MHP
A PORSCHE COMPANY

Der Wettlauf gegen den Q-Day: Zu spät für die Quantenära?

Status, Risiken und Umsetzungsbarrieren der Post-Quantum-Kryptographie in Deutschland und den USA

KEY FACTS

9 von 10 Unternehmen beschäftigen sich mit PQC

Post-Quantum-Kryptographie (engl. PQC) ist **kein Zukunftsthema mehr**: In Deutschland befassen sich rund 86,6 % der Unternehmen mit dem Thema – in den USA 87,3 %.

Q-Day wird zeitnah erwartet

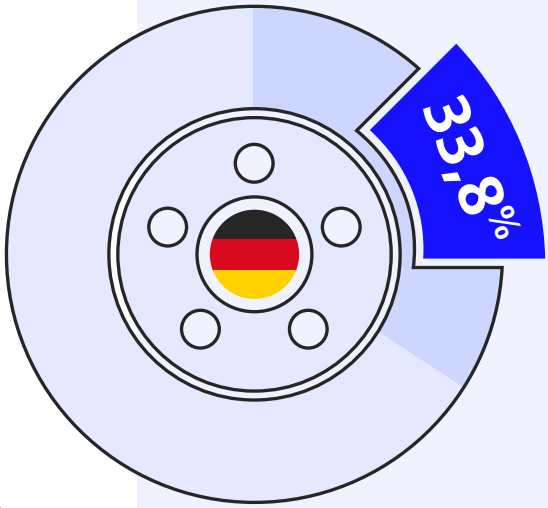
In Deutschland erwarten 45,3 % den Q-Day innerhalb der nächsten fünf Jahre (bis 2031), in den USA sogar 55,2 %. Weitere 39 % in Deutschland und 33,5 % in den USA in den nächsten zehn Jahren – bis 2036.

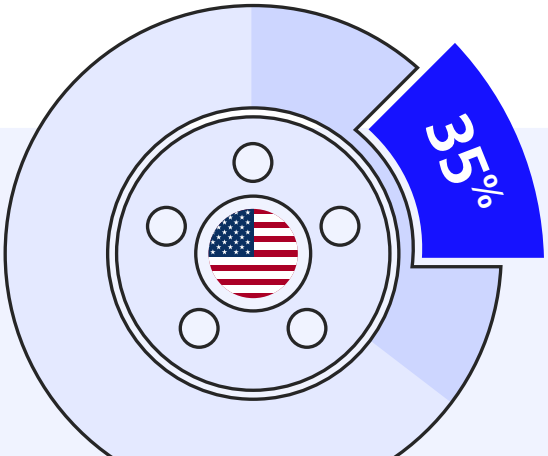
45,3%

55,2%

Altsysteme bremsen den Fortschritt

Komplexe Altsysteme sind der Hauptfaktor für die langsame Umstellung auf PQC. In Deutschland betrifft das 33,8 %, in den USA 35 % der befragten Unternehmen.





Einleitung

Quantencomputer entwickeln sich zunehmend von einem theoretischen Konzept zu einer praktisch relevanten Technologie. Mit ihrem Fortschritt eröffnen sich neue Anwendungsfelder, gleichzeitig entstehen jedoch substanzielle Risiken für die IT-Sicherheit. Insbesondere besteht die Gefahr, dass etablierte kryptografische Verfahren künftig nicht mehr den erforderlichen Schutz bieten. Der Zeitpunkt, ab dem Quantencomputer in der Lage sind, heute gängige Verschlüsselungsverfahren zu kompromittieren, wird als „Q-Day“ bezeichnet.

Die Bedrohung beschränkt sich nicht nur auf die Zukunft: Bereits heute können verschlüsselte Daten abgefangen und gespeichert werden, um sie später mit leistungsfähigen Quantencomputern zu entschlüsseln. Dieses Vorgehen wird als „store now, decrypt later“ bezeichnet. Vor diesem Hintergrund gewinnt die frühzeitige Auseinandersetzung mit Post-Quantum-Kryptographie (PQC) an Bedeutung. Ziel ist es, kryptografische Verfahren zu etablieren, die auch gegenüber Angriffen durch Quantencomputer resistent sind, und bestehende Produkte sowie Systeme schrittweise entsprechend auszurichten.

Um einen Überblick über den Status der Post-Quantum-Kryptographie in Deutschland und den USA geben zu können, hat die Management- und IT-Beratung MHP 1.060 IT-Expertinnen und -Experten aus Unternehmen mit mindestens 500 Mitarbeitenden befragt.

Die Ergebnisse liefern ein valides Stimmungsbild über den Fortschritt in Deutschland und den USA – zwei der weltweit führenden Volkswirtschaften.[1]

[1] Größte Volkswirtschaften (BIP) weltweit 2024 | Statista

„Wir reden hier über ein Zeitfenster, das sich gerade schließt: Die Mehrheit der Unternehmen erwartet den Q-Day innerhalb der nächsten fünf bis zehn Jahre, aber die Migration auf neue Verschlüsselung dauert oft genauso lange. Das ist ein strukturelles Problem, kein technisches Detail. Wer heute noch in Legacy-Systemen feststeckt, riskiert, dass sensible Daten bereits kompromittiert sind, bevor die eigene Transformation überhaupt abgeschlossen ist."

Markus Wambach
Group COO – MHP Management- und IT-Beratung GmbH

Aufmerksamkeit statt Nische

PQC spielt nicht mehr nur eine untergeordnete Rolle – weder in Deutschland noch in den USA.

