WHITEPAPER

Umfrage 2017 IT-Sicherheit

Cybersicherheit: Selbstüberschätzung kann gefährlich sein

Untersuchung von SolarWinds® MSP zum Sicherheitsstatus von Unternehmen in Großbritannien und den USA

solarwinds msp

ZUSAMMENFASSUNG

SolarWinds hat im Jahr 2017 Unternehmen zum Thema Cybersicherheit befragt. Das Ergebnis: Sowohl größere Unternehmen als auch kleinere Betriebe (KMU) halten sich in puncto Sicherheit für gut aufgestellt, mit gutem Datenschutz und geringen Sicherheitslücken. In allen befragten Funktionskategorien – CIO, IT-Leitung und CISO – scheint man der Meinung zu sein: Unsere Systeme sind sicher.

Die wachsende Anzahl an hochspezifischen Hackerangriffen und Datenpannen, regelmäßig mit finanziellen Einbußen und Imageschäden verbunden, haben die Unternehmen inzwischen für das Thema IT-Sicherheit sensibilisiert. Allerorten werden Security-Budgets aufgestockt: Das Gefühl, sicher zu sein, lassen sich Unternehmen Jahr für Jahr mehr kosten.

Laut unserer Umfrage sind IT-Dienstleister mit dem Sicherheitszustand ihrer Betriebe zufrieden. Ist ihre Einschätzung berechtigt?

Keineswegs, wie unsere Umfrage zeigt.

ZU DIESER UMFRAGE

Anfang 2017 befragte SolarWinds MSP 400 kleinere und größere Unternehmen zum Thema Cybersicherheit, zu den ergriffenen Maßnahmen, Erfolgen und Misserfolgen. Die Unternehmen stammten zu gleichen Teilen aus Großbritannien und den USA.

Zwar vertrauen 87 % der Unternehmen ihrer Sicherheitstechnik und ihren Prozessen vollkommen – 59 % hielten sich zum Umfragezeitpunkt sogar für weniger gefährdet als im Jahr davor –, dennoch war es bei 71 % dieser Unternehmen in den 12 Monaten vor der Umfrage zu einem Sicherheitsvorfall gekommen. „Bei uns kann so etwas nicht passieren“ – diese Annahme erweist sich leider als völlig falsch.

Wie kommt es zu dieser Fehleinschätzung? Einfach gesagt: Es mangelt am Bewusstsein für die folgenden sieben Kardinalfehler in der Cybersicherheit:

1. Inkonsistenz bei der Durchsetzung von Sicherheitsrichtlinien
2. Halbherzigkeit bei der Sicherheitsschulung der Systembenutzer
3. Kurzsichtigkeit beim Einsatz technischer Maßnahmen
4. Nachlässigkeit beim Reporting zu Schwachstellen
5. Mangelnde Flexibilität bei der Anpassung von Prozessen nach einem Sicherheitsvorfall
6. Zögerlichkeit beim Ergreifen von Präventionsmaßnahmen
7. Trägheit bei der Erkennung und Behandlung von Vorfällen

Unternehmen, die ihre Sicherheit verbessern wollen, sollten diese Kardinalfehler tunlichst vermeiden. Andernfalls riskieren sie mit ihrer Selbstüberschätzung das Aus ihres Geschäfts.

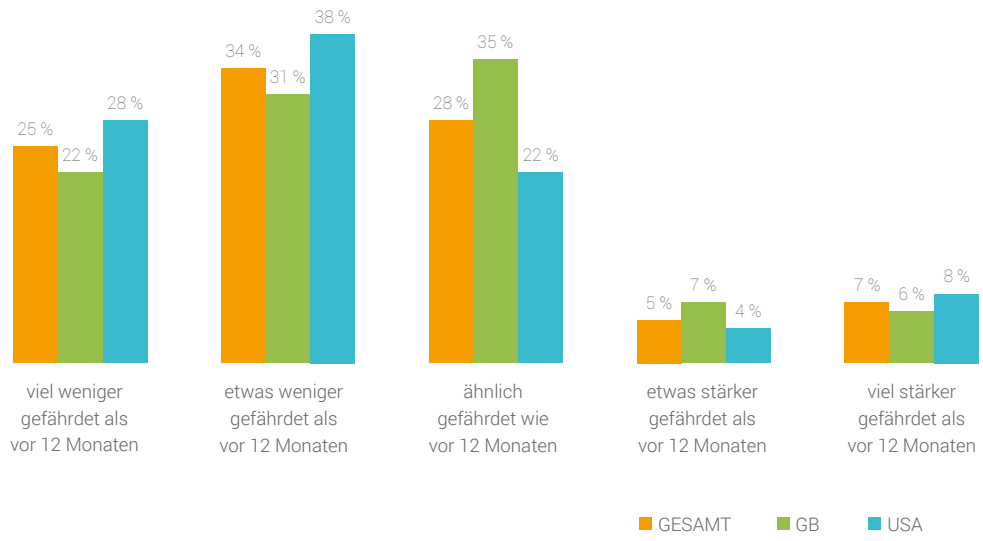
VIELE IT-LEITER HABEN BEIM THEMA SICHERHEIT DIE ROSA BRILLE AUF

Auf den ersten Blick mag der Optimismus der Befragten nachvollziehbar wirken. Mit 87 % hält der weitaus größte Teil die eigenen Mechanismen und die eingesetzte Technik für mindestens durchschnittlich gut. 61 % geben an, mit einer Aufstockung ihres Sicherheitsbudgets rechnen zu können, und gehen davon aus, dass dies ihre Lage weiter verbessern wird.

87 % halten ihre IT-Sicherheit für mindestens durchschnittlich gut.

