Whitepaper, gesponsert von DigiCert | Juni 2024

Die Entwicklung des digitalen Geschäfts erfordert eine moderne Krypto-Landschaft

Jennifer Glenn
Forschungsleiterin,
Security and Trust Group, IDC

Inhaltsverzeichnis

KLICKEN SIE AUF EINE ÜBERSCHRIFT, UM DIREKT ZUR ENTSPRECHENDEN SEITE ZU GELANGEN.

Zusammenfassung

Das digitale Geschäft ist die neue Realität für die meisten Unternehmen. In der IDC-Umfrage *Future Enterprise Resiliency and Spending Survey* vom Januar 2024 **bezeichneten sich 47 % der Befragten entweder als überwiegend digitales als oder als digital natives Unternehmen.** Einer der Hauptvorteile des digitalen Geschäftsbetriebs besteht darin, dass Daten problemlos über mehrere Anwendungen, Webfunktionen, Geräte, Abteilungen und Benutzer hinweg gemeinsam genutzt werden können. Dadurch können Unternehmen Telearbeit ermöglichen, sicher über die gesamte Lieferkette hinweg kommunizieren und digitale Dienstleistungen und Produkte entwickeln, die die Kunden zufrieden stellen.

Die Realität eines digitalen Unternehmens besteht darin, dass es eine komplexe Umgebung benötigt, die mehrere Cloud-Infrastrukturen und digitale Daten sowie ältere Hardware und Daten kombiniert, um einen optimalen Geschäftsbetrieb zu gewährleisten. Außerdem gibt es einfach mehr von allem: mehr Geräte, die miteinander kommunizieren, mehr Nutzer, die aus der Ferne auf Unternehmensressourcen zugreifen, und mehr Anwendungen, die in verschiedenen Clouds oder vor Ort laufen. Die Menge und der Wert der Datenbestände nehmen exponentiell zu. Die Aufrechterhaltung der Sicherheit und Integrität dieser komplexen Umgebung – und der Schutz all dieser Assets – ist für den Geschäftserfolg von entscheidender Bedeutung.

Gute Verschlüsselung ist entscheidend für wirksame Sicherheit; Krypto-Agilität ist entscheidend für wirksame Verschlüsselung

Es gibt viele Möglichkeiten, Daten im gesamten Unternehmen und seinem Ökosystem zu sichern. Verschlüsselung in ihren verschiedenen Formen ist eine gemeinsame Sicherheitsfunktion zum Schutz der Integrität von Verbindungen und Daten in jeder dieser Umgebungen. Beispielsweise verhindert Verschlüsselung, dass Daten auf Geräten von unbefugten Nutzern eingesehen werden können. Sie schützt die Daten auf öffentlichen Websites vor einer Kompromittierung. Sie schützt auch Daten, die zwischen Geräten für Software-Updates oder für die Kommunikation zwischen dem Software-Agenten und seinen Hosts übertragen werden.

Unternehmen können mehrere Verschlüsselungsalgorithmen verwenden, um Daten zu verbergen, insbesondere wenn die zu schützenden Daten als vertraulich oder sensibel eingestuft werden. Verschlüsselung ist eine übliche und notwendige Sicherheitskomponente. In der IDC-Umfrage zu *Datensicherheit und Datenschutz* vom März 2024 gaben fast 80 % der Befragten an, Verschlüsselung als Mittel zum Schutz der Privatsphäre einzusetzen (siehe **Abbildung 1,** nächste Seite). Das Verfahren zur Ver- und Entschlüsselung von Informationen zwischen Geräten und/oder Benutzern erfordert zusätzliche Technologien zur Bestätigung der Legitimität und Autorisierung.

Zu diesen Technologien gehören:

Kryptographische Schlüssel:
Die Generierung und Verwaltung von kryptographischen Schlüsseln, mit denen Daten verschlüsselt und anschließend von der vorgesehenen Einheit (Benutzer, Gerät, Anwendung usw.) entschlüsselt werden können.