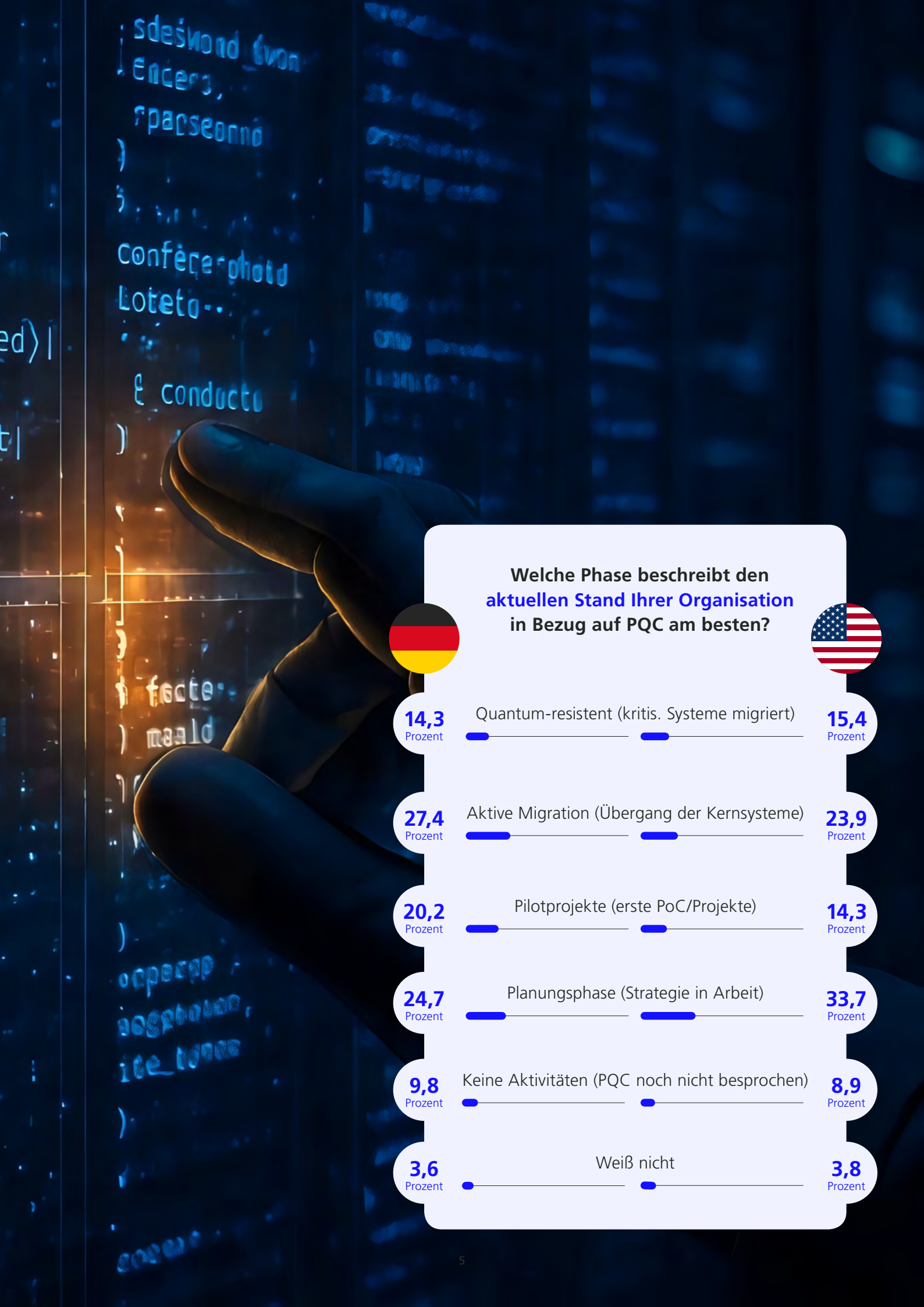
86,6%

der Firmen in Deutschland befassen sich mit dem Thema, in den USA

87,3%

Sowohl in Deutschland (86,6 %) als auch in den USA (87,3 %) beschäftigt sich die große Mehrheit der Unternehmen aktiv damit. Besonders bemerkenswert: In Deutschland befinden sich bereits 27,4 % der Organisationen in der aktiven Migration, weitere 14,3 % haben sogar schon kritische Systeme auf PQC umgestellt und gelten damit als „quanten-resistent". Die USA liegen nahezu gleichauf, mit 23,9 % aktiver Migration und 15,4 % quanten-resistenten Systemen.

Gleichzeitig bleibt ein besorgniserregender Rest: 9,8 % der deutschen und 8,9 % der US-Unternehmen geben an, dass sie bislang überhaupt keine Aktivitäten begonnen haben. Vor dem Hintergrund der erwarteten Q-Day-Zeitfenster und der „store now, decrypt later"-Problematik zeigt sich hier ein strategisches Risiko – denn wer heute noch nicht handelt, plant faktisch, die Migration erst dann zu starten, wenn die Bedrohung bereits real geworden ist.



Welche Phase beschreibt den aktuellen Stand Ihrer Organisation in Bezug auf PQC am besten?

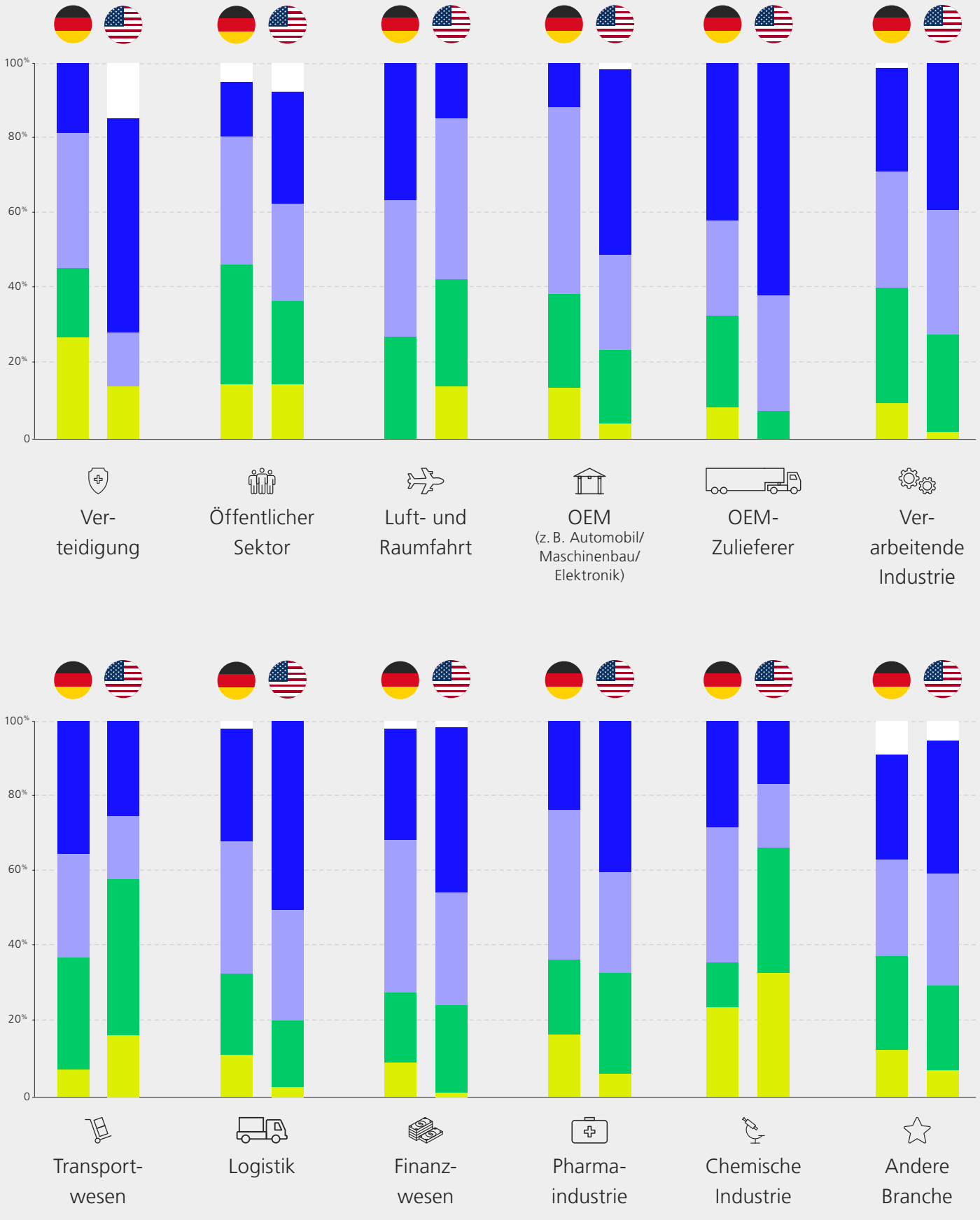
14,3 Prozent	Quantum-resistent (kritis. Systeme migriert)	15,4 Prozent
27,4 Prozent	Aktive Migration (Übergang der Kernsysteme)	23,9 Prozent
20,2 Prozent	Pilotprojekte (erste PoC/Projekte)	14,3 Prozent
24,7 Prozent	Planungsphase (Strategie in Arbeit)	33,7 Prozent
9,8 Prozent	Keine Aktivitäten (PQC noch nicht besprochen)	8,9 Prozent
3,6 Prozent	Weiß nicht	3,8 Prozent

