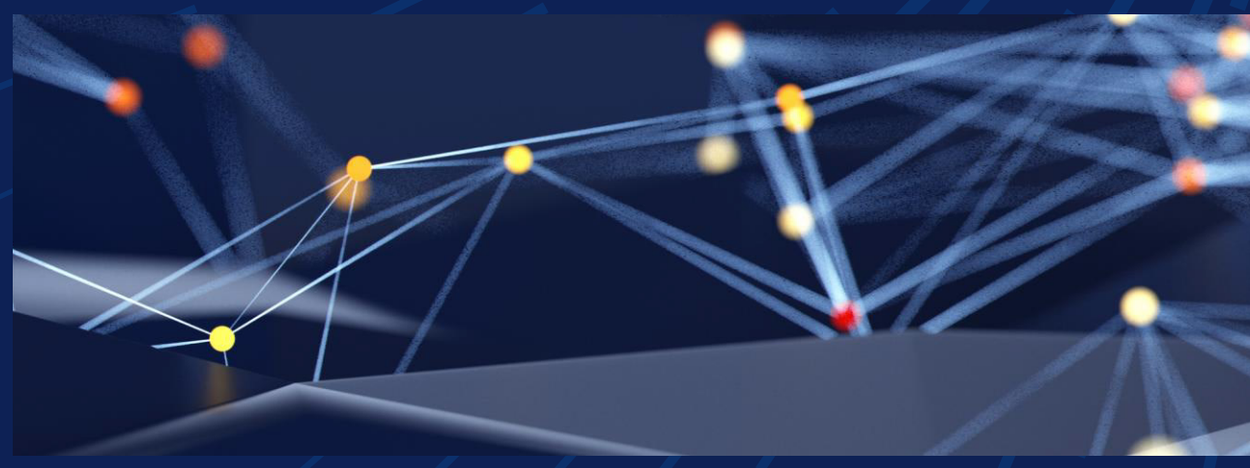
Die Zukunft der Cybersicherheit:

Anpassung an ein neues digitales Zeitalter



CybersicherheitsexpertInnen konzentrieren sich oft auf die Verhinderung von Angriffen und die Erstellung von Recovery-Plänen. Dabei entwickelt sich das gesamte Cybersicherheitsumfeld kontinuierlich weiter. Aus diesem Grund ist es wichtig, die Zukunft zu planen.

Im Hinblick auf die Zukunft zeichnen sich drei Bereiche ab: die Post-Quanten-Kryptografie, die sich ändernde regulatorische Landschaft und aufkommende Bedrohungen. Unternehmen sollten jetzt handeln, indem sie Lösungen planen und implementieren, sobald sie verfügbar sind.

Der Beginn der Post-Quanten-Kryptografie

Quantencomputing verspricht, ganze Branchen zu transformieren, und soll eine erstaunliche Rechenleistung mit einer Kapazität zur Problemlösung bieten, die weit über die Möglichkeiten herkömmlicher Computer hinausgeht. Diese Leistung könnte jedoch dazu führen, dass die aktuellen kryptografischen Methoden obsolet werden. Algorithmen wie RSA und ECC, die einen Großteil der heutigen sicheren Kommunikation unterstützen, könnten von einem fortschrittlichen Quantencomputer innerhalb von Sekunden geknackt werden. Diese aufziehende Bedrohung macht die Post-Quanten-Kryptografie zu einer immer dringender werdenden Notwendigkeit.

Die Post-Quanten-Kryptografie (PQC) stellt die Entwicklung kryptografischer Algorithmen dar, die in einem Quantencomputing-Zeitalter sicher bleiben. Das National Institute of Standards and Technology (NIST) hat dieses bevorstehende Risiko erkannt und ist führend bei der Standardisierung quantenresistenter Algorithmen.

Für Unternehmen ist die Vorbereitung auf diese Umstellung nicht verhandelbar. Die frühzeitige Einführung von PQC-Lösungen sorgt dafür, dass Daten sicher bleiben, wenn AngreiferInnen Zugriff auf Quantencomputing-Funktionen erhalten.