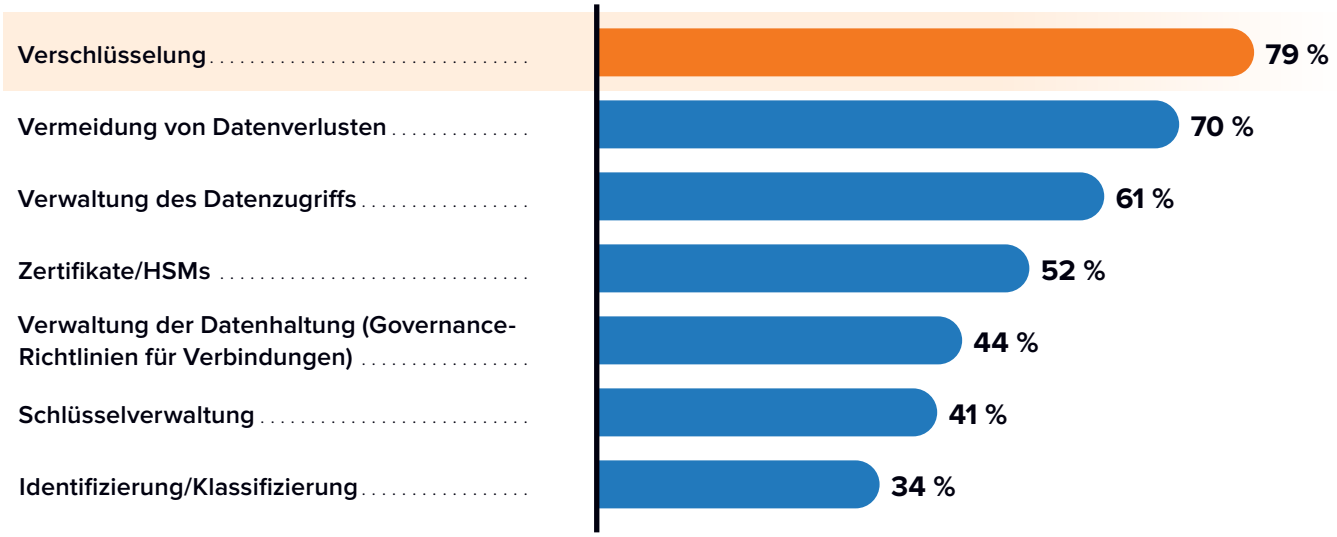
Digitale Zertifikate:
Die Verknüpfung einer Identität mit einem kryptographischen Schlüssel, um zu bestätigen, dass das Gerät, die Anwendung oder der Benutzer gültig und legitim ist. (Zertifikate werden von einer Zertifizierungsstelle [Certificate Authority, CA] ausgestellt, die Industriestandards verwendet, um die Identität eines Benutzers oder Computers zu überprüfen. Diese Validierungen sind zeitabhängig und können ablaufen oder widerrufen werden, wenn ein kryptographischer Schlüssel kompromittiert wird oder sich die Standards ändern. Eine Public Key Infrastructure [PKI] bietet den Rahmen für die Ausstellung digitaler Zertifikate).

ABBILDUNG 1

Gängige Datensicherheitstechnologien zur Einhaltung des Datenschutzes

Welche Datensicherheitstechnologien werden zum Nachweis des Datenschutzes/der Einhaltung der Vorschriften eingesetzt?

(% der Teilnehmer)



Hinweis: Mehrfachnennungen waren möglich. n = 619; Quelle: *IDC-Umfrage zu Datensicherheit und Datenschutz*, März 2024