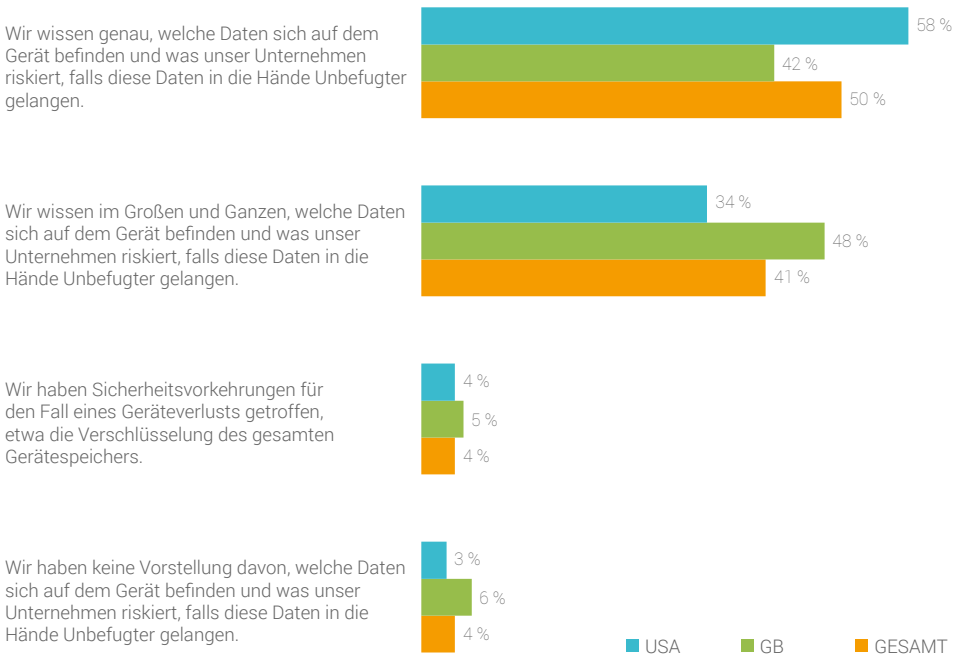
Auch im Jahr zuvor hatte SolarWinds eine vergleichbare Umfrage mit derselben Zielgruppe von Unternehmen durchgeführt. Damals hatten 50 % der Befragten ihr Unternehmen als weniger gefährdet eingestuft als in den vorangegangenen 12 Monaten. Diese Zahl ist jetzt auf 59 % gestiegen.

Für wie gefährdet halten Sie Ihr Unternehmen?



Die Befragten geben sich nicht nur zu ihrem Sicherheitszustand ganz allgemein optimistisch, sondern auch, was den Umgang mit ganz konkreten Gefahren und Szenarien angeht. So behaupten 50 %, im Fall eines abhanden kommenden Mobilgeräts sicher zu wissen, welche Daten sich auf dem Gerät befinden, und welches Risiko der Verlust für ihr Unternehmen bedeutet. Trotz immer wieder neuer Datenpannen und Sicherheitsvorfälle halten 57 % der Befragten ihre Maßnahmen zum Schutz der personenbezogenen Daten von Kunden und Mitarbeitern für sicher.

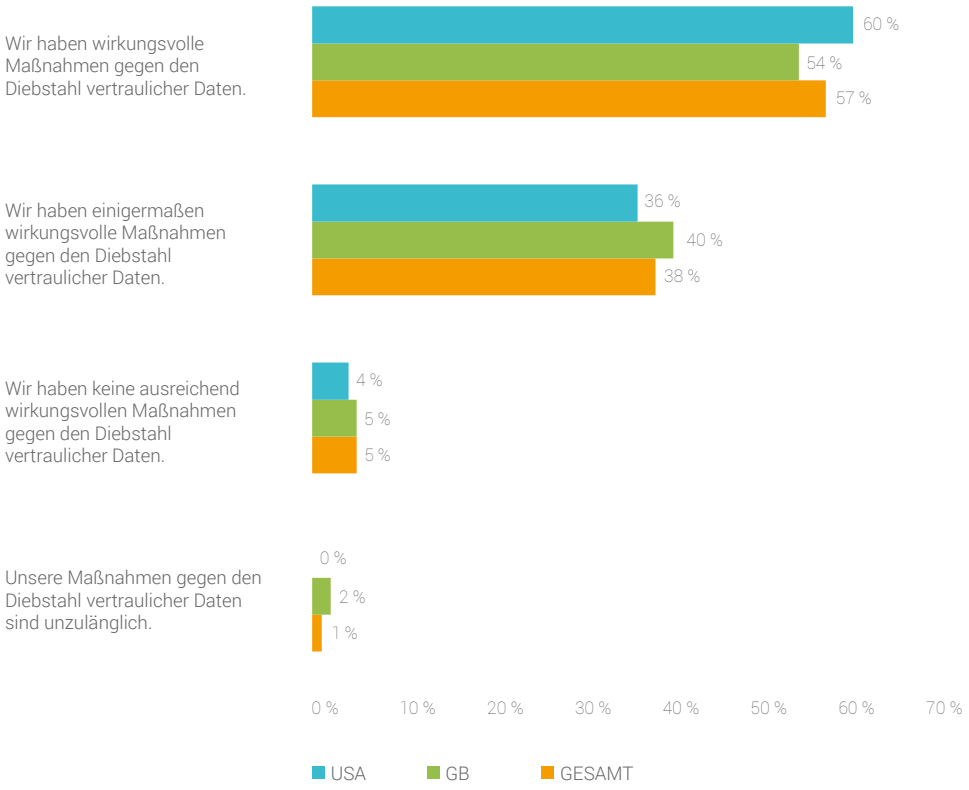
Einer Führungskraft aus der Personalabteilung/ dem Vorstand/der Unternehmensleitung kommt das Smartphone abhanden. Welche der folgenden Aussagen würden Sie bestätigen?



Weniger als 50 % der Unternehmen implementieren nach einem Sicherheitsvorfall neue Technik.

14 % unternehmen gar nichts.

Ihr Unternehmen ist verpflichtet, personenbezogene Daten seiner Kunden und Mitarbeiter zu schützen. Welche der folgenden Aussagen trifft am ehesten auf Sie zu?



57 % der IT-Leiter halten die Sicherheit ihrer Systeme für gut – offensichtlich eine Fehleinschätzung.

WIE ES WIRKLICH AUSSIEHT

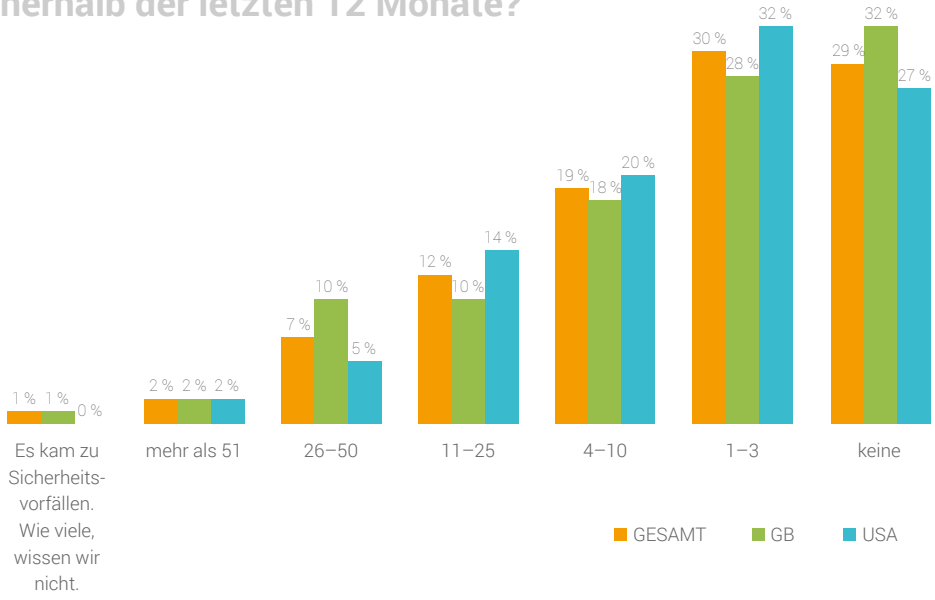
Ironie des Schicksals: 87 % der Befragten stufen ihre Cybersicherheit mindestens durchschnittlich gut ein und hielten ihr Unternehmen zum Zeitpunkt der Umfrage für weniger gefährdet als 12 Monate zuvor. Dennoch berichten 71 % aus dieser Gruppe gleichzeitig, im letzten Jahr mindestens einen Sicherheitsvorfall erlebt zu haben. In der Vorjahresumfrage 2016 hatte dieser Wert nur bei 29 % gelegen.

