Fraunhofer SIT

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT
HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

Krypto-Agilität

Leitfaden für langfristige IT-Sicherheit

Leonie Wolf

Krypto-Agilität

Leitfaden für langfristige IT-Sicherheit

Impressum

Layout und Satz
Julia Kudalska

Kontakt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

© Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, 2024

Hinweise
Dieser Beitrag entstand im Rahmen eines Projektes mit dem Hessischen Ministerium des Inneren, für Sicherheit und Heimatschutz.

Titelbild: pixabay, insspirito

Die in diesem Beitrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Autorin

Leonie Wolf
ATHENE | Fraunhofer SIT

Mehr Infos zu sicherer Verschlüsselung

Liebe Leserin, lieber Leser,

sichere, vertrauenswürdige digitale Kommunikation bildet die Grundlage jeder Zusammenarbeit, sei es beispielsweise zwischen Bürgerinnen und Bürgern und Verwaltung, innerhalb und zwischen Unternehmen oder im privaten Bereich. Um digitale Kommunikation effektiv zu schützen, werden Verschlüsselungsverfahren eingesetzt. In der Welt der Verschlüsselung gibt es ein ständiges Wettrennen zwischen immer sichereren Verfahren und den Bemühungen, diese zu umgehen. Nicht nur für den Standort Hessen ist eine sichere digitale Infrastruktur, die widerstandsfähig gegenüber Schwachstellen und Cyberangriffen ist, von grundlegender Bedeutung.

In Hessen gründet der Schutz der digitalen Welt auf einem ganzheitlichen Ansatz. Dieser Ansatz beinhaltet unter anderem die Förderung der Cybersicherheitsforschung durch das Hessische Ministerium des Innern, für Sicherheit und Heimatschutz.

Der vorliegende Leitfaden „Krypto-Agilität" ist ein Ergebnis dieser gezielten Forschungsförderung. Die praktischen Empfehlungen im Leitfaden wurden unter Berücksichtigung aktueller Forschungsergebnisse sowie der konkreten Herausforderungen und Bedürfnisse von Bürgerinnen und Bürgern, Unternehmen sowie staatlichen und kommunalen Einrichtungen vor Ort erarbeitet. Krypto-Agilität ist ein Konzept, das die Flexibilität und Anpassungsfähigkeit von Verschlüsselungstechnologien in der digitalen Kommunikation betont. Indem Sie beispielsweise diesen Text online lesen oder die Webseite des Hessischen Ministeriums des Innern, für Sicherheit und Heimatschutz besuchen, nutzen Sie schon Krypto-Agilität, denn diese Seiten – wie die meisten Webseiten – sind über das Internetprotokoll TLS abgesichert. Dabei wird automatisch zwischen verschiedenen kryptografischen Verfahren ausgewählt.

In einer zunehmend vernetzten und digitalen Welt ist es von immenser Bedeutung, dass die Sicherheit unserer digitaler Kommunikation gewährleistet und auf dem neuesten Stand ist. Die Fähigkeit, Verschlüsselungstechnologien flexibel anzupassen, ist ein wesentlicher Bestandteil dieses Bemühens. Krypto-Agilität ermöglicht es, den Schutz von Informationen kontinuierlich zu verbessern und vor den ständig wachsenden Bedrohungen aus dem Cyberraum zu verteidigen. Dieser Leitfaden ist ein wichtiger Schritt auf diesem Weg und trägt dazu bei, die Sicherheit in der digitalen Welt zu erhöhen.

Prof. Dr. Roman Poseck

Hessischer Minister des Innern, für Sicherheit und Heimatschutz

Inhalt

Einleitung

Die Idee, Nachrichten zu verschlüsseln oder zu signieren, ist uralt. In der analogen wie digitalen Welt sind die Gründe gleich: Man möchte verhindern, dass Nachrichten von Unbefugten mitgelesen oder verändert werden. Außerdem soll niemand unbefugt Nachrichten im Namen einer anderen Person verschicken können.

Fast ebenso alt wie die Kryptografie selbst ist der Versuch, sie zu brechen. Auch in diesem Bereich der Kryptanalyse gibt es immer wieder Fortschritte, und so verlieren kryptografische Verfahren mit der Zeit an Sicherheit.