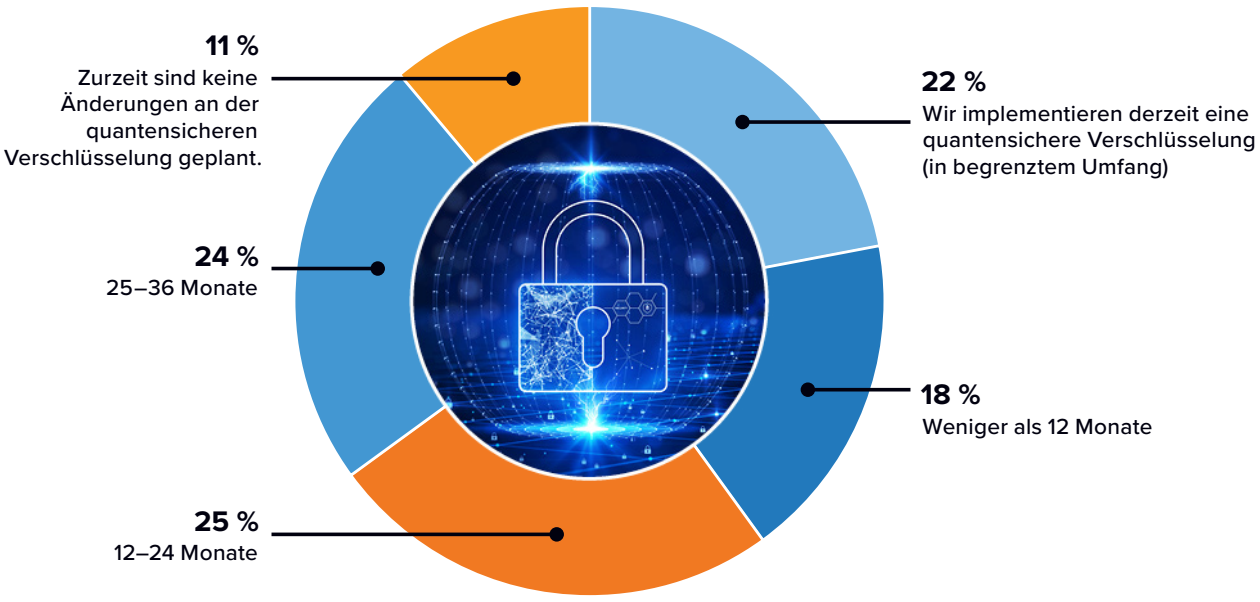
Dieser gesamte Prozess spielt eine wichtige Rolle beim Aufbau von Digital Trust. Wie die Infrastruktur, die er schützt, muss aber auch der Prozess sich weiterentwickeln und modernisieren, um die Sicherheit von Daten und Systemen zu gewährleisten. Angreifer können die Vorteile leistungsfähigerer Rechenprozesse nutzen, um Verschlüsselungsalgorithmen zu knacken. Gesetzliche Normen ändern sich. Die Kryptographie wird sich weiterentwickeln und fortschreiten. Die digitalen Unternehmen von heute brauchen nicht nur Modernisierung, sondern auch Kryptoagilität.

Kryptoagilität ermöglicht es Unternehmen, kryptografische Algorithmen, Parameter oder Methoden schnell anzupassen oder zu ändern, ohne die Infrastruktur grundlegend überarbeiten zu müssen. Dies wird wichtig sein, wenn sich Unternehmen auf Schwachstellen durch Quantencomputing vorbereiten. Das Quantencomputing verspricht eine schnellere Rechenleistung, mit der bestehende Verschlüsselungen in Sekundenschnelle geknackt werden können. Viele Unternehmen setzen bereits aktiv quantensichere Verschlüsselung ein, um diese Verbindungen und Daten sicher zu halten. In derselben IDC-Umfrage zu *Datensicherheit und Datenschutz* gaben 22 % der Befragten an, dass sie derzeit in begrenztem Umfang quantensichere Verschlüsselung einsetzen. Weitere 18 % der Befragten planen die Einführung einer quantensicheren Verschlüsselung in weniger als einem Jahr (siehe **Abbildung 2**).

ABBILDUNG 2

Die Implementierung einer quantensicheren Verschlüsselung ist bereits im Gange

Wann planen Sie, quantensichere Verschlüsselung in Ihrem Unternehmen einzuführen?
(% der Teilnehmer)



n = 415; Quelle: *IDC-Umfrage zu Datensicherheit und Datenschutz,* März 2024

Neben der Vorbereitung auf das Quantencomputing kann die Einführung kryptoagiler Prozesse auch bei der Bewältigung anderer Herausforderungen helfen, die sich aus der Vielfalt von Cloud- und Legacy-Infrastrukturen ergeben:

Erhöhtes Volumen der Zertifikate:
Mit der Zunahme hybrider und Multi-Cloud-Infrastrukturen hat sich die Anzahl der Verbindungen innerhalb des Ökosystems eines Unternehmens erhöht. Diese Zertifikate können in verschiedenen Abteilungen unterschiedliche Inhaber haben. Die Gültigkeitsdauer der einzelnen Zertifikate hängt von ihrer Verwendung ab. Darüber hinaus verkürzen Web-Properties im Namen der Sicherheit den Lebenszyklus ihrer Zertifikatsvalidierung. Gleichzeitig ist der Wunsch, Vertrauen in diese Verbindungen zu demonstrieren, für die meisten Unternehmen zu einer Priorität geworden. Insgesamt sind dadurch Tausende von Zertifikaten und Attributen hinzugekommen, die verwaltet werden müssen, so dass es schwierig ist, den Status jedes einzelnen zu kennen.