Management-Aufmerksamkeit und Budget – PQC wird Chefsache

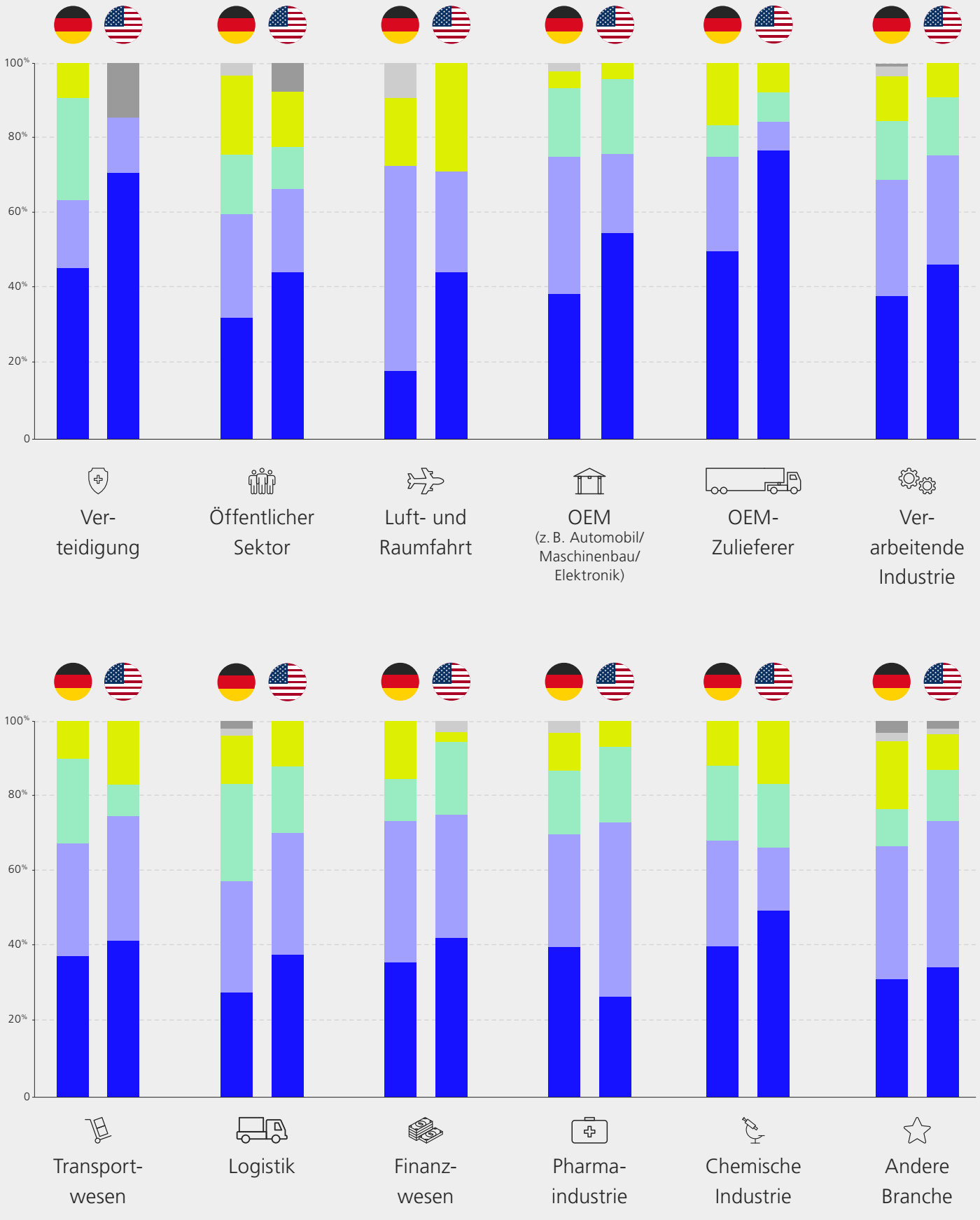
Die breite Auseinandersetzung mit PQC zeigt sich nicht nur in technischen Aktivitäten, sondern zunehmend auch auf Führungsebene. In 25,8 % der deutschen Unternehmen ist PQC bereits ein strategisches Vorstandsthema, in den USA sogar bei 39,7 %. Damit ist PQC in vielen Organisationen längst aus der Experten-Nische herausgewachsen und zu einem Thema der Unternehmen avanciert, das aktiv im Top-Management adressiert wird. Nur 12,3 % der deutschen und 6,2 % der US-Unternehmen geben an, dass PQC überhaupt nicht auf dem Radar der Führungsetage ist.

