Post-Quanten-Kryptografie: Warum Umstellung mehr ist als ein Softwareupdate

C2.1 - QUANTENTECHNOLOGIEN UND SICHERHEIT: WENN VERSCHLÜSSELUNG VERALTET

Wortschatz zum Text

Deutsch	Englisch / Erklärung
die Post-Quanten-Kryptografie	post-quantum cryptography
die Umstellung	transition / migration
die Migration	migration
die Migrationsfähigkeit	migration capability
das Kryptoinventar	cryptographic inventory
die Kryptoagilität	crypto-agility
die Standardisierung	standardization
die Implementierungssicherheit	implementation security
die Interoperabilität	interoperability
die Rückwärtskompatibilität	backward compatibility
die Übergangslösung	transitional solution
das Hybridverfahren	hybrid approach
die Schlüsselgröße	key size
die Signaturgröße	signature size
die Rechenlast	computational load
die Bandbreite	bandwidth
die Speicheranforderung	storage requirement
das eingebettete System	embedded system
die Altanlage	legacy system
die Lieferkette	supply chain

Deutsch	Englisch / Erklärung
die Softwarebibliothek	software library
die Zertifikatskette	certificate chain
die Schlüsselverwaltung	key management
die Sicherheitszertifizierung	security certification
die Testumgebung	test environment
die Fehlkonfiguration	misconfiguration
die Seitenkanalanalyse	side-channel analysis
die Implementierungslücke	implementation flaw
die Protokollanpassung	protocol adaptation
die Betriebsunterbrechung	service interruption
die Verfügbarkeitsanforderung	availability requirement
die kritische Infrastruktur	critical infrastructure
die Beschaffungsrichtlinie	procurement guideline
die Governance-Struktur	governance structure
die Risikopriorisierung	risk prioritization
die Übergangsfrist	transition period
die Abhängigkeit	dependency
die Schulung	training
die Dokumentationspflicht	documentation duty
die Auditierbarkeit	auditability
die Sicherheitsökonomie	security economics
migrationsfähig	migration-capable
interoperabel	interoperable
ressourcenintensiv	resource-intensive
standardkonform	standard-compliant
zertifizierbar	certifiable

Meine zusätzlichen Wörter / Notizen:

Post-Quanten-Kryptografie: Warum Umstellung mehr ist als ein Softwareupdate

C2.1 - QUANTENTECHNOLOGIEN UND SICHERHEIT: WENN VERSCHLÜSSELUNG VERALTET

Post-Quanten-Kryptografie wird häufig so dargestellt, als müsse man nur einen alten Algorithmus durch einen neuen ersetzen. Diese Vorstellung ist bequem, aber gefährlich. Kryptografie ist in modernen Systemen selten ein isolierter Baustein. Sie ist in Protokolle, Geräte, Softwarebibliotheken, Zertifikatsketten, Identitätsdienste, Bezahlprozesse, Produktionsanlagen, Verwaltungsverfahren, Cloud-Infrastrukturen und mobile Anwendungen eingebettet. Eine Umstellung betrifft daher nicht nur Code, sondern auch Organisation, Beschaffung, Standards, Schulung, Prüfung und Verantwortung.

Der erste Schritt ist oft der schwierigste: herausfinden, wo Kryptografie überhaupt verwendet wird. Viele Organisationen besitzen kein vollständiges Kryptoinventar. Sie wissen vielleicht, welche Verfahren in zentralen Servern laufen, aber nicht, welche Algorithmen in älteren Geräten, eingebetteten Steuerungen, VPN-Gateways, Archivsystemen, Softwarebibliotheken oder Zulieferkomponenten stecken. Ohne diese Übersicht wird Migration zur Vermutung. Man aktualisiert das Sichtbare und übersieht das Eingebaute. Gerade solche übersehenen Abhängigkeiten können später Sicherheitslücken erzeugen.

