digitales.hessen
Intelligent. Vernetzt. Für Alle

QUANTENCOMPUTER UND „NEXT GENERATION CRYPTO“

Handlungsempfehlungen für Unternehmen

HESSEN

TECHNOLOGIELAND HESSEN

EINLEITUNG

Ohne Informations- und Kommunikationstechnik können die meisten Unternehmen nicht mehr arbeiten. Dies betrifft jedoch nicht nur die Unterstützung interner Verfahren, sondern Unternehmen sind heute eng mit anderen Unternehmen, ihren Kunden oder staatlichen Einrichtungen elektronisch verbunden. Dies steigert die Wirtschaftlichkeit von Prozessen und ermöglicht völlig neue Geschäftsmodelle. Gleichzeitig entstehen jedoch auch neue Risiken, denn es werden in vielfältiger Weise kritische und vertrauliche Informationen gespeichert, bearbeitet und übertragen, die wirkungsvoll zu schützen sind.

Um dieses Ziel zu erreichen, werden Verschlüsselungstechniken eingesetzt. Mit Hilfe kryptografischer Verfahren gelingt es, die Vertraulichkeit von Informationen sicherzustellen. Mit dem Leitfaden „Vertraulichkeitsschutz durch Verschlüsselung" hat die Landesregierung eine Broschüre hierzu veröffentlicht, die Unternehmen dabei unterstützen soll, diese Techniken zu nutzen, um die Risiken von Vertraulichkeitsverletzungen zu minimieren und ihr Know-how zu schützen.

Kryptografische Verfahren sind jedoch interessante Ziele von Angreifern, die durch die Entschlüsselung der Daten Zugriff auf die Informationen erhalten wollen. Dazu kommt der technische Fortschritt im Bereich der Quantencomputer, der eine ernste Bedrohung für die aktuell genutzten Verschlüsselungsverfahren darstellt. Unternehmen müssen sich dieser Gefährdung bewusst sein und immer wieder die genutzten Verfahren überprüfen.

Die vorliegende Broschüre soll ihnen dabei eine Orientierung bieten. Sie wurde erstellt vom Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) in Darmstadt, einer der Einrichtungen, die zur internationalen Spitzenstellung Hessens in der IT-Sicherheit beitragen. Das Fraunhofer SIT ist neben der Technischen Universität, der Hochschule Darmstadt und des Fraunhofer IGD einer der Partner des Center for Research in Security and Privacy – CRISP. Dieser Verbund zählt zur Spitze der internationalen Cybersicherheitsforschung. Die dort erzielten Forschungsergebnisse fließen u. a. in Publikationen wie diese Broschüre ein und werden damit für die Unternehmen in Hessen nutzbar.

1 ZUSAMMENFASSUNG

Vertrauliche Kommunikation per E-Mail, Onlinebanking, Blockchain-Technologie, Sicherheitsmechanismen für das Internet der Dinge – diese und viele weitere Anwendungen sind angewiesen auf Kryptografie. Die sichere Übertragung von vertraulichen Daten (z. B. Kreditkartennummern, Steuererklärungen, Staatsgeheimnissen) über unsichere Kanäle (z. B. Telefonie, Internet) wäre ohne diese Schlüsseltechnik unmöglich. Unternehmen verwenden Kryptografie, um ihre eigenen vertraulichen Daten und IT-Systeme zu schützen und Kunden und Verbrauchern sichere Dienste und Leistungen anbieten zu können. Sensible Informationen sind aber auch für Angreifer von großem Interesse. Daher gibt es einen Rüstungswettlauf zwischen Angreifern, die versuchen, kryptografische Schlüssel, Verfahren, Protokolle oder Implementierungen zu knacken, und den Anbietern, Entwicklern und Anwendern von kryptografischen Produkten, die bekannt gewordene Schwachstellen zu beseitigen versuchen. Systeme, die Kryptografie verwenden, müssen gepflegt werden, um der steigenden Macht der Angreifer widerstehen zu können. Die Industrie muss außerdem darauf vorbereitet sein, zur nächsten Kryptografie-Generation überzugehen, wann immer die Sicherheit von bewährten Verfahren oder Parametern nicht länger gewährleistet werden kann. Der technologische Fortschritt im Bereich Quantencomputer bedeutet in dieser Hinsicht eine besonders ernsthafte Herausforderung für die Sicherheit vieler derzeit verbreiteter kryptografischer Verfahren.

Diese Bedrohung betreffen ebenfalls kleine und mittlere Unternehmen, denn auch sie sichern viele Anwendungen mit kryptografischen Verfahren ab:

- Auf Laptops werden Dateien auf verschlüsselten Festplatten abgelegt, damit sie im Fall eines Verlustes vor dem Zugriff Unbefugter geschützt sind.
- Besonders sensible Informationen wie personenbezogene Daten oder kritisches Firmen-Know-how werden auf internen Servern verschlüsselt abgelegt.
- E-Mails mit vertraulichem Inhalt werden verschlüsselt, damit sie nur für den Adressaten lesbar sind.
- Der Zugriff auf Webserver wird mit dem Protokoll SSL/TLS (Secure Socket Layer/Transport Layer Security) gesichert.
- Bei der Arbeit im Home Office wird die Datenverbindung durch ein virtuelles privates Netzwerk (VPN) geschützt.

Daher ist es auch für mittelständische Unternehmen sehr wichtig, immer aktuelle und sichere kryptografische Verfahren zu nutzen, um angemessen gegen mögliche Angriffe geschützt zu sein.

Unternehmen sind darauf angewiesen, dass ihnen ihre Dienstleister und die Hersteller kryptografischer Produkte hinreichend sichere Verfahren bereitstellen. Gleichwohl können sie aber auch selber aktiv zu einem auch langfristig wirksamen Vertraulichkeitsschutz durch Verschlüsselung beitragen, wenn sie die folgenden Empfehlungen beachten:

1. Sensible Informationen verschlüsseln

Unternehmen müssen Daten, deren Vertraulichkeit wichtig ist, bei Speicherung und Übertragung mit guten Verfahren verschlüsseln.

2. Sicherheit kryptografischer Verfahren verfolgen

Entscheider, IT und IT-Sicherheitsverantwortliche sollten wissen, dass kryptografische Verfahren angreifbar sind und kontinuierlich aktualisiert werden müssen, um Angriffen widerstehen zu können.

3. Verzeichnis der in den Anwendungen eingesetzten kryptografischen Verfahren führen

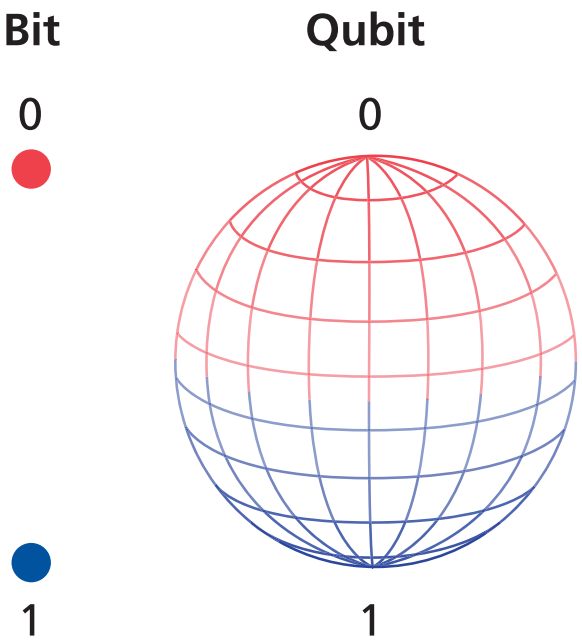
Ein solches Verzeichnis erleichtert es Unternehmen, auf bekanntgewordene Schwachstellen zu reagieren und die eingesetzten kryptografischen Verfahren anzupassen.

4. Bei Beschaffungen auf Aktualität und Anpassbarkeit der kryptografischen Verfahren achten

Bei der Beschaffung von Anwendungen, die kryptografische Komponenten nutzen, sollte darauf geachtet werden, dass sie den aktuellen Sicherheitsempfehlungen genügen und leicht an künftige Herausforderungen anpassbar sind. Entscheider sollten hier gezielt nachfragen und flexible Lösungen vertraglich vereinbaren.

5. Bei Verbänden und Interessenvertretungen auf Unterstützung und Zertifizierung hinwirken

Unternehmen sollten bei ihren Interessenvertretungen und Verbänden auf die Problematik veränderter Sicherheitsanforderungen und die Notwendigkeit von Lösungen hinweisen. Hierzu gehört auch die Forderung nach unabhängigen Zertifizierungen. Auch die Bereitstellung von Informationen zur Handhabung sicherer Kryptografie sollte hier angefragt werden.



