Presseinformation

Bitte zur sofortigen Veröffentlichung

IS4IT Kritis präsentiert auf der itsa 2026 Lösungen für Quantenresilienz

Vom 27. bis 29. Oktober stellt der IBM Gold Partner IS4IT Kritis auf der it-sa 2026 in Nürnberg erstmals Lösungen vor, die Unternehmen dabei unterstützen, ihre Systeme langfristig quantenresilient zu machen.

Obrigheim, 07. Oktober 2026 – Kryptografie durchdringt jeden Bereich der digitalen Welt und ist unverzichtbar, um bei der zunehmenden Bedrohungslage Cybersicherheit zu gewährleisten. Durch die absehbaren Entwicklungen im Bereich Quantentechnologie sind Unternehmen gezwungen, sich bereits heute auf die Gefahren von morgen vorzubereiten. Dafür müssen sie im ersten Schritt auf Post-Quantum-Verschlüsselungsalgorithmen umstellen und ihre Cybersicherheitsmaßnahmen innerhalb der gesamten Organisation entsprechend modernisieren.

Unverzichtbar: Vorbereitung auf Cyberattacken in der Welt von morgen

Obwohl die derzeitigen Verschlüsselungsverfahren durch die momentan verfügbare Technologie nicht entschlüsselt werden können, sind sie aufgrund der Entwicklung leistungsfähiger Quantencomputer absehbar gefährdet. Hauptproblematik ist das Szenario „Harvest Now, Decrypt Later“, bei dem verschlüsselte Daten heute abgefangen und gespeichert werden, um sie in Zukunft zu dechiffrieren. Betroffen sind vor allem Informationen mit langer Schutzdauer wie Gesundheits- oder Forschungsdaten, aber auch staatliche Dokumente, die besonderer Geheimhaltung unterliegen.

Lt. BSI ist Quantenresilienz die Fähigkeit einer Organisation, ihre kryptografischen Verfahren so zu verwalten und weiterzuentwickeln, dass sie auch im Zeitalter leistungsfähiger Quantencomputer ein angemessenes Sicherheitsniveau aufrechterhalten kann. Diese Fähigkeit basiert auf quantensicheren kryptografischen Verfahren, kryptografischer Agilität, einer vollständigen Krypto-Inventarisierung und einer geplanten risikobasierten Migration.

„Mit verschiedenen IBM-Werkzeugen aus dem Bereich IBM Quantum Safe lassen sich kryptografische Risiken erkennen, Post-Quantum-Kryptografie einführen und Systeme langfristig quantenresistent machen. Das ist Sicherheit, die in die Zukunft reicht und somit unverzichtbar für wirklich sicherheitsrelevante Daten unserer Kunden. IBM gehört zu den wenigen Unternehmen, die mit ihrer Plattform den gesamten Migrationsprozess zur Quantenresilienz abdecken – von der Bestandsaufnahme über die Planung und Umsetzung bis zum Betrieb. Wir haben uns daher entschieden, unser Produktportfolio entsprechend zu erweitern", sagt Manuel Noe, Geschäftsführer von IS4IT Kritis und IBM Gold Partner. „Da aufgrund von ‚Harvest Now, Decrypt Later’

absehbarer Handlungsdruck besteht, haben wir uns entschieden, die Lösungen gemeinsam mit IBM auch gleich auf der it-sa zu präsentieren. Damit wollen wir sicherstellen, dass es die Unternehmen in Zukunft nicht wirklich kalt erwischt. Denn wer denkt heute schon daran, dass in wenigen Jahren die jetzigen Schutzmechanismen obsolet sind?"

IBM-Werkzeuge für Quantenresilienz

Wie bei allen Methoden im Bereich Cybersicherheit geht es auch beim Aufbau quantenresilienter IT-Umgebungen um drei wesentliche Aspekte:

- Bestandsaufnahme – Analyse der Risiken und Schwachstellen
- Planung und Umsetzung – Behebung der Defizite durch Umstieg auf neue Technologien
- Betrieb – Automatisierte Administration für langfristige Sicherheit

Mit IBM Quantum Safe Explorer, IBM Quantum Safe Remediator und IBM Guardium Cryptography Manager adressiert IBM in ihrer Plattform sämtliche Anforderungen.

Der IBM Quantum Safe Explorer unterstützt Unternehmen dabei, kryptografische Risiken in ihrer IT-Landschaft transparent zu machen und sich frühzeitig auf das Zeitalter des Quantencomputings vorzubereiten. Die Lösung identifiziert kryptografische Verfahren, Zertifikate, Schlüssel und Abhängigkeiten in Anwendungen, Systemen und Netzwerken. Dadurch erhalten Organisationen einen umfassenden Überblick über potenzielle Schwachstellen sowie den Handlungsbedarf für eine Migration zu quantensicheren Verfahren. Mit detaillierten Analysen und Berichten schafft der IBM Quantum Safe Explorer die Grundlage für eine strukturierte und risikobasierte Modernisierung der Kryptografie.