In der Kryptografie gibt es also seit ihren Anfängen ein Wettrennen zwischen immer sichereren Verfahren und immer besseren Möglichkeiten, diese Verfahren zu brechen.

Neu ist der Ansatz, diesen ewigen Wettlauf zwischen besseren Angriffen und besseren kryptografischen Verfahren von vornherein mitzubedenken. Dieser Ansatz nennt sich Krypto-Agilität. Dies beinhaltet, dass überall dort, wo Kryptografie genutzt wird, ein Austausch oder ein Update der kryptografischen Verfahren schnell und einfach möglich sein muss. Krypto-agil sind also Systeme, die jederzeit anpassungsfähig sind.

Im Zentrum steht die Frage: Was kann heute schon getan werden, um Kryptografie anpassungsfähig zu machen und sie so heute und in Zukunft risikoadäquat einsetzen zu können?

Diese Broschüre soll einen Einblick in das Thema Krypto-Agilität bieten. Ziel ist die Verknüpfung des aktuellen Forschungsstandes mit praktischen Empfehlungen für mehr Krypto-Agilität. Sie richtet sich an alle mit Interesse für nachhaltigen Einsatz von Kryptografie, insbesondere Entscheidungsträgerinnen und -träger, die (noch) keine Expertinnen bzw. Experten in dem Themenbereich sind. Erstellt wurde diese Broschüre vom Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt. Das Fraunhofer SIT ist eine herausragende Einrichtung für angewandte IT-Sicherheitsforschung und als Teil des Nationalen Forschungszentrums ATHENE hervorragend vernetzt in der hessischen Spitzenforschung.

Kapitel 1 – Kryptografie heute

Kapitel 1.1: Nichts ist vollkommen sicher

Kryptografische Verfahren ermöglichen uns, sicher digital zu kommunizieren. Ziele, die mit Kryptografie erreicht werden sollen, sind:

1. Wir können geheime Daten austauschen, ohne dass sie mitgelesen werden.

2. Wir können unser digitales Gegenüber eindeutig identifizieren, ohne getäuscht zu werden

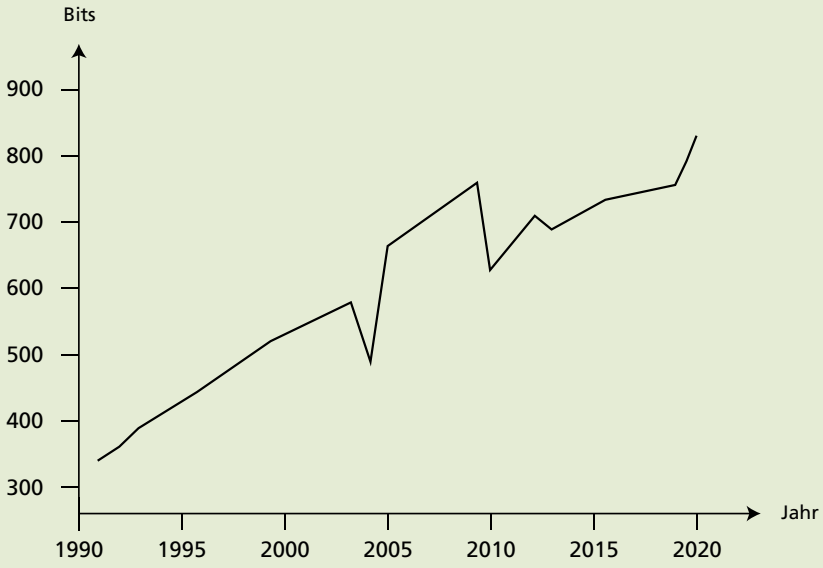
3. Wir können auf den Inhalt von Nachrichten vertrauen, ohne befürchten zu müssen, dass sie verändert wurden.