Bei 71 % der Befragten gab es im letzten Jahr mindestens einen Sicherheitsvorfall.

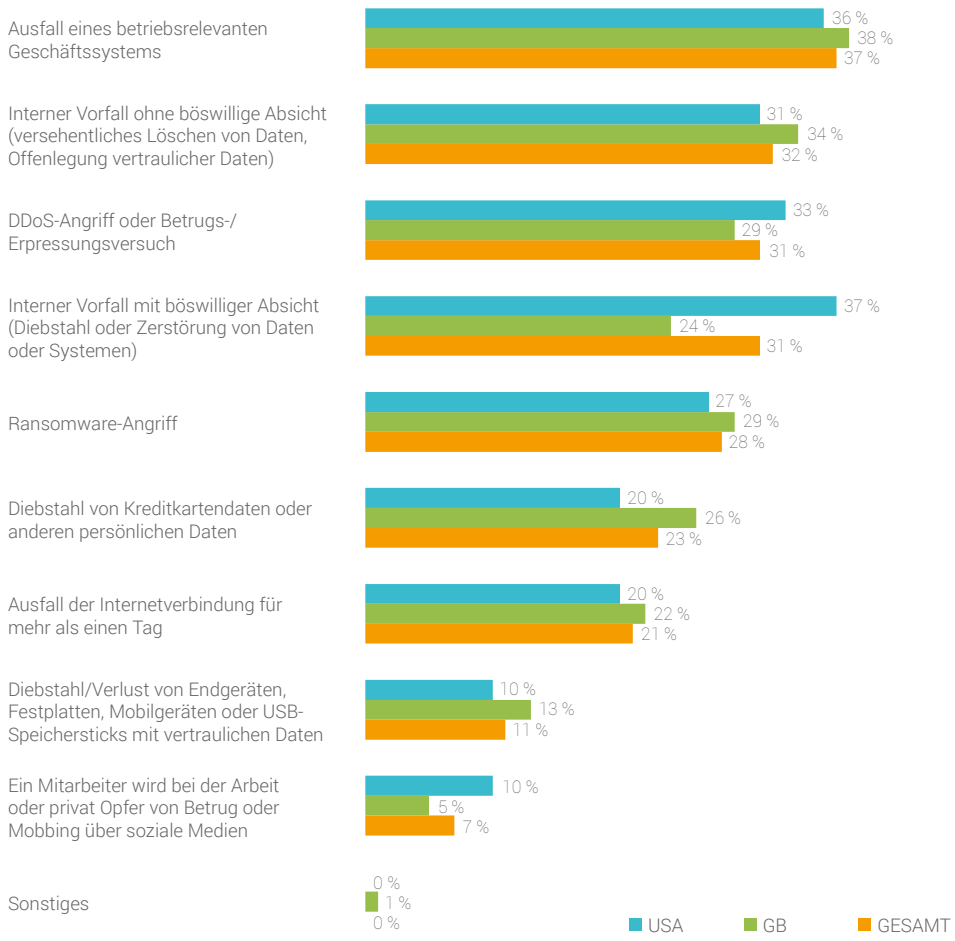
Dies lässt zwei mögliche Schlüsse zu:

1. Entweder sind die meisten Hackerangriffe inzwischen so raffiniert, dass sie durchschnittliche bis gute Schutzmechanismen aushebeln.
2. Oder die Befragten sehen die Abwehrstärke ihrer IT durch die rosa Brille.

Wie viele Sicherheitsvorfälle gab es in Ihrem Unternehmen innerhalb der letzten 12 Monate?



Um welche Vorfälle handelte es sich? (Antwort der 283 Befragten, bei denen es in den letzten 12 Monaten zu einem Vorfall gekommen war)



Fast ein Drittel aller Sicherheitsvorfälle (31 %) sind DDoS-Angriffe, Betrug und kriminelles Verhalten von Insidern.

WELCHE FOLGEN DROHEN

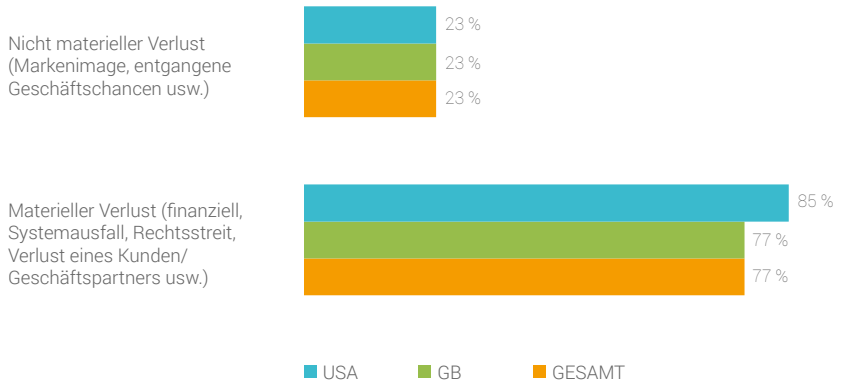
Die Konsequenzen dieser Sicherheitsvorfälle sind erheblich.

Nur 13 % der Befragten, bei denen es zu Sicherheitspannen gekommen war, registrierten Verluste, die sich unmittelbar damit in Zusammenhang bringen ließen. Ein Teil dieser Verluste war materieller Art, etwa der Verlust eines Kunden oder Geschäftspartners, finanzielle Einbußen oder die Störung des Geschäftsbetriebs zum Beispiel durch Systemausfälle. Als nicht materielle Verluste werden die Schädigung des Markenimages oder entgangene Geschäftschancen genannt.

Bei 77 % der Unternehmen führt ein Sicherheitsvorfall zu konkret bezifferbaren Verlusten.

23 % registrieren immaterielle Verluste.

Welche Verluste hat Ihr Unternehmen durch den zuletzt aufgetretenen Sicherheitsvorfall erfahren? (Antworten der 52 Befragten, die einen nachvollziehbaren Verlust registriert hatten)



Was also kostet ein Unternehmen seine lückenhafte Sicherheit im Schnitt, rein betriebswirtschaftlich gesprochen? Welche Gefahren drohen jenseits direkter Konsequenzen, wie sie der Verlust eines Kunden, der Ausfall von Systemen oder eine entgangene Geschäftschance darstellen?