Post-Quanten-Verfahren bringen zudem technische Eigenschaften mit, die nicht automatisch in bestehende Systeme passen. Manche haben größere öffentliche Schlüssel, größere Signaturen oder höhere Rechenlast. Das ist für einen modernen Server vielleicht beherrschbar, für eine Chipkarte, ein medizinisches Gerät, ein industrielles Steuerungssystem oder einen Satellitenkanal aber nicht trivial. Bandbreite, Speicher, Energieverbrauch und Antwortzeiten können sicherheitsrelevant werden. Ein Algorithmus kann theoretisch stark sein und trotzdem in einer bestimmten Umgebung schlecht funktionieren.

Auch Interoperabilität ist ein Kernproblem. Digitale Kommunikation funktioniert, weil Systeme auf beiden Seiten dieselben Protokolle, Formate und Standards verstehen. Wenn eine Behörde, ein Unternehmen oder ein Hersteller zu früh oder zu isoliert umstellt, können Verbindungen abbrechen. Wenn alle zu lange warten, entsteht ein gemeinsames Risiko. Übergangsarchitekturen müssen deshalb alte und neue Verfahren zeitweise parallel unterstützen. Hybridverfahren können helfen, indem sie klassische und post-quanten-resistente Methoden kombinieren. Doch auch hybride Lösungen erhöhen Komplexität und müssen sorgfältig implementiert werden.

Die Standardisierung spielt dabei eine doppelte Rolle. Einerseits schafft sie Vertrauen, Vergleichbarkeit und gemeinsame technische Grundlagen. Organisationen brauchen standardkonforme Verfahren, um Beschaffung, Zertifizierung und Haftung zu klären. Andererseits kostet Standardisierung Zeit. Wer zu früh auf ein nicht ausreichend geprüftes Verfahren setzt, riskiert spätere Umstellungen. Wer zu spät beginnt, riskiert Migrationsstau. Der richtige Zeitpunkt ist daher kein rein technisches Datum, sondern eine strategische Entscheidung unter Unsicherheit.

Implementierungssicherheit ist mindestens so wichtig wie algorithmische Sicherheit. Viele Angriffe brechen nicht die Mathematik, sondern die konkrete Umsetzung. Fehlerhafte Zufallszahlen, unsichere Schlüsselverwaltung, unvollständige Prüfungen, Seitenkanäle, Timing-Informationen oder Fehlkonfigurationen können selbst robuste Verfahren schwächen. Post-Quanten-Verfahren sind in dieser Hinsicht anspruchsvoll, weil neue mathematische Strukturen auch neue Implementierungsrisiken mitbringen. Sicherheit entsteht nicht dadurch, dass ein Algorithmusname auf einer Liste steht. Sie entsteht durch korrektes Design, geprüften Code, sichere Betriebsprozesse und kontinuierliche Überwachung.

Besonders schwierig ist die Umstellung in kritischen Infrastrukturen. Energieversorgung, Telekommunikation, Verkehr, Gesundheitswesen, Finanzsysteme und staatliche Register haben hohe Verfügbarkeitsanforderungen. Sie können nicht beliebig experimentieren oder Systeme kurzfristig abschalten. Gleichzeitig schützen sie Daten und Prozesse mit hohem Schadenspotenzial. Migration muss daher getestet, gestaffelt und rückfallfähig sein. Eine schlecht geplante Sicherheitsumstellung kann selbst zum Betriebsrisiko werden.

Auch Beschaffungspolitik ist betroffen. Wenn heute neue Geräte gekauft werden, die über fünfzehn Jahre betrieben werden sollen, müssen sie migrationsfähig sein. Es reicht nicht, aktuelle Sicherheitsstandards zu erfüllen, wenn absehbar ist, dass diese Standards während der Lebensdauer veralten. Verträge, Ausschreibungen und Sicherheitszertifizierungen müssen Anforderungen an Kryptoagilität, Updatefähigkeit und Dokumentation enthalten. Sonst werden neue Altlasten geschaffen: Systeme, die frisch gekauft, aber kryptografisch schwer anpassbar sind.

