Die quantensichere Ende-zu-Ende-Verschlüsselung wird Stand der Technik – auch für elektronische Rechnungen. Nutzerinnen Freier Software könnenen dazu „direkt einen Mehrwert für die Allgemeinheit generieren.“

Von Joachim Jakobs

Die Digitalisierung geht mit Risiken und Rechtsfolgen einher – die E-Rechnung zeigt das wie unter einem Brennglas: „Eine E-Rechnung stellt Rechnungsinhalte [...] in einem strukturierten, maschinenlesbaren XML-Datensatz dar. Dies gewährleistet, dass Informationen, die in dieser Form vom Rechnungssteller ausgestellt werden, elektronisch übermittelt und empfangen, sowie medienbruchfrei und automatisiert weiterverarbeitet und zur Auszahlung gebracht werden können.“

Ohne Zettelwirschaft hofft der Deutsche Industrie- und Handelkammertag. dass die elektronische Segnung „langfristig für mehr Effizienz" sorgt. Seit 1. Januar 2025 ist sie unter Firmen „obligatorisch“. Soweit so gut. Wenige Monate später die Ernüchterung: „Hacker fälschen Rechnungen und kassieren 100.000 Euro“. Gut möglich, dass die Gläubigerin auf dem Schaden sitzen bleibt; unter Berufung auf ein Urteil des Oberlandesgerichts (OLG) Schleswig-Holstein teilt der Bitkom mit: „Ende-zu-Ende-Verschlüsselung für E-Mail-Rechnungen erforderlich“

Die elektronische Rechnung ist logische Konsequenz der hypervernetzten Welt:
„Der Übergang von traditionellen Papierrechnungen zu hochentwickelten digitalen Rechnungen stellt einen gewaltigen Sprung in der Finanzverwaltung dar. Diese Veränderung wird durch den unbestreitbaren Bedarf an mehr Effizienz, Genauigkeit und Flexibilität in einer hypervernetzten Weltwirtschaft vorangetrieben.“

Bild: Pixabay, Lizenz: Pixabay License

Ein Chinesischer Elektronikanbieter zur Vernetzung (industrieller) Dinge jubelt: „Die Welt ist in eine neue Ära der Hyperkonnektivität eingetreten, in der ein zuverlässiger Hochgeschwindigkeits-Internetzugang kein Luxus mehr, sondern eine Notwendigkeit ist. 5G-Pocket-WiFi-Router haben sich als die ultimative Lösung für Profis, Reisende und digitale Nomaden herausgestellt, die überall glasfaserähnliche Geschwindigkeiten verlangen.“

Damit sollen gar „Super-Edge-Computing-Funktionen, integrierte Datenerfassung, -verarbeitung, -ausführung, Echtzeitanalyse, sicher und effizient“ für „5G-Industrierouter“ möglich sein.

Die IoT-Spezialistin melita.io -- eine Beteiligung der Großbank Goldman Sachs – bestätigt „Mit dieser hohen Geschwindigkeit werden Nutzer und Geräte die Möglichkeit haben, in Echtzeit auf Dateien, Programme und Remote-Anwendungen zuzugreifen, Cloud-Dienste effizienter zu nutzen und weniger auf internen Speichermedien und das Horten von lokalen Daten angewiesen zu sein.“

Und liefert Praxisbeispiele für die „Intelligente“ „Stadt“, „Industrie“, „Mobilität“, „Landwirtschaft“ und „Gesundheitsfürsorge“.

Das schafft Echtzeit-Transparenz – Nicolaos Debowiak, Chef bei Forterro, schwärmt:
„Durch diese umfassende Transparenz und Vernetzung erhalten die Verantwortlichen – vom Produktionsmitarbeiter bis zur Geschäftsführung – einen Echtzeitüberblick über die tatsächliche Situation in der Fertigung. Sie sehen jederzeit, welcher Auftrag auf welcher Maschine läuft, wie viele Teile bereits produziert wurden und ob Planungsfehler oder Überkapazitäten vorliegen.

Abweichungen zwischen geplanten und tatsächlichen Produktionszeiten, etwa durch ungeplante Stillstände oder Materialengpässe, werden in Echtzeit erkannt. Das System kann automatisch Alarmmeldungen generieren oder Maschinenzustände, zum Beispiel Produktion, Störungen und Wartungen, durch ein Ampelsystem visualisieren. So werden die Entscheidungsträger umgehend informiert und können zeitnah Gegenmaßnahmen einleiten.“

Richtig spannend wird das, wenn das industrielle Internet mit Quantencomputern und Maschinellem Lernen – dem „Quanten-Machine-Learning“ (QML) kombiniert wird – etwa in der Materialwissenschaft: „Es könnte dazu beitragen, neue Materialien mit bestimmten Eigenschaften zu entwickeln, indem es die Struktur und das Verhalten von Atomen und Molekülen simuliert. Dies könnte zu Fortschritten in Bereichen wie der Energiespeicherung, der Elektronik und der Luft- und Raumfahrt führen.“

Es stellt sich jedoch die Frage, welchem Verantwortlichen in Produktion und Geschäftsführung Zugriff auf welche Daten zu gewähren sind – je mehr Menschen Zugriff haben, desto größer das Risiko – es könnte ja sein, dass auch Kriminelle innovative Technik nutzen?!

