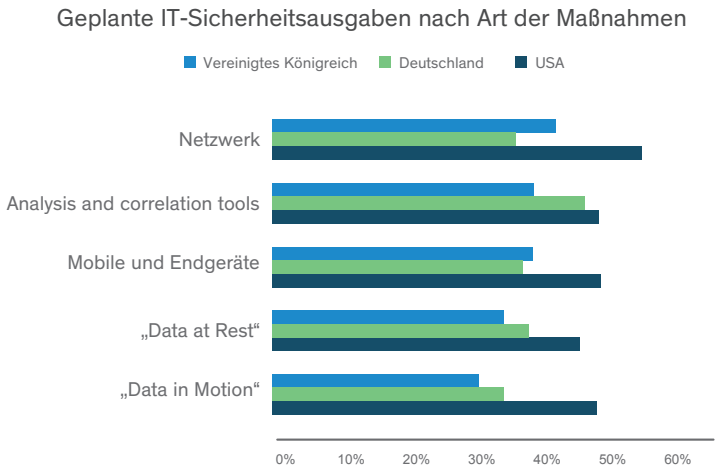

Diagramm 2: Geplante IT-Sicherheitsausgaben nach Art der Maßnahmen

Wir hoffen, dass die gesamte Sicherheitsbranche – insbesondere in Deutschland und im Vereinigten Königreich – sich mit der Zeit der Tatsache bewusst wird, dass Produkte für den Perimeterschutz nur wenig gegen Multi-Stage-Attacken ausrichten können. Wenn Daten geschützt werden sollen, nachdem der Perimeterschutz umgangen wurde, haben sich Ansätze mit Datei- und Anwendungsverschlüsselung sowie Zugriffskontrollen als effektiv erwiesen, und es steht zu hoffen, dass diesen bald mehr Aufmerksamkeit – und ein angemessenes Budget – gewährt wird.

DEUTSCHE FÜHLEN SICH BESONDERS ANGREIFBAR

Deutschland und das Vereinigte Königreich unterscheiden sich auch sehr stark, wenn es um eingetretene Datensicherheitsvorfälle und die wahrgenommene Angreifbarkeit geht. In Deutschland gaben 72 Prozent der Befragten an, bereits Opfer eines Sicherheitsvorfalls geworden zu sein. Nur in Australien ist diese Zahl mit 85 Prozent noch höher. Außerdem berichteten 37 Prozent der deutschen Unternehmen, allein im vergangenen Jahr Opfer eines Sicherheitsvorfalls geworden zu sein. Diese Zahl ist höher als in allen anderen Regionen und liegt deutlich über dem weltweiten Durchschnitt von 22 Prozent. So ist es wenig überraschend, dass sich die deutschen Umfrageteilnehmer relativ bedroht fühlen: 40 Prozent gaben an, sich im Hinblick auf Datenbedrohungen von innen und außen „sehr“ oder „äußerst“ angreifbar zu fühlen.

Im Vereinigten Königreich berichteten dagegen 64 Prozent der Befragten, dass sie schon einmal einem Sicherheitsvorfall zum Opfer gefallen waren (leicht über dem weltweiten Durchschnitt von 61 Prozent). Allerdings fühlen sich die britischen Umfrageteilnehmer deutlich weniger bedroht als ihre deutschen Kollegen: Nur 23 Prozent bezeichneten sich im Hinblick auf Datenbedrohungen als „sehr“ oder „äußerst“ angreifbar. Damit liegen sie unter dem weltweiten Durchschnitt von 30 Prozent. Darüber hinaus waren die Studienteilnehmer im Vereinigten Königreich trotz des Hacker-Angriffs auf TalkTalk im Jahr 2015 am wenigsten dazu bereit, ihre Ausgaben für Verschlüsselung und Datensicherheit aufgrund eines bekannten Sicherheitsvorfalls zu erhöhen (46 Prozent im Vergleich zu 49 Prozent in Deutschland, 64 Prozent in den USA und 53 Prozent im weltweiten Durchschnitt).

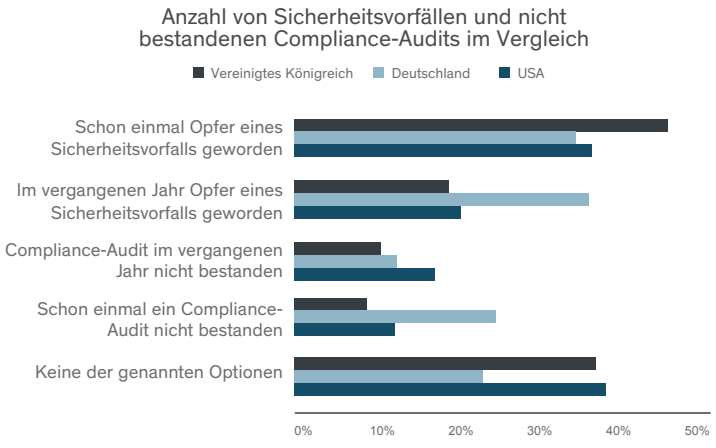

Diagramm 3: Anzahl von Sicherheitsvorfällen und nicht bestandenen Compliance-Audits im Vergleich

DIE WICHTIGSTEN ERGEBNISSE:

Es gibt noch viel zu tun

- Im Vereinigten Königreich steht das Thema Netzwerksicherheit bei den Ausgabeprioritäten für die kommenden zwölf Monate an erster Stelle (42 Prozent), während der Schutz von „Data at Rest" den vorletzten Platz belegt (34 Prozent).

- In Deutschland erachteten 81 Prozent der Befragten Netzwerk-Sicherheitsmaßnahmen als „sehr" oder „äußerst" effektiv für den Schutz sensibler Daten.

- 72 Prozent der Studienteilnehmer in Deutschland und 63 Prozent im Vereinigten Königreich sind bereits Opfer eines Sicherheitsvorfalls geworden. Der weltweite Durchschnitt beträgt hier lediglich 61 Prozent. 37 Prozent der deutschen Befragten berichteten, dass sie allein im vergangenen Jahr einem Sicherheitsvorfalls zum Opfer gefallen seien. Diese Zahl ist höher als in allen anderen Regionen und liegt deutlich über dem weltweiten Durchschnitt von 22 Prozent.

- 40 Prozent der deutschen Umfrageteilnehmer fühlten sich im Hinblick auf Bedrohungen von innen und außen „sehr" oder „äußerst" angreifbar.