Unkotrollierte Ausbreitung von Zertifikaten:
Der Übergang zu Multi-Cloud- und hybriden Infrastrukturen schafft mehr Zugangspunkte von mehr Standorten aus. Zertifikate können sowohl von Produktteams als auch von IT-Betriebsgruppen für verschiedene Zwecke benötigt werden. Oft arbeiten diese Teams nicht zusammen und verwenden möglicherweise unterschiedliche Zertifizierungsstellen. Ohne eine einheitliche Sicht ist die Verwaltung der gesamten kryptographischen Prozesse eines Unternehmens nahezu unmöglich.

Mangel an qualifiziertem Personal/Mangel an strategischer Ausrichtung der Ressourcen:
Die Kryptografie ist als Spezialgebiet meist in der IT-Abteilung angesiedelt. Für diejenigen, die diese Rolle zu einem bestimmten Zweck übernommen haben, kann es schwierig sein, einen geschäftlichen Nutzen nachzuweisen (abgesehen davon, dass die Zertifikate verwaltet werden). Infolgedessen werden oft zusätzliche Aufgaben an den Mitarbeiter delegiert. Häufig übernehmen Praktiker die Stelle durch Fluktuation. In beiden Fällen wird die Fähigkeit zur effektiven Steuerung der Verschlüsselungsprozesse beeinträchtigt.

Implementierung einer modernen digitalen Vertrauensinfrastruktur

Digital Trust ermöglicht Unternehmen, Zuversicht und Integrität in die Verbindungen und Daten zu demonstrieren, die sie ihren Kunden anbieten. Die Implementierung einer kryptoagilen Infrastruktur ist ein entscheidendes Element, um Digital Trust jetzt und in Zukunft zu gewährleisten.

Um Digital Trust wirklich umzusetzen, bedarf es eines mehrstufigen Ansatzes, der Technologie und Prozesse kombiniert:

Sicherheitshygiene:
Die Grundlage der Kryptoagilität ist ganz einfach das Wissen darüber, welche kryptographischen Elemente im Umlauf sind. Dies beinhaltet eine Bestandsaufnahme der Zertifikate im gesamten Unternehmen, einschließlich Besitz, Lebenszyklus und Relevanz. Darüber hinaus müssen die Unternehmen die Standards für die Ausstellung dieser Zertifikate kennen und wissen, welche Änderungen anstehen. Wie bereits erwähnt, kann dies im derzeitigen Geschäftsumfeld eine Herausforderung darstellen.

Erfolg definieren:
Mit dem Wissen, was verwaltet werden muss, ist der nächste Schritt, zu bestimmen, wie der Erfolg für das Unternehmen aussieht und welche Maßnahmen dazu umgesetzt werden müssen. Dies umfasst:

- **Zielsetzung:**
  Bestimmen Sie, welche Elemente für den Geschäftsbetrieb wesentlich sind. Für viele ist dies die Service-Verfügbarkeit, d. h. keine Ausfälle aufgrund des Ablaufs von Zertifikaten. Für diejenigen, die in großem Umfang am Internet of Things teilnehmen, wird der Erfolg davon abhängen, ob sie gewährleisten können, dass ihre Geräte sicher aktualisiert werden. Weitere Schwerpunkte sind die Gewährleistung der Produktsicherheit und -validität sowie eine sichere Remote-Arbeitsumgebung.

- **Prioritäten setzen:**
  Ermitteln Sie, welche Systeme/Ergebnisse am meisten gefährdet sind. Angesichts der Vielzahl kryptographischer Ressourcen, die ein modernes Unternehmen ausmachen, müssen zwangsläufig Prioritäten gesetzt werden. Es kann auch wichtig sein zu wissen, welche Systeme schnell aktualisiert werden können und welche eine umfassende Überholung benötigen.

- **Investitionen in Ressourcen:**
  Planen und budgetieren Sie die für die Durchführung der Aufgabe erforderlichen Produkte, Partner und Mitarbeiter. Qualifiziertes Personal und das Budget stellen immer eine Herausforderung dar. Die Priorisierung wichtiger Aufgaben kann helfen.

Zentralisierte Sichtbarkeit und Verwaltung:
Die Lokalisierung und Planung dieser Assets ist von entscheidender Bedeutung – aber auch die Schaffung eines kontinuierlichen Prozesses für die Verwaltung aller Assets ist ein wichtiger Bestandteil der Kryptoagilität. Die Zusammenführung von Assets aus dem gesamten Unternehmen in einer einzigen Ansicht bietet einen Überblick darüber, was möglicherweise fehlt, sowie über den Status, den Eigentümer und den Bedarf jedes einzelnen Assets.