Ausführliche Informationen zu Grundlagen und Anwendungsfeldern der Kryptografie finden sich in der vom Fraunhofer SIT verfassten und vom Hessischen Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung herausgegebenen Broschüre „Vertraulichkeitsschutz durch Verschlüsselung". Die Lektüre dieser einführenden Darstellung wird zum besseren Verständnis der nachfolgenden Ausführungen empfohlen.

wirtschaft.hessen.de/sites/default/files/media/hmwvl/leitfaden_vertraulichkeitsschutz_durch_verschluesselung.pdf

DEFINITION (MIT TECHNOLOGY REVIEW)

„Im Zentrum von Quantum-Computing befindet sich das Quantum-Bit, oder QuBit, eine Informations-Grundeinheit, analog zur den in Computern von Transistoren dargestellten 0ern und 1ern. Wegen zweier einzigartiger Merkmale besitzen QuBits wesentlich mehr Leistung als klassische Bits: Sie können zur selben Zeit sowohl 1 als auch 0 darstellen, und sie können anhand eines Phänomens – der Quantenverschränkung – andere QuBits beeinflussen. Dadurch können Quantencomputer bei bestimmten Arten von Berechnungen Abkürzungen zu den richtigen Antworten nehmen."

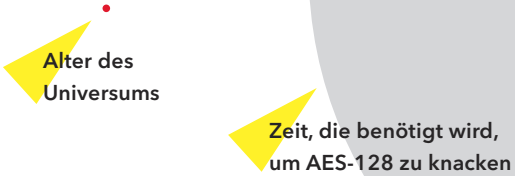
2 EINFÜHRUNG

Kryptografie ist ein entscheidender Baustein für das Erreichen von IT-Sicherheit in einer modernen, vernetzten Welt. Die Sicherheit fast aller kryptografischen Systeme ist aber nicht statisch, sondern an den technischen Fortschritt gebunden. Angreifer verfügen über immer höhere Rechenleistung und entwickeln immer bessere Angriffe auf kryptografische Systeme. Neue Technologien wie Quantencomputer stellen ebenso eine Bedrohung für die gängige Kryptografie dar. Prozesse und Produkte, deren Sicherheit auf Kryptografie angewiesen ist, müssen daher wandlungsfähig und leicht an die sich verändernden Bedingungen anpassbar sein.

2.1 EROSION KRYPTOGRAFISCHER VERFAHREN UND PARAMETER

Praktisch die gesamte Kryptografie, die heutzutage eingesetzt wird, basiert auf Berechnungskomplexität. Das bedeutet, dass es in der Theorie zwar möglich ist, derart verschlüsselte Botschaften zu knacken, dass aber ein Angreifer hierfür eine ungeheure Menge an Rechenleistung und Rechenzeit benötigt.

Wie lange dauert es, AES-128 mit der heutigen Technologie zu knacken?



Wenn ein Angreifer z. B. versuchen würde, eine Verschlüsselung nach dem verbreiteten Advanced Encryption Standard mit einer Schlüssellänge von 128 Bit (AES-128) durch Austesten aller möglichen Schlüssel zu knacken, würde er bei Verwendung des größten derzeit verfügbaren öffentlichen Supercomputers mindestens eine Zeit benötigen, die etwa 12.000 mal dem Alter des Universums entspricht.

In der Vergangenheit gab es allerdings viele Fälle, in denen kryptografische Verfahren und Parameter aufgrund von Verbesserungen in der Rechnerleistung geknackt wurden. Als im Jahr 1977 das US-Amerikanische National Institute of Standards and Technology (NIST, zur damaligen Zeit das „National Bureau of Standards") den Data Encryption Standard (DES) einführte, hielt man den Aufwand, dieses Verfahren durch Ausführen von bis zu 2^{56} = 72.057.594.037.927.936 individueller DES-Verschlüsselungen zu knacken, für nicht machbar.

Heute ist dies mit Hilfe spezieller Hardware innerhalb von einem Tag möglich. Wegen seiner rechnerischen Schwäche wurde DES daher bereits Anfang dieses Jahrtausends durch den oben genannten und bislang sicheren AES ersetzt. Trotzdem gibt es auch heute immer noch viele Altsysteme und -anwendungen, die den verwundbaren DES einsetzen oder unterstützen.

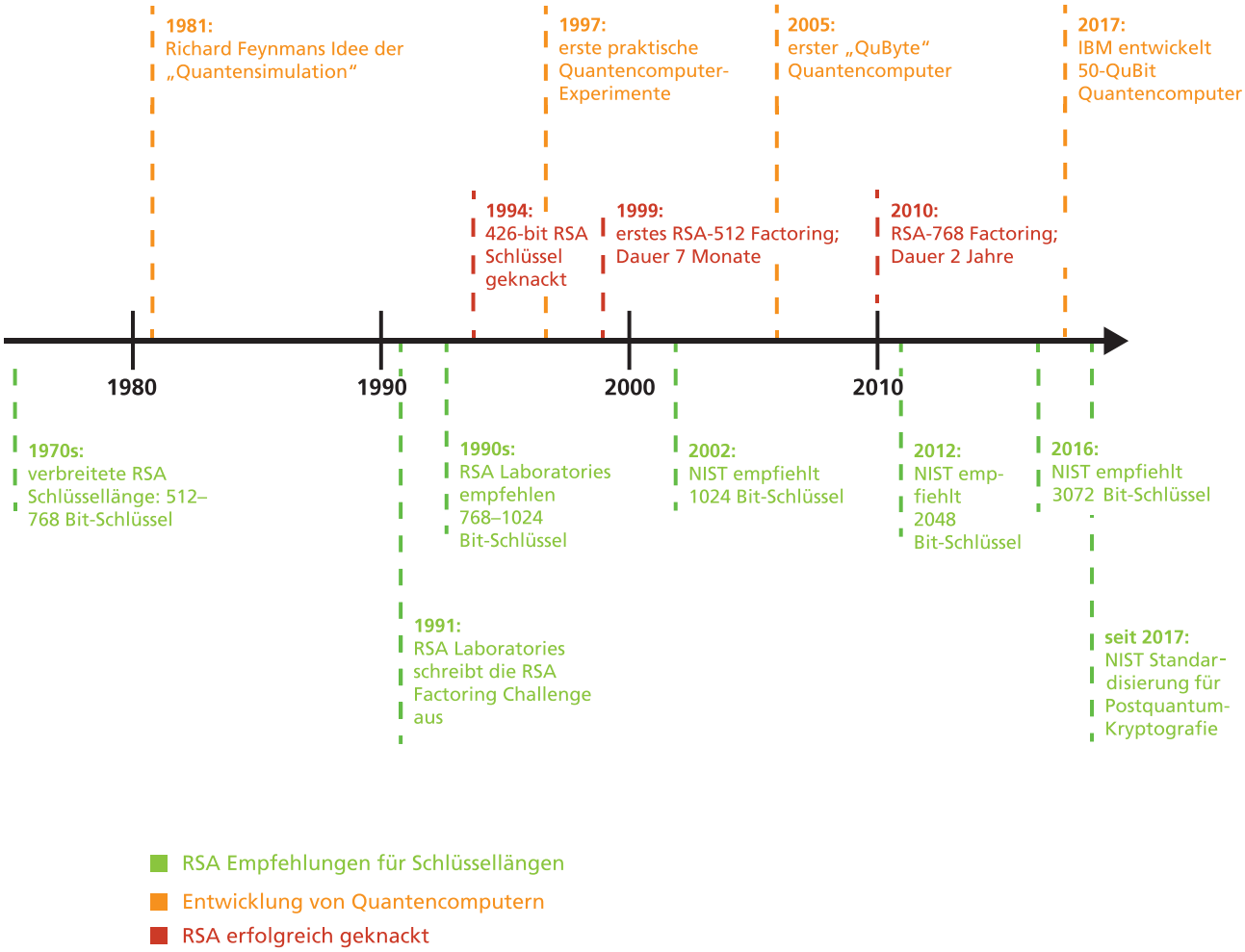
Ein weiteres Beispiel für verwundbare kryptografische Verfahren ist der Hash-Standard Message Digest 5 (MD5), der von Ron Rivest in den frühen 1990ern entwickelt wurde und zum Beispiel für die Erzeugung von digitalen Signaturen, zur Sicherung der Datenintegrität und zur Erzeugung elektronischer Zertifikate (etwa für die Authentisierung im Internet) genutzt wurde. Im Jahr 1996 hat das NIST eine MD5-Variante als SHA-1 (Secure Hash Algorithm) zum Standard gemacht. Nachdem schon in den Vorjahren eine Reihe an Schwachstellen in MD5 entdeckt wurde, gelang es Forschern im Jahr 2008 ein gefälschtes und von echten Zertifikaten der Zertifikatsausgabestelle nicht zu unterscheidendes Zertifikat unter Nutzung von MD5 zu erzeugen. Dadurch konnten sie Zertifikate für beliebige Internetdomains erstellen und konnte somit vorgetäuscht werden, dass es sich bei diesen Domains um z. B. Google, Facebook, eine Bank, eine Regierungsbehörde oder einen E-Mail-Anbieter handeln würde. Obwohl schon 2002 NIST den Standard SHA-2 und nach einem achtjährigen öffentlichen Standardisierungsprozess im Jahr 2015 SHA-3 als sichere Alternativen zu MD5 und SHA-1 eingeführt hatte, ist MD5 heute immer noch in Gebrauch.