In ihrer Studie „2016 Cost of Data Breach Study: Global Analysis“[1], beziffern IBM und Ponemon die Standardkosten pro verlorenem/gestohlenem Datensatz auf 158 US-Dollar beziehungsweise 122 britische Pfund. Dieser Wert setzt sich zusammen aus direkten Kosten (Beauftragung eines Forensikdienstes, Schalten einer externen Hotline für Kunden, Wiedergutmachung bei Kunden durch Rabatte u. Ä.) und indirekten Kosten (eigene Nachforschungen, interne Kommunikation u. Ä.). Die Studie beziffert auch die typischen Kosten eines Kundenverlusts oder von Imageschäden, die die Gewinnung neuer Kunden erschweren.

Kombiniert mit unseren eigenen Ergebnissen lässt sich mühelos ersehen, dass die Konsequenzen für kleine wie große Unternehmen beträchtlich sind:

	KMU	UNTERNEHMEN
gespeicherte Datensätze* durchschnittlich	**482**	5.946
Kosten pro verlorenem/gestohlenem Datensatz* (IBM/Ponemon)	**GBP 122** **USD 158**	GBP 122 USD 158
typische Kosten eines Sicherheitsvorfalls	**GBP 58.703** **USD 76.214**	GBP 723.596 USD 939.444
durchschnittliche Zahl der Vorfälle in den letzten 12 Monaten	**0,32**	1,05
typische Kosten eines Sicherheitsvorfalls jährlich	**GBP 18.844** **USD 24.465**	GBP 757.251 USD 983.139

*Definition: Ein Datensatz ist ein Informationselement/Datenfeld, das mit einem oder mehreren anderen Informationselementen/Datenfeldern verknüpft ist, die persönliche Daten enthalten.

Eigentlich kann sich kein Unternehmen ein solches Haftungsrisiko leisten. Deshalb haben wir uns genauer angeschaut, warum es denn um die Sicherheit so schlecht bestellt ist. Die Fehleinschätzung verdankt sich einem mangelnden Bewusstsein für insgesamt sieben Fehlerquellen.

1 Quelle: https://securityintelligence.com/media/2016-cost-data-breach-study/

DIE SIEBEN KARDINALFEHLER DER CYBERSICHERHEIT

In unserer Umfrage kristallisierten sich die sieben Fehler heraus, die Unternehmen erheblichen finanziellen Risiken aussetzen – bis hin zum drohenden Aus des Geschäftsbetriebs.

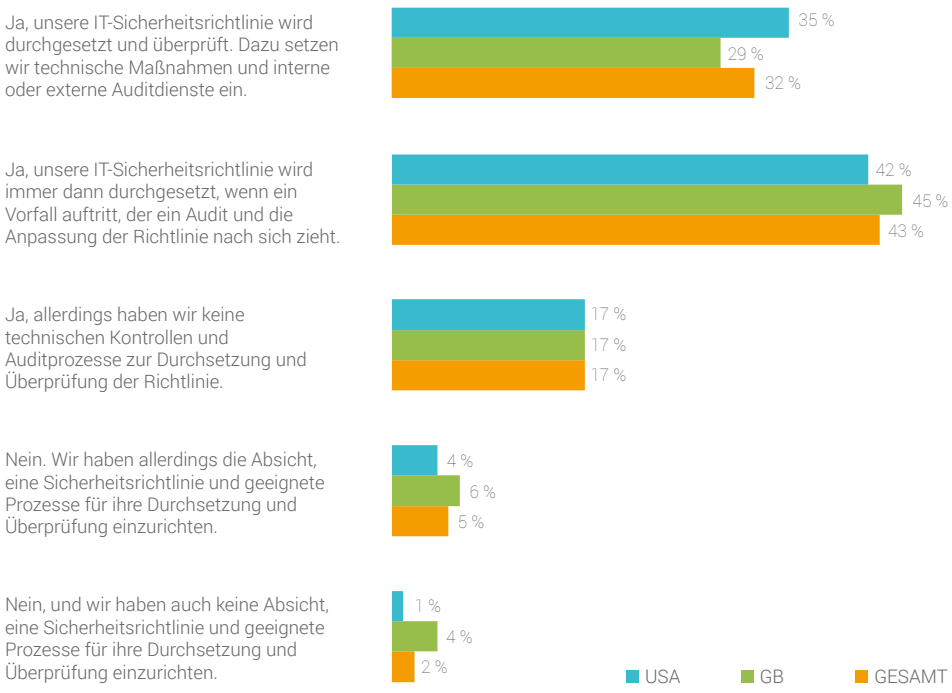
1. INKONSISTENZ

BEI DER DURCHSETZUNG VON SICHERHEITSRICHTLINIEN

Sicherheitsrichtlinien sind wertlos, wenn sie nicht durchgesetzt und regelmäßig auf ihre Eignung geprüft werden. In unserer Umfrage sagen jedoch nur 32 %, dass in ihrem Betrieb Richtlinien zuverlässig angewendet und regelmäßig überprüft werden. Weitere 43 % der Befragten setzen Richtlinien nur sporadisch durch, 17 % prüfen ihre Tauglichkeit nicht und 7 % haben gar keine Richtlinien.

In 68 % der Unternehmen mangelt es an einer zuverlässigen Durchsetzung und Überprüfung von Sicherheitsrichtlinien.

Gibt es in Ihrem Unternehmen Sicherheitsrichtlinien, die das Anlegen und die Verarbeitung von Mitarbeiter- und Kundendaten regeln?