Die Umstellung ist außerdem eine Governance-Aufgabe. Wer entscheidet, welche Systeme zuerst migrieren? Wer trägt Kosten? Wer bewertet Daten mit Langzeitvertraulichkeit? Wer kontrolliert Zulieferer? Wer dokumentiert Ausnahmen? Wer haftet, wenn eine Übergangslösung versagt? Ohne klare Verantwortlichkeiten wird Post-Quanten-Migration zu einem diffusen technischen Projekt, das zwischen IT-Abteilung, Rechtsabteilung, Einkauf und Management hin- und hergeschoben wird. Dabei ist sie ein strategisches Risikothema.

Kryptoagilität ist deshalb mehr als ein technisches Schlagwort. Sie verlangt Architekturen, in denen Algorithmen, Schlüsselgrößen und Zertifikate austauschbar bleiben. Sie verlangt Prozesse, in denen Sicherheitsänderungen geplant, getestet, ausgerollt und dokumentiert werden können. Sie verlangt Personal, das kryptografische Abhängigkeiten versteht. Und sie verlangt Führung, die Sicherheit nicht nur als einmalige Anschaffung, sondern als dauerhafte Pflege einer Vertrauensinfrastruktur begreift.

Die Kosten dieser Umstellung sind sichtbar, der Nutzen häufig nicht. Wenn Migration gelingt, passiert im besten Fall nichts: Verbindungen funktionieren, Daten bleiben vertraulich, Signaturen bleiben verlässlich. Genau diese Unsichtbarkeit erschwert Investitionen. Doch Untätigkeit ist ebenfalls eine Entscheidung. Wer heute keine Inventur macht, keine Beschaffungsvorgaben ändert und keine Testumgebungen aufbaut, verschiebt Risiken in eine Zukunft, in der die Umstellung unter Zeitdruck teurer und gefährlicher wird.

Post-Quanten-Kryptografie ist daher kein einzelnes Produkt, das man installiert. Sie ist ein Transformationsprozess. Er verbindet Mathematik mit Verwaltung, Softwaretechnik mit Beschaffung, Datenschutz mit Infrastrukturpolitik und Risikoanalyse mit Organisationskultur. Die Frage lautet nicht nur, welcher Algorithmus quantenresistent ist. Die entscheidende Frage lautet, ob Institutionen in der Lage sind, ihre eigene Sicherheitsarchitektur rechtzeitig zu erkennen, zu verändern und dabei funktionsfähig zu bleiben.

Fragen zum Text

1. Warum ist Post-Quanten-Umstellung mehr als ein Algorithmuswechsel?

2. Warum ist ein Kryptoinventar notwendig?

3. Warum ist Migration ohne Kryptoinventar riskant?

4. Welche technischen Eigenschaften post-quanten-resistenter Verfahren können Probleme erzeugen?

5. Warum sind eingebettete Systeme besonders schwierig?

6. Was bedeutet Interoperabilität?

7. Warum sind Übergangsarchitekturen notwendig?

8. Was sind Hybridverfahren?

9. Warum ist Standardisierung ambivalent?

10. Warum reicht algorithmische Sicherheit allein nicht aus?

11. Warum sind kritische Infrastrukturen besonders heikel?

12. Warum ist Beschaffungspolitik Teil der Migration?

13. Welche Governance-Fragen nennt der Text?

14. Warum ist Kryptoagilität mehr als ein technisches Schlagwort?

15. Warum ist der Nutzen erfolgreicher Migration schwer sichtbar?

16. Warum ist Untätigkeit ebenfalls eine Entscheidung?

17. Was ist die zentrale Schlussfolgerung des Textes?

Multiple Choice

1. Warum ist die Post-Quanten-Migration kein simples Softwareupdate?

- [ ] A) Kryptografie ist in viele technische und organisatorische Strukturen eingebettet.
- [ ] B) Algorithmen haben nie mit Systemen zu tun.
- [ ] C) Alle Geräte aktualisieren sich automatisch.
- [ ] D) Verschlüsselung existiert nur in Browsern.