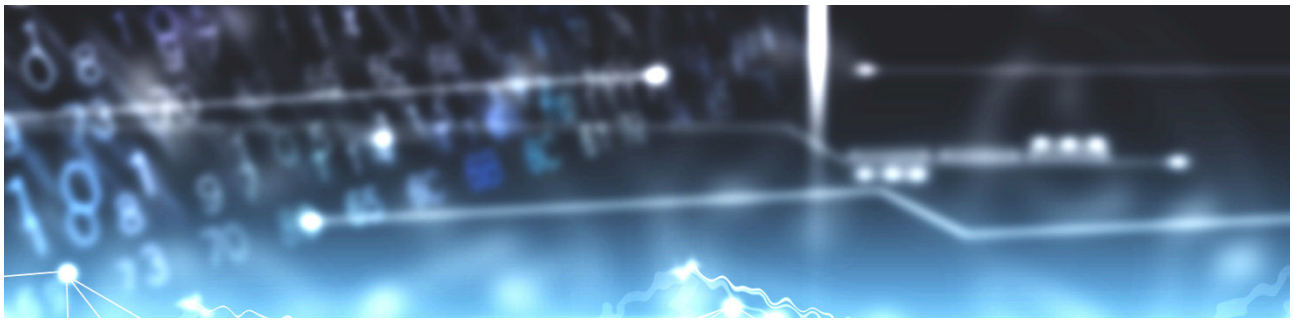
Solche Beispiele zeigen, dass bei einem signifikanten Fortschritt in der Kryptoanalyse oder der Rechenleistung im schlimmsten Fall ganze kryptografische Verfahren ausgetauscht werden müssen. Die Folgen sind allerdings nicht immer derart dramatisch. In manchen Fällen genügt es, die Sicherheitsparameter von Verfahren zu erhöhen, z. B. die Länge eines kryptografischen Schlüssels. Dies gilt bislang etwa für das asymmetrische Verschlüsselungsverfahren RSA (benannt nach den Nachnamen der Erfinder des Algorithmus Rivest, Shamir, Adleman), dessen Empfehlungen für sichere Schlüssellängen in den letzten zwanzig Jahren dreimal nach oben korrigiert wurden. Bei der Einführung in den 1970er Jahren schienen 512 oder 768 Bit lange Schlüssel ausreichend sicher zu sein. In den 1990ern eröffneten die RSA Laboratories die RSA Factoring Challenge, bei der dazu herausgefordert wurde, eine Reihe an RSA-Schlüsseln verschiedener Länge zu faktorisieren.

Da einige Aufgaben dieser Challenge sehr schnell gelöst wurden, empfahlen die RSA Laboratories die Verwendung von 768 bis 1024 Bit langen RSA-Schlüsseln. 1999 wurde RSA-512 zum ersten Mal öffentlich geknackt und drei Jahre später empfahl NIST, Schlüssel mit 1024 Bit Länge zu verwenden. Im Jahr 2010 konnten Forscher RSA-768 nach einer zwei Jahre dauernden Berechnung brechen. 2011 empfahl NIST Schlüssellängen von 2048 Bit und 2016 die US-amerikanische Sicherheitsbehörde NSA (National Security Agency) von 3072 Bit.

Manchmal beruhen kryptografische Standards oder Implementierungen auf falschen Annahmen. So hatten Kryptologen geglaubt, dass es unschädlich sei, einen bestimmten Parameter des Diffie-Hellman-Schlüsseltauschs, nämlich den PrimModulus, für alle Implementierungen dieses Verfahrens zu verwenden. Heute wissen wir, dass Angreifer, sobald sie einen mehrfach verwendeten Modulus geknackt haben, dadurch leicht eine beliebige Anzahl an Verbindungen knacken können. Ein solcher Angriff ist für einen Angreifer somit auch bei hohem Aufwand äußerst wertvoll.

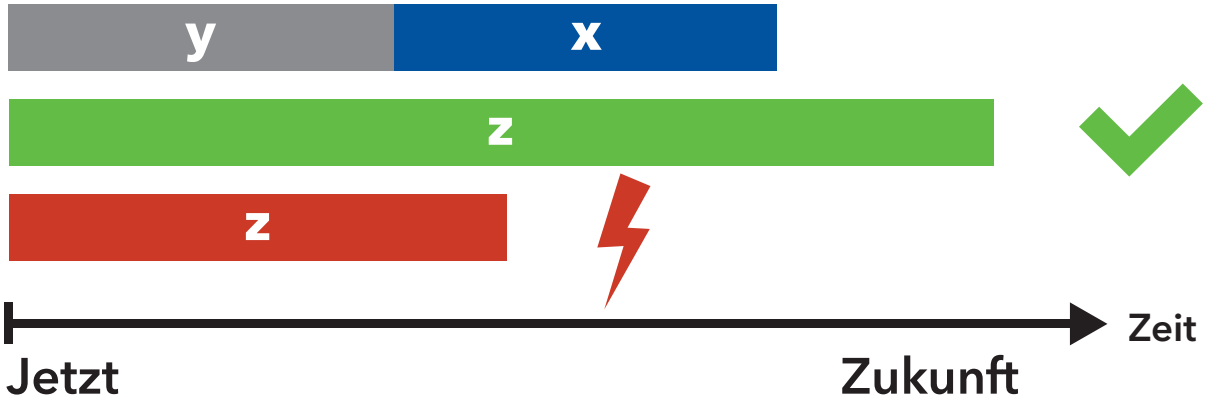
All diese Beispiele zeigen, dass kryptografische Verfahren, Parameter und Prinzipien mit der Zeit erodieren und unsicher werden. Als Gegenmaßnahmen muss ab und zu die Schlüssellänge angepasst werden, gelegentlich müssen aber auch ganze kryptografische Verfahren durch neue und sichere Alternativen ersetzt werden. Verfahren und Produkte, die auf Kryptografie beruhen, müssen daher gepflegt und möglicherweise während ihrer gesamten Lebensdauer aktualisiert werden. Je früher diese Anforderung in den Entwicklungsprozess für ein sicheres System eingebaut wird, desto einfacher und kostengünstiger wird der Wechsel zu neuen Parametern und Verfahren.


1981:
Richard Feynmans Idee der „Quantensimulation“
1997:
erste praktische Quantencomputer-Experimente
2005:
erster „QuByte“ Quantencomputer
2017:
IBM entwickelt 50-QuBit Quantencomputer
1994:
426-bit RSA Schlüssel geknackt
1999:
erstes RSA-512 Factoring; Dauer 7 Monate
2010:
RSA-768 Factoring; Dauer 2 Jahre
1980
1990
2000
2010
1970s:
verbreitete RSA Schlüssellänge: 512–768 Bit-Schlüssel
1990s:
RSA Laboratories empfehlen 768–1024 Bit-Schlüssel
2002:
NIST empfiehlt 1024 Bit-Schlüssel
2012:
NIST empfiehlt 2048 Bit-Schlüssel
2016:
NIST empfiehlt 3072 Bit-Schlüssel
1991:
RSA Laboratories schreibt die RSA Factoring Challenge aus
seit 2017:
NIST Standardisierung für Postquantum-Kryptografie
RSA Empfehlungen für Schlüssellängen
Entwicklung von Quantencomputern
RSA erfolgreich geknackt



Offene Frage: Wie groß ist die Bedrohung durch Quantencomputer?

Da es schwierig ist, *z* vorherzusagen, bleibt die Frage offen.



x: die Zeit, in der Geheimnisse geheim bleiben müssen
y: die Zeit, die es braucht, um Quantencomputer-sichere Kryptografie bereitzustellen
z: die Zeit, die es dauert, bis jetzige Kryptografie von Quantencomputern geknackt werden kann

Wenn z größer als x+y ist, dann ist alles in Ordnung. Wenn es kleiner ist, dann wird es gefährlich für uns!

2.2 POST-QUANTUM-KRYPTOGRAFIE

Quantencomputer stellen eine ernsthafte Bedrohung für die heutige Kryptografie dar. Üblicherweise werden asymmetrische Verfahren (z. B. RSA), die für Authentifizierung, Schlüsselaustausch, digitale Signaturen und Zertifikate im Internet sowie sichere Anwendungen verwendet werden, und symmetrische Verfahren (z. B. AES), mit denen übertragene und gespeicherte Daten geschützt werden, unterschieden. Quantencomputer bedrohen beide Ausprägungen und somit die gesamte heutzutage im Internet oder anderen sensiblen Anwendungen verwendete Kryptografie:

- Wenn genügend große Quantencomputer gebaut werden können, dann können sie unter Einsatz des vom amerikanischen Mathematiker Peter Shor entwickelten Quantenalgorithmus asymmetrische Kryptografie in praktisch durchführbarer Zeit knacken.
- Bei Verwendung des vom indisch-amerikanischen Informatikers Lov Grovers entwickelten Quantenalgorithmus bedrohen Quantencomputer darüber hinaus symmetrische Verschlüsselungsverfahren wie AES. Experten empfehlen, die Schlüssellänge bei AES von 128 auf 256 Bit zu verdoppeln, um sich gegen große, mächtige Quantencomputer zu schützen. Vielfach wird dieser Empfehlung bereits gefolgt.