- 67 Prozent der Befragten in Deutschland erachteten Compliance-Anforderungen als „sehr" oder „äußerst" effektiv, um Datensicherheitsvorfälle zu verhindern. Der weltweite Durchschnitt liegt bei 64 Prozent.

  Es gab jedoch durchaus auch motivierende Ergebnisse. Beispielweise war der Anteil der Befragten im Vereinigten Königreich am höchsten (59 Prozent), die die Einführung von Best Practices als strategischen Grund für den Einsatz von Verschlüsselung wählten (vs. 53 Prozent im weltweiten Durchschnitt). Britische Umfrageteilnehmer stuften zudem die Sicherheit von „Data at Rest" als effektivste Möglichkeit für den Schutz sensibler Daten ein (75 Prozent).

  Darüber hinaus mehren sich die Anzeichen dafür, dass die Befragten in Deutschland und im Vereinigten Königreich die Implementierung „neuerer" Sicherheitstools planen. Zu den Kategorien mit den größten geplanten Budgeterhöhungen im Datensicherheitsbereich in Deutschland gehören Mehrfaktor-Authentifizierung (54 Prozent), Identitätsverwaltung für privilegierte Benutzer (47 Prozent) und SIEM- sowie Analyse-Tools (45 Prozent). Im Vereinigten Königreich lagen hier Verschlüsselung auf Anwendungsebene (52 Prozent), Tokenisierung (49 Prozent) und Mehrfaktor-Authentifizierung (44 Prozent) vorne. Insgesamt machen Deutschland und das Vereinigte Königreich vieles richtig – sie müssten nur noch mehr tun.

Was Organisationen richtig machen

- Im Vereinigten Königreich wurde die Sicherheit von „Data at Rest" als effektivstes Mittel für den Schutz sensibler Daten eingestuft (75 Prozent).

- Für deutsche Befragte waren Best Practices der wichtigste Grund für den Einsatz von Verschlüsselung (48 Prozent vs. 53 Prozent im weltweiten Durchschnitt).

- 42 Prozent der Umfrageteilnehmer in Deutschland und 53 Prozent im Vereinigten Königreich planen, Verschlüsselung auf Anwendungsebene einzuführen (vs. 40 Prozent im weltweiten Durchschnitt).

- 49 Prozent der Befragten im Vereinigten Königreich haben vor, Tokenisierung einzuführen – das höchste Ergebnis aller Regionen, das deutlich über dem weltweiten Durchschnitt von 39 Prozent liegt.

- Deutschland (40 Prozent) und das Vereinigte Königreich (41 Prozent) waren unter den Ländern mit den höchsten geplanten Budgets für Cloud-Verschlüsselungs-Gateways (vs. 38 Prozent im weltweiten Durchschnitt).

  In den folgenden Abschnitten werden wichtige Themen in Bezug auf Deutschland und das Vereinigte Königreich aufgezeigt und interessante Beispiele für Fälle genannt, in denen sich die beiden Länder von anderen Regionen unterschieden.

"IM VEREINIGTEN KÖNIGREICH WURDE DIE SICHERHEIT VON „DATA AT REST" ALS EFFEKTIVSTES MITTEL FÜR DEN SCHUTZ SENSIBLER DATEN EINGESTUFT (75 PROZENT)."

ÜBER DIESEN BERICHT

Der Bericht zu Datenbedrohungen 2016 von Vormetric basiert auf einer Studie, die im Oktober und November 2015 von 451 Research durchgeführt wurde. Dabei wurden aus jeder Region mehr als 100 Führungskräfte aus dem IT-Sicherheitsbereich befragt. In diesem Bericht werden die Ergebnisse kurz zusammengefasst und gegebenenfalls mit Resultaten aus anderen wichtigen Regionen wie den USA, Lateinamerika und dem Asien-Pazifik-Raum (APAC) verglichen.

Compliance ist NICHT gleich Sicherheit, auch wenn sich die Geister in Deutschland und dem Vereinigten Königreich scheiden

Viele Sicherheitsexperten rund um den Globus scheinen Compliance nach wie vor mit Sicherheit gleichzusetzen. Fast zwei Drittel (64 Prozent) der Befragten weltweit erachteten Compliance-Anforderungen als „sehr" bzw. „äußerst" effektiv bei der Verhinderung von Sicherheitsvorfällen (vs. 59 Prozent im vergangenen Jahr). Während Compliance jedoch als Ansatzpunkt oder Basis für jedes Informationssicherheits-Programm dienen kann, macht die stetig zunehmende Anzahl von Datenschutzverletzungen deutlich, dass wir für den Schutz unserer Daten weitaus mehr tun müssen, als schlicht das Thema Compliance abzuhaken.

Doch auch im Bereich Compliance gingen die Einschätzungen in Deutschland und im Vereinigten Königreich auseinander. Deutschland gehört hier zu den optimistischsten Regionen: 67 Prozent der Befragten erachteten Compliance-Anforderungen als „sehr" oder „äußerst" effektiv bei der Verhinderung von Sicherheitsvorfällen. Damit lag das Land über dem weltweiten Durchschnitt von 64 Prozent und wurde nur von Brasilien (83 Prozent) und Australien (68 Prozent) überboten. In Deutschland haben in der Vergangenheit jedoch mehr Organisationen ein Compliance-Audit nicht bestanden (36 Prozent) als in den meisten anderen Regionen. Nur in Australien ist diese Zahl höher (mit 61 Prozent ein bemerkenswerter Ausreißer). Der weltweite Durchschnitt liegt bei 32 Prozent.

So ist es wenig erstaunlich, dass Compliance in Deutschland als Hauptgrund für den Schutz sensibler Daten angesehen wird (47 Prozent). Dies entspricht genau dem weltweiten Durchschnitt. Durchaus überraschend war jedoch, dass nur 39 Prozent der Befragten in Deutschland Compliance als Cloud-Sicherheitsproblem erachteten. Damit ist es das am niedrigsten eingestufte Cloud-Problem in Deutschland, deutlich unter dem weltweiten Durchschnitt von 62 Prozent. Bemerkenswert war zudem, dass 47 Prozent der Teilnehmer Anforderungen von Geschäftspartnern, Kunden und potenziellen Neukunden als genauso wichtig erachteten wie Compliance-Vorschriften. Damit liegt Deutschland deutlich über dem weltweiten Durchschnitt von 37 Prozent und direkt hinter Spitzenreiter Japan (50 Prozent). Dies könnte zum Teil den wachsenden Befürchtungen in Europa geschuldet sein, wegen des mangelnden Schutzes von Kundendaten öffentlich an den Pranger gestellt zu werden. Die Einführung von Best Practices war in Deutschland der dritthäufigste Grund für den Schutz sensibler Daten (39 Prozent). Diese Zahl liegt etwas unter dem weltweiten Durchschnitt von 44 Prozent. Zudem hatte Deutschland unter allen Regionen die wenigsten Bedenken in puncto Reputations- und Markenschutz (33 Prozent), während im weltweiten Durchschnitt hier die größten Befürchtungen liegen (51 Prozent). Abgesehen von den japanischen Studienteilnehmern wählten die deutschen Befragten am seltensten den Reputations- und Markenschutz als strategischen Faktor für den Einsatz von Verschlüsselung.