2. Was ist ein Kryptoinventar?

- [ ] A) Eine Übersicht darüber, wo welche kryptografischen Verfahren eingesetzt werden.
- [ ] B) Eine Liste aller Büroklammern.
- [ ] C) Ein Ersatz für Sicherheitsstandards.
- [ ] D) Ein Verbot von Migration.

3. Warum können größere Schlüssel oder Signaturen problematisch sein?

- [ ] A) Sie können Bandbreite, Speicher, Rechenlast und Antwortzeiten belasten.
- [ ] B) Sie reduzieren immer automatisch jede Last.
- [ ] C) Sie betreffen nur gedruckte Dokumente.
- [ ] D) Sie machen Interoperabilität überflüssig.

4. Was bedeutet Interoperabilität?

- [ ] A) Systeme können miteinander kommunizieren, weil sie gemeinsame Formate und Protokolle verstehen.
- [ ] B) Systeme müssen isoliert bleiben.
- [ ] C) Algorithmen werden nicht standardisiert.
- [ ] D) Schlüssel dürfen nie ausgetauscht werden.

5. Warum können Hybridverfahren sinnvoll sein?

- [ ] A) Sie können klassische und post-quanten-resistente Ansätze in Übergangsphasen verbinden.
- [ ] B) Sie verbieten jede alte Methode sofort.
- [ ] C) Sie ersetzen Tests vollständig.
- [ ] D) Sie verhindern Komplexität immer.

6. Warum ist Implementierungssicherheit wichtig?

- [ ] A) Angriffe nutzen oft Umsetzungsfehler statt mathematische Schwächen.
- [ ] B) Algorithmische Sicherheit macht Implementierungen irrelevant.
- [ ] C) Fehlkonfigurationen sind unmöglich.
- [ ] D) Seitenkanäle betreffen nur Lautsprecher.

7. Was ist ein Risiko in kritischen Infrastrukturen?

- [ ] A) Eine schlecht geplante Sicherheitsumstellung kann die Verfügbarkeit gefährden.
- [ ] B) Sie brauchen keine Verschlüsselung.
- [ ] C) Sie können immer beliebig abgeschaltet werden.
- [ ] D) Sie enthalten keine alten Systeme.

8. Warum muss Beschaffung Kryptoagilität berücksichtigen?

- [ ] A) Neue langfristige Systeme sollen später aktualisierbar bleiben.
- [ ] B) Beschaffung betrifft nie Sicherheit.
- [ ] C) Frisch gekaufte Systeme veralten nie.
- [ ] D) Verträge können keine Sicherheitsanforderungen enthalten.

9. Was ist eine Governance-Frage der Migration?

- [ ] A) Wer priorisiert Systeme, trägt Kosten und dokumentiert Ausnahmen?
- [ ] B) Welche Farbe hat das Rechenzentrum?
- [ ] C) Welche Geräte sind am schwersten?
- [ ] D) Wer ignoriert Zulieferer?

10. Welche Schlussfolgerung passt?

- [ ] A) Post-Quanten-Kryptografie ist ein Transformationsprozess von Technik, Organisation und Verantwortung.
- [ ] B) Man kann sie als einzelnes Programm installieren.
- [ ] C) Sie betrifft nur Forschungslabore.
- [ ] D) Sie benötigt keine Standards.