Welche Aussage beschreibt, die Priorität der Umstellung auf Post-Quanten-Kryptografie (PQC) auf der strategischen Agenda der Führungsetage/des Vorstands Ihres Unternehmens, am besten?

25,8 Prozent	Wichtige strategische Initiative des Vorstands	39,7 Prozent
34,2 Prozent	Teil der regulären Sicherheits-Roadmap	28,8 Prozent
25,1 Prozent	Wird beobachtet, aber kein wichtiger Treiber	22,6 Prozent
12,3 Prozent	Nicht auf dem Radar des Managements	6,2 Prozent
2,6 Prozent	Weiß nicht	2,7 Prozent


100%
80%
60%
40%
20%
0
Ver-
teidigung
Öffentlicher
Sektor
Luft- und
Raumfahrt
OEM
(z. B. Automobil/
Maschinenbau/
Elektronik)
OEM-
Zulieferer
Ver-
arbeitende
Industrie
Transport-
wesen
Logistik
Finanz-
wesen
Pharma-
industrie
Chemische
Industrie
Andere
Branche
Nicht auf dem Radar des Managements
Wird beobachtet, aber kein wichtiger Treiber
Teil der regulären Sicherheits-Roadmap
Wichtige strategische Initiative des Vorstands
Weiß nicht

Dieser Führungsfokus spiegelt sich auch in den Ressourcen wider: Rund 67,3 % der Unternehmen in Deutschland und 73,5 % in den USA stellen bereits ein dezidiertes Budget für ihre PQC-Migration bereit, teilweise ergänzt um speziell eingeführte Rollen. Die Zahlen belegen klar: PQC ist kein Randaspekt der Cybersicherheit mehr, sondern ein strategisches Transformationsprogramm, das organisatorisch wie finanziell verankert ist.


100%
80%
60%
40%
20%
0
Ver-
teidigung
Öffentlicher
Sektor
Luft- und
Raumfahrt
OEM
(z. B. Automobil/
Maschinenbau/
Elektronik)
OEM-
Zulieferer
Ver-
arbeitende
Industrie
Transport-
wesen
Logistik
Finanz-
wesen
Pharma-
industrie
Chemische
Industrie
Andere
Branche
Spezielles Budget und spezielle Rollen
Budget, Nutzung von vorhandenem IT-Personal
Zugewiesene Experten, kein explizites Budget
Kein spezielles Budget oder Rollen
Andere Zuweisungsstrategien
Weiß nicht

„Der Fortgang dieser Entwicklung ist nicht aufzuhalten. Umso wichtiger wird es, das Thema PQC noch stärker in den Fokus zu rücken. Der Einfluss von Quantencomputern auf die Cybersicherheit ist real und kein fernes Zukunftsszenario.“

Dr. Jan Wehinger
Partner – MHP Management- und IT-Beratung GmbH

Ein wichtiger Faktor: Die Inventarisierung

Auch bei der Inventarisierung zeigt sich ein Reifeunterschied: Während US-Unternehmen stärker auf automatisierte Verfahren setzen, dominieren in Deutschland weiterhin manuelle Ansätze.

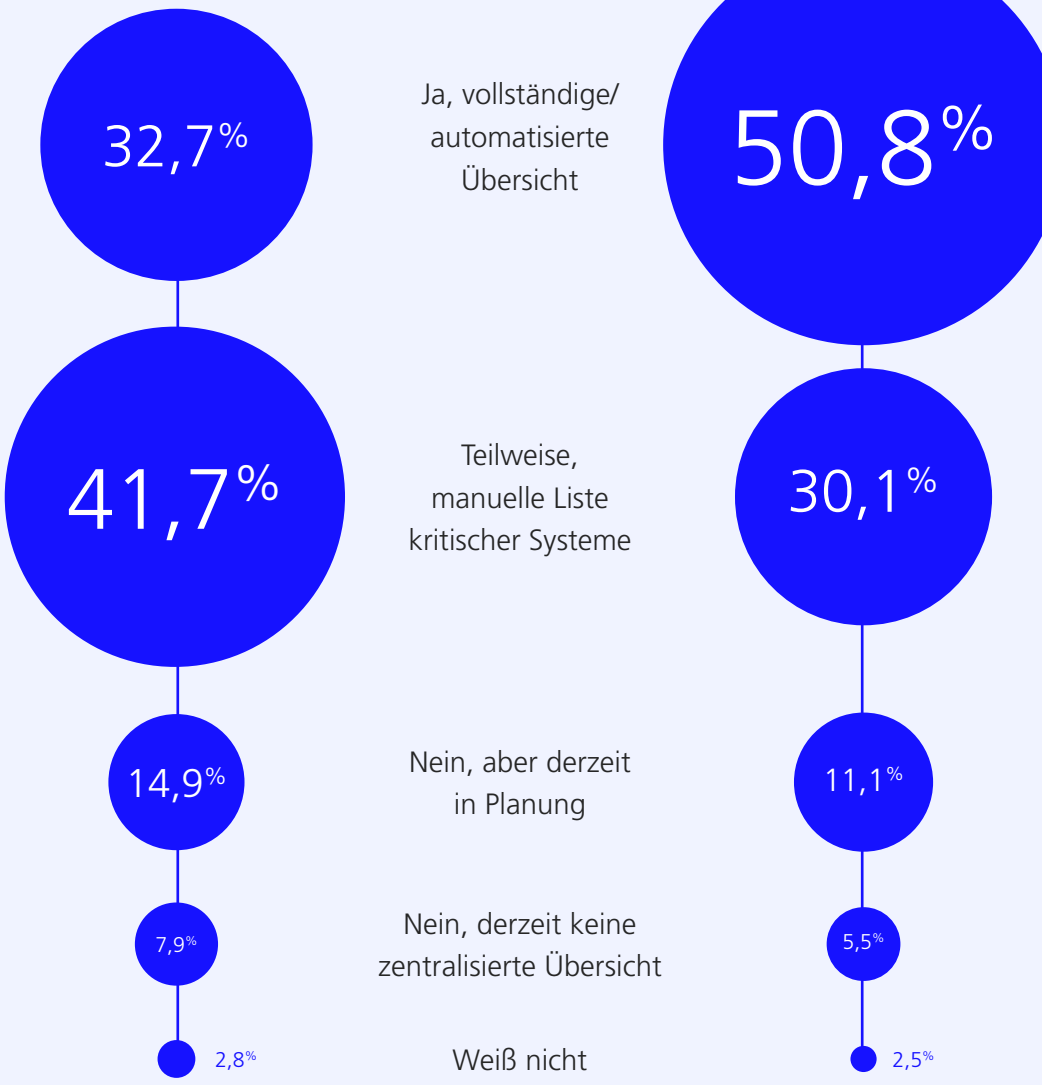
Ein weiterer entscheidender Unterschied zwischen den USA und Deutschland zeigt sich bei der kryptografischen Inventarisierung, einem wichtigen Schritt bei der PQC-Migration. Während 50,8 % der US-Unternehmen bereits eine vollständige und weitgehend automatisierte Übersicht über ihre kryptografischen Assets besitzen, liegt Deutschland mit 32,7 % deutlich zurück. Die Mehrheit arbeitet weiterhin mit manuellen Listen, die weder vollständig noch aktuell genug sind, um eine Migration effizient zu planen oder im Ernstfall schnell zu reagieren.