Berichterstattung und Rechtfertigung:
Ein wichtiger Teil jedes Geschäftsprozesses ist der Nachweis des Erfolgs. Dies gilt auch für die Kryptoagilität. Fachkräfte sollten darauf vorbereitet sein, Schlüsselindikatoren im Zusammenhang mit der Erfolgsplanung zu kommunizieren, einschließlich der Anzahl der vermiedenen Ausfälle und der Maßnahmen, die ergriffen wurden, um das Risiko für Remote-Mitarbeiter zu verringern.

Anpassung:
Ein oft übersehener Bereich für die Umsetzung von Kryptoagilität ist die Anpassung. Das Ziel des Krypto-Agilitätsprozesses ist Flexibilität für das Unternehmen – aber der Prozess selbst kann einige Anpassungen erfordern. Wo muss das Unternehmen aufgrund der Ergebnisse Änderungen vornehmen? Gibt es Redundanz? Gibt es Bereiche, in denen die Effizienz gesteigert oder die Sicherheit erhöht bzw. deutlicher demonstriert werden kann?

Vorteile der PKI-Modernisierung/ Kryptoagilität

Kryptoagilität bereitet Unternehmen auf das quantensichere Computing vor und trägt gleichzeitig dazu bei, verschiedene andere Ziele wie etwa Automatisierung zu erreichen. Wie bereits erwähnt, kann es in einem Unternehmen Hunderttausende von digitalen Zertifikaten mit unterschiedlichen Eigentümern, Verwendungszwecken, Standards und Lebenszyklen geben. Die Einführung von Krypto-Agilitätsprozessen erleichtert die Automatisierung der Erkennung, Bereitstellung und Verwaltung dieser Assets.

Automatisierung bietet im Vergleich zu manuellen Prozessen eine Reihe von Vorteilen für das Unternehmen:

Kosteneinsparungen:
Durch die verbesserte Transparenz haben Unternehmen einen besseren Überblick über die Zertifikate und Kryptoassets, die sie besitzen. Das ist der erste Schritt zur Beseitigung nicht mehr benötigter Assets. Darüber hinaus kann die Automatisierung Unternehmen helfen, mit weniger Mitarbeitern mehr zu erreichen.

Zeitersparnis:
Dies bringt unmittelbare Zeitersparnisse mit sich, u. a. eine Verkürzung des gesamten Prozesses um mehrere Wochen. Es bietet auch einige indirekte Zeitersparnisse, da es weniger Ausfälle gibt, bei denen die Teams ihre Arbeit unterbrechen müssen, um sich um das abgelaufene Zertifikat zu kümmern.

Verbesserte Einhaltung interner und externer Audits:
Die alten Methoden der Zertifikatsverwaltung mit manuellen Prozessen und Skripten machen Unternehmen anfällig für Ausfälle und Sicherheitslücken, die durch unentdeckte abgelaufene Zertifikate verursacht werden. Wie in NIST SP 1800-16 beschrieben, ist die automatisierte Verwaltung des Lebenszyklus von Zertifikaten – von der Identifizierung bis zur Erneuerung oder zum Widerruf – entscheidend für die Minimierung von Risiken und die Einhaltung von Vorschriften.

Flexibilität am Arbeitsplatz:
Die Automatisierung digitaler Vertrauensprozesse, wie z. B. die Verwaltung von Zertifikaten, ermöglicht eine skalierbare Authentifizierung, die für die Flexibilität am Arbeitsplatz von entscheidender Bedeutung ist. Mit der erweiterten passwortlosen Authentifizierung können Unternehmen ihren Mitarbeitern die Möglichkeit geben, zu arbeiten, wie und wo sie wollen, ohne sich um die Integrität und Sicherheit ihrer Verbindungen sorgen zu müssen.

DigiCert für die Modernisierung des Digital Trust

DigiCert mit Sitz in Lehi, Utah, ist ein weltweiter Anbieter von Digital Trust Lösungen. Das Angebotsportfolio ist darauf ausgerichtet, Unternehmen eine quantensichere Zukunft zu ermöglichen.