Was die Effektivität von Compliance-Anforderungen angeht, liegt das Vereinigte Königreich am entgegengesetzten Ende des Spektrums: Lediglich 61 Prozent erachten Compliance-Vorschriften hier als „sehr" oder „äußerst" effektiv, gefolgt von den Schlusslichtern Mexiko (57 Prozent) und Japan (33 Prozent). Für britische Befragte ist Compliance nach wie vor einer der wichtigsten Gründe für den Schutz sensibler Daten (47 Prozent, dem weltweiten Durchschnitt entsprechend). Der Hauptgrund für den Schutz sensibler Daten im Vereinigten Königreich ist der Reputations- und Markenschutz (50 Prozent vs. 51 Prozent im weltweiten Durchschnitt).

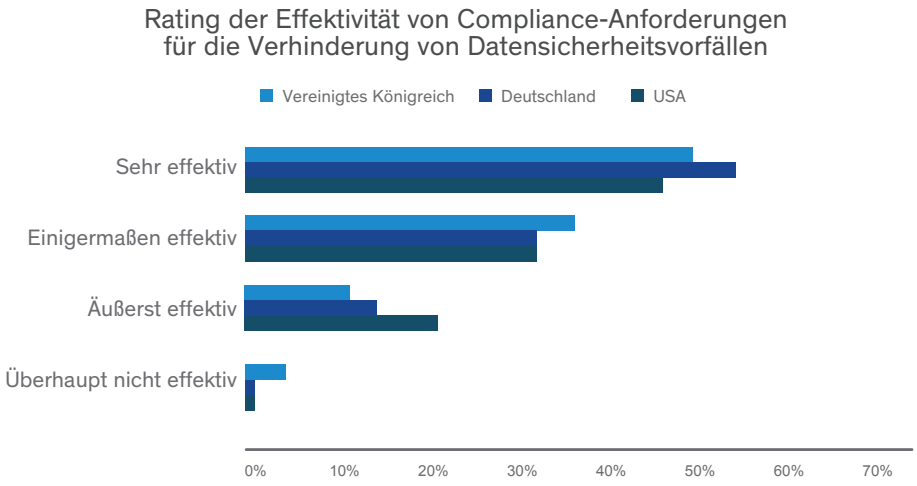

Diagramm 4: Rating der Effektivität von Compliance-Anforderungen für die Verhinderung von Datensicherheitsvorfällen

DERZEIT IN DER DISKUSSION STEHENDE REGELUNGEN ZUR DATENHOHEIT KÖNNTEN DIE DATENSICHERHEIT VERBESSERN, INSBESONDERE MASSNAHMEN WIE VERSCHLÜSSELUNG, DATENMASKIERUNG UND TOKENISIERUNG

Compliance-Vorschriften können zwar als effektive Basis dienen, doch viele von ihnen sind zu ungenau. Vorschriften mit detaillierten Sicherheitsanforderungen hingegen veralten aufgrund der sich rasch entwickelnden Technologien und Angriffsmethoden häufig bereits nach kurzer Zeit. Die kürzlich von der EU verabschiedete Datenschutz-Grundverordnung (DS-GVO) wird jedoch höhere Sicherheitsstandards für Unternehmen und Sicherheitsexperten einführen. Die DS-GVO hat zwar viele Nuancen, scheint jedoch eine größere Durchschlagskraft als viele andere Compliance-Vorschriften zu haben. So sieht sie zum Beispiel hohe Geldstrafen für Organisationen vor, die die ihnen anvertrauten Daten nicht ausreichend schützen. Die DS-GVO nennt außerdem einige Sicherheitsmaßnahmen, die Unternehmen ergreifen können, um ihr Gesamtrisiko zu senken, wie Verschlüsselung, Datenmaskierung und Tokenisierung.

Neben der DS-GVO gibt es in Ländern wie Kanada und Australien, die großen Wert auf Datenschutz legen, sowie in Asien und Lateinamerika etwa 100 nationale und regionale Gesetze, die den Schutz personenbezogener Daten vorschreiben. Deshalb haben wir in der diesjährigen Umfrage mehrere Fragen gestellt, um herauszufinden, welche Bedeutung den Themen Datenschutz und Datenhoheit beigemessen wird.

Die Einhaltung lokaler Datenhoheits-Vorschriften wurde weltweit als viertwichtigster Grund für die Verschlüsselung von Daten eingestuft (38 Prozent), hinter Best Practices, Compliance-Anforderungen (PCI, HIPAA etc.) und der Vermeidung von Reputationsschäden. Interessanterweise wurde das Thema Datenhoheit in Deutschland, dem Vereinigten Königreich und Japan mit jeweils 33 Prozent unter allen Regionen am niedrigsten eingestuft. Man könnte jedoch argumentieren, dass die DS-GVO in gleichem Maße – wenn nicht noch mehr – auf Nicht-EU-Länder wie die USA abzielt.

Im Zusammenhang mit Cloud-Ressourcen kamen Bedenken hinsichtlich der Datenhoheit deutlicher zum Ausdruck. Auf die Frage nach den größten Sicherheitsproblemen im Zusammenhang mit der Nutzung der öffentlichen Cloud wurde die Datenhoheit im weltweiten Durchschnitt als drittgrößtes Problem gewertet (65 Prozent), nach Sicherheitsvorfällen bei Cloud-Anbietern und Problemen durch gemeinsam genutzte Infrastrukturen. Im Vereinigten Königreich wurde die Datenhoheit dagegen als größtes (66 Prozent), in Deutschland als zweitgrößtes Problem (60 Prozent) angesehen. Genauso wurden Datenschutzverletzungen durch in unterschiedlichen Ländern gespeicherte Daten im Zusammenhang mit Big Data weltweit an dritter Stelle (40 Prozent), im Vereinigten Königreich jedoch an erster Stelle (43 Prozent) und in Deutschland an zweiter Stelle (44 Prozent) eingestuft.