Kryptologen arbeiten an alternativen Verschlüsselungsverfahren, insbesondere für asymmetrische Kryptografie, von denen nicht bekannt ist, dass sie für Quantencomputer anfällig sind. Dieses Feld der Kryptografie wird als „Post-Quantum-Kryptografie" bezeichnet. Es gibt eine große Bandbreite an schwierigen mathematischen Problemen, bei denen nicht bekannt ist, dass ein Quantencomputer bei deren Lösung von bahnbrechendem Vorteil wäre, z. B. bei Problemen der Kodierungstheorie, zur Gittertheorie oder beim Lösen von multivariaten Polynomen.

Darüber hinaus können kryptografisch sichere Hashfunktionen verwendet werden, um Signatursysteme zu erstellen. Es gibt derzeit eine Debatte darüber, welcher dieser Ansätze zu den sichersten und effizientesten Kryptosystemen führt. Das amerikanische National Institut for Standards and Technologie – NIST hat 2017 einen Standardisierungsprozess für Post-Quantum-Kryptografie begonnen. Es ist daher zu erwarten, dass praktisch einsetzbare, gegen Quantencomputerangriffe robuste Verfahren bald verfügbar sein werden.

Der Nachteil der meisten heutigen Post-Quantum-Verfahren ist der im Vergleich mit klassischen kryptografischen Verfahren höhere Anspruch an Ressourcen: Generell sind private und öffentliche Schlüssel sowie Ciphertexte und Signaturen länger und die Anforderungen an die Rechnerleistung höher. Für eingebettete Systeme mit geringen Ressourcen und ebenso für Internetserver, die eine große Anzahl an sicheren Verbindungen zu bewältigen haben, ist dies besonders problematisch. Es wird daher derzeit intensiv dazu geforscht, wie die Ressourcenanforderungen der Post-Quantum-Verfahren unter Beibehaltung der Sicherheit reduziert werden können. Im Vergleich zu den derzeit verwendeten klassischen Verfahren haben einige Post-Quantum-Verfahren außerdem Zusatzanforderungen. Einige hash-basierte Signatursysteme müssen z. B. einen Zustand speichern, der sich mit jeder Signatur ändert. Bei Rückkehr zu einem vorherigen Zustand wird die Sicherheit des Signatursystems beeinträchtigt. Dies bedeutet neue Anforderungen an die Backup-Strategie für geheime Signierschlüssel.

Eine typische Anforderung an geheime oder sensible Daten ist, dass sie für mindestens x Jahre sicher verwahrt sein müssen, wobei x von der Sensibilität der Daten abhängig ist. Wenn wir y Jahre für die Umstellung auf Post-Quantum-Kryptografie benötigen und annehmen, dass große Quantencomputer in z Jahren verfügbar sein werden, dann muss $y + x$ kleiner sein als z.

Geheimnisse, die zum Ende einer Prä-Quantum-Ära gespeichert werden, könnten dann geknackt werden, sobald Quantencomputer verfügbar sind und noch bevor diese Geheimnisse ihre Sensibilität verlieren. Wenn wir mit der Umstellung auf Post-Quantum-Verfahren warten, bis wir sicher sein können, dass Quantencomputer tatsächlich eine Gefahr darstellen, ist es vielleicht bereits zu spät, um unsere Geheimnisse noch schützen zu können. Außerdem darf man nicht vergessen, dass ein Quantencomputer nur eine von vielen Bedrohungen ist. Auch wenn Quantencomputer, welche die derzeitige Kryptografie knacken könnten, vielleicht nie gebaut werden, so müssen wir doch für ausreichend Flexibilität sorgen, um auf künftige Bedrohungen aus Entwicklungen in der klassischen Kryptoanalyse und klassischer Rechenleistung reagieren zu können.

2.3 KRYPTO-AGILITÄT

Kryptografie ist eine sehr dynamische Technologie:

- Die Erosion von kryptografischen Parametern und Verfahren ist schwer abzuschätzen.
- Plötzliche Fortschritte in der Kryptoanalyse könnten uns jederzeit dazu zwingen, Verfahren zu ersetzen, Implementierungen zu verbessern oder Schlüssellängen zu erhöhen.
- Quantencomputer wird es nicht über Nacht geben, aber die Bedrohung durch sie ist so ernst, dass wir uns auf eine Umstellung auf Post-Quantum Kryptografie vorbereiten sollten.

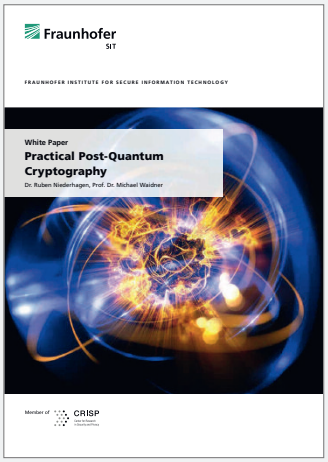
Am besten bereitet man sich auf diese dynamischen Veränderungen mit „Krypto-Agilität" vor, d. h. mit der Fähigkeit, Parameter oder Verfahren dynamisch zu verändern, wobei Vorgänge wie Protokolle, Anwendungen und Prozesse beibehalten werden. Für Krypto-Agilität ist eine API zwischen dem Krypto-Layer und dem Rest der Applikation erforderlich, wodurch die Einzelheiten der verwendeten kryptografischen Verfahren versteckt werden können und somit der Austausch von kryptografischen Parametern oder Verfahren mit keinen bzw. nur geringfügigen Auswirkungen auf die restliche Anwendung ermöglicht werden kann.

Krypto-Agilität sollte von Anfang an bei der Entwicklung von sicheren Prozessen und Anwendungen eingebaut werden. Bereits bestehende Anwendungen sollten aktualisiert werden, um Krypto-Agilität zu ermöglichen. Wenn eine Anwendung angepasst wird, z. B. von RSA auf Elliptische-Kurven-Kryptografie (ECC), sollte eine fest integrierte RSA-Implementierung nicht durch eine fest integrierte ECC-Implementierung ausgetauscht werden, sondern neue ECC-Verfahren sollten bei Bedarf einfach und dynamisch durch andere zukünftige Verfahren ersetzt werden können. Hierfür muss Forschung zur Standardisierung von kryptografischen Schnittstellen für typische Anwendungsfälle und Applikationen betrieben werden, sodass der Tausch der zugrundeliegenden Verfahren nur minimale Auswirkung auf das restliche System hat.

Weitere Lektüre:

Practical Post-Quantum Cryptography
R. Niederhagen, M. Waidner, 2017 Fraunhofer SIT

www.sit.fraunhofer.de/de/reports/#c4742



3 KRYPTO-BEREITSCHAFT DER INDUSTRIE

Kryptografie ist heutzutage eine der Haupttechnologien, um IT-Sicherheit zu erreichen. Da die digitale Kommunikation die Hauptsäule unserer modernen Gesellschaft und Wirtschaft ist, spielt Kryptografie eine wichtige Rolle in nahezu jedem wirtschaftlichen Bereich. Nachfolgend sind die drei wichtigsten Industriegruppen aufgelistet, geordnet nach ihrer Interaktion mit Kryptografie:

1. Die meisten Firmen – auch kleine und mittlere Unternehmen – verwenden Kryptografie, um ihre IT-Anwendungen und Daten zu schützen. Firmen, die passiv Kryptografie nutzen, interessieren sich nicht für die technischen Details. Sie verwenden von Herstellern bereitgestellte Standardprodukte.
2. IT-Systementwickler implementieren Kryptografie häufig ebenfalls nicht selbst, sondern integrieren externe kryptografische Bibliotheken oder Module in ihre Produkte. Sie müssen wissen, welche kryptografischen Verfahren und Parameter für ihre Produkte nötig sind, benötigen hierfür aber keine Kenntnisse zu den Details ihrer Implementierung.
3. Krypto-Zulieferer stellen den Systementwicklern die von diesen benötigten kryptografischen Bibliotheken und Module zur Verfügung.

All diese Mitwirkenden sehen sich eigenen Herausforderungen gegenüber.