Ordne zu

A	B
Post-Quanten-Kryptografie	verlangt organisatorische und technische Migration.
Kryptoinventar	macht kryptografische Abhängigkeiten sichtbar.
Eingebettete Systeme	sind oft schwer zu aktualisieren.
Schlüsselgröße	kann Bandbreite und Speicher beeinflussen.
Signaturgröße	kann Protokolle und Zertifikate belasten.
Rechenlast	ist für kleine Geräte besonders relevant.
Interoperabilität	verhindert Kommunikationsabbrüche zwischen Systemen.
Rückwärtskompatibilität	kann nötig sein, aber Risiken verlängern.
Hybridverfahren	kombinieren alte und neue kryptografische Ansätze.
Standardisierung	schafft Vergleichbarkeit und Beschaffungssicherheit.
Implementierungssicherheit	schützt vor Fehlern jenseits der Mathematik.
Seitenkanalanalyse	nutzt messbare Nebeninformationen aus.
Fehlkonfiguration	kann starke Verfahren schwächen.
Kritische Infrastruktur	braucht gestaffelte und getestete Migration.
Verfügbarkeitsanforderung	begrenzt experimentelle Umstellungen.
Beschaffungsrichtlinien	sollten Kryptoagilität verlangen.
Zulieferer	können versteckte kryptografische Abhängigkeiten einbringen.
Governance-Struktur	klärt Prioritäten, Kosten und Verantwortung.
Schulung	befähigt Personal zur sicheren Umstellung.
Dokumentationspflicht	macht Entscheidungen auditierbar.
Kryptoagilität	verbindet Architektur, Prozesse und Austauschbarkeit.
Testumgebung	reduziert Migrationsrisiken vor dem Einsatz.
Altanlagen	können neue Sicherheitsstandards blockieren.

A	B
Sicherheitszertifizierung	kann Umstellung verlangsamen und absichern.
Betriebsunterbrechung	ist ein Risiko schlechter Planung.
Migrationsfähigkeit	muss schon beim Kauf neuer Systeme bedacht werden.
Sicherheitsökonomie	macht unsichtbaren Nutzen schwer vermittelbar.
Übergangsfrist	strukturiert parallele Nutzung alter und neuer Verfahren.

Bringe in die richtige Reihenfolge

Nr.	Satz / Ereignis	Reihenfolge
1.	Danach wird das Kryptoinventar als schwieriger erster Schritt beschrieben.	
2.	Der Text beginnt mit der Kritik an der Vorstellung eines einfachen Algorithmuswechsels.	
3.	Später wird Interoperabilität als zentrales Migrationsproblem eingeführt.	
4.	Anschließend wird Kryptografie als tief eingebettete Infrastruktur erklärt.	
5.	Zum Schluss wird Post-Quanten-Migration als Transformationsprozess verstanden.	
6.	Danach werden technische Eigenschaften neuer Verfahren als Integrationsproblem analysiert.	
7.	Es wird gezeigt, warum Ressourcenbeschränkungen kleiner Geräte relevant sind.	
8.	Der Text beschreibt anschließend Übergangsarchitekturen und Hybridverfahren.	
9.	Später wird Standardisierung als notwendig und zugleich zeitkritisch dargestellt.	
10.	Danach wird Implementierungssicherheit gegenüber bloßer algorithmischer Sicherheit betont.	
11.	Ein weiterer Schritt ist die besondere Lage kritischer Infrastrukturen.	
12.	Danach wird Beschaffungspolitik als sicherheitsstrategischer Hebel erklärt.	
13.	Der Text führt Governance-Fragen zu Priorität, Kosten und Haftung ein.	
14.	Später wird Kryptoagilität als organisatorisch-technische Fähigkeit beschrieben.	
15.	Am Ende wird die Unsichtbarkeit erfolgreichen Sicherheitsnutzens problematisiert.	
16.	Es folgt die Warnung, dass heutige Untätigkeit spätere Risiken erhöht.	
17.	Die Rolle von Schulung und Dokumentation wird als Teil dauerhafter Sicherheitsarbeit sichtbar.	