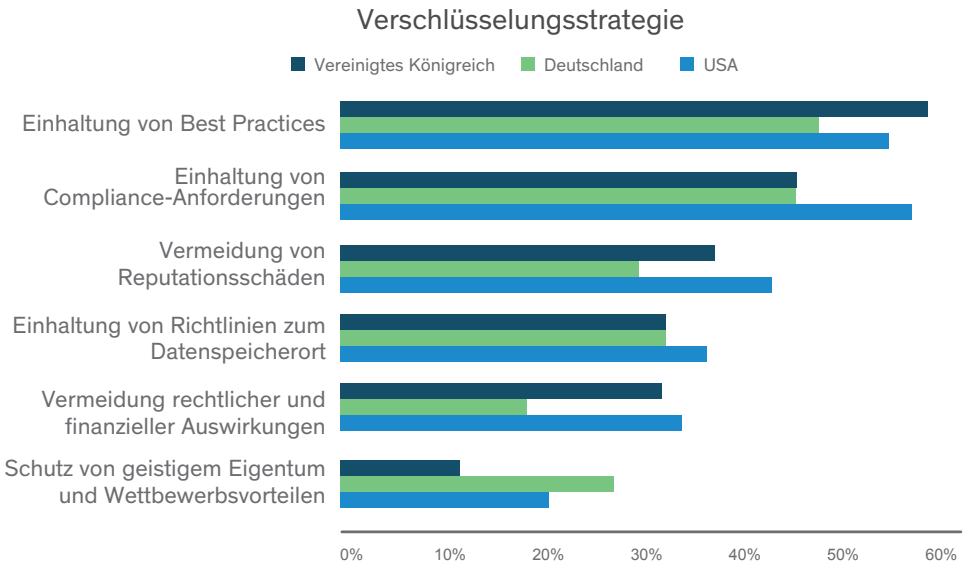

Diagramm 5: Verschlüsselungsstrategien – Gründe für den Einsatz von Verschlüsselung in Organisationen