3.1 HERAUSFORDERUNGEN FÜR KRYPTOGRAFIE-ANWENDER

Unternehmen setzen Kryptografie ein, um Systeme und Prozesse abzusichern – und dies insbesondere für folgende Anwendungen:

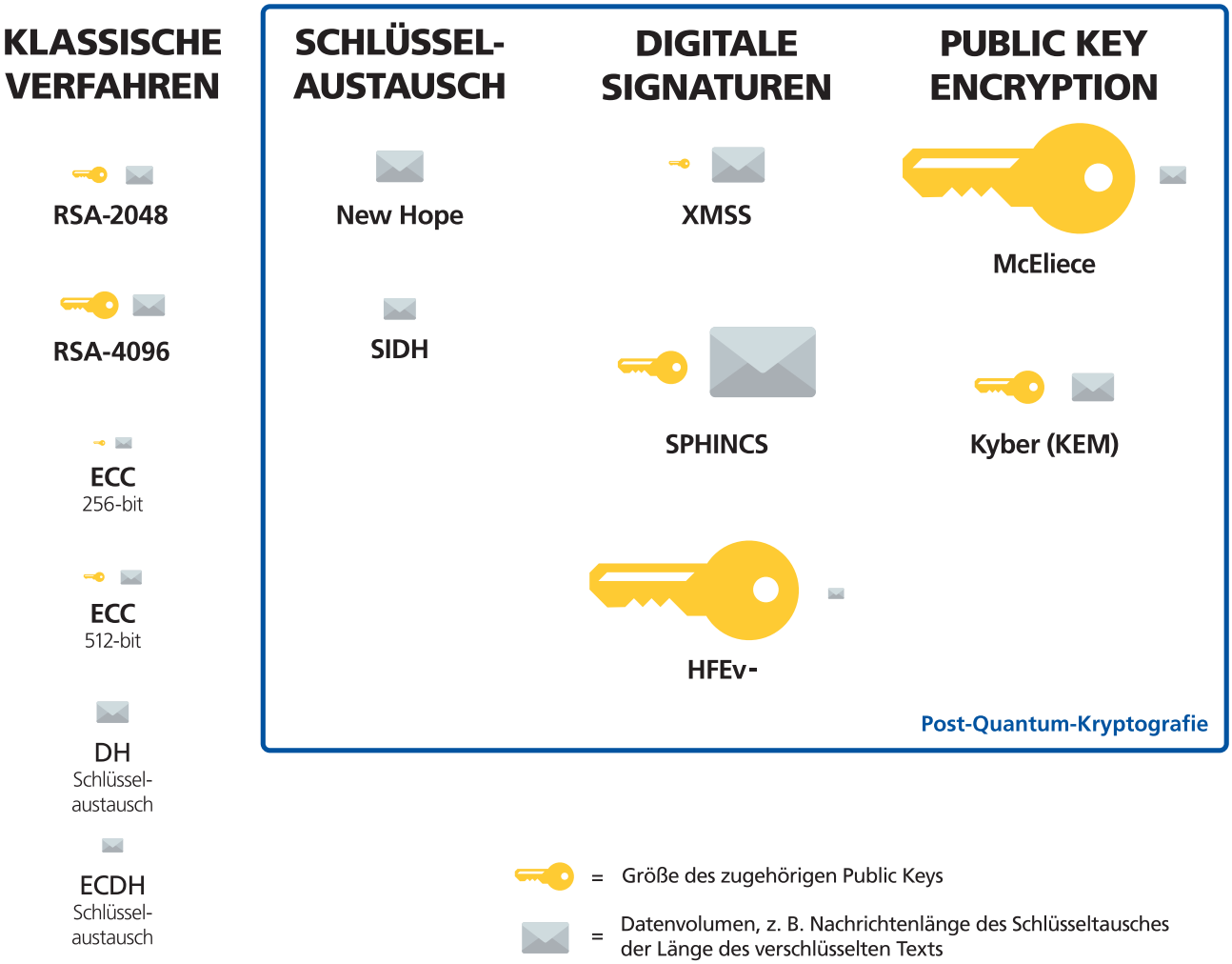
- Verschlüsselung von Daten bei der Speicherung auf Datei-, Dateisystem oder Festplattenebene sowohl auf stationären und mobilen Geräten als auch in der Cloud,
- vertrauliche und vertrauenswürdige Kommunikation via E-Mail oder Messaging-Dienst mit Hilfe von Verschlüsselung und digitalen Signaturen zur Gewährleistung der Integrität der übertragenen Informationen sowie
- das sichere und vertrauliche Bewegen im Internet.

Hierzu nutzen die Unternehmen Funktionen ihres Betriebssystems, zusätzliche Produkte zur Festplattenverschlüsselung und sichere Clouddienste. Auch der E-Mail-Client muss durch die Integration von Zertifikaten erlauben, eine E-Mail für einen Adressaten zu verschlüsseln und der Internet Browser muss für kryptografische Verfahren vorbereitet sein.

Unternehmen brauchen für diese Zwecke standardisierte, einsatzfertige Lösungen. Sie haben kein Interesse an den technischen Details, mit denen Anbieter für die Sicherheit ihrer Produkte und Dienste sorgen. Sie wollen, dass sich ihre Investitionen auszahlen, aber sie können nur begrenzte Ressourcen einsetzen, um Produkte unterschiedlicher Anbieter zu bewerten und zu vergleichen. Vertiefte Produktvergleiche vor einer Einsatzentscheidung sind damit meist ausgeschlossen.

Insbesondere mittelständische Unternehmen möchten, dass ihre Anwendungsfälle leicht auf das jeweils beste und günstigste Produkt abgebildet werden können, ohne dass sie verstehen müssen, was genau die Sicherheitsanforderungen der Anwendungsfälle sind oder wie der Anbieter diese Anforderungen technisch erfüllt. Da wäre es sehr hilfreich, wenn es für die oben aufgeführten Anwendungsfälle öffentlich zugängliche Kataloge gäbe, die Produkte und Versionen von Produkten auflisten, bei denen die (Sicherheits-)Qualität der implementierten kryptografischen Verfahren durch unabhängige Zertifizierungen bestätigt ist. Dies würde den Unternehmen beispielsweise ermöglichen, zu prüfen, ob die Version des von ihnen eingesetzten E-Mail-Clients oder die zur Festplattenverschlüsselung gewählte Lösung aktuellen Sicherheitsanforderungen genügt. Leider gibt es ein derartiges Informationsangebot, das z. B. von einer öffentlichen Behörde bereitgestellt werden könnte, derzeit in dieser Form noch nicht.

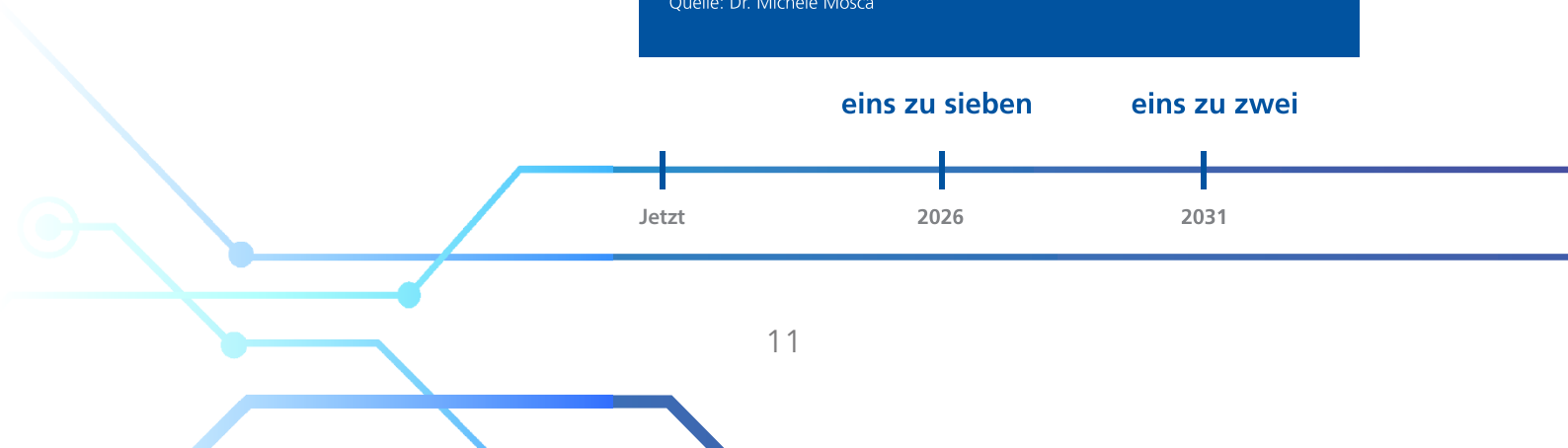
Schlüssellänge und Nachrichtenlänge



Es gibt eine Reihe an Verfahren zur Post-Quantum-Kryptografie, die allerdings jeweils individuelle Vor- und Nachteile haben. Derzeit kann also noch keines dieser Verfahren eindeutig favorisiert werden, zumal bislang keines davon durch das NIST standardisiert wurde.