Klassische Beispiele für die Anwendung von Kryptografie im Alltag sind Online-Banking oder Messengerdienste. Selbst bei weniger sensiblen Informationen wie beim Surfen im Internet, Aktualisieren von Software, Einloggen in WLANs oder digitalem Datenaustausch, finden kryptografische Verfahren Anwendung. Aber die Kryptografie, die wir heute tagtäglich verwenden, kann keine hundertprozentige Sicherheit garantieren. In der Theorie basiert die Sicherheit von Verschlüsselungsverfahren auf der Annahme, dass verschiedene mathematische Probleme schwierig zu lösen sind. Schwierig – aber nicht unmöglich. Mit genügend Zeit und Rechenkapazitäten lassen sich selbst in der Theorie alle heute genutzten Verfahren brechen.

Exkurs: Brute-Force-Angriff

Immer möglich ist der sogenannte Brute-Force-Angriff. Der Ansatz ist simpel: Wer ein Zahlenschloss öffnen möchte, aber die richtige Zahlenkombination nicht kennt, kann „einfach" alle möglichen Kombinationen durchprobieren. Mit genügend Zeit und Ausdauer in den Fingern kann so jedes Zahlenschloss geknackt werden. Ähnlich verhält es sich mit der Kryptografie: Ein Angreifer probiert alle möglichen Schlüssel nacheinander aus, bis er den richtigen geheimen Schlüssel gefunden hat und damit eine Nachricht entschlüsseln kann. Wie bei dem Zahlenschloss werden für diesen Angriff aber sehr viel Zeit und Ressourcen benötigt. In der Praxis sind oft sogar bessere Angriffe bekannt.

Beispiel: RSA (Verfall kryptografischer Verfahren)[1]



1 https://eprint.iacr.org/2021/894.pdf (Seite 7)

Kapitel 1.2: Die vier großen Bedrohungen

Die theoretische Bedrohung für Kryptografie lässt sich in der Praxis in vier Kategorien aufteilen. Für all diese unterschiedlichen Bedrohungen gibt es theoretische Lösungen, die hier ebenfalls präsentiert werden:

1. Steigerung der Rechenleistung

Moore's Law besagt, dass sich die Anzahl von Rechenoperationen, die auf einem Chip pro Zeiteinheit stattfinden, alle ein bis zwei Jahre verdoppelt.[2]

Das lässt sich zwar nicht eins zu eins auf die Rechenleistung insgesamt übertragen, weil dabei noch weitere Faktoren bedacht werden müssen. Dennoch ist die Entwicklung hier ähnlich. So können Daten heute schneller signiert oder verschlüsselt werden als vor einigen Jahren. Allerdings hat auch die Geschwindigkeit, mit der Angriffe auf diese kryptografischen Verfahren durchgeführt werden, zugenommen.

Lösung:

Wir erinnern uns: Die Sicherheit von Verschlüsselungsverfahren basiert auf der Annahme, dass verschiedene mathematische Probleme schwierig zu lösen sind. Um weiterhin ein ähnliches Sicherheitsniveau garantieren zu können, kann die Lösung des zugrundeliegenden mathematischen Problems eines bestimmten kryptografischen Verfahrens erschwert werden. Dazu vergrößert man den Suchraum und damit die Zahlen, mit denen gerechnet wird. Das bedeutet: Die Schlüssel werden länger.

2 https://ourworldindata.org/grapher/transistors-per-microprocessor

2. Protokoll- und Implementierungsfehler

Immer wieder werden sicherheitsrelevante Fehler in bereits genutzter Software gefunden. Besonders spektakulär war der Fall der Playstation 3. Die Playstation 3 hatte anfänglich ein Sicherheitsprotokoll, bei dem feste Werte anstelle von zufälligen Zahlen für kryptografische Verfahren verwendet wurden. Dies führte zu erheblichen Sicherheitsproblemen, da Hackergruppen diesen Mangel ausnutzten, um den geheimen Schlüssel der Konsole zu berechnen. Mit diesem Schlüssel konnten sie nicht autorisierte Software ausführen und die Sicherheitsschranken der Konsole umgehen.[3]

Lösung:

Patches und Updates installieren. Alle Software aktuell halten und die aktuellen Standards nutzen.