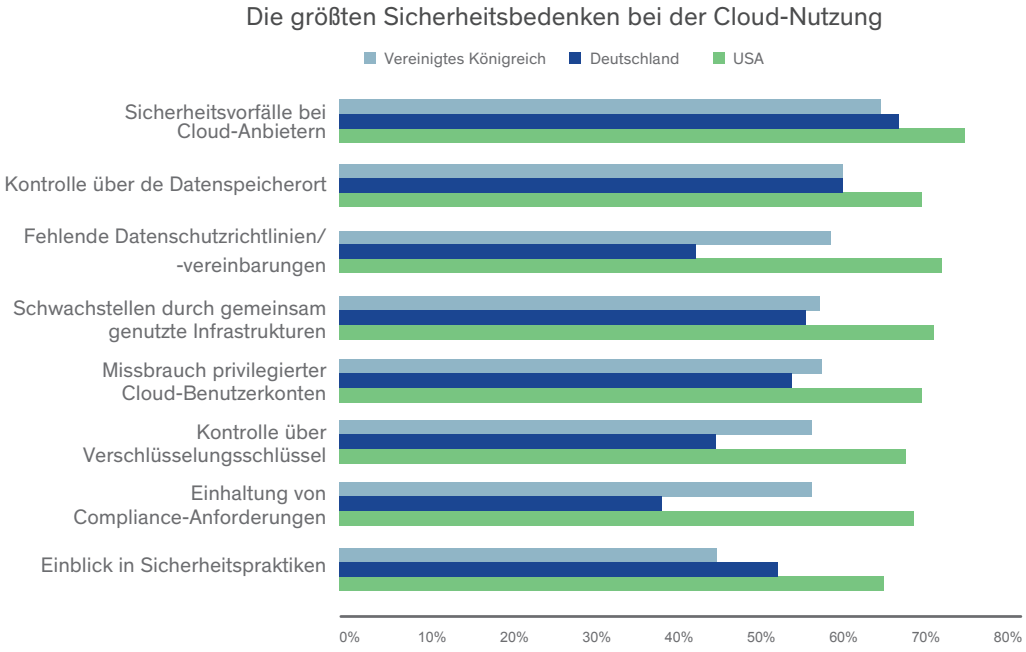

Diagramm 6: Die größten Sicherheitsbedenken bei der Cloud-Nutzung

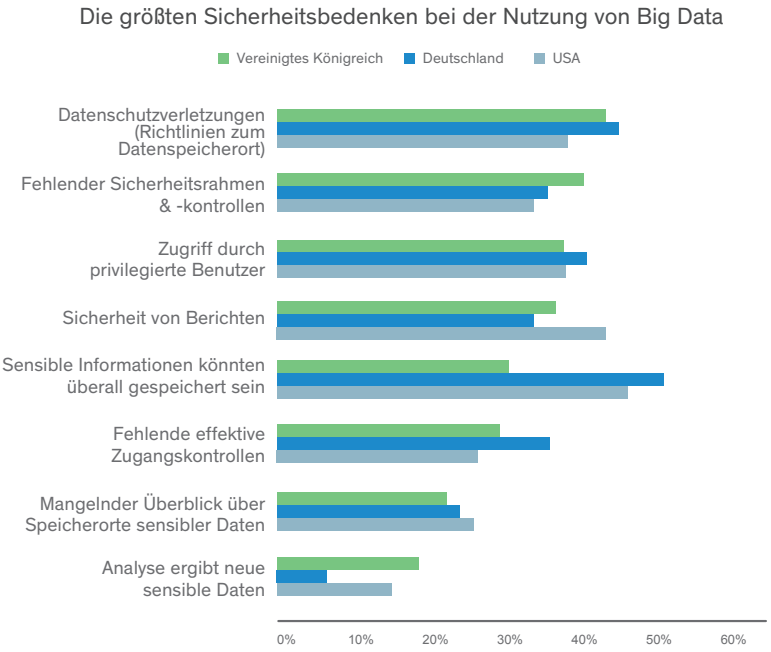

Diagramm 7: Die größten Sicherheitsbedenken bei der Nutzung von Big Data

KOMPLEXITÄT ALS GRÖSSTE DATENSICHERHEITSBARRIERE – AUCH IN DEUTSCHLAND UND IM VEREINIGTEN KÖNIGREICH

Die Installation und Wartung von Datensicherheitslösungen wird häufig als schwierig erachtet. Die Komplexität der Implementierung hängt jedoch stark von der jeweiligen Art der geschützten Daten ab und davon, wo im IT-Stack die Lösung bereitgestellt wird, also auf Festplatten-, Datei- oder Anwendungsebene. Folglich wurde „Komplexität" in beiden Ländern als größte Barriere für die umfassendere Einführung von Datensicherheitsstrategien eingestuft. In Deutschland war diese Zahl mit 71 Prozent besonders eindeutig. Im Vereinigten Königreich betrug sie 56 Prozent, der weltweite Durchschnitt 57 Prozent. Komplexe Bereitstellungen bringen in der Regel auch einen erhöhten Personalbedarf mit sich. So wurde „Fehlendes Personal für die Verwaltung" im weltweiten Durchschnitt (38 Prozent) sowie in Deutschland (35 Prozent) als zweitgrößte Barriere genannt. Die Studienteilnehmer im Vereinigten Königreich dagegen hatten unter allen Regionen die geringsten Bedenken hinsichtlich des Personalbedarfs (29 Prozent). Sie sorgten sich mehr über die möglichen Auswirkungen der Datensicherheit auf die Systemleistung und Geschäftsprozesse (33 Prozent).

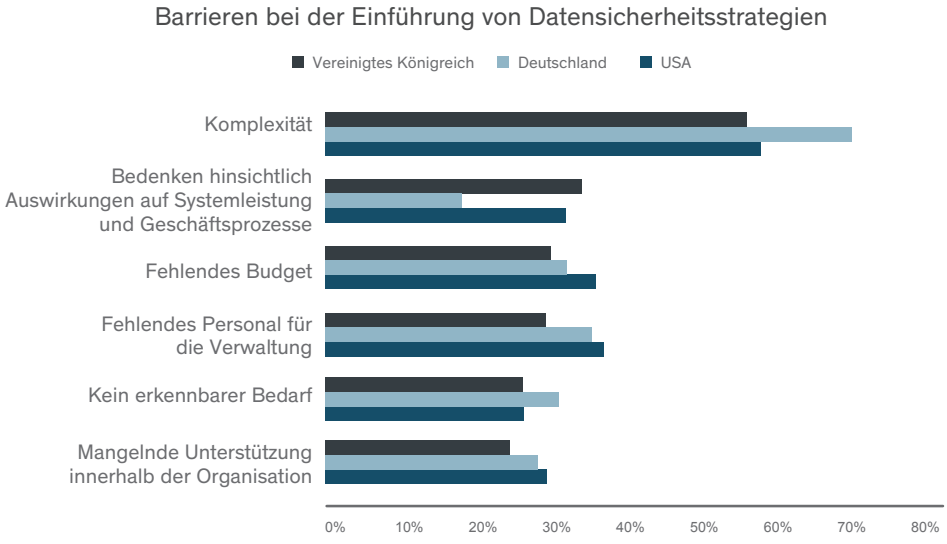

Diagramm 8: Barrieren bei der Einführung von Datensicherheitsstrategien

DEUTSCHLAND UND VEREINIGTES KÖNIGREICH AM MISSTRAUISCHSTEN GEGENÜBER INSIDERN MIT ERHÖHTEN RECHTEN, JEDOCH GROSSE UNTERSCHIEDE BEI ANDEREN INSIDER-BEDROHUNGEN

Was Risiken für sensible Daten durch Insider angeht, klafften die Ansichten in Deutschland und im Vereinigten Königreich insbesondere in Bezug auf normale Mitarbeiter und Top-Führungskräfte erneut auseinander. Wie die meisten Regionen identifizierten zwar auch Deutschland (58 Prozent) und das Vereinigte Königreich (59 Prozent) Insider mit erhöhten Rechten als größte Bedrohung, was dem weltweiten Durchschnitt entspricht (58 Prozent). Das Vereinigte Königreich lag auch mit seiner zweithäufigsten (Top-Führungskräfte, 39 Prozent) und dritthäufigsten Antwort (Konten von Lieferanten, 38 Prozent) im weltweiten Durchschnitt.

Für die Befragten in Deutschland waren dagegen normale Mitarbeiter ein größerer Grund zur Besorgnis (45 Prozent vs. 33 Prozent im weltweiten Durchschnitt) als für jedes andere Land außer Japan (ebenfalls 45 Prozent). Deutschland sieht unter allen Regionen zudem das geringste Problem in Top-Führungskräften (30 Prozent vs. 45 Prozent im weltweiten Durchschnitt). Nur Japan sah die Sache ähnlich (36 Prozent).

Cyber-Kriminelle gelten sowohl in Deutschland (84 Prozent) als auch im Vereinigten Königreich (81 Prozent) als die größten externen Bedrohungsakteure. Damit liegen die beiden Länder leicht über dem weltweiten Durchschnitt von 79 Prozent. „Hacktivisten" landeten in beiden Ländern auf dem zweiten Platz, obwohl die Befragten im Vereinigten Königreich (72 Prozent) sich hier mehr Sorgen zu machen scheinen als in Deutschland (64 Prozent). Der weltweite Durchschnitt lag bei 66 Prozent.