Wahrscheinlichkeit, dass grundlegende Public Key Krypto durch Quantencomputer geknackt wird

Quelle: Dr. Michele Mosca



3.2 HERAUSFORDERUNGEN AN UNTERNEHMEN, DIE KRYPTOGRAFIE INTEGRIEREN

Bezüglich Leistung, Effizienz und Sicherheit benötigen IT-Systementwickler qualitativ hochwertige Implementierungen. Open-Source-Bibliotheken bieten öffentlich überprüfte und anwenderfreundliche Kryptografie. Diese Hersteller benötigen jedoch langfristige Unterstützung und bei einem Sicherheitsvorfall schnelle Reaktionszeiten, was häufig bei Open-SourceProjekten nicht garantiert ist: Sicherheitsupdates müssen für eine lange Zeit zur Verfügung gestellt werden, besondere Anforderungen ihrer Kunden müssen schnell implementiert werden.

IT-Systementwickler müssen Sicherheitsentscheidungen auf Basis der Anforderungen ihrer Kunden treffen und die richtigen Verfahren und Implementierungen von ihren Krypto-Zulieferern anfordern. Diese Entscheidungen haben einen tiefgreifenden Einfluss auf Produktsicherheit und -leistung. Oft gibt es ein sehr breites Feld an kryptografischen Verfahren, aus dem ausgewählt werden kann. Von diesen Verfahren hat jedes seine spezifischen Anforderungen und Eigenschaften. Entwickler stehen also vor der nicht immer trivialen Herausforderung, aus dem möglichen Spektrum an Lösungen eine angemessene Auswahl zu treffen.

Ein Beispiel hierfür ist die Elliptische-Kurven-Kryptografie (ECC). Bei ECC muss der Entwickler eine spezifische Kurve als Grundlage für die kryptografischen Verfahren auswählen.

Obwohl ein breiter Konsens hinsichtlich der Sicherheitsanforderungen für die Kurvenauswahl besteht, gibt es eine riesige Anzahl an unterschiedlichen Kurven, die von verschiedenen Standards, Firmen und Sicherheitsexperten beworben werden. In den USA werden üblicherweise von NIST standardisierte Kurven verwendet. Vor Kurzem wurden jedoch diese NIST-Kurven einer genaueren Prüfung unterzogen, da vermutet wird, dass der amerikanische Geheimdienst NSA in die Auswahl der Kurven involviert gewesen sein könnte, sie also „Hintertüren" enthalten könnten, was grundsätzlich auch bei anderen Verfahren nicht ausgeschlossen werden kann. Außerdem sind diese Kurven nicht unbedingt die beste Wahl in Bezug auf Leistung und Effizienz. In Deutschland empfiehlt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verwendung von sogenannten Brainpool-Kurven. Sowohl an den NIST- als auch an den BSI-Kurven wird bemängelt, dass sie ohne Berücksichtigung von Leistung und Effizienz definiert wurden. Eine weitere Option ist die hoch effiziente und optimierte Kurve „curve25519" des Kryptologen Daniel J. Bernstein, die ausdrücklich auf Leistung als Entwicklungskriterium ausgerichtet ist. Diese Kurve durchläuft zwar derzeit den Standardisierungsprozess der Internet Engineering Taskforce (IETF) für den kommenden TLS 1.3 Standard, ist aber ansonsten nicht weiter standardisiert.

3.3 HERAUSFORDERUNGEN AN KRYPTO-ZULIEFERER

Krypto-Zulieferer implementieren kryptografische Verfahren und Protokolle und stellen Systementwicklern kryptografische Bibliotheken und Lösungen zur Verfügung – vielfach mit Hilfe von Open-Source-Software. Krypto-Zulieferer wissen oft nicht, für welche spezifischen Anwendungen und Produkte ihre Bibliotheken verwendet werden. Sie müssen daher eine breite Palette an Parametern und Verfahren vorhalten, können sie aber nicht immer für bestimmte Anwendungsfälle oder Plattformen optimieren.

Die Wettbewerbsfähigkeit verlangt, dass sie günstig sein müssen, was sie andererseits aber wieder davon abhält, ihre Produkte an die tatsächlichen Einsatzumgebungen und Anwendungsfälle anzupassen. Krypto-Zulieferer beschränken sich daher auf standardisierte Kryptografie-Angebote.

Ihre Kunden fragen in der Regel nicht nach neuen, noch nicht standardisierten Lösungen. Es gibt keinen Markt für ‚Orchideen'; Lösungen müssen günstig, standardisiert, handelsüblich und leicht anwendbar sein.

4 HERAUSFORDERUNGEN FÜR KRYPTO-AGILITÄT

In Bezug auf Kryptografie sind heutige Anwendungen nicht ausreichend flexibel. In großen Systemen, die mit der Zeit durch Beiträge unterschiedlicher Teams gewachsen sind, sind dieselben kryptografischen Verfahren oft mehrfach und unabhängig voneinander implementiert. Beispielsweise können ein Desktop-Client, ein mobiler Client und der dazugehörige Server (mehrere) individuelle SHA-1 Umsetzungen aufweisen.

Wenn SHA-1 nun durch eine sicherere Alternative (z. B. SHA-2 oder SHA-3) ersetzt werden soll, müssen alle einzelnen SHA-1-Implementierungen ausfindig gemacht und ersetzt werden. Dies macht Krypto-Agilität entweder sehr teuer oder verhindert sie gar. Wenn alle Clients und Server dieselbe Krypto-Bibliothek verwenden würden, wäre es viel einfacher, stets aktuelle Versionen der eingesetzten kryptografischen Anwendungen bereitzustellen.

Es ist daher erforderlich, dass Krypto-Agilität von Beginn an Teil der Systementwicklung wird. Jedes neu begonnene Vorhaben, für das Kryptografie notwendig ist, muss KryptoAgilität berücksichtigen. Dazu gehören eine Strategie für sichere Updates, verfahrensunabhängige Krypto-APIs sowie agile kryptografische Protokolle.

Wenn Krypto-Agilität nicht Teil des Designs für ein System war, dann muss das System so bald wie möglich entsprechend angepasst werden. Dies kann stufenweise erfolgen, solange die verwendeten kryptografischen Parameter und Verfahren noch sicher sind. Mit jedem planmäßigen Update sollten mehr und mehr kryptografische Module auf den Einsatz einer Krypto-API umgeschrieben werden; individuelle Implementierungen von kryptografischen Verfahren sollten durch Aufrufe einer Krypto-Bibliothek ersetzt werden. In diesem Zusammenhang sind auch Vorkehrungen gegen Angriffe zu berücksichtigen, bei denen die beteiligten Instanzen (z. B. ein Webserver und ein Webclient) dazu gebracht werden, für eine Transaktion veraltete und schwächere oder sogar überhaupt keine Verschlüsselung zu verwenden.

Während dieser Übergangszeit sollten Protokolle so modifiziert werden, dass sie rückwärtskompatibel eine Änderung von Parametern und Verfahren zulassen. Sobald alle Systeme migriert sind und Krypto-Agilität für das Gesamtsystem etabliert ist, sollten veraltete Protokolle, Verfahren und Parameter deaktiviert werden.

In einem komplexen System, das keine Krypto-Agilität unterstützt oder sich in der Übergangsphase zur Agilität hin befindet, werden im schlimmsten Fall die kryptografischen Verfahren und Parameter unsicher. Hier bleibt das System dann verwundbar, bis alle Teile ausgebessert sind. Die Kosten für ein sicheres System erhöhen sich mit zunehmendem Druck und geringem Zeitrahmen. Sollten Angreifer während dieses Zeitraums Schwächen ausnutzen können, könnten Geheimnisse unwiderruflich offengelegt werden.

Welche Verfahren sind von Quantencomputern bedroht?

	KLASSISCH	POST-QUANTUM
PUBLIC KEY-VERSCHLÜSSELUNG	RSA ECC	McEliece Kyber (KEM)
SIGNATUREN	RSA DSA ECDSA	XMSS HFEv-
SCHLÜSSEL-AUSTAUSCH	DH ECDH	NewHope
SYMMETRISCHE SCHLÜSSEL VERSCHLÜSSELUNG	AES-128	
	AES-256	
HASHFUNKTIONEN	SHA2 SHA3	

5 FÜNF EMPFEHLUNGEN ZUR VORBEREITUNG AUF DIE KRYPTOGRAFIE DER NÄCHSTEN GENERATION

Die folgenden Abschnitte enthalten fünf Empfehlungen für kleine und mittlere Unternehmen dazu, wie sie sich angemessen auf die Herausforderungen durch Quantencomputer und andere Bedrohungen für die langfristige Sicherheit ihrer kryptografischen Anwendungen und kryptografisch geschützten Daten vorbereiten können.