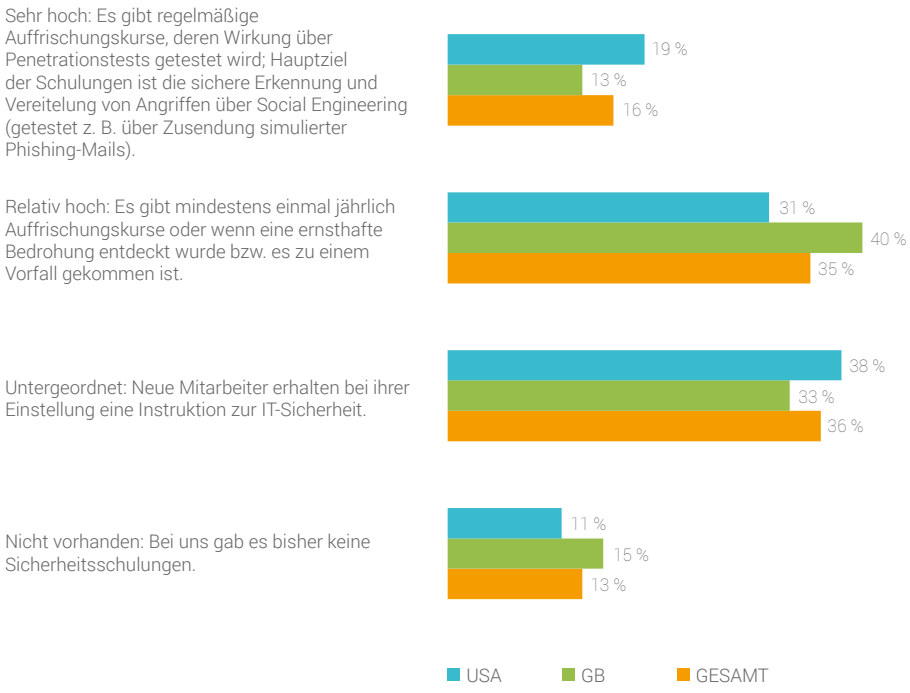
2. HALBHERZIGKEIT

BEI DER SICHERHEITSSCHULUNG DER SYSTEMBENUTZER

Die Sensibilisierung von Benutzern für die Sicherheit von IT-Systemen gilt gemeinhin als wichtig. Trotzdem räumen nur 16 % der Umfrageteilnehmer Sicherheitsschulungen einen prioritären Stellenwert ein. 71 % betreiben diesen Punkt eher halbherzig, indem sie neues Personal einmalig bei der Einstellung instruieren oder eine jährliche Auffrischungsschulung anbieten. Der Rest (13 %) gibt an, nichts dergleichen zu unternehmen.

Nur 16 % der Unternehmen messen Sicherheitsschulungen einen hohen Stellenwert zu.

Wie ist der Stellenwert von Sicherheitsschulungen in Ihrem Unternehmen?



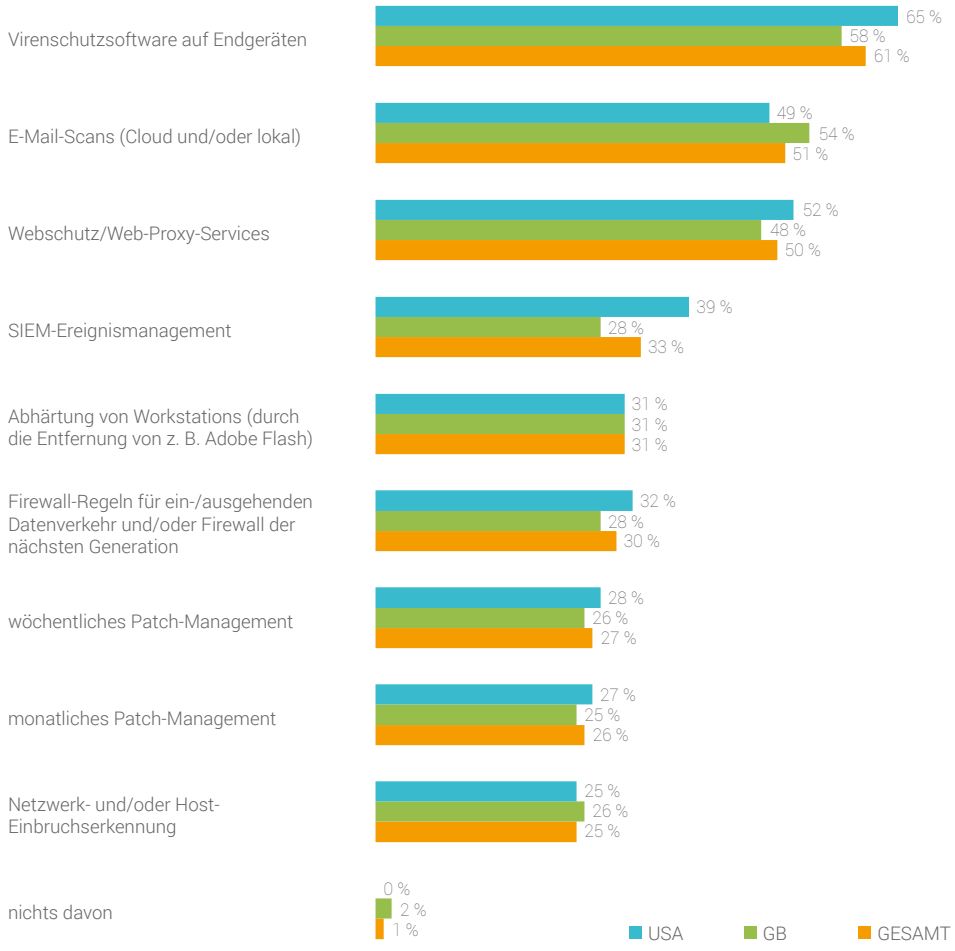
3. KURZSICHTIGKEIT

BEIM EINSATZ TECHNISCHER MASSNAHMEN

Sechs der Top-neun-Techniken für optimale Cybersicherheit finden sich nur bei einer Minderheit der Unternehmen. E-Mail-Scans, Webschutz und Virenschutz sind noch relativ häufig anzutreffen: 50 % bis 61 % der Befragten nennen sie. Doch die sechs weiteren Maßnahmen (u. a. SIEM, Firewall-Regeln und Patch-Management) finden sich nur noch bei 25 % (Einbruchserkennung) bis maximal 33 % (SIEM).

6 von 9 der wichtigsten technischen Sicherheitsmaßnahmen finden sich nur bei höchstens 31 % der Unternehmen.

Welche technischen Maßnahmen setzen Sie lokal zur Verhinderung von Sicherheitsvorfällen ein?