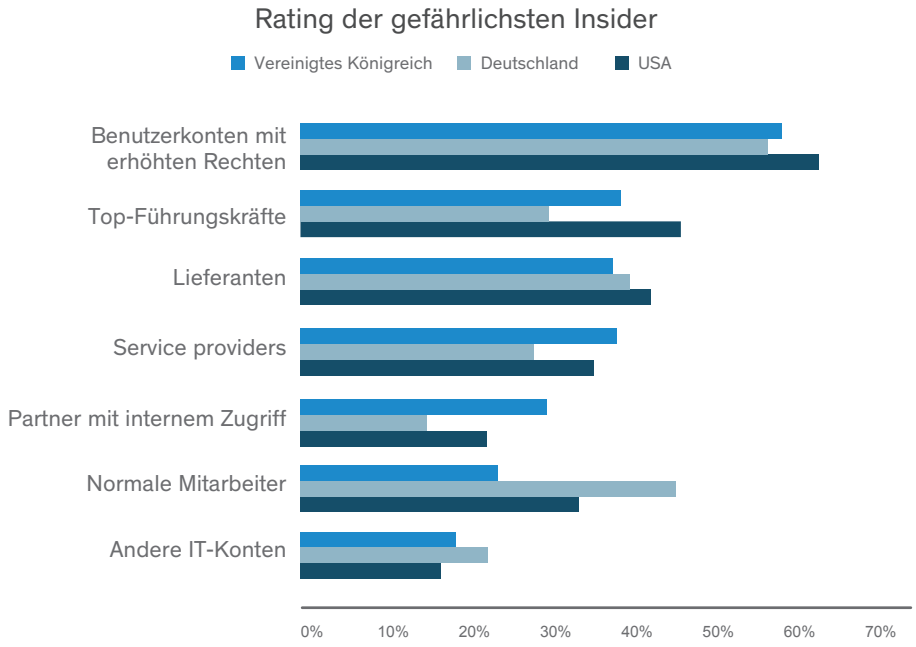

Diagramm 9: Rating der gefährlichsten Insider (Auswahl der drei größten Risikoakteure)

NEUE HERAUSFORDERUNGEN DURCH DIE CLOUD, BIG DATA UND DAS INTERNET DER DINGE (IOT)

Die speziellen Sicherheitsherausforderungen von Big Data, Cloud-Computing und dem Internet der Dinge (IoT) wurden auf verschiedenste Weise angegangen. In allen drei Fällen werden Ressourcen genutzt, die sich großteils außerhalb herkömmlicher Unternehmensserver vor Ort befinden. Deshalb sind ältere Sicherheits-Tools und Ansätze, bei denen der Parameter geschützt wird, um die bisherige Vorstellung von „intern" vs. „extern" durchzusetzen, dieser Aufgabe nicht mehr gewachsen. Gleichzeitig werden Sicherheitsbedenken immer wieder als Hauptbarriere für die umfassendere Nutzung dieser neuen Modelle genannt.

Die Cloud

Auch in puncto Cloud-Ressourcen waren die Ansichten in Deutschland und im Vereinigten Königreich sehr unterschiedlich. Insgesamt deuten die Antworten aus dem Vereinigten Königreich auf eine konservativere Einstellung gegenüber öffentlichen Cloud-Ressourcen als in den restlichen Regionen hin, insbesondere im Vergleich zu Ländern wie Brasilien und Mexiko, deren Pläne für die öffentliche Cloud zu den aggressivsten gehören. So lagen die Pläne der britischen Umfrageteilnehmer zur Speicherung sensibler Daten in der öffentlichen Cloud im Hinblick auf drei wichtige Bereitstellungsmodellen unter dem weltweiten Durchschnitt: SaaS (Vereinigtes Königreich 44 Prozent, weltweit 53 Prozent); IaaS (Vereinigtes Königreich 50 Prozent, weltweit 53 Prozent) und PaaS (Vereinigtes Königreich 44 Prozent, weltweit 49 Prozent). Deutsche Befragte lagen mit ihren Plänen zur Nutzung der öffentlichen Cloud über dem weltweiten Durchschnitt für Saas (56 Prozent vs. 53 Prozent weltweit) und PaaS (56 Prozent vs. 49 Prozent weltweit). Nur in Bezug auf IaaS-Umgebungen lagen sie mit 46 Prozent unter dem weltweiten Durchschnitt von 53 Prozent.

Was die Nutzung von Ressourcen in der öffentlichen Cloud angeht, zeigten die deutschen und britischen Umfrageteilnehmer im Allgemeinen geringere Bedenken. In Bezug auf spezifische Sicherheitsprobleme entsprachen die Antworten aus den beiden Ländern etwa denen anderer Regionen: Hier wurden Sicherheitsvorfälle bei Cloud-Anbietern, Schwachstellen durch gemeinsam genutzte Infrastrukturen und die Datenhoheit als größte Probleme genannt. Das mit 70 Prozent weltweit am häufigsten genannte Sicherheitsproblem – Sicherheitsvorfälle bei Cloud-Anbietern – landete auch in Deutschland ganz oben auf der Liste (66 Prozent), im Vereinigten Königreich an zweiter Stelle (65 Prozent). Das weltweit am dritthäufigsten genannte Problem der Datenhoheit (65 Prozent) wurde in Deutschland an zweiter Stelle (60 Prozent), im Vereinigten Königreich an erster Stelle (66 Prozent) eingestuft.

Neben diesen leichten Abweichungen bei den Top-Sicherheitsbedenken waren die beiden Länder auch in Bezug auf die Kontrolle über Verschlüsselungsschlüssel, Compliance und Service-Level-Agreements (SLAs) geteilter Meinung. Beispielsweise wählten lediglich 39 Prozent der deutschen Befragten das Thema Compliance als Cloud-Sicherheitsproblem, das dadurch an letzter Stelle stand und deutlich unter dem weltweiten Durchschnitt von 62 Prozent lag. Ebenso sahen nur 43 Prozent der deutschen Teilnehmer fehlende Datenschutzrichtlinien oder SLAs als Problem (65 Prozent im weltweiten Durchschnitt).

Welche Möglichkeiten gibt es, um die Bedenken hinsichtlich der Cloud-Nutzung in Deutschland und im Vereinigten Königreich auszuräumen? Wie die meisten Regionen wählten auch Deutschland und das Vereinigte Königreich die Verschlüsselung sensibler Daten in der Cloud auf den ersten Platz. Für die Cloud-Sicherheit ist es jedoch von zentraler Bedeutung, wo die Schlüssel gespeichert sind und wer sie verwaltet. Die Aufbewahrung der Schlüssel vor Ort ist eine kritische Anforderung vieler Compliance-Vorschriften. Deshalb stuften die Studienteilnehmer dies als den wichtigsten Faktor ein, um ihre Bereitschaft zur Nutzung der öffentlichen Cloud zu erhöhen (48 Prozent im weltweiten Durchschnitt). Deutschland und das Vereinigte Königreich zeigten eine starke Präferenz für Verschlüsselung mit gleichzeitiger Aufbewahrung der Schlüssel vor Ort: Deutschland lag hier im weltweiten Vergleich mit 62 Prozent an erster, das Vereinigte Königreich mit 55 Prozent an zweiter Stelle. Im Ländervergleich wählten im Vereinigten Königreich zudem die wenigsten Befragten die Verschlüsselung mit Aufbewahrung der Schlüssel durch den Service-Provider (29 Prozent vs. 35 Prozent im weltweiten Durchschnitt).