Dabei ist genau diese Übersicht ein strategischer Schlüsselfaktor: Ohne zu wissen, wo kryptografische Verfahren eingesetzt werden, welche Protokolle betroffen sind und welche Abhängigkeiten bestehen, ist die PQC-Migration kaum möglich. Relevant für diese Migration, aber auch unabhängig davon, ist Crypto Agility in Unternehmen. Das ist die Fähigkeit, kryptografische Verfahren flexibel und schnell auszutauschen, diese hängt unmittelbar von einer solchen Inventarisierung ab.

Wer seine Kryptolandschaft nicht kennt, kann auf neue Bedrohungslagen schlicht nicht rechtzeitig reagieren.

Die Zahlen zeigen damit deutlich: Die USA haben nicht nur früher angefangen, sondern die Voraussetzung geschaffen, um Migration wirklich umzusetzen. Deutschland hingegen riskiert, durch manuelle Prozesse wertvolle Zeit zu verlieren, in einer Phase, in der Zeit selbst zur kritischen Ressource wird.

Führt Ihr Unternehmen eine zentralisierte „Cryptography Bill of Materials“ (CBOM) oder ein vollständiges Inventar aller kryptografischen Vermögenswerte und deren Standorte?



Paradox: Bewusstsein vs. Zeit

In Deutschland erwarten 45,3 % den Q-Day innerhalb der nächsten fünf Jahre. In den USA erwarten das sogar 55,2 % der Befragten. Weitere 39 % in Deutschland und 33,5 % in den USA erwarten ihn in den nächsten zehn Jahren – bis spätestens 2036.

Diese Einschätzung teilen auch etablierte Sicherheitsinstitutionen und Analystenhäuser: So bezeichnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) Post-Quantum-Kryptografie bereits seit Jahren als eine der zentralen sicherheitspolitischen Prioritäten und weist regelmäßig darauf hin, dass Organisationen proaktiv mit der Migration beginnen müssen, da selbst moderate Schätzungen eine Bedrohung innerhalb des kommenden Jahrzehnts sehen. Auch internationale Analysten kommen zu ähnlichen Prognosen.

Die Analysten von Gartner bringen es in ihren Tech Trends 2025 prägnant auf den Punkt:

„By 2029, advances in quantum computing will make most conventional asymmetric cryptography unsafe to use."

Besonders alarmierend ist allerdings der technologische Trend der letzten Jahre. Die theoretisch benötigte Zahl an physikalischen Qubits, um RSA-Schlüssel zu brechen, ist in den vergangenen zehn Jahren kontinuierlich gesunken, und zwar nicht durch Hardware-Durchbrüche allein, son-dern vor allem durch Fortschritte in Algorithmik und Fehlerkorrektur.

- 2012 schätzten Forscher (Fowler et al.) den Bedarf noch auf rund 1 Milliarde physikalische Qubits.
- 2025 kamen Google-Quantum-AI-Wissenschaftler (Gidney et al.) in einer neuen Analyse bereits auf etwa 1 Million Qubits – eine Reduktion um den Faktor 1.000.
- 2026 stellte ein Preprint von Webster et al (Iceberg Quantum) sogar die Möglichkeit in den Raum, dass unter 100.000 physikalische Qubits ausreichen könnten, um RSA (Rivest-Shamir-Adleman – eines der heute am weitesten verbreiteten Verschlüsselungsverfahren, das unter anderem für sichere Internetverbindungen verwendet wird) zu brechen.

Diese Entwicklung zeigt einen klaren Trend: Die Schwelle zur kryptografischen Relevanz sinkt schneller, als ursprünglich angenommen wurde. Noch brisanter wird die Lage, wenn diese Zahlen mit den Roadmaps der führenden Hardware-Hersteller abgeglichen werden:

- Das US-Unternehmen IonQ plant, bis 2029 Quantencomputer mit rund 200.000 Qubits zu entwickeln – und bis 2030 sogar Systeme mit bis zu 2 Millionen Qubits.

Selbst wenn man technologische Realitäten traditionell konservativ beurteilt, ergibt die Kombination aus:

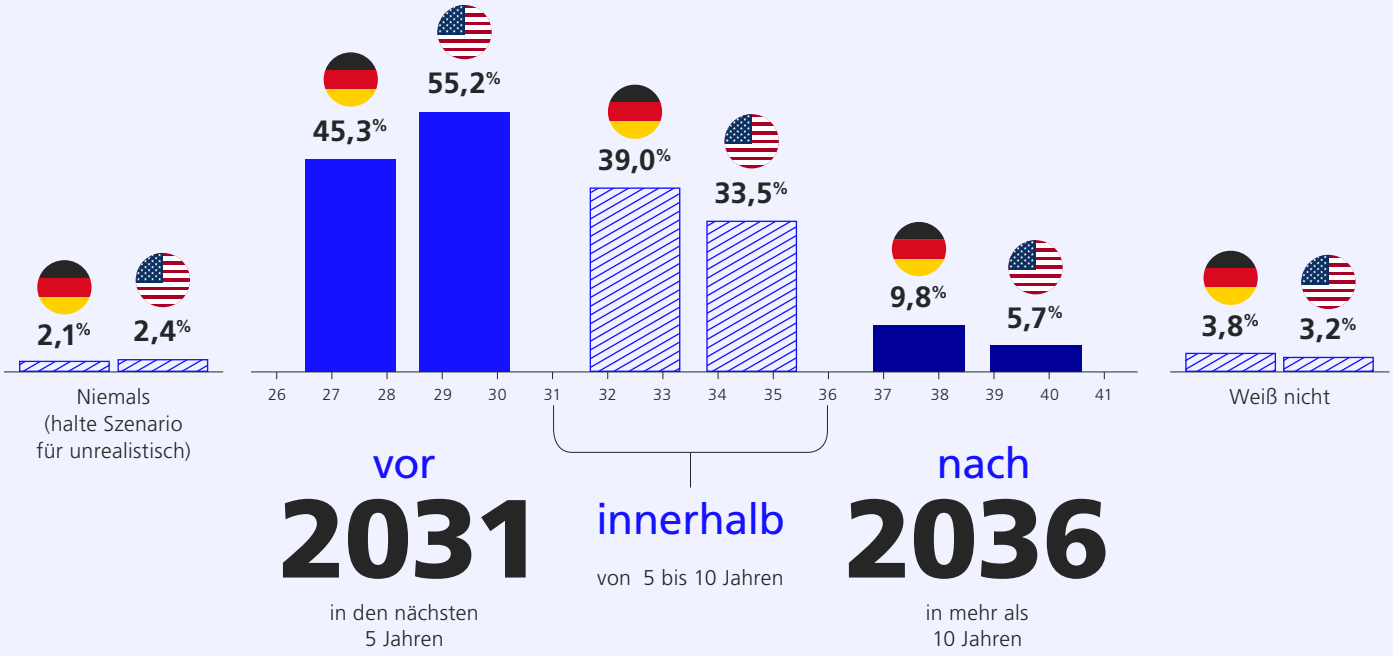
→ sinkenden Qubit-Anforderungen,
→ zunehmend effizienten Algorithmen,
→ massiv beschleunigten Entwicklungsroadmaps