Nr.	Satz / Ereignis	Reihenfolge
18.	Der Text fragt abschließend, ob Institutionen ihre Sicherheitsarchitektur rechtzeitig verändern können.	

Finde den Fehler im Inhalt

1. Post-Quanten-Kryptografie bedeutet, nur einen Algorithmusnamen in einer Datei auszutauschen.

2. Organisationen wissen immer vollständig, wo Kryptografie eingesetzt wird.

3. Nur zentrale Server enthalten kryptografische Verfahren.

4. Größere Schlüssel und Signaturen haben keinerlei Einfluss auf bestehende Systeme.

5. Eingebettete Systeme lassen sich immer sofort und problemlos aktualisieren.

6. Interoperabilität ist bei kryptografischer Migration unwichtig.

7. Hybridverfahren reduzieren Komplexität immer auf null.

8. Standardisierung ist überflüssig, weil jede Organisation beliebige Verfahren nutzen sollte.

9. Algorithmische Sicherheit garantiert automatisch sichere Implementierung.

10. Kritische Infrastrukturen können Sicherheitsumstellungen beliebig experimentell durchführen.

11. Beschaffung hat mit Post-Quanten-Sicherheit nichts zu tun.

12. Governance ist bei Kryptomigration irrelevant.

13. Kryptoagilität ist nur ein Marketingwort ohne praktische Bedeutung.

14. Der Nutzen erfolgreicher Migration ist immer spektakulär sichtbar.

15. Untätigkeit ist neutral und verursacht keine späteren Kosten.

Schreibaufgabe

320-380 Wörter

Erörtere, warum die Einführung von Post-Quanten-Kryptografie als organisatorischer Transformationsprozess verstanden werden muss. Gehe auf Kryptoinventar, Interoperabilität, Hybridverfahren, Implementierungssicherheit, kritische Infrastrukturen, Beschaffungspolitik, Governance und Kryptoagilität ein.

Lösungen

Fragen zum Text

1. Kryptografie ist tief in Protokolle, Geräte, Prozesse, Software, Zertifikate und Organisationen eingebettet.
2. Organisationen müssen wissen, wo welche kryptografischen Verfahren eingesetzt werden, bevor sie gezielt migrieren können.
3. Sichtbare Systeme werden aktualisiert, während eingebettete oder alte Abhängigkeiten übersehen werden können.
4. Größere Schlüssel, größere Signaturen, höhere Rechenlast, mehr Bandbreite, Speicherbedarf oder Energieverbrauch können problematisch sein.
5. Sie haben oft begrenzte Ressourcen, lange Lebensdauer und sind schwer zu aktualisieren.
6. Systeme müssen dieselben Protokolle, Formate und Standards verstehen, damit Kommunikation funktioniert.
7. Alte und neue Verfahren müssen zeitweise parallel funktionieren, damit Verbindungen nicht abbrechen.
8. Hybridverfahren kombinieren klassische und post-quanten-resistente Methoden, um Übergangsrisiken zu verringern.
9. Sie schafft Vertrauen und Vergleichbarkeit, kostet aber Zeit und kann frühe oder späte Entscheidungen riskant machen.
10. Konkrete Implementierungen können durch Fehler, Seitenkanäle, Fehlkonfigurationen oder schlechte Schlüsselverwaltung unsicher werden.
11. Sie haben hohe Verfügbarkeitsanforderungen und können Sicherheitsumstellungen nicht beliebig experimentell durchführen.
12. Neue Systeme mit langer Lebensdauer müssen updatefähig, kryptoagil und dokumentiert sein, sonst entstehen neue Altlasten.
13. Wer priorisiert, bezahlt, bewertet Langzeitdaten, kontrolliert Zulieferer, dokumentiert Ausnahmen und haftet bei Fehlern.
14. Sie umfasst Architekturen, Prozesse, Schulung, Dokumentation und Führung.
15. Wenn Migration gelingt, funktionieren Systeme einfach weiter und Sicherheitsprobleme treten nicht ein.
16. Wer heute nicht plant, verschiebt Risiken in eine spätere, teurere und gefährlichere Übergangsphase.
17. Post-Quanten-Kryptografie ist ein organisatorischer Transformationsprozess, nicht nur ein installierbares Produkt.