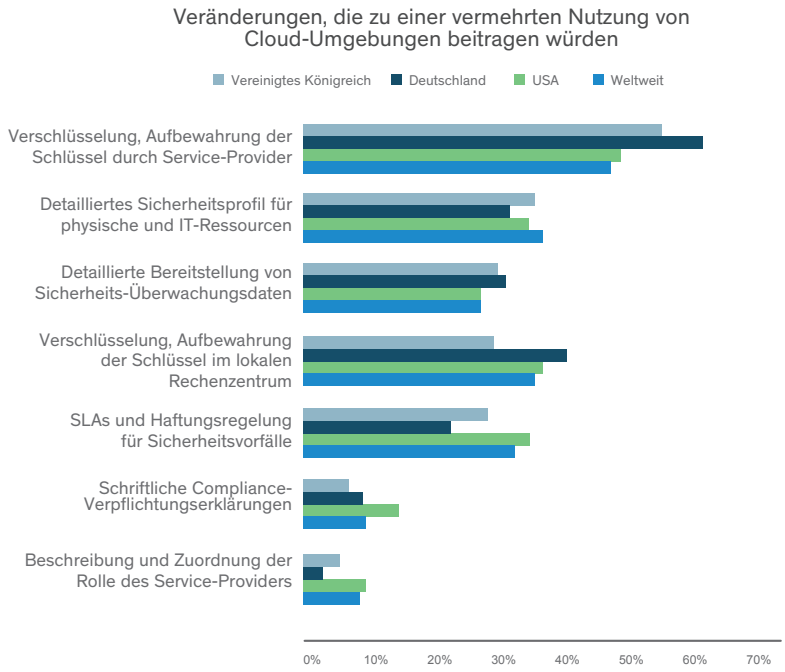

Diagramm 10: Veränderungen, die zu einer vermehrten Nutzung von Cloud-Umgebungen beitragen würden

Big Data

Im Hinblick auf die Pläne zur Speicherung sensibler Daten in Big-Data-Umgebungen gab es erneut Unterschiede zwischen Deutschland und dem Vereinigten Königreich. Während die deutschen Befragten hier über dem weltweiten Durchschnitt lagen (56 Prozent vs. 50 Prozent weltweit), platzierten sich die britischen Teilnehmer mit 45 Prozent eher im unteren Bereich. Was die Risiken von Big Data angeht, stimmten die beiden Länder etwa mit dem weltweiten Durchschnitt überein: 23 Prozent der Befragten in Deutschland und 26 Prozent im Vereinigten Königreich erachteten Big Data als einen der riskantesten Speicherorte für sensible Daten (im Vergleich zu 21 Prozent im weltweiten Durchschnitt). Weltweit wurde die Sicherheit von Big-Data-Berichten, die sensible Daten enthalten, als größtes Sicherheitsproblem in Bezug auf Big Data eingestuft (42 Prozent). Für deutsche (34 Prozent) und britische (36 Prozent) Befragte scheint dies ein weniger dringendes Problem zu sein. Angesichts der weltweit gesteigerten Bedenken in puncto Datenhoheit, insbesondere in Europa, bewerteten auch Deutschland (44 Prozent) und das Vereinigte Königreich (43 Prozent) Daten, die aus unterschiedlichen Ländern stammen, als eines der größten Datenschutzprobleme (40 Prozent im weltweiten Durchschnitt). Unter deutschen Befragten löste jedoch die Tatsache, dass sensible Daten in einer Big-Data-Umgebung überall gespeichert sein können, die größten Bedenken aus (51 Prozent vs. 41 Prozent im weltweiten Durchschnitt).

Das Internet der Dinge (IoT)

Auch wenn das Internet der Dinge (Internet of Things, IoT) zur größten Sicherheitshürde aller Zeiten werden könnte, sobald es von der breiten Masse genutzt wird, entsprechen die aktuellen Sicherheitsbedenken hinsichtlich des IoT noch den relativ geringen derzeitigen Anwenderzahlen. Dies gilt sowohl für die weltweiten als auch für die deutschen und britischen Ergebnisse. Mit seinen Plänen zur Speicherung sensibler Daten in IoT-Umgebungen liegt das Vereinigte Königreich an vorletzter Stelle (25 Prozent vs. 33 Prozent im weltweiten Durchschnitt), gefolgt von Japan (17 Prozent). Die deutschen Befragten zeigten sich hier etwas weniger konservativ (30 Prozent). Bei den riskantesten Speicherorten für sensible Daten liegt das IoT in beiden Ländern relativ weit unten – in Deutschland auf dem siebten, im Vereinigten Königreich auf dem zehnten Platz.

Angesichts der enormen Menge verbundener Geräte, die in den nächsten Jahren bereitgestellt werden sollen, ist die Sicherheit der von IoT-Geräten generierten sensiblen Daten ein wichtiger Punkt für die meisten Sicherheitsexperten weltweit (35 Prozent), insbesondere im Vereinigten Königreich (42 Prozent). Deutsche Studienteilnehmer hatten im Hinblick auf IoT-Geräte weniger Bedenken (27 Prozent). Hier wurden fehlende Branchenstandards zur Sicherung von IoT-Geräten als Hauptproblem angesehen (30 Prozent). Datenschutzverletzungen durch IoT-Geräte rangierten sowohl in Deutschland als auch im Vereinigten Königreich auf dem zweiten Platz (jeweils 29 Prozent im Vergleich zu 30 Prozent im weltweiten Durchschnitt).

EMPFEHLUNGEN

Die letzten Jahre gestalteten sich für die gesamte IT-Sicherheitsbranche schwierig – genauso wie für nahezu alle Beteiligten: Endbenutzer, Unternehmen und Sicherheitsanbieter. Wenn uns die Ereignisse der letzten Zeit etwas gelehrt haben, so ist es die Erkenntnis, dass unsere alten Methoden zum Schutz unserer Ressourcen nicht mehr ausreichen. Für viele Organisationen trifft hier das (etwas abgewandelte) berühmte Zitat von Albert Einstein zu: Immer wieder das Gleiche zu tun und andere Ergebnisse zu erwarten, ist vielleicht nicht die Definition von Wahnsinn, aber doch ein sicheres Rezept, um Ihre kritischen Daten in Gefahr zu bringen.