DigiCert Trust Lifecycle Manager (TLM) wurde entwickelt, um die Anforderungen in jeder Phase der Modernisierung des kryptographischen Prozesses zu erfüllen, einschließlich:

Identifizierung:
Kryptoagilität beginnt damit, Bewusstsein und Kontrolle über alle Assets zu haben. TLM bietet einen umfassenden Überblick über die kryptografische Landschaft eines Unternehmens, unabhängig davon, ob die Zertifikate von einer öffentlichen oder privaten Zertifizierungsstelle ausgestellt wurden. Das bedeutet, dass kryptographische Ressourcen wie öffentliche und private Zertifikate im gesamten Unternehmen identifiziert, katalogisiert und verfügbar gemacht werden müssen. Mit diesen Informationen können Unternehmen Schwachstellen, ineffiziente Verfahren und gefälschte Zertifikate leichter erkennen.

Management:
Eine agile Kryptoumgebung erkennt proaktiv Sicherheits- oder Betriebsprobleme. DigiCert TLM bietet Funktionen zur Verwaltung des Lebenszyklus von Zertifikaten über ein einziges Dashboard und zur Zusammenführung von privaten und öffentlichen PKIs. Zu den Verwaltungsfunktionen gehören auch wichtige Zeitplan- und Genehmigungskriterien, z. B. Informationen darüber, wann Zertifikate ablaufen und welche Zertifikate aufgrund von Normenänderungen ersetzt werden müssen.

Automatisierung:
Die zunehmende Anzahl von Krypto-Assets im digitalen Unternehmen macht eine Automatisierung für Krypto-Agilitätsinitiativen erforderlich. DigiCert TLM enthält Vorlagen und Konfigurationen zur Automatisierung von Zertifikatsabläufen und Zugriffsrechten. Durch die Entlastung der Krypto-Teams werden diese besser für Skalierbarkeit und Agilität positioniert.

DigiCert Trust Lifecycle Manager ist ein zentraler Bestandteil der DigiCert ONE Plattform für Digital Trust. Neben der Software bietet DigiCert auch PKI-Dienstleistungen an, um Unternehmen eine komplette Umgebung für die Einrichtung, Verwaltung und Migration von Zertifikaten zur Verfügung zu stellen. Diese Umgebung umfasst Hardware-Sicherheitsmodule, vordefinierte Richtlinien, Widerrufsfunktionen und mehrere Zertifikatstypen.

Neben der Software bietet DigiCert auch PKI-Dienstleistungen an, um Unternehmen eine komplette Umgebung für die Einrichtung, Verwaltung und Migration von Zertifikaten zur Verfügung zu stellen.

Herausforderungen und Chancen

Kryptoagilität (und Kryptographie im Allgemeinen) ist für die meisten Unternehmen ein sehr technisches Konzept. Während IT- und Sicherheitsteams die Verwaltung von Zertifikaten als wichtig erachten – insbesondere wenn es um Ausfälle und Eigentumsrechte geht – investieren sie häufig Zeit und Ressourcen in andere Sicherheitsinitiativen, die für das Management leichter nachzuvollziehen sind, wie z. B. den Schutz sensibler Daten vor generativen KI-Modellen und die Bekämpfung von Ransomware.

Wenn es um Quantencomputer und quantensichere Kryptografie geht, werden Sicherheits- und IT-Teams wahrscheinlich Schwierigkeiten haben, die Kosten für diese Technologien zu rechtfertigen, selbst bei Angriffen, bei denen Daten mit der Absicht exfiltriert werden, sie später zu entschlüsseln. Quantencomputer sind noch einige Jahre von einer breiten Anwendung entfernt, und obwohl es einige Ansätze gibt, die Bedrohungen zu antizipieren, ist ein groß angelegter Übergang zu quantensicheren Anwendungen unwahrscheinlich, solange es nicht zu einem signifikanten Angriff oder einer Kompromittierung kommt. Diese langsame Akzeptanz könnte für Anbieter wie DigiCert eine Herausforderung darstellen, da Unternehmen in andere Bereiche investieren wollen.

Allerdings geht es bei der Kryptoagilität nicht nur um quantensicheres Computing. Es geht darum, schnell und einfach zu navigieren und Schutzmaßnahmen anzupassen. Hinsichtlich der Risiken langfristiger Projekte ist Kryptoagilität – oder die Notwendigkeit, Digital Trust zu gewährleisten – ein berechtigtes Anliegen. Für Teams, die Schwierigkeiten haben, die Ausgaben für quantensichere Verschlüsselung zu rechtfertigen, kann die Konzentration auf Ansätze und Anbieter, die tiefergehende Fähigkeiten – wie z. B. Kryptoagilität – bieten, eine Möglichkeit sein, sich auf die Post-Quantenwelt vorzubereiten und gleichzeitig andere Geschäftsanforderungen zu erfüllen.