5.1 SENSIBLE INFORMATIONEN VERSCHLÜSSELN

Auch in kleinen und mittleren Unternehmen werden besonders schutzwürdige Informationen verarbeitet, gespeichert und übertragen. Dazu zählen wichtiges Firmen-Know-how, Daten, die der Vorbereitung von Angeboten dienen und die für Konkurrenten sehr wichtig sein können, beispielsweise Preise und Kalkulationsformeln, aber auch Kundendaten, die wegen des Datenschutzrechts besonderen Schutzanforderungen unterliegen. Vertraulichkeit und Integrität solcher Informationen können mit kryptografischen Verfahren gesichert werden.

Empfehlung: Unternehmen sollten den Schutzbedarf ihrer Informationen sorgfältig analysieren und geeignete Maßnahmen zur Absicherung treffen. Hier gibt es eine Fülle von technischen und organisatorischen Maßnahmen, etwa eine geeignete Absicherung des Unternehmensnetzes durch ein Firewallsystem oder ein aktuell gehaltener Malwareschutz. Auch sorgfältig geplante und überwachte Zugriffsregelungen für die IT-Systeme sind unerlässlich. Das schärfste Schwert zur Sicherung der Vertraulichkeit und der Integrität von Daten ist jedoch die Nutzung kryptografischer Verfahren. Verschlüsselung und elektronische Signaturen gewährleisten, dass nur Berechtigte auf die Informationen zugreifen und Integritätsverletzungen erkannt werden können. Auch mittelständische Unternehmen sollten diese Verfahren unbedingt nutzen.

Hinweise hierzu gibt die eingangs erwähnte Broschüre „Vertraulichkeitsschutz durch Verschlüsselung – Strategien und Lösungen für Unternehmen“, die über das Hessische Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung und die Internetseiten des Fraunhofer SIT zugänglich ist.

Nutzen: Auch wenn kryptografische Verfahren im Zeitablauf ihre Wirksamkeit verlieren können, schützen sie – sorgfältig eingesetzt – die wichtigen Informationen eines Unternehmens und verhindern den Abfluss von Know-how, Schutzrechtsverletzungen und den Missbrauch personenbezogener Daten und damit möglicherweise auch hohe Strafzahlungen.

5.2 SICHERHEIT KRYPTOGRAFISCHER VERFAHREN VERFOLGEN

Entscheider sowie IT- und IT-Sicherheitsverantwortliche in Unternehmen müssen wissen, dass auch kryptografische Verfahren von Hackern angegriffen werden und diese daher kontinuierlich aktualisiert werden müssen, um den Angriffen widerstehen zu können. Sie müssen auch darauf vorbereitet sein, dass Quantencomputer schon in wenigen Jahren die heute verwendeten kryptografischen Verfahren entwerten können.

Empfehlung: Um kryptografische Verfahren in aller Tiefe zu verstehen, sind spezielle mathematische Kenntnisse erforderlich. Die Entwicklung solcher Verfahren und die Integration in Anwendungen ist Aufgabe von Spezialisten. Aber auch Anwender sollten die Grundlagen kryptografischer Verfahren etwa zur Verschlüsselung oder zum Schutz vor unerwünschten Veränderungen von Informationen kennen, da dies den kompetenten Einsatz dieser wirksamen Schutzmechanismen erleichtert.

Es gibt inzwischen viele Informationen hierzu, die auch dem Laien verständlich sind. Neben der eingangs erwähnten Broschüre „Vertraulichkeitsschutz durch Verschlüsselung" lassen sich weitere Broschüren hierzu über den IT-Sicherheitsnavigator, den das Bundesministerium für Wirtschaft und Energie bereitstellt, finden.

www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Angebote/it-sicherheitsnavigator.html

Nutzen: Bei einem grundlegenden Verständnis für kryptografische Verfahren können auch Entscheider in mittelständischen Unternehmen diese Verfahren angemessen nutzen. Sie sind zudem kompetente Partner ihrer IT-Lieferanten. Basiskompetenz zum Thema Kryptografie trägt dazu bei, durch die Wahl geeigneter Anwendungen die Unternehmensdaten wirksam zu schützen.

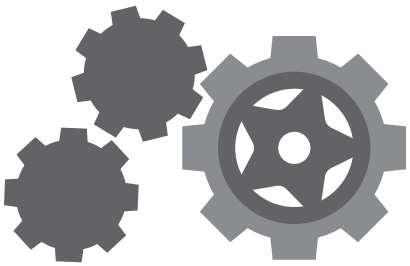
5.3 VERZEICHNIS DER IN DEN ANWENDUNGEN EINGESETZTEN KRYPTOGRAFISCHEN VERFAHREN FÜHREN

Bei Anwendungen, die die Speicherung und Übertragung von Informationen steuern, werden kryptografische Verfahren zur Absicherung eingesetzt. Jedes Unternehmen nutzt eine Vielzahl von Anwendungen dieser Art: Dateiverschlüsselung, E-Mail-Clients, Browser für die Internetkommunikation. Da fällt es schwer, die Art und Güte der genutzten kryptografischen Verfahren immer im Blick zu halten. So kann es passieren, dass ein Verfahren verwendet wird, das nicht mehr sicher ist.

Empfehlung: Unternehmen sollten ein Verzeichnis der Anwendungen erstellen, die kryptografische Verfahren nutzen, um diese aktuell halten zu können. Dabei ist es auch wichtig zu dokumentieren, welche Verfahren eingesetzt werden.

Hierzu müssen unter Umständen weitere Informationen vom Lieferanten eingeholt werden. Die IT-Verantwortlichen in den Unternehmen, sollten immer prüfen, ob die Verfahren noch einen sicheren Schutz bieten und zeitnah den Wechsel eines Verfahren betreiben oder Parameter wie Schlüssellängen verändern. Dies erfordert die Mitwirkung der IT-Lieferanten der Unternehmen.

Nutzen: Nur aktuell gehaltene kryptografische Verfahren sichern Informationen wirkungsvoll. Ein Verzeichnis unterstützt hier bei den im Bedarfsfall notwendigen zeitnahen Aktualisierungen.



5.4 BEI BESCHAFFUNGEN AUF AKTUALITÄT UND ANPASSBARKEIT DER KRYPTOGRAFISCHEN VERFAHREN ACHTEN

Entscheider und Beschaffer in mittelständischen Unternehmen sind keine Kryptografie-Experten. Sie sind darauf angewiesen, dass Hard und Softwarelieferanten ihnen gute Produkte bereitstellen. Sie müssen jedoch Vorgaben in ihren Ausschreibungen machen, angebotene Lösungen bewerten und den sicheren Betrieb ihrer kryptografischen Anwendungen überwachen können.

Empfehlung: Bei der Beschaffung kryptografischer Produkte (z. B. für die Verschlüsselung von E-Mails oder Daten auf Laptops) und Anwendungen mit kryptografischer Funktionalität sollte ein Unternehmen oder ein von diesem beauftragter IT-Dienstleister darauf achten, dass diese

- Algorithmen und Schlüssellängen verwenden, deren Sicherheit hinreichend belegt ist,
- keine bekannten Sicherheitslücken enthalten und bei denen
- ein leichter Austausch der kryptografischen Verfahren möglich ist, wenn Schwachstellen offenbar werden.

Hilfestellung bei der Bewertung der Sicherheit kryptografischer Verfahren und Schlüssellängen bieten beispielsweise technische Richtlinien des BSI.

Insbesondere auch zur leichten Anpassbarkeit kryptografischer Produkte sollten Entscheider gezielt nachfragen und flexible Lösungen vertraglich vereinbaren. Je häufiger Unternehmen diese Anforderung in den Beschaffungsvorgängen adressieren, umso eher werden die Hersteller sie erfüllen.

Für den sicheren Betrieb der kryptografischen Anwendungen ist neben grundlegenden Maßnahmen wie

- einer gegen Missbräuche geschützten Erzeugung, Übertragung und Speicherung der verwendeten geheimen Schlüssel,
- dem Vorhandensein von Vorkehrungen für Notfallszenarien etwa zur Entschlüsselung wichtiger Daten bei Verlust oder Beschädigung der ursprünglich hierfür vorgesehenen Schlüssel sowie
- klaren Regelungen und einer ausreichenden Schulung für die Benutzung der kryptografischen Verfahren

vor allem auch darauf zu achten, sich kontinuierlich über die Güte und mögliche Schwachstellen kryptografischer Verfahren zu informieren und bekanntgewordene Sicherheitslücken frühzeitig zu beheben. Die zeitnahe Beseitigung von Sicherheitsmängeln fällt umso leichter, je stärker bereits bei der Beschaffung einer kryptografischen Lösung auf deren einfache Anpassbarkeit an neue Algorithmen und Schlüssellängen geachtet wurde.

Nutzen: Unternehmen erhalten angemessene kryptografische Verfahren zur Absicherung ihrer Anwendungen, wenn dies Bestandteil der Lieferverträge wird. Je mehr Firmen hierauf achten, umso stärker ist der Impuls für die IT-Industrie, diese Verfahren auch bereitzustellen. Dies wird auch die Entwicklung von Lösungen beschleunigen, die den Leistungen von Quantencomputern oder anderen Bedrohungen für die Sicherheit der derzeit genutzten kryptografischen Verfahren widerstehen können.