Bobbie Stempfley, VP of Cybersecurity und Business Unit Security Officer bei Dell, weist darauf hin, dass Unternehmen den Umstellungsprozess mit zwei Schlüsselbereichen beginnen sollten:

Identifizierung und Bestandsaufnahme aller derzeit verwendeten kryptografischen Modelle

Zu berücksichtigen sind dabei auch In-Flight-Daten, nicht nur Data at Rest. Dazu gehören Schlüsselmanagement, Codesignierung, Gerätekennungen, sicherer Zugriff und Telemetrie. Machen Sie eine umfassende Bestandsaufnahme und erstellen Sie dann eine Roadmap.

Berücksichtigung des Status von Lieferanten

Angesichts der Tatsache, dass moderne Unternehmen Tausende von Lieferanten haben können, sollten Sie sich der Risiken bewusst sein, die von ihnen ausgehen können. Stellen Sie sicher, dass sie sich ebenfalls auf künftige Veränderungen vorbereiten.

Über diese Ausgangspunkte hinaus sollten Sie Risikobewertungen durchführen, um anfällige Systeme zu identifizieren, hybride kryptografische Modelle zu implementieren, um während der Umstellung betriebsfähig zu bleiben, und mit Anbietern zusammenarbeiten, die quantensichere bereits Lösungen erforschen. Beachten Sie jedoch, dass es nicht den einzigen Anbieter oder die einzige Technologie geben wird, der bzw. die eine schlüsselfertige Lösung für all diese Punkte bietet.

Regulatorische Veränderungen in einer globalisierten Welt

Ein weiterer wichtiger Faktor für die Zukunft der Cybersicherheit ist die sich ändernde regulatorische Umgebung. Vorschriften gehen jetzt weit über die reine Compliance hinaus – sie werden zu einem wichtigen Framework, um Verantwortungsbewusstsein zu vermitteln, technologische Verbesserungen voranzutreiben und die BürgerInnen in einer vernetzten, datengesteuerten Welt zu schützen. Sie entwickeln sich jedoch schnell weiter und variieren je nach Region erheblich, was die Compliance deutlich komplizierter macht.

Allerdings gehen diese Bestimmungen über Strafen für Nichteinhaltung hinaus – sie dienen als Katalysatoren für bessere Cybersicherheitspraktiken. Unternehmen, die ihre Politiken aktiv an die regulatorischen Anforderungen anpassen, können neue Maßstäbe an Vertrauen und Betriebseffizienz erreichen. Dazu sollten sie Governance-Frameworks einrichten, die sich flexibel bei regulatorischen Veränderungen anpassen lassen. Außerdem sollten sie regelmäßige Compliance-Audits durchführen und in Schulungen für MitarbeiterInnen zu investieren, damit sie vertrauliche Informationen gemäß den neuesten Standards verarbeiten können.

Bei der Optimierung von Compliance-Maßnahmen müssen Cybersicherheits-Führungskräfte sicherstellen, dass sie verständlich kommunizieren und von ihren KollegInnen verstanden werden. Zu oft verwenden Sicherheitsfachleute Begriffe, die Kunden, Regulierungsbehörden und andere Interessengruppen möglicherweise nicht verstehen. SicherheitsexpertInnen müssen dafür sorgen, dass sie verstanden werden und dass die Personen, an die ihre Worte gerichtet sind, diese nicht erst interpretieren müssen.

> Stellen Sie sich die Umstellung auf Post-Quanten-Kryptographie wie einen Umzug mit einem komplett ausgestatteten Haus vor. Genauso schwierig wird es sein und die Herausforderung besteht darin, während der Umstellung nichts kaputt zu machen.“
>
> ***Bobbie Stempfley***
> *VP, Cybersecurity und Business Unit Security Officer, Dell Technologies*

Die Evolution der Bedrohungs- (und Abwehr-) Landschaft

KI revolutioniert die Geschäftswelt, steigert die Produktivität und erschließt neue Möglichkeiten des menschlichen Potenzials. In Bezug auf Cybersicherheit profitieren sowohl böswillige AkteurInnen als auch für ihre Gegenparts von der KI:

Böswilliger Einsatz: KI ermöglicht raffiniertere Angriffe, z. B. äußerst überzeugendes Spear-Phishing und Deepfakes.