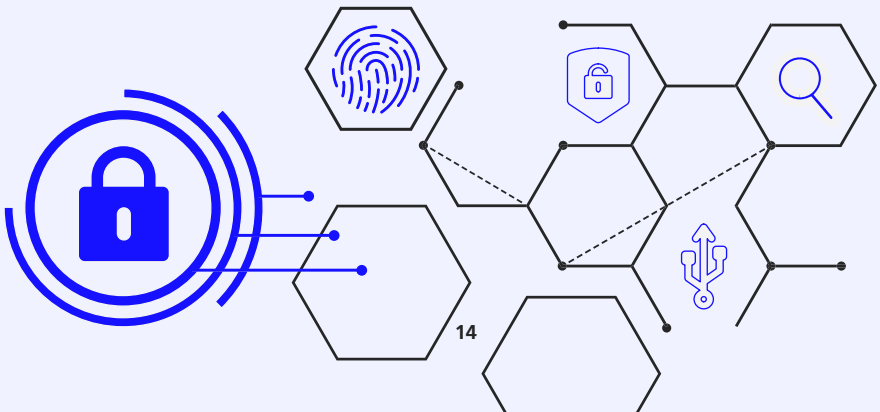
ein konsistentes, globales Bild: **Der Q-Day wird eher „nach vorne" gezogen als nach hinten.**

→ Das europäische Quanten-Start-up IQM verfolgt ähnliche Ziele: Bis 2031 sollen Systeme mit 100.000 Qubits entstehen, bis 2033 sogar mit bis zu 1 Million Qubits.

Damit erscheint das von der Mehrheit der Befragten angenommene Zeitfenster von 5 bis 10 Jahren realistisch, möglicherweise sogar zu optimistisch.

In welchem Jahr wird ein kryptografisch relevanter Quantencomputer (CRQC) Ihrer fachlichen Einschätzung nach in der Lage sein, die derzeitige RSA/ECC-Verschlüsselung zu entschlüsseln?





Unternehmen wissen um die Menge sensibler Daten und wie lange diese zu schützen sind.

Ein wesentlicher, oft unterschätzter Faktor ist der Anteil an Daten, die länger als zehn Jahre geschützt werden müssen. Laut unserer Umfrage gilt dies bei 43,8 % der deutschen und 44,6 % der US-Unternehmen für mehr als die Hälfte ihrer sensiblen Informationen (Kategorien „51–75 %“ und „76–100 %“). Gerade für diese Organisationen stellt die „store now, decrypt later“-Bedrohung ein erhebliches Risiko dar:

Daten, die heute abgegriffen werden, bleiben auch dann verwertbar, wenn der Q-Day erst in fünf oder zehn Jahren eintritt. Damit gilt besonders für Unternehmen mit langfristig schützenswerten Informationen: Jede Verzögerung erhöht die Wahrscheinlichkeit, dass Angreifer bereits im Besitz von Daten sind, die später entschlüsselt werden können.

43,8 %

der deutschen Unternehmen müssen mehr als die Hälfte ihrer sensiblen Informationen länger als 10 Jahre schützen.

44,6 %

der US-Unternehmen müssen mehr als die Hälfte ihrer sensiblen Informationen länger als 10 Jahre schützen.

Wie viel Prozent der sensiblen Daten Ihres Unternehmens erfordern eine Vertraulichkeitsfrist von 10 Jahren oder mehr (z. B. wegen langfristigen gesetzlichen Anforderungen oder Gesundheitsdaten)?

	🇩🇪	🇺🇸
0–25 %	7,9 %	11,5 %
26–50 %	46,4 %	41,6 %
51–75 %	32,8 %	33,5 %
76–100 %	11,0 %	11,1 %
Weiß nicht	1,9 %	2,3 %

Die prognostizierten Migrationszeiträume unterstreichen, dass verspätete oder bislang ausbleibende Aktivitäten zu strukturellen Rückständen führen können.

Während ein Großteil der Unternehmen den Q-Day innerhalb der kommenden fünf bis zehn Jahre erwartet, rechnen sie selbst gleichzeitig mit Migrationszeiträumen, die exakt in dieses kritische Fenster fallen.

In Deutschland gehen

53,4 %

der Befragten von einer PQC-Migration innerhalb von 2 bis unter 5 Jahren aus, weitere

27,5 %

erwarten 5 bis 10 Jahre.

In den USA zeigt sich ein sehr ähnliches Bild:

51,8 %

kalkulieren mit 2 bis 5 Jahren,

21,8 %

mit 5 bis 10 Jahren.

Damit liegt ein strukturelles Risiko offen:

Wer heute noch nicht begonnen hat, wird die Migration nicht vor dem prognostizierten Eintreten des Q-Days abschließen können.

Das „store now, decrypt later“-Problem verschärft diese Situation zusätzlich, denn die Daten, die heute abgegriffen werden, können in fünf bis zehn Jahren entschlüsselt werden, wenn Unternehmen noch mitten in ihrer Migration stecken.

Diese Einschätzung deckt sich nicht nur mit Analysten und Forschungseinrichtungen, sondern auch mit politischen Vorgaben und Warnungen.