„Insbesondere komplexe Angriffe wie quantenunterstütztes Phishing oder das Knacken biometrischer Daten könnten die quantenbasierte Mustererkennung in bisher ungekanntem Ausmaß ausnutzen. Diese Fähigkeiten stellen eine direkte Bedrohung für Authentifizierungsmechanismen, Zugriffskontrollen und das Vertrauen der Nutzer dar.“

Hat die Angreiferin einmal die fortschrittlichen Zungangskontrollen überwunden, hat sie gewaltige Möglichkeiten: „*Die Einflussmöglichkeiten des Angreifers* umfassen alle externen Größen, die auf den Lernprozess einwirken und so potenziell eine Einflussnahme gestatten. Bei einem Angriff auf Trainingsgrundlagen (Causative Attack) hat der Angreifer die Möglichkeit, die Menge der Trainingsdaten zu verändern. Da die Daten die Güte des Modells bedingen, kann das Lernergebnis auf diese Weise stark beeinflusst werden, auch wenn vielleicht nur ein kleiner Teil der Trainingsdaten verändert oder hinzugefügt wird. Das ist insbesondere bei extremen Inputdaten der Fall.“

So droht eine „Vergiftung der Lieferkette“, „bei der böswillige Akteure Beschaffungsunterlagen manipulieren oder Materialspezifikationen ändern und so versteckte Schwachstellen schaffen, die den Produktionsprozess erheblich stören können. Noch alarmierender ist, dass Lieferanten 3D-Drucker oder Software mit eingebettetem bösartigen Code liefern können, wodurch Angreifer die Möglichkeit erhalten, den Druckprozess zu manipulieren oder sogar die vollständige Kontrolle über das System zu übernehmen und damit die gesamte Produktionskette zu gefährden. Diese Sicherheitsverletzungen gefährden nicht nur die Produktqualität, sondern können auch katastrophale Folgen für die Sicherheit, Zuverlässigkeit und Betriebseffizienz haben.“

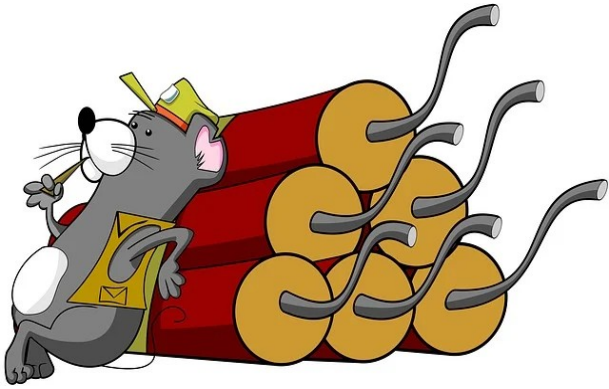

Bild: Pixabay, Lizenz: Pixabay License

Bereits 1982 – lange bevor Liese und Otto Normalverbraucher von der Vernetzung von Dingen schwafelten – hat die damalige Sowjetunion erfahren, wie wichtig korrekte Daten sind – und die Software, die diese verarbeitet; die USA stellten fest, wie eifrig Moskaus Schlapphüte US-Technik kopierten, um so Entwicklungskosten bei der Gasförderung zu sparen; in einer raffinierten Operation wurde den Sowjetischen Spionen manipulierte Technik untergeschoben: „Um die sowjetische Gasversorgung, ihre Deviseneinnahmen aus dem Westen und die interne russische Wirtschaft zu stören, wurde die Pipeline-Software, die die Pumpen, Turbinen und Ventile steuern

sollte, so programmiert, dass sie nach einer angemessenen Zeitspanne verrückt spielte und die Pumpendrehzahlen und Ventileinstellungen zurücksetzte, um Drücke zu erzeugen, die weit über den für Pipeline-Verbindungen und Schweißnähte akzeptablen Werten lagen“. Das Ergebnis soll eine „Explosion mit einer Sprengkraft von 3 Kilotonnen irgendwo in Sibirien“ gewesen sein. Nach Angaben von Wikipedia sollen dabei „keine Toten“ zu beklagen gewesen sein. Sollte ein solches Ereignis nicht im einsamen Sibirien, sondern in einer Großstadt geschehen, könnte das anders aussehen.

1982! Vor einem halben Jahrhundert war ein Heer von Spezialisten notwendig, um eine gewaltige Explosion auszulösen. Mit der Digitalisierung, der breitbandigen Vernetzung (industrieller) Dinge per Glasfaser, 5G und ihrer Steuerung per KI/ML-Quantencomputern könnte sich das ändern:

So hat das Sicherheitsunternehmen Waterfall Security Solutions im Jahr 2022 insgesamt 218 Vorfällen festgestellt. 57 davon sollen industrielle Systeme betroffen haben, „die physische Folgen in der realen Welt hatten“.

Im folgenden Jahr „stieg die Zahl der Cyberangriffe um 140 Prozent, wobei über 150 Industriebetriebe betroffen waren. Nach Prognosen des Unternehmens könnten bei einer Fortsetzung dieses Wachstumstrends innerhalb der nächsten fünf Jahre bis