Für die Planung und Umsetzung der Migration auf quantensichere Kryptografie kommt IBM Quantum Safe Remediator zum Einsatz. Aufbauend auf den Erkenntnissen aus der Analyse priorisiert die Lösung betroffene Anwendungen, Systeme und kryptografische Abhängigkeiten und erstellt konkrete Handlungsempfehlungen. Sie hilft dabei, Migrationsprozesse zu strukturieren, Risiken zu bewerten und die Umstellung effizient zu koordinieren. So lassen sich komplexe Transformationsprojekte nachvollziehbar steuern und Compliance-Anforderungen erfüllen. Unternehmen können ihre kryptografische Infrastruktur schrittweise modernisieren und gleichzeitig den laufenden Geschäftsbetrieb absichern.

Der IBM Guardium Cryptography Manager ermöglicht die zentrale Verwaltung und Automatisierung kryptografischer Schlüssel, Zertifikate und Richtlinien über hybride IT-Umgebungen hinweg. Die Lösung vereinfacht den gesamten Lebenszyklus kryptografischer Assets – von der Bereitstellung über die Rotation bis hin zur Erneuerung und Stilllegung. Durch die Integration unterschiedlicher Schlüsselmanagement- und PKI-Systeme verbessert sie Transparenz, Sicherheit und Compliance. Automatisierte Prozesse reduzieren den administrativen Aufwand und minimieren das Risiko fehlerhafter Konfigurationen. So unterstützt der IBM Guardium Cryptography Manager Unternehmen dabei, ihre Kryptografie effizient zu verwalten und langfristig auf zukünftige Sicherheitsanforderungen vorzubereiten.

Weitere Informationen zum IBM-Produktportfolio auf https://www.ibm.com/quantum/quantum-safe

Interessenten und Kunden, die die it-sa 2026 besuchen, können sich direkt am Stand 101 in Halle 8 über Chancen und Risiken des Quantencomputings sowie über Maßnahmen für ein Maximum an Quantenresilienz informieren und sich dazu mit den Expertinnen und Experten von IBM und IS4IT Kritis austauschen. Darüber hinaus hält Manuel Noe (Geschäftsführer IS4IT Kritis GmbH) und Bob Kalka (Global Lead, IBM Security) im Rahmen des it-sa Expo & Congress am Dienstag, 27. Oktober 2026, um 16:30 Uhr einen Fachvortrag zum Thema: **Die Sicherheitslücke bei agentischen Operationen schließen: Von Null zu Best Practice** im Forum D in Halle 7. Neben dem zweifachen Olympiasieger Jochen Lochner steht die IS4IT Kritis zusammen mit den Partnern des Security-Ligateams – IBM, IS4IT, IS4IT Schweiz und die SIEVERS-GROUP – für Fachgespräche zur Verfügung.

IS4IT KRITIS GmbH

Die IS4IT KRITIS GmbH hat ihren Hauptsitz in Obrigheim und eine Niederlassung in Oberhaching bei München. Der zertifizierte Cybersecurity-Spezialist und Experte für Künstliche Intelligenz (KI) bietet Informationssicherheit für kritische Infrastrukturen und richtet sich mit seinem Full-Service-Angebot an Firmen und Organisationen mit erhöhtem IT-Schutzbedarf. Darüber hinaus werden im Geschäftsbereich KI auf Grundlage der KI-Plattform watsonx von IBM Prozesse und Arbeitsabläufe in allen Unternehmensbereichen optimiert.

Das Cybersecurity-Lösungsportfolio deckt Themen wie Security Consulting, Identitätsmanagement, Hochleistungsspeicher & Quantenresilienz, Security Operations Center, Security Testing, OT Security sowie Security Infrastructure umfassend ab. IBM watsonx bildet die Technologiebasis für den KI-Geschäftsbereich der IS4IT Kritis. Mit watsonx.governance werden Unternehmen bei der Erfüllung des EU AI Act unterstützt, watsonx Orchestrate sorgt unternehmensweit für die KI-gestützte Prozessoptimierung.

Die von IS4IT Kritis konzipierten Lösungen können umgesetzt und als Managed Services gemeinsam mit renommierten Partnern betrieben werden, wobei IS4IT Kritis für den Kunden stets die Gesamtkoordination und -verantwortung übernimmt. IS4IT Kritis ist nach ISO/IEC 27001 und ISO 9001 zertifiziert und aktives Mitglied im Bundesverband für den Schutz Kritischer Infrastrukturen e.V. (BSKI), im Bundesverband IT-Sicherheit e.V. (TeleTrusT) sowie in der Allianz für Cyber-Sicherheit. Die Unternehmensgruppe IS4IT, zu der die IS4IT KRITIS GmbH, die IS4IT GmbH, die IS4IT Schweiz AG und die IS4IT Cyber Security Austria GmbH gehören, betreut mit ihrer Zentrale in Oberhaching bei München sowie den Standorten Berlin, Eschborn, Leinfelden-Echterdingen, Nürnberg, Obrigheim, Schwaig, Wien und Zug Kunden in Deutschland, Österreich und der Schweiz.

Kontaktinformationen für Rückfragen

IS4IT KRITIS GmbH
Manuel Noe
Kraichgaublick 13
74847 Obrigheim

Telefon +49 6261 31944-0
info@is4it-kritis.de
www.is4it-kritis.de