Die Handlungsstrategie der Bundesregierung für Quantum Computing (2023) formuliert unmissverständliche Meilensteine für 2026:

- → Weiterführung der Migration zu Post-Quanten-Kryptografie für den Hochsicherheitsbereich
- → Einleiten der Migration zu Post-Quanten-Kryptografie in weiteren sicherheitskritischen Bereichen

Der implizite Befund:

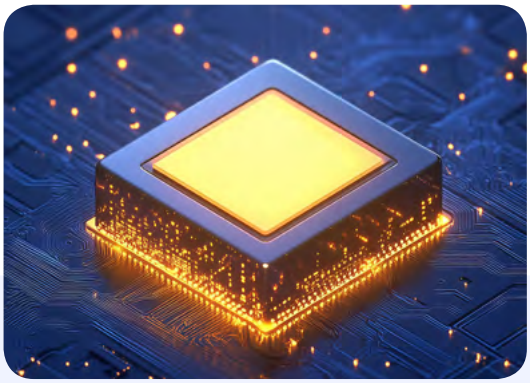
Für Hochsicherheitsbereiche hätte die Migration längst laufen müssen. Und für alle übrigen kritischen Sektoren ist spätestens jetzt der Startpunkt erreicht. Diese Dringlichkeit wird europaweit unterstrichen. In einem gemeinsamen Statement von 18 EU-Mitgliedstaaten und ihren nationalen Cyber-Sicherheitsbehörden heißt es, zusammengefasst:

„Wir fordern öffentliche Verwaltungen, kritische Infrastrukturen, IT-Dienstleister und die gesamte Industrie auf, die Transition zu Post-Quantum Kryptografie zur Top-Priorität zu machen. Organisationen und Regierungen sollten jetzt mit den ersten Schritten beginnen."

Im Zusammenspiel entsteht ein klares Lagebild:

- → Q-Day nähert sich schneller als erwartet, weil sowohl Qubit-Anforderungen als auch Hardware-Roadmaps in Richtung Beschleunigung zeigen.
- → Die erwarteten Migrationszeiträume vieler Unternehmen liegen gefährlich nahe am prognostizierten Q-Day.
- → Regierungen fordern explizit, dass die Migration jetzt beginnen muss, um die sicherheitspolitische Handlungsfähigkeit zu bewahren.

Die strategische Konsequenz lautet daher:
Wer in diesem Jahr nicht beginnt, plant faktisch eine Migration in ein bereits kompromittiertes Kryptosystem hinein.