3 https://www.heise.de/security/meldung/27C3-Sicherheitssystem-der-Playstation-3-ausgehebelt-1161876.html

3. Mathematische Fortschritte

Die gegenwärtige Kryptografie fußt auf mathematischen Problemen, die als schwierig zu lösen gelten. Dennoch existieren keine unwiderlegbaren Beweise für ihre schwierige Lösbarkeit. Es bleibt theoretisch möglich, dass es einfache, aber bislang unentdeckte Lösungsansätze für diese Probleme gibt. Je länger erfolglos nach einfachen Lösungswegen gesucht wird, umso größer wird das Vertrauen in die Schwierigkeit des mathematischen Problems und damit in die Sicherheit des kryptografischen Verfahrens. Das mathematische Problem, das dem RSA-Kryptosystem zugrunde liegt, ist die Primzahlfaktorisierung. Damit haben sich schon die alten griechischen Mathematiker Jahrhunderte vor unserer Zeitrechnung beschäftigt. Bis heute ist dafür kein effizienter Algorithmus bekannt.[4]

Aber es gibt auch Gegenbeispiele: Im Juli 2022 wurde eine mathematischer Methode entdeckt, um den fünf Jahre alten Verschlüsselungsalgorithmus SIKE zu brechen.[5]

Lösung:

Wird ein solcher neuer Angriff bekannt, sollte auf ein kryptografisches Verfahren gewechselt werden, das auf anderen mathematischen Problemen basiert.

4 Zumindest für klassische Computer

5 https://www.microsoft.com/en-us/msrc/sike-cryptographic-challenge

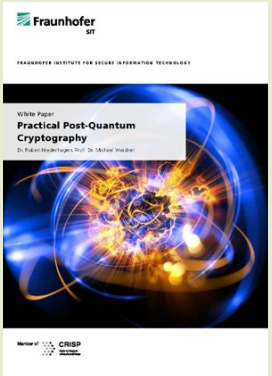
4. Quantencomputer

Glichen bisher die Entwicklung besserer kryptografischer Verfahren und besserer Angriffe einem Wettrennen, so stellt die Entwicklung eines praktisch einsatzfähigen Quantencomputers – im wahrsten Sinne des Wortes – einen Quantensprung dar. Auf einen Schlag würde nahezu all unsere heute genutzte Kryptografie unsicher und damit auch ihre Anwendungen, wie beispielsweise sicherer E-Mail-Versand, Online-Banking, sichere Chat-Anwendungen und vieles mehr.

Lösung:

Die Lösungen werden gerade erst entwickelt unter dem Stichwort Post-Quanten-Kryptografie. Damit sind verschiedene neue kryptografische Verfahren gemeint, die auch einem Angriff durch einen Quantencomputer standhalten können. Seit 2016 läuft unter breiter Beteiligung der Community dazu ein Prozess des US-amerikanischen National Institute for Standards and Technology (NIST). In den nächsten Jahren, also für 2023/24, wird die Standardisierung von quanten-resistenter Kryptografie – oder Post-Quanten-Kryptografie erwartet. Das Bundesamt für Sicherheit in der IT (BSI) hat bereits Handlungsrichtlinien veröffentlicht.

Weiterführende Literatur zu Post-Quanten-Kryptografie



Zwischenfazit:

Für sichere digitale Kommunikation gibt es vielfältige Bedrohungen. Für alle Probleme, die dadurch verursacht werden, ist die Lösung zumindest theoretisch bekannt. Man kann ihnen durch den Einsatz von besseren kryptografischen Verfahren begegnen. Doch oft geschieht dies nicht, und in der Praxis werden weiterhin veraltete und unsichere Verfahren verwendet.

Wie lassen sich die Lösungen von der Theorie in die Praxis übertragen, wie lässt sich Kryptografie dauerhaft sicher halten, wie lassen sich Aktualisierungen schnell und praxistauglich einsetzen? Damit beschäftigt sich Krypto-Agilität.

Side note: Auch die besseren kryptografischen Verfahren werden mit der Zeit an Sicherheit verlieren, weil sie mit denselben Bedrohungen konfrontiert sind.

Kapitel 2: Was ist Krypto-Agilität?