Wie geht es jetzt weiter? Genau wie die meisten Regionen und vertikalen Märkte müssen auch europäische Organisationen einsehen, dass sie ihre Sicherheitsposition nicht verbessern können, indem sie mehr vom Gleichen tun. Branchen und Regionen müssen sich intensiver mit neuen Methoden zur Verhinderung von Angriffen beschäftigen, um potenzielle Bedrohungen schneller zu erkennen und das Gefährdungszeitfenster einzugrenzen.

Wenn Unternehmen die Einschränkungen herkömmlicher Sicherheitsansätze erkennen, entwickelt sich das Thema Datensicherheit zu einer kritischen Komponente jeder umfassenden Sicherheitsstrategie. Cloud-, Big-Data- und IoT-Umgebungen generieren riesige Mengen sensibler Daten, die auf eine immer größere Anzahl von Geräten verteilt sind. Organisationen aller Größen und in allen Regionen sollten deshalb den Einsatz von Data Discovery, Datenklassifizierung, DLP und Verschlüsselung in Erwägung ziehen. Für Länder wie Deutschland und das Vereinigte Königreich, die zunehmende Bedenken hinsichtlich der Datenhoheit hegen und an neue Vorschriften wie die Datenschutz-Grundverordnung gebunden sind, könnten auch Gateway-Verschlüsselung und Tokenisierung hilfreiche Erweiterungen ihres Sicherheitsrepertoires darstellen.

Doch wie wir gesehen haben, birgt auch die Datensicherheit selbst ihre Herausforderungen. Der umfassendere Einsatz von Verschlüsselung und anderen Datensicherheitsmethoden könnte mit einer Vielzahl neuer Einzelfunktionsprodukte einhergehen, die für immer breiter gefächerte Anwendungsfälle benötigt werden, was wiederum die Komplexität und den Personalbedarf in die Höhe treiben kann. Nachdem insbesondere in Deutschland, aber auch im Vereinigten Königreich die Faktoren Komplexität und Personalmangel als größte Datensicherheitshürden genannt wurden, ist die Botschaft für Unternehmen und Datensicherheitsanbieter eindeutig. Für eine flächendeckendere Nutzung von Datensicherheitsprodukten müssen Letztere kosteneffektiver und benutzerfreundlicher werden und weniger Personal für Bereitstellung, Betrieb und Wartung in

Anspruch nehmen. Insbesondere im Vereinigten Königreich sollten Hersteller und Unternehmen die möglichen Auswirkungen von Datensicherheitslösungen auf die Systemleistung und Geschäftsprozesse prüfen.

Organisationen in Europa sollten Hersteller von Lösungen mit einer breiten Palette von Datensicherheitsoptionen bevorzugen, um sowohl die Anschaffungskosten als auch die laufenden Betriebskosten für die Datensicherheit zu senken. Unterschiedliche Datensicherheits-Tools wie DLP, Verschlüsselung, Schlüsselverwaltung, Verwaltung digitaler Zertifikate etc. werden mittlerweile auch als Services angeboten, und wir gehen davon aus, dass sich dieser Trend in den nächsten Jahren noch verstärken wird.

Schließlich empfehlen wir Kunden, sich neben Verschlüsselung weitere Sicherheitsanalyse-Techniken anzusehen, die einen zusätzlichen Schutz bieten können. Zum Beispiel verfolgt 451 Research neue Entwicklungen bei der Bedrohungsanalyse und Methoden zur Überwachung von Datenzugriffsmustern. So lassen sich Profile mit „normalen" Aktivitäten erstellen, anhand derer potenzielle Sicherheitsvorfälle identifiziert und möglicherweise betroffene Ressourcen leichter erkannt werden können.

ZUSAMMENFASSUNG UNSERER EMPFEHLUNGEN

DISCOVERY UND DATENKLASSIFIZIERUNG	Verschaffen Sie sich einen besseren Überblick über die Speicherorte sensibler Daten, insbesondere in Cloud-, Big-Data- und IoT-Umgebungen.
VERSCHLÜSSELUNG UND ZUGRIFFSKONTROLLE	**Rechenzentrum:** Ziehen Sie eine Strategie zur Verschlüsselung aller Daten in Betracht. **Cloud:** Setzen Sie Verschlüsselung ein und verwalten Sie die Schlüssel lokal. **Big Data:** Setzen Sie Discovery als Ergänzung zur Verschlüsselung ein. **IoT:** Erwägen Sie die Geräteauthentifizierung und -verschlüsselung sowie die Verschlüsselung von „Data in Transit"
DATENHOHEIT	Ziehen Sie die Einführung von Verschlüsselung und Tokenisierung in Betracht, um wachsende Compliance-Anforderungen hinsichtlich der Datenhoheit (z. B. DS-GVO) zu erfüllen.
DATENSICHERHEITS-PLATTFORMEN	Setzen Sie Plattformlösungen ein, um ein Wirrwarr aus Einzelprodukten zu vermeiden und die Kosten niedrig zu halten.
SERVICEBASIERTE BEREITSTELLUNG	Halten Sie nach servicebasierten Angeboten oder Partnerprogrammen Ausschau, um den Personalbedarf zu reduzieren.

ANALYST PROFILE

Garrett Bekker is a Senior Analyst in the Information Security Practice at 451 Research. He brings a unique and diverse background, having viewed enterprise security from a variety of perspectives over the past 15 years. Garrett spent more than 10 years as an equity research analyst at several investment banking firms, including Merrill Lynch, where he was the lead enterprise security analyst, as an investment banker, and also in sales and marketing roles with early-stage enterprise security vendors. Throughout his career, Garrett has focused on a wide variety of subsectors within enterprise security and is now focusing primarily on identity and access management (IAM) and data security, with a special interest in applying the former to cloud-based resources..

Garrett Bekker
Senior Analyst
451 Research

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organisations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

ABOUT VORMETRIC, A THALES COMPANY

Vormetric's comprehensive high-performance data security platform helps companies move confidently and quickly. Our seamless and scalable platform is the most effective way to protect data wherever it resides–any file, database and application in any server environment. Advanced transparent encryption, powerful access controls and centralised key management let organisations encrypt everything efficiently, with minimal disruption. Regardless of content, database or application–whether physical, virtual or in the cloud–Vormetric Data Security enables confidence, speed and trust by encrypting the data that builds business.

Please visit **WWW.VORMETRIC.CO.UK** and find us on Twitter **@VORMETRIC**

Vormetric
A Thales company

Vormetric.com/DataThreat/2016