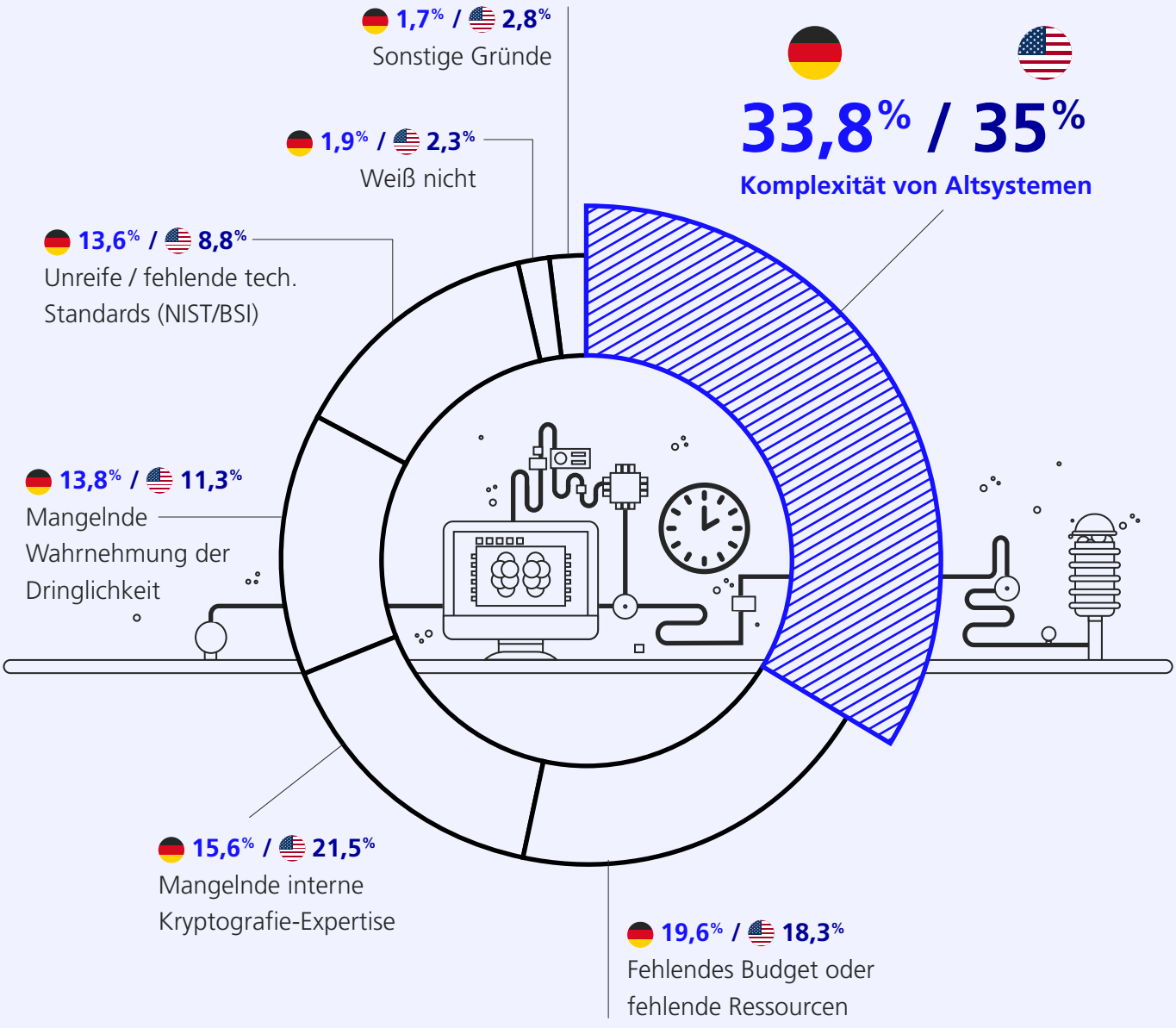


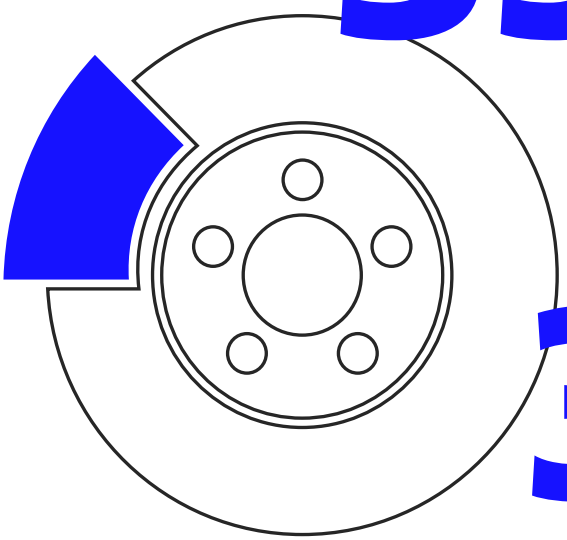
Wie viele Jahre werden Ihrer Einschätzung nach erforderlich sein, um die technische Migration zur Post-Quantum-Cryptography (PQC) in Ihrem gesamten Unternehmen abzuschließen?

Gründe für die langsame Umsetzung

Unabhängig von Branche und Region erweisen sich komplexe Altsysteme als der dominierende Bremsfaktor bei der Einführung von PQC. Organisatorische und personelle Faktoren – etwa begrenzte finanzielle Mittel oder mangelnde interne Kryptographie Expertise – erschweren die PQC Migration zusätzlich.

Was ist derzeit der Hauptfaktor, der die Umstellung Ihres Unternehmens auf Post-Quantum-Cryptography (PQC) verlangsamt oder verhindert?





33,8%

Komplexe Altsysteme sind der Hauptfaktor für die langsame Umstellung auf PQC bei den befragten Unternehmen.

35%

„Wer seine Altsysteme unter Kontrolle bringt, schafft auch den zeitnahen Umstieg auf PQC – weitere Zeit verlieren sollte man jedoch nicht“, erklärt Christian Zgardea, Partner bei MHP. „Zu verlieren gibt es nichts. Auch abseits von PQC lohnt es sich, seine eigenen Systeme stetig unter Kontrolle zu haben und Wildwuchs einzugrenzen.“

Christian Zgardea
Partner Cyber Security

Fazit

Die Ergebnisse zeigen zwei Seiten derselben Entwicklung: Deutschland und die USA haben in bemerkenswertem Tempo begonnen, Post-Quantum-Kryptografie zum festen Bestandteil ihrer Sicherheitsstrategie zu machen. Mit zusammen über 40 % der Unternehmen, die sich bereits in der aktiven Migration oder sogar schon im quantum-resistenten Zustand befinden, ist der Transformationsprozess vielerorts nicht nur angestoßen, sondern weit fortgeschritten. Das zeigt: PQC ist kein theoretisches Konzept mehr – es wird praktisch umgesetzt, in kritischen Systemen verankert und zunehmend strategisch gesteuert.

Gleichzeitig bleibt die Kernbotschaft eindeutig: Der Q-Day rückt schneller näher als viele Organisationen realisieren und die selbst prognostizierten Migrationszeiträume reichen gefährlich nah an diesen Zeitpunkt heran.

Dazu kommt der hohe Anteil langfristig schützenswerter Daten und die wachsende Diskrepanz zwischen technologischem Fortschritt auf Seiten der Quantenhardware und den noch vorhandenen Legacy-Hürden in den Unternehmen. Die Kombination aus wachsender Awareness, steigender Management-Attention und steigenden Investitionen ist ein starkes Signal – doch sie reicht nicht aus, solange ein signifikanter Rest noch zögert.

Die eigentliche Herausforderung besteht nun darin, den bestehenden Schwung zu nutzen und die Transformation vom Ausnahmeprojekt zur flächendeckenden Praxis zu machen.

Wer heute handelt, kann seine Systeme zukunftssicher aufstellen und eine der zentralen Sicherheits-herausforderungen des kommenden Jahrzehnts entschärfen.

Wer wartet, riskiert, die Migration erst dann zu beginnen, wenn die Kryptografie der Gegenwart bereits kompromittiert ist.

Herausgeber

MHP Management- und IT-Beratung GmbH

MHP ist eine international agierende Management- und IT-Beratung mit Hauptsitz in Ludwigsburg, Deutschland. Seit nahezu drei Jahrzehnten begleitet das Unternehmen die Transformation der Prozesse und Produkte seiner rund 300 Kunden in den Branchen Automotive, Manufacturing, Aerospace, Public und Defense. Das Unternehmen der Porsche AG berät sowohl strategisch als auch operativ in zentralen Themenfeldern wie Customer Experience und Workforce Transformation, Fabrikplanung, Supply Chain Management, Cloud Solutions, Integration und Skalierung, Cyber Security, Big Data und Künstliche Intelligenz, Plattformen und Ökosystemen sowie Industrie 4.0 und Intelligent Products. Ziel ist es, Geschwindigkeit, Souveränität und Resilienz nachhaltig zu steigern. Die Unternehmensberatung verfügt über Tochtergesellschaften in den USA, Mexiko, Indien, Großbritannien, Rumänien und China. Rund 4.500 MHPlerinnen und MHPler vereint der Anspruch nach Exzellenz und nachhaltigem Erfolg. Dieser Anspruch treibt das Unternehmen weiter an – heute und in Zukunft.
mhp.com/newsroom

Befragungssteckbrief

Befragungszeitraum: 05.–16. Februar (online). **Befragt** wurden 1.060 IT-Expertinnen und -Experten aus Unternehmen mit mindestens 500 Mitarbeitenden in Deutschland und den USA. Die Ergebnisse sind repräsentativ und wurden mittels Quotierung ausgewertet und berücksichtigen einen statistischen Fehler von 4,3 Prozentpunkten.

Layout & Design: www.freiland-design.de

Kontakt

MHP
A PORSCHE COMPANY

SPONSOR
Dr. Jan Wehinger
Partner

E-Mail: jan.wehinger@mhp.com

AUTOR
Julian Seyfarth
Associate

E-Mail: julian.seyfarth@mhp.com

EXPERTE
Kevin Euler
Associated Partner Cyber Security

E-Mail: kevin.euler@mhp.com

AUTOR
Mirko Geyer
Sprecher AI, Cyber Security,
Aerospace & Defense

E-Mail: mirko.geyer@mhp.com

EXPERTE
Christian Zgardea
Partner Cyber Security

E-Mail: christian.zgardea@mhp.com