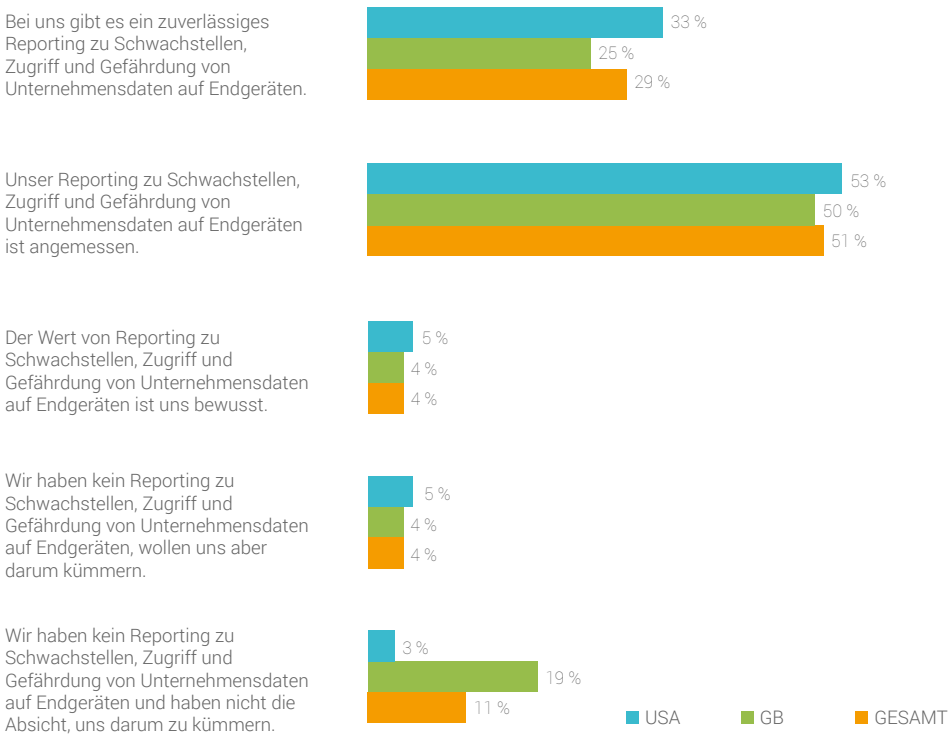
4. NACHLÄSSIGKEIT

BEIM REPORTING ZU SCHWACHSTELLEN

Richtig überzeugt von der Zuverlässigkeit ihrer Berichterstattung zu Schwachstellen sind nur 29 %, die Mehrzahl der Befragten (51 %) bezeichnet sie optimistisch als „angemessen". Überraschenderweise haben ganze 19 % überhaupt kein Schwachstellen-Reporting und 11 % wollen seine potenziellen Vorzüge noch nicht einmal eruieren.

Nur 29 % der Unternehmen sind von ihrem Schwachstellen-Reporting richtig überzeugt.

Welche der folgenden Beschreibungen trifft am besten auf Ihre Berichterstattung zu Schwachstellen zu?



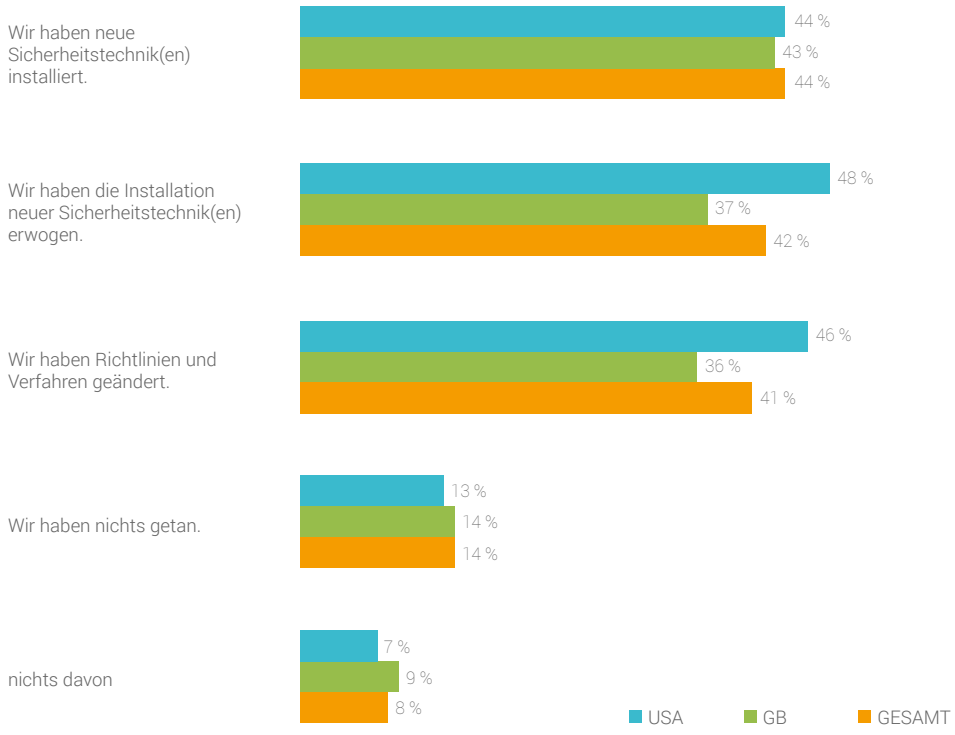
5. MANGELNDE FLEXIBILITÄT

BEI DER ANPASSUNG VON PROZESSEN NACH EINEM SICHERHEITSVORFALL

Nach einem Sicherheitsvorfall (den 71 % der Umfrageteilnehmer bereits erlebt haben) haben nur 44 % neue Technik eingeführt und nur 41 % ihre Prozesse neu ausgerichtet. 42 % nahmen einen Vorfall zum Anlass, sich mit neuer Technik zu beschäftigen, 14 % unternahmen ganz bewusst gar nichts.

Nur 44 % der Unternehmen haben nach einer Sicherheitspanne neue Technik installiert.

Wie haben Sie auf den letzten Sicherheitsvorfall in Ihrem Unternehmen reagiert?