Fazit

Die digitale Wirtschaft hat die Zahl der Verbindungen und Datenbestände, die durch kryptographische Algorithmen geschützt werden, exponentiell erhöht.

Mit zunehmendem Volumen steigt nicht nur das Risiko der Kompromittierung, sondern auch das Risiko, dass wichtige Updates in der Flut übersehen werden. Dieses Problem wird sich im Laufe der Zeit noch verschärfen, da die Datenmengen weiter zunehmen und das Post-Quantum-Computing Einzug hält. Die Modernisierung kryptografischer Prozesse im Hinblick auf Agilität und Skalierbarkeit ist eine wichtige Grundlage für strategische Unternehmen. Sie bietet eine starke Sicherheit und die Fähigkeit, sich an sich ändernde Standardanforderungen anzupassen, um die kryptographische Infrastruktur in einer Post-Quantum-Welt zu schützen.

Über die IDC-Analystin

Jennifer Glenn
Forschungsleiterin, Security and Trust Group, IDC

Als Forschungsleiterin bei der IDC Security and Trust Group ist Jennifer Glenn verantwortlich für den Bereich Informations- und Datensicherheit. Zu ihren Kernkompetenzen gehört ein breites Spektrum an Technologien, darunter Messaging-Sicherheit, Verwaltung sensibler Daten, Verschlüsselung, Tokenisierung, Rechteverwaltung, Schlüsselverwaltung und Zertifikate. Im Rahmen dieser Forschung befasst sie sich mit der entscheidenden Rolle der Datensicherheit bei wichtigen Unternehmensinitiativen wie dem Aufbau von Kundenvertrauen und der digitalen Transformation.

Mehr über Jennifer Glenn

Hinweis des Sponsors

digicert®

DigiCert ist ein weltweit führendes Unternehmen im Bereich des Digital Trust, das Einzelpersonen und Unternehmen ermöglicht, sich online zu bewegen mit der Gewissheit, dass ihre digitalen Fußabdrücke sicher sind.

Als Plattform für Digital Trust bietet DigiCert ONE Unternehmen eine zentrale Übersicht und Kontrolle über ein breites Spektrum öffentlicher und privater Vertrauensbedürfnisse und sichert Websites, Unternehmenszugang und Kommunikation, Software, Identitäten, Inhalte und Geräte. DigiCert verbindet seine preisgekrönte Software mit seiner Branchenführerschaft in den Bereichen Standards, Support und Betrieb und ist einer der führenden Anbieter von Digital Trust Lösungen für die größten Unternehmen weltweit.

Weitere Informationen finden Sie unter www.digicert.com.

Folgen Sie @digicert

IDC Custom Solutions

Diese Veröffentlichung wurde von IDC Custom Solutions erstellt. Die Meinung, Analyse und die Forschungsergebnisse, wie hier präsentiert, stammen aus einem umfassenderen Forschungs- und Analyseprojekt, das von IDC unabhängig durchgeführt und veröffentlicht wurde, es sei denn, der entsprechende Hersteller ist als Sponsor angegeben. IDC Custom Solutions stellt IDC-Inhalte in einer Vielzahl von Formaten für den Vertrieb durch verschiedene Unternehmen bereit. Dieses IDC-Material ist für die externe Verwendung lizenziert, und die Verwendung oder Veröffentlichung von IDC-Forschungsergebnissen bedeutet in keiner Weise, dass IDC Produkte oder Strategien des Sponsors oder Lizenznehmers unterstützt.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
Tel.: +1 508 872 8200

idc.com @idc @idc

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation sowie der Verbrauchertechnologiemärkte. Mit mehr als 1.300 Analysten weltweit bietet IDC globale, regionale und lokale Expertise zu Chancen und Trends in Technologie und Wirtschaft in mehr als 110 Ländern. IDC-Analysen und -Erkenntnisse unterstützen IT-Profis, Führungskräfte und Investoren bei fundierten Entscheidungen über Technologien und beim Erreichen ihrer wichtigsten Geschäftsziele.