Einsatz in der Gefahrenabwehr: KI unterstützt die Cyberabwehr durch:

- Schnelle Verarbeitung großer Mengen von Sicherheitsdaten.
- Effektivere Priorisierung von Bedrohungen.
- Bessere Erkennungs- und Reaktionsfähigkeiten.

Die Sicherheitstools werden sich jedoch nur weiter verbessern, da die Verarbeitung natürlicher Sprache es Sicherheitsfachleuten ermöglicht, direkt mit ihren Systemen zu interagieren und Systeme in die Lage zu versetzen, proaktive Cybersicherheitsmaßnahmen zu ergreifen.

Unternehmen sollten darauf hinarbeiten, die Funktionen simultan zu nutzen und gleichzeitig sicherzustellen, dass ihre Schulungen und andere Abwehrmechanismen auf dem neuesten Stand sind. Schulungen sind der beste Weg, um zu verhindern, dass MitarbeiterInnen raffinierteren Angriffen zum Opfer fallen.

Eine kennwortlose Welt

Kennwörter sind nicht mehr die sicherste Methode des Identitäts- und Zugriffsmanagements.

Herkömmliche kennwortbasierte Systeme weisen erhebliche Sicherheitslücken auf, die sie angesichts der Anforderungen der modernen Cybersicherheit immer unzureichender erscheinen lassen. Kennwörter sind anfällig für Angriffe wie Credential Stuffing, Phishing und Brute-Force-Versuche, die Unternehmen oft unnötigen Risiken aussetzen. Darüber hinaus werden diese Sicherheitslücken durch inadäquates Nutzerverhalten – wie die Wiederverwendung von Kennwörtern oder die Erstellung schwacher Kennwörter – verstärkt.

Kennwortlose Authentifizierungsmethoden wie biometrische Daten, Zertifikate und Hardwaretokens bieten eine stärkere und sicherere Alternative, da sie ganze Klassen von kennwortbezogenen Bedrohungen eliminieren können. Die Umstellung auf kennwortlose Systeme markiert eine kritische Weiterentwicklung im Bereich der Identitäts- und Zugriffsverwaltung und passt Sicherheitsmaßnahmen an die zunehmende Komplexität der Cyberbedrohungen an.

Die Einführung kennwortloser Technologien bietet außerdem zahlreiche Vorteile, darunter die Reduzierung der Angriffsfläche, die Verbesserung des Nutzererlebnisses durch schnellere, nahtlose Anmeldungen und die Senkung der IT-Kosten durch die Reduzierung der Anzahl kennwortbezogener Incidents. Die Verwendung fortschrittlicher Methoden sorgt für einen stärkeren Sicherheitsstatus und hilft Unternehmen, behördliche Compliance-Standards einzuhalten. Die Umstellung auf kennwortlose Systeme ist nicht nur ein Trend, sondern ein notwendiger Schritt zum Aufbau eines sichereren, effizienteren digitalen Ökosystems für Einzelpersonen und Unternehmen.

Fazit

Cybersicherheit tritt in ein transformatives Zeitalter ein, das durch Quanten-Computing, sich ändernde Vorschriften und immer ausgefeiltere Bedrohungen geprägt ist. Um einen Schritt voraus zu sein, müssen Unternehmen Innovationen wie Post-Quanten-Kryptographie, KI-gestützte Abwehrmaßnahmen und kennwortlose Authentifizierung einführen. Durch Priorisierung von Bereitschaft, Zusammenarbeit und strategischen Investitionen können Unternehmen eine sicherere und widerstandsfähige digitale Umgebung aufbauen. Es ist an der Zeit, zu handeln.

Dell Produkte und Lösungen, die helfen können

Dell Lösung	Beschreibung
Beratungsservices für Cybersicherheit	Fachkundige Beratung, die Sie bei der Planung der sich entwickelnden Bedrohungslandschaft unterstützen kann, einschließlich aktueller und neuer Bedrohungen.
vCISO	Virtual Chief Information Security Officer, bietet Cybersicherheits-Fachkompetenz und kann bei der Erkennung und Verwaltung von Risiken und der strategischen Entscheidungsfindung helfen.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **dell.com/cybersecuritymonth.**