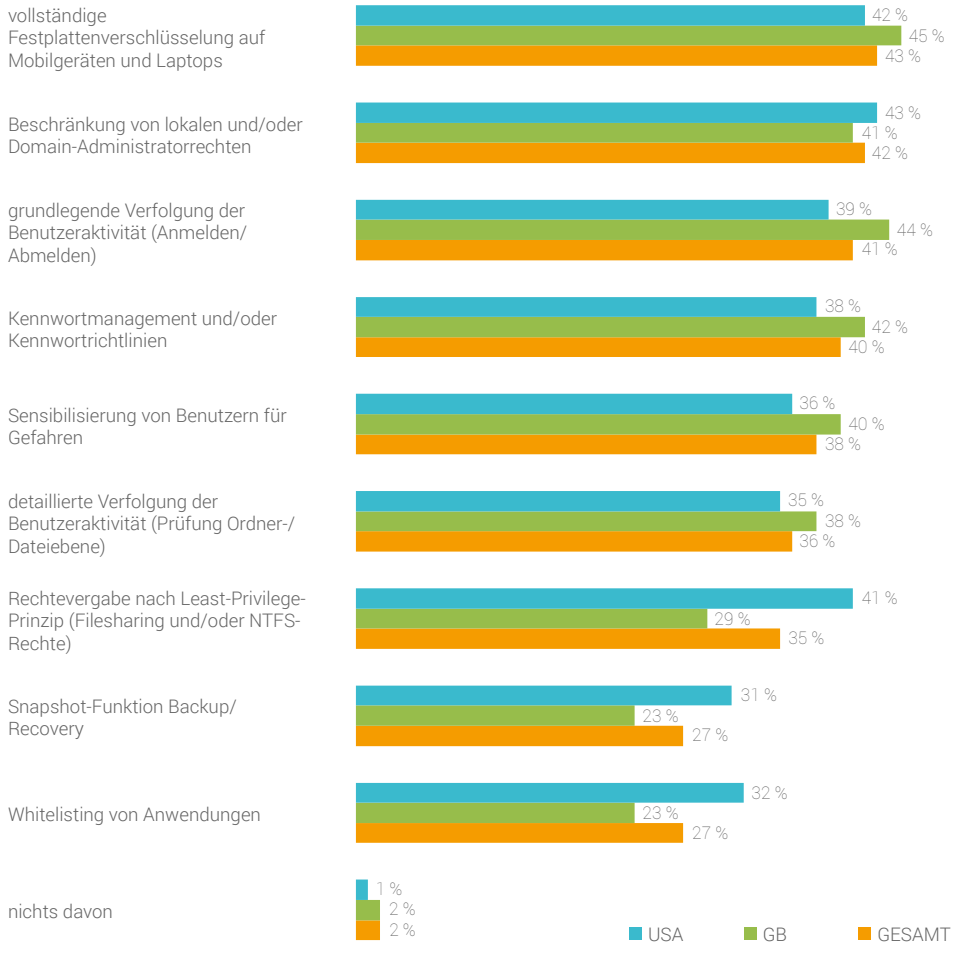
6. ZÖGERLICHKEIT

BEIM ERGREIFEN VON PRÄVENTIONSMASSNAHMEN

Nur ein geringer Teil der Befragten greift auf alle neun genannten Präventionsmaßnahmen zurück. Am häufigsten genannt – allerdings auch nur von insgesamt 43 % – wird die vollständige Festplattenverschlüsselung auf Mobilgeräten und Laptops. Whitelisting von Anwendungen betreiben nur 38 %, nur 41 % protokollieren die Aktivität authentifizierter Benutzer.

Nur eine Minderheit der Unternehmen setzt alle 9 Präventionsmaßnahmen ein.

Welche Präventionsmaßnahmen setzen Sie lokal zur Verhinderung von Sicherheitsvorfällen ein?

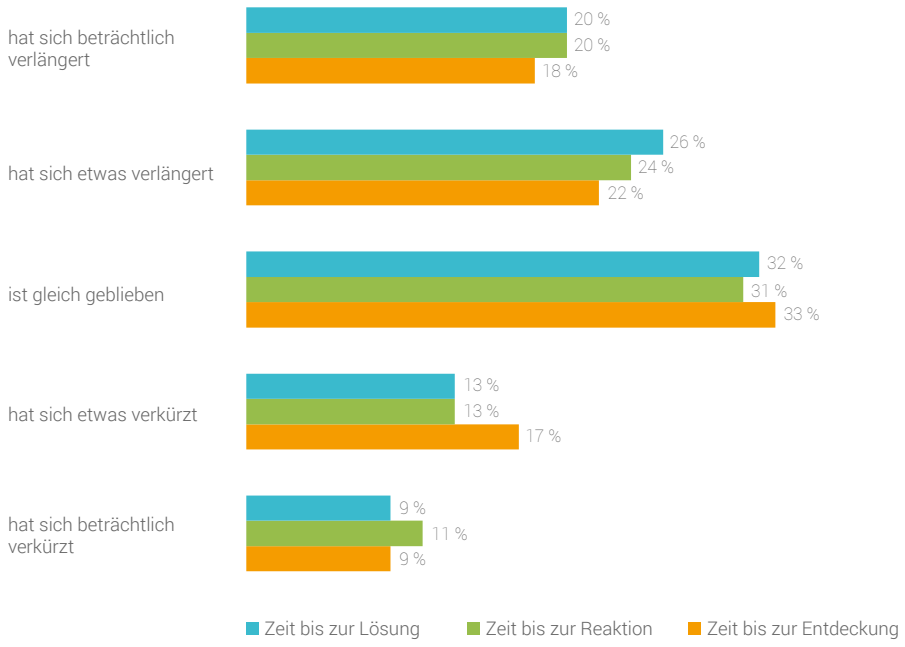


7. TRÄGHEIT

BEI DER ERKENNUNG UND BEHANDLUNG VON VORFÄLLEN

Im Laufe der letzten 12 Monate hat die Zeit bis zur Entdeckung eines Sicherheitsproblems bei 40 % der Befragten zugenommen und bei 44 % auch die Zeit bis zur Reaktion auf einen Vorfall. Die Zeit bis zur Lösung wiederum verlängerte sich bei 46 %. In der Vorjahresumfrage lagen die entsprechenden Werte noch bei 28 % (Zeit bis zur Entdeckung), 28 % (Zeit bis zur Reaktion) und 27 % (Zeit bis zur Lösung). Ganz offensichtlich lassen Vorfallerkennung und -behandlung in Unternehmen nach und werden zunehmend auf die leichte Schulter genommen.

Wie hat sich die Zeit bis zur Entdeckung, Reaktion auf und Behebung von Sicherheitsvorfällen in Ihrem Unternehmen 2016 gegenüber 2015 verändert?



Beunruhigende Zahlen:

Die Zeit bis zur Erkennung hat sich bei 40 % verlängert.

Die Zeit bis zur Reaktion hat sich bei 44 % verlängert.

Die Zeit bis zur Lösung hat sich bei 46 % verlängert.

TIPPS FÜR MSPS

Die Umfrageergebnisse zeigen mit bestürzender Klarheit: **Unternehmen und KMU sehen ihren Sicherheitsstatus durch die rosa Brille**.

Ihnen als Managed Services Provider eröffnet dies verschiedene Gelegenheiten zur geschäftlichen Weiterentwicklung:

GELEGENHEIT 1: IHREN KUNDEN SICHERHEITSSCHULUNGEN ANBIETEN
Die Sensibilisierung von Systembenutzern ist ein wichtiger Baustein der Unternehmenssicherheit. Um sich erfolgreich gegen Bedrohungen zu wappnen, brauchen Ihre Kunden das entsprechende Wissen. Ob Sie Schulungen als Dienstleistung abrechnen oder Ihr wertvolles Know-how zwecks Kundenbindung kostenlos weitergeben, bleibt ganz Ihnen überlassen. Fest steht: Sicherheitsschulungen helfen die Zahl der Sicherheitsvorfälle zu senken. Für Sie bedeutet das: Weniger Pannendienst und zufriedenere Kunden.

GELEGENHEIT 2: VOR DER EIGENEN TÜRE KEHREN Als MSP mit dem Standbein Sicherheit sollten Sie selbst eine tadellose Sicherheitspraxis haben, sprich neueste Technik und aktuelle Best Practices anwenden. Davon abgesehen sollten Sie auch zukunftsorientiert denken: Erfüllt Ihr Sicherheitskonzept den aktuellen und künftigen Bedarf typischer kleiner bis großer Unternehmen? Funktioniert es lokal, in der Cloud und als Hybridmodell? Können Sie Kunden aus stark regulierten Branchen unterstützen?