Multiple Choice

1. A) Kryptografie ist in viele technische und organisatorische Strukturen eingebettet.
2. A) Eine Übersicht darüber, wo welche kryptografischen Verfahren eingesetzt werden.
3. A) Sie können Bandbreite, Speicher, Rechenlast und Antwortzeiten belasten.
4. A) Systeme können miteinander kommunizieren, weil sie gemeinsame Formate und Protokolle verstehen.
5. A) Sie können klassische und post-quanten-resistente Ansätze in Übergangsphasen verbinden.

Lösungen

Multiple Choice (Fortsetzung)

6. A) Angriffe nutzen oft Umsetzungsfehler statt mathematische Schwächen.
7. A) Eine schlecht geplante Sicherheitsumstellung kann die Verfügbarkeit gefährden.
8. A) Neue langfristige Systeme sollen später aktualisierbar bleiben.
9. A) Wer priorisiert Systeme, trägt Kosten und dokumentiert Ausnahmen?
10. A) Post-Quanten-Kryptografie ist ein Transformationsprozess von Technik, Organisation und Verantwortung.

Zuordnung

1. 1. Post-Quanten-Kryptografie — verlangt organisatorische und technische Migration.
2. 2. Kryptoinventar — macht kryptografische Abhängigkeiten sichtbar.
3. 3. Eingebettete Systeme — sind oft schwer zu aktualisieren.
4. 4. Schlüsselgröße — kann Bandbreite und Speicher beeinflussen.
5. 5. Signaturgröße — kann Protokolle und Zertifikate belasten.
6. 6. Rechenlast — ist für kleine Geräte besonders relevant.
7. 7. Interoperabilität — verhindert Kommunikationsabbrüche zwischen Systemen.
8. 8. Rückwärtskompatibilität — kann nötig sein, aber Risiken verlängern.
9. 9. Hybridverfahren — kombinieren alte und neue kryptografische Ansätze.
10. 10. Standardisierung — schafft Vergleichbarkeit und Beschaffungssicherheit.
11. 11. Implementierungssicherheit — schützt vor Fehlern jenseits der Mathematik.
12. 12. Seitenkanalanalyse — nutzt messbare Nebeninformationen aus.
13. 13. Fehlkonfiguration — kann starke Verfahren schwächen.
14. 14. Kritische Infrastruktur — braucht gestaffelte und getestete Migration.
15. 15. Verfügbarkeitsanforderung — begrenzt experimentelle Umstellungen.
16. 16. Beschaffungsrichtlinien — sollten Kryptoagilität verlangen.
17. 17. Zulieferer — können versteckte kryptografische Abhängigkeiten einbringen.
18. 18. Governance-Struktur — klärt Prioritäten, Kosten und Verantwortung.
19. 19. Schulung — befähigt Personal zur sicheren Umstellung.
20. 20. Dokumentationspflicht — macht Entscheidungen auditierbar.
21. 21. Kryptoagilität — verbindet Architektur, Prozesse und Austauschbarkeit.
22. 22. Testumgebung — reduziert Migrationsrisiken vor dem Einsatz.

Lösungen

Zuordnung (Fortsetzung)

23. 23. Altanlagen — können neue Sicherheitsstandards blockieren.
24. 24. Sicherheitszertifizierung — kann Umstellung verlangsamen und absichern.
25. 25. Migrationsfähigkeit — muss schon beim Kauf neuer Systeme bedacht werden.
26. 26. Betriebsunterbrechung — ist ein Risiko schlechter Planung.
27. 27. Übergangsfrist — strukturiert parallele Nutzung alter und neuer Verfahren.
28. 28. Sicherheitsökonomie — macht unsichtbaren Nutzen schwer vermittelbar.

