PRESSEMITTEILUNG / PUBLIKATIONSANKÜNDIGUNG

Bundesverband IT-Sicherheit e.V. (TeleTrusT) veröffentlicht Handreichung zu Kryptoagilität

Berlin, 16.11.2026 - Eine aktuelle Handreichung der TeleTrusT-Arbeitsgruppe "Kryptoagilität" adressiert die wachsende Notwendigkeit, kryptografische Verfahren unter veränderten Bedrohungslagen, regulatorischen Anforderungen und technologischen Entwicklungen kontrolliert und mit vertretbarem Aufwand anpassen zu können.

https://www.teletrust.de/publikationen/broschueren/kryptoagilitaet/

In der heutigen digitalen Welt ist die Fähigkeit, kryptografische Verfahren flexibel anzupassen, von zentraler Bedeutung - insbesondere im Hinblick auf die bevorstehende Migration zu Post-Quanten-Algorithmen.

Kryptoagilität bezeichnet in diesem Kontext einen strukturierten Prozess, mit dem Hersteller und Anwender kryptografische Bausteine - etwa Algorithmen, Protokolle, Schlüssel, Zertifikate oder Bibliotheken - schnell und ohne Beeinträchtigung der Kernfunktionalität eines IT-Systems austauschen können. Dabei handelt es sich nicht nur um eine rein technische Fähigkeit, sondern um eine übergreifende Kompetenz, die organisatorische Klarheit, technische Entkopplung und kontinuierliche Anpassungsmechanismen vereint. Externe Einflüsse wie neu entdeckte Schwachstellen, geänderte regulatorische Vorgaben, aktualisierte Standards, neue Bedrohungsszenarien oder technologische Entwicklungen (z.B. Quanten-Computing) müssen zeitnah und strukturiert adressiert werden, sodass das System stets dem aktuellen Sicherheitsniveau entspricht.

Um kryptoagile Prozesse zu ermöglichen, müssen klare organisatorische Strukturen etabliert werden. Hersteller sind für das Design und die Bereitstellung austauschbarer Schnittstellen verantwortlich, während die Anwender im Betrieb die Umsetzung und das Monitoring übernehmen. Eine Kryptostrategie legt Grundsätze wie Austauschbarkeit und Konfigurierbarkeit fest und verankert sie in internen Richtlinien. Zentral ist zudem das Kryptoinventar (oder Krypto-Kataster), das transparent aufzeigt, welche kryptografischen Objekte wo eingesetzt werden. Auf Basis dieses Inventars können Risiko- und Migrationsanalysen durchgeführt sowie Abhängigkeiten, Verantwortlichkeiten und Entscheidungsprozesse definiert werden.

Die technische Realisierung kryptoagiler Systeme beruht auf einer konsequenten Abstraktion kryptografischer Funktionen. Statt Algorithmen fest im Produkt zu verankern, werden Schnittstellen definiert, die nur den Zweck (z.B. "Daten verschlüsseln", "Nachricht signieren") beschreiben. Implementierungen können dann die zugrunde liegenden kryptografischen Algorithmen austauschen, beispielsweise über Updates, ohne dass das übrige System angepasst werden muss. Durch diese Entkopplung bleibt die Fachlogik des Systems unverändert, während kryptografische Komponenten flexibel und kontrolliert ersetzt werden können.

Durch diese strukturierten Prozesse können Unternehmen sicherstellen, dass ihre Kryptografie stets den aktuellen Bedrohungen und regulatorischen Anforderungen gewachsen ist.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breitgefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT), Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
https://www.teletrust.de