5.5 BEI VERBÄNDEN, INTERESSENVERTRETUNGEN AUF UNTERSTÜTZUNG UND ZERTIFIZIERUNG HINWIRKEN

Mittelständische Unternehmen sind über Kammern organisiert und sind Mitglied in einer Vielzahl von Fachverbänden. Viele dieser Organisationen halten Informationen zu wichtigen IT-Themen für ihre Mitglieder bereit. Auch Branchenverbände wie der Bitkom unterstützen Unternehmen mit Online-Informationen oder Broschüren bei aktuellen IT-Fragestellungen.

Empfehlung: Unternehmen sollten bei ihren Interessenvertretungen und Verbänden gezielt auf die Problematik erodierender kryptografischer Verfahren und die Bedrohung durch Quantencomputer sowie die Notwendigkeit von Lösungen hinweisen. Diese Entwicklungen sind nicht nur ein Problem eines einzelnen Unternehmens, sondern bedrohen das Know-how der mittelständischen Wirtschaft, die das Rückgrat der deutschen Volkswirtschaft bildet. Mittelständische Unternehmen sollten über ihre Verbände und Standesorganisationen praxisnahe Informationen einfordern, aber auch unabhängige Zertifizierungen und öffentliche Kataloge zu wirksamen Kryptografiekomponenten anmahnen. Dies wird die Bereitstellung solcher Instrumente beschleunigen und dazu beitragen, dass Unternehmen schneller über gute Hilfestellungen verfügen.

Nutzen: Viele Gremien, Verbände und auch die Politik haben Programme zur Unterstützung des digitalen Wandels aufgelegt. Die Weiterentwicklung kryptografischer Verfahren ist ein zentraler Baustein für die Absicherung digitaler Prozesse. Nur Unternehmen, die angemessen informiert sind, die aus zertifizierten Produkten auswählen können und öffentlich zugängliche Verzeichnisse zu bewährten Lösungen vorfinden, können sichere digitale Verfahren implementieren.


Sensible Informationen verschlüsseln
Sicherheit kryptografischer Verfahren verfolgen
Verzeichnis der in den Anwendungen eingesetzten kryptografischen Verfahren führen
Bei Beschaffung auf Aktualität und Anpassbarkeit der kryptografischen Verfahren achten
Bei Verbänden, Interessenvertretungen auf Unterstützung und Zertifizierung hinwirken

FAZIT

IT-Systeme müssen zahlreichen und vielfältigen Sicherheitsherausforderungen gerecht werden. Dabei gehören die Risiken, die aus Angriffen auf kryptografische Komponenten aufgrund von technologischem Fortschritt und QuantenComputing resultieren, zu einer besonderen Ordnung. Eine Schwachstelle, die lediglich ein einziges Produkt oder einen einzelnen Dienst betrifft, ist in ihrer Wirkung begrenzt. Wird hingegen ein kryptografisches Verfahren geknackt, kann eine Vielzahl an Anwendungen unsicher und potenziell das grundsätzliche Vertrauen erschüttert werden, das die Menschen in weite Teile des Internets und seiner Angebote haben.

Sogar schwere Schwachstellen, die eine riesige Menge an verschiedenen Systemen betreffen, können mit Software-Updates oder Hardware-Upgrades behoben werden. Wenn aber ein kryptografischer Algorithmus einmal geknackt ist, dann sind alle mit diesem Algorithmus verschlüsselten Daten sofort und unumkehrbar offengelegt und unbefugten Zugriffen zugänglich. Quantencomputer und andere Entwicklungen mit ähnlich fataler Wirkung auf Kryptografie können daher weiten Teilen unserer Wirtschaft schweren Schaden zufügen und das Funktionieren der Gesellschaft in besonderer Weise gefährden. Die Umstellung auf Krypto-Agilität und Next-Generation-Kryptografie braucht viel Zeit und Vorbereitung und kann nur erfolgreich sein, wenn kryptografische Alternativen verfügbar sind und deren Entwicklung breit gefördert und unterstützt wird.

Auch mittelständische Unternehmen müssen sich dieses Risikos bewusst sein und sich auf die Entwicklung vorbereiten. Auf die Nutzung kryptografischer Verfahren angesichts dieser Unsicherheit zu verzichten, wäre aber eine falsche Entscheidung. Nach wie vor bietet die Kryptografie wirkungsvolle Instrumente zur Sicherung der betrieblichen Informationen. Unternehmer müssen sich jedoch über die aktuelle Wirksamkeit der von ihnen eingesetzten Lösungen informieren, sie müssen dokumentieren, welche ihrer Anwendungen welche Verfahren nutzen und vor allem müssen sie bei ihren IT-Lieferanten aktuelle und flexible Komponenten nachfragen und sich entsprechende Mechanismen vertraglich zusichern lassen.

Darüber hinaus sollten die Unternehmen bei ihren Verbänden auf die Erosion kryptografischer Verfahren und die Bedrohungen durch Quantencomputer und ähnlicher Verfahren hinweisen und geeignete Maßnahmen fordern. So können sie ihrem Bedarf an offenen Katalogen und zertifizierten Lösungen Ausdruck verleihen und die Bereitstellung entsprechender Verfahren beschleunigen.

ABKÜRZUNGSVERZEICHNIS

3DES Triple Digital Encryption Standard
AES Advanced Encryption Standard
API Application Programming Interface
BSI Bundesamt für Sicherheit in der Informationstechnik
DES Digital Encryption Standard
DH Diffie-Hellman
ECC Elliptic Curve Cryptography
ECDH Elliptic Curve Diffie-Hellman
ECDSA Elliptic Curve Digital Signature Algorithm
IDEA International Data Encryption Algorithm
IETF Internet Engineering Taskforce
IT Informationstechnik
KEM Key-Encapsulation Mechanism
KMU Kleine und mittlere Unternehmen
MD5 Message-Digest Algorithm 5
MIT Massachusetts Institute of Technology
NIST National Institute of Standards and Technology
NSA National Security Agency
OEM Original Equipment Manufacturer
RC5 Rivest Cipher 5
RSA Rivest, Shamir, Adleman
SHA Secure Hash Algorithm
SSL Secure Socket Layer
TLS Transport Layer Security
USB Universal Serial Bus
VPN Virtual Private Network
XMSS Extended Merkle Signature Scheme

IMPRESSUM

Diese Broschüre basiert auf der Dokumentation des Eberbacher Gesprächs zu „Next Generation Crypto“ vom Januar 2018

Herausgeber
Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung (HMWEVL)
Kaiser-Friedrich-Ring 75
65185 Wiesbaden
www.wirtschaft.hessen.de

Projektträger
Hessen Trade & Invest GmbH
Konradinerallee 9
65189 Wiesbaden

Christian Flory
Themenfeldleiter Informationstechnologien
Telefon 0611 95017-8423
christian.flory@htai.de

Redaktion
Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Landesentwicklung (HMWEVL)
Dr. Marei Waidmann

Hessen Trade & Invest GmbH
Christian Flory

Autoren
Dr. Michael Kreutzer, Dr. Ruben Niederhagen, Prof. Dr. Michael Waidner, Reiner Kraft, Mechthild Stöwer

Fraunhofer SIT
Marketing und PR
Rheinstraße 75
64295 Darmstadt

redaktion@sit.fraunhofer.de

Gestaltung
Theißen-Design, www.theissen-design.de

Druck
www.printworld.com

Klimaneutraler Druck

Klimaneutral Druckprodukt
ClimatePartner.com/12755-1811-1100

Bildnachweis
fotolia.com: Oleksii (Cover + S.14)
RS-Studios (S.6 + S.7)

Freepik.com und Fraunhofer SIT (S.14)
Weitere Grafiken und Icons: Fraunhofer SIT

Oktober 2018, 1. Auflage

Ausschluss Wahlwerbung

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Hessischen Landesregierung herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Landtags-, Bundestags- und Kommunalwahlen.

Missbräuchlich ist insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen und Werbemittel.

Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die Druckschrift nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte. Die genannten Beschränkungen gelten unabhängig davon, wann, auf welchem Weg und in welcher Anzahl diese Druckschrift dem Empfänger zu gegangen ist.

Den Parteien ist es jedoch gestattet, die Druckschrift zur Unterrichtung ihrer eigenen Mitglieder zu verwenden.

Verzicht auf Geschlechterdifferenzierung

Aus Gründen der leichteren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung von Funktions- bzw. personenbezogenen Bezeichnungen, wie zum Beispiel Teilnehmer / Innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung für beide Geschlechter.

HESSEN
Hessisches Ministerium für
Wirtschaft, Energie, Verkehr
und Landesentwicklung

Projektträger
HESSEN
TRADE & INVEST
Wirtschaftsförderer für Hessen