Reihenfolge

1. 1. Der Text beginnt mit der Kritik an der Vorstellung eines einfachen Algorithmuswechsels.
2. 2. Anschließend wird Kryptografie als tief eingebettete Infrastruktur erklärt.
3. 3. Danach wird das Kryptoinventar als schwieriger erster Schritt beschrieben.
4. 4. Danach werden technische Eigenschaften neuer Verfahren als Integrationsproblem analysiert.
5. 5. Es wird gezeigt, warum Ressourcenbeschränkungen kleiner Geräte relevant sind.
6. 6. Später wird Interoperabilität als zentrales Migrationsproblem eingeführt.
7. 7. Der Text beschreibt anschließend Übergangsarchitekturen und Hybridverfahren.
8. 8. Später wird Standardisierung als notwendig und zugleich zeitkritisch dargestellt.
9. 9. Danach wird Implementierungssicherheit gegenüber bloßer algorithmischer Sicherheit betont.
10. 10. Ein weiterer Schritt ist die besondere Lage kritischer Infrastrukturen.
11. 11. Danach wird Beschaffungspolitik als sicherheitsstrategischer Hebel erklärt.
12. 12. Der Text führt Governance-Fragen zu Priorität, Kosten und Haftung ein.
13. 13. Später wird Kryptoagilität als organisatorisch-technische Fähigkeit beschrieben.
14. 14. Die Rolle von Schulung und Dokumentation wird als Teil dauerhafter Sicherheitsarbeit sichtbar.
15. 15. Am Ende wird die Unsichtbarkeit erfolgreichen Sicherheitsnutzens problematisiert.
16. 16. Es folgt die Warnung, dass heutige Untätigkeit spätere Risiken erhöht.
17. 17. Zum Schluss wird Post-Quanten-Migration als Transformationsprozess verstanden.
18. 18. Der Text fragt abschließend, ob Institutionen ihre Sicherheitsarchitektur rechtzeitig verändern können.

Lösungen

Fehler finden

1. Sie erfordert eine umfassende Migration von Technik, Prozessen, Standards und Verantwortung.
2. Viele Organisationen besitzen kein vollständiges Kryptoinventar.
3. Kryptografie steckt auch in Geräten, Altanlagen, Softwarebibliotheken, VPNs, Archiven und Zulieferkomponenten.
4. Sie können Bandbreite, Speicher, Rechenlast und Antwortzeiten beeinflussen.
5. Sie haben oft begrenzte Ressourcen, lange Lebensdauer und schwierige Updatewege.
6. Systeme müssen gemeinsame Protokolle und Formate verstehen, sonst brechen Verbindungen ab.
7. Sie können Übergänge erleichtern, erhöhen aber auch Komplexität und Implementierungsanforderungen.
8. Standardisierung schafft Vertrauen, Vergleichbarkeit, Beschaffungssicherheit und Zertifizierbarkeit.
9. Implementierungen können durch Seitenkanäle, Fehlkonfigurationen oder schlechte Schlüsselverwaltung unsicher werden.
10. Sie haben hohe Verfügbarkeitsanforderungen und brauchen gestaffelte, getestete Migration.
11. Neue Systeme müssen updatefähig, dokumentiert und kryptoagil beschafft werden.
12. Prioritäten, Kosten, Verantwortlichkeiten, Zulieferer und Haftungsfragen müssen geklärt werden.
13. Sie beschreibt die Fähigkeit, Verfahren kontrolliert auszutauschen und Sicherheitsänderungen zu organisieren.
14. Im Idealfall bleiben Systeme einfach funktionsfähig und sicher, wodurch der Nutzen unsichtbar wirkt.
15. Untätigkeit verschiebt Risiken und kann spätere Migration teurer und gefährlicher machen.