Krypto-Agilität bezeichnet die Fähigkeit eines Systems oder einer Organisation, die genutzte Kryptografie flexibel anzupassen und so schnell auf neu entdeckte Schwachstellen zu reagieren. Ziel ist es, die in Kapitel 1 vorgestellten theoretischen Lösungen auch praktisch einsetzbar zu machen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die amerikanische Standardisierungsbehörde NIST (entspricht dem Deutschen Institut für Normung DIN) haben Krypto-Agilität wie folgt definiert:

NIST:

Many information systems lack crypto agility – that is, they are not designed to encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure.[6]

BSI:

Bei der Neu- und Weiterentwicklung von Anwendungen sollte vor allem darauf geachtet werden, die kryptografischen Mechanismen möglichst flexibel zu gestal ten, um auf alle denkbaren Entwicklungen reagieren, kommende Empfehlungen und Standards umsetzen und möglicherweise in Zukunft Algorithmen, die nicht mehr das gewünschte Sicherheitsniveau garantieren, austauschen zu können („Kryptoagilität"). Dies gilt insbesondere aufgrund der Bedrohung durch Quantencomputer – aber nicht ausschließlich: Auch klassische Angriffe können sich weiterentwickeln und einstmals als sicher eingestufte Verschlüsselungsverfahren oder Schlüssellängen obsolet machen. Kryptoagilität sollte also – unabhängig von der Entwicklung von Quantencomputern – zum Designkriterium für neue Produkte werden.[7]

6 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

7 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?

Krypto-Agilität kann auf verschiedenen Ebenen umgesetzt werden. Ob es um flexible Hardware, einzelne tauschbare Funktionen oder ganze Ciphersuites, also zusammenhängende kryptografische Verfahren geht – verschiedene Maßnahmen können sich dabei gegenseitig ergänzen oder ersetzen. Doch alles zu flexibilisieren scheint nicht sinnvoll, denn mehr Krypto-Agilität macht Systeme auch immer komplexer und oft langsamer. Deshalb müssen Maßnahmen abhängig von den Schutzzielen sorgfältig abgewogen werden. Jede Änderung der Risikobewertung (Verweis auf Kapitel 1) oder der Anforderungen an die Sicherheit sollte zu einer Überprüfung der kryptografischen Verfahren führen. In einem krypto-agilen System kann auf diese Überprüfung direkt eine Anpassung der Verfahren erfolgen.

Kapitel 2.1: Wie wird Krypto-Agilität umgesetzt?

Auf dem Weg zur Umsetzung von Krypto-Agilität unterscheiden wir fünf Handlungsfelder.[8] Denn zur praktischen Umsetzung müssen unterschiedliche Bereiche vom Management über den Einkauf bis in die IT einen Beitrag leisten und möglichst reibungslos ineinander greifen. Das Ziel ist eine gute Vorbereitung, um im Fall des Falles – also wenn ein kryptografisches Verfahren an Sicherheit verliert –schnelle Änderungen in der genutzten Kryptografie umsetzen zu können. Im Idealfall stehen sogar verschiedene kryptografische Verfahren zur Auswahl, zwischen denen gewählt werden kann, sodass man schnell zu einem anderen wechseln kann, wenn eines zu unsicher geworden ist. Im Folgenden werden die Handlungsfelder kurz vorgestellt:

1. Wissen über Krypto-Agilität

Ziel: Es können fundierte Entscheidungen im Bereich der Kryptografie getroffen werden.

Umsetzung: In der Organisation ist Wissen verfügbar zu verschiedenen aktuell verwendeten kryptografischen Verfahren und Alternativen, auch der Post-Quanten-Kryptografie. Weiterhin gibt es theoretisches und praktisches Wissen zu Krypto-Agilität und wie sie umgesetzt werden kann.

8 vgl. CAMM https://camm.h-da.io/ und CASC https://www.sit.fraunhofer.de/fileadmin/folien/casc-presentation.pdf?

2. Systemwissen

Ziel: Die Organisation ist im eigenen System handlungsfähig mit Blick auf Kryptografie.

Umsetzung: Es ist geklärt, bekannt und dokumentiert, wer wie verantwortlich ist für welche Teile des Systems, wie sie upgedatet werden können und welche Zugänge dafür nötig sind. Es ist bekannt, wo Kryptografie eingesetzt wird, wie diese aufgerufen wird und welche kryptografischen Algorithmen verwendet werden.

3. Agilität im Prozess

Ziel: Entscheidungsprozesse sind so aufgebaut, dass sie agiles Handeln in der Kryptografie unterstützen.

Umsetzung: In der Einrichtung gibt es ein zentrales Gremium, das Entscheidungen zur IT-Sicherheit treffen kann. Es arbeitet effektiv anhand von Guidelines, zum Beispiel vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder übergeordneten Behörden, die grundsätzlich festlegen, welche kryptografischen Verfahren genutzt werden. Es existieren festgelegte Prozesse für Updates, die umfangreiches Testen beinhalten.

4. Agilität im System

Ziel: Im System sind genügend Kapazitäten für die Nutzung anderer kryptografischer Verfahren vorhanden – auch quanten-resistenter Verfahren.

Umsetzung: Auch die Hardware ist modular aufgebaut. Einzelne Komponenten können ohne großen Aufwand ausgetauscht werden. Insbesondere sind Hard- und Software unabhängig voneinander austauschbar. Rechenleistung, Speicher, Schnittstellen – alle Bestandteile des Systems haben genügend Puffer für komplexere Berechnungen und größere Schlüssel, verschlüsselte Nachrichten und Signaturen.

5. Agilität der Algorithmen

Ziel: Es stehen softwareseitig verschiedene kryptografische Algorithmen zur Verfügung, die flexibel genutzt werden können.

Umsetzung: Die Software ist modular aufgebaut. Einzelne Komponenten können ohne großen Aufwand ausgetauscht werden. Kryptografie wird über abstrakte Schnittstellen genutzt. Es ist möglich, schnell und unkompliziert kryptografische Algorithmen hinzuzufügen und zu entfernen.

Kapitel 2.2: Krypto-Agilität im Best-Case-Szenario

Ein ideales Beispiel: In einer Bank wird ein kryptografisches Verfahren genutzt, um mit den Kundinnen und Kunden zu kommunizieren. Dann wird ein neuer Angriff bekannt. Die Verantwortliche für IT-Sicherheit weiß sofort, was zu tun ist: Sie holt das eingespielte Team (3. Agilität im Prozess) mit dem nötigen Wissen über die Sicherheitsanforderungen, die Sicherheitsarchitektur und die verwendeten Verfahren (2. Systemwissen) zusammen. Das Team kommt zu dem Schluss, dass das kryptografische Verfahren mit dem neuen Angriff nicht mehr den Sicherheitsanforderungen genügt. Das Team hat die nötigen Kompetenzen (3. Agilität im Prozess) um direkt zu entscheiden, dass ein anderes Verfahren genutzt werden soll.

Da in den Jahren zuvor viel Wissen zu Krypto-Agilität gesammelt wurde (1. Wissen über Krypto-Agilität) wurde die Sicherheitsarchitektur entsprechend geplant, um jetzt schnell das Verfahren wechseln zu können. Weil die Hard- und Software nicht auf ein Verfahren spezialisiert ist und genug Kapazitäten im System vorhanden sind (4. Agilität im System) ist es möglich, das andere Verfahren direkt anzuwenden. Schließlich wurde beim Aufbau des Systems darauf geachtet, dass kryptografische Verfahren schnell und einfach getauscht werden können (5. Agilität der Algorithmen). So bedarf es nach einigen Tests nur eines Knopfdrucks, und der Austausch des unsicheren kryptografischen Verfahrens funktioniert automatisch.

Kapitel 3: Krypto-Agilität – Was kann ich tun?

Um den unterschiedlichen Startbedingungen von Unternehmen und Organisationen gerecht zu werden, sind die Empfehlungen in die Kategorien kurzfristige, mittelfristige und langfristig Maßnahmen unterteilt. Je weiter eine Organisation bei der Umsetzung von Krypto-Agilität ist, umso weniger kurzfristige Maßnahmen werden nötig sein. Der Fokus sollte umso mehr auf den mittel- und langfristigen Maßnahmen liegen.

Kurzfristige Maßnahmen

Im ersten Schritt steht der Aufbau von Kompetenzen im Mittelpunkt. Wissen über klassische und Post-Quanten-Kryptografie sowie Weiterbildungen zum Thema Krypto-Agilität selbst bilden die absolute Grundlage, um Krypto-Agilität in der eigenen Organisation umzusetzen. Dafür müssen auch Personalressourcen bereit gestellt werden. Fortbildungen erfordern keine strukturellen Änderungen und können kurzfristig umgesetzt werden.

- Kompetenzen in Kryptografie aufbauen
- Kompetenzen in Post-Quanten-Kryptografie aufbauen
- Kompetenzen in Krypto-Agilität aufbauen

Mittelfristige Maßnahmen

Im zweiten Schritt geht es darum, als Organisation handlungsfähig zu werden mit Blick auf Krypto-Agilität. Im Zentrum steht deswegen die Analyse des Ist-Zustandes, sowohl der Kryptografie als auch der Zugänge und Updatemechanismen des eigenen Systems. Mit diesem gesammelten Wissen nachhaltig handlungsfähig werden kann eine Organisation nur, wenn dieses Wissen auch langfristig nutzbar bleibt. Dafür sollte ein geeignetes Wissensmanagement etabliert werden.

- Wissen über das eigene System sammeln
- Selbst genutzte Kryptografie analysieren
- Wissensmanagement etablieren/verbessern

Langfristige Maßnahmen

Langfristig sollen auch die internen Abläufe und Strukturen so angepasst werden, dass Krypto-Agilität an den entscheidenden Stellen bedacht werden kann. Dafür ist es wünschenswert, die Entscheidungen über Kryptografie in einem zentralen, dafür zuständigen Gremium zusammenzufassen. Dieses soll insbesondere Einfluss auf Ausschreibungen, Vergaben und Einkauf nehmen können. Auch Migration zu Post-Quanten-Kryptografie soll langfristig bedacht werden.

- Zentrales Gremium für Entscheidungen über Kryptografie
- Krypto-Agilität bei Ausschreibungen und Vergaben beachten
- Migration zu Post-Quanten-Kryptografie

Fazit und Checkliste

Was kann heute schon getan werden, um Kryptografie anpassungsfähig zu machen und sie so heute und in Zukunft risikoadäquat einsetzen zu können?

Für die nachhaltige Nutzung von Kryptografie kann und sollte heute schon in Krypto-Agilität investiert werden. Allerdings ist maximale Flexibilität an allen Stellen nicht zu empfehlen. Denn mehr Krypto-Agilität bedeutet mehr Komplexität und ermöglicht damit auch neue Angriffsvektoren. Dennoch ist Krypto-Agilität die Möglichkeit, sich heute schon vorzubereiten auf den Umgang mit Angriffen, die noch gar nicht bekannt sind.

Die beiden folgenden Checklisten sollen bei der Umsetzung von Krypto-Agilität helfen.

Technische Umsetzung von Krypto-Agilität:

- ☐ Updates können ausgeführt werden
- ☐ Zusätzliche Kapazitäten in Hard- und Software für andere kryptografische Verfahren sind vorhanden
- ☐ Zusätzliche Kapazitäten auch für Post-Quanten-Kryptografie
- ☐ Hard- und Software sind modular aufgebaut und unabhängig austauschbar
- ☐ Kryptografie wird über Schnittstellen genutzt
- ☐ Kryptografische Funktionen werden über Bibliotheken verwendet
- ☐ Kryptografische Algorithmen können hinzugefügt und ausgeschlossen werden

Organisatorische Umsetzung von Krypto-Agilität:

- ☐ Kompetenzen in Kryptografie aufbauen
- ☐ Kompetenzen in Post-Quanten-Kryptografie aufbauen
- ☐ Kompetenzen in Krypto-Agilität aufbauen
- ☐ Wissen über das eigene System sammeln
- ☐ Selbst genutzte Kryptografie analysieren
- ☐ Wissensmanagement etablieren/verbessern
- ☐ Zentrales Gremium für Entscheidungen über Kryptografie
- ☐ Krypto-Agilität bei Ausschreibungen und Vergaben beachten
- ☐ Migration zu Post-Quanten-Kryptografie