GELEGENHEIT 3: DEN NOTFALL VORWEGNEHMEN Als MSP können Sie Ihren Kunden Ernstfallsimulationen und Stresstests anbieten. In vielen Bereichen des Wirtschaftslebens werden Worst-case-Szenarien immer wieder geprobt: Marketingteams spielen ihre Reaktion auf eine PR-Krise durch, Finanzdienstleister unterziehen Portfolios von Anlegern Stresstests, Logistiker treffen Vorkehrungen für den plötzlichen Ausfall eines Knotenpunkts. Auch als MSP können Sie die Leistung der Technik und Prozesse Ihrer Kunden im Ernstfall testen. So zeigt sich, wo es Lücken gibt und wie diese sich schließen lassen. Sind Kommunikationswege und Systemkomponenten zuverlässig genug? Sind die Erwartungen vernünftig und die Kennzahlen belastbar? Welche Umsatzquellen Sie hier erschließen können, werden Sie mit der Zeit herausfinden.

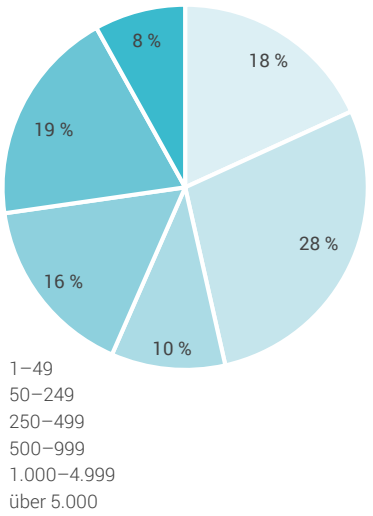
GELEGENHEIT 4: PARTNER UND KNOW-HOW AUFBAUEN Viele Sicherheitsvorfälle erfordern das Know-how von Spezialisten, und Sie sollten diese nicht erst suchen müssen, wenn der Ernstfall eingetreten ist. Ob Abwehr eines DDoS-Angriffs, Absicherung der IoT-Architektur oder Implementierung von Funktionen für Forensik und Vorfallsmanagement: Sorgen Sie dafür, dass Sie für all dies Experten an Ihrer Seite haben – im eigenen Haus oder von auswärts. Denn: Ist erst einmal Feuer unterm Dach, müssen Sie handeln. Zeit zum Aufbau des entsprechenden Know-hows haben Sie dann nicht.

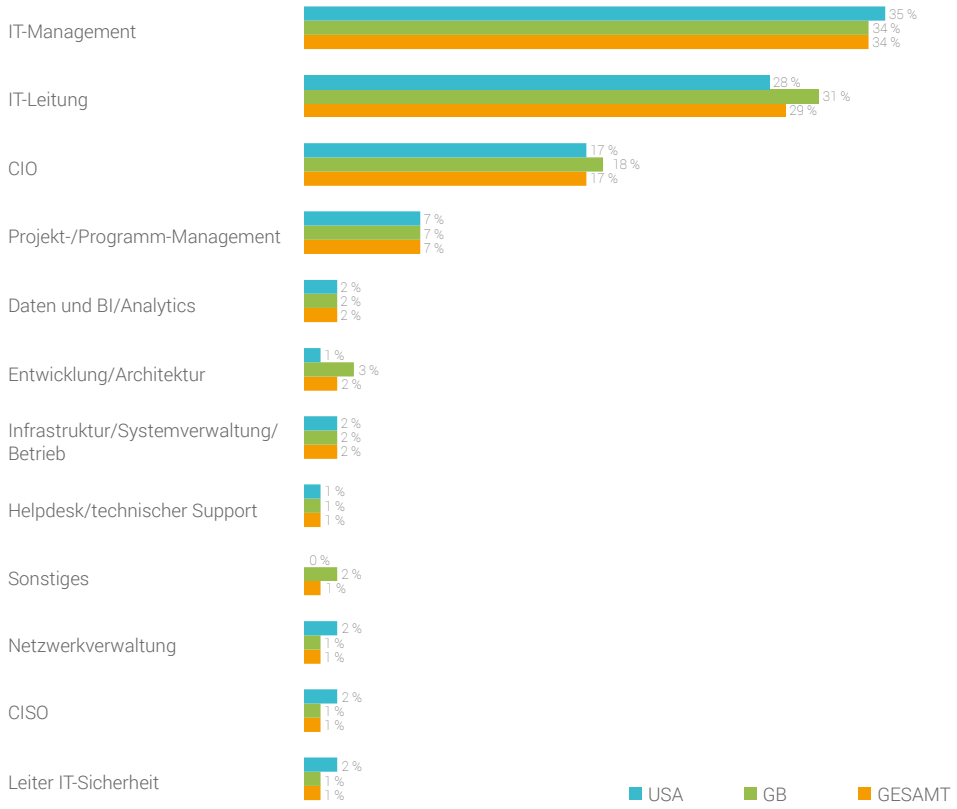
Der Optimismus vieler Unternehmen im Hinblick auf den eigenen Sicherheitszustand, kombiniert mit einem mangelnden Bewusstsein für die sieben Kardinalfehler in der Cyber-Sicherheit, spielt kriminellen Hackern definitiv in die Hände. Durch Sensibilisierung Ihrer Kunden und mit tragfähigen Konzepten, der Unterstützung kompetenter Spezialisten und den richtigen Tools können Sie als MSP aus dieser Situation Kapital schlagen.

ZUR UMFRAGEMETHODE

Im Januar 2017 hatte SolarWinds MSP Sapio Research mit der Befragung von 401 Unternehmen beauftragt. Thema war die Einschätzung der Befragten zum Sicherheitsstatus ihres Unternehmens. 50 % der befragten Unternehmen waren KMU (weniger als 250 Mitarbeiter), 50 % größere Unternehmen (über 250 Mitarbeiter). Eine Hälfte der Unternehmen hatte ihren Sitz in Großbritannien, die andere in den USA.

MITARBEITERZAHL DES BEFRAGTEN UNTERNEHMENS	GESAMT (401)	GB (200)	USA (201)
1–49	18 %	22 %	14 %
50–249	28 %	27 %	29 %
250–499	10 %	11 %	10 %
500–999	16 %	15 %	16 %
1.000–4.999	19 %	20 %	19 %
über 5.000	8 %	6 %	11 %





MEHRSCHICHTIGE SICHERHEIT KOLLEKTIVE INTELLIGENZ INTELLIGENTE AUTOMATISIERUNG

SolarWinds MSP unterstützt IT-Serviceanbieter mit Technik für die Erbringung eines professionellen und rentablen Service. Lokal installiert und in der Cloud bieten unsere Lösungen mehrschichtige Sicherheit, kollektive Intelligenz sowie intelligente Automatisierung und schaffen datenbasierte Einblicke, dank derer Provider ihre Arbeit schneller und einfacher erledigen. SolarWinds MSP hilft IT-Anbietern, sich auf das Wesentliche zu konzentrieren: die Erfüllung ihrer SLAs und den Aufbau eines gewinnbringenden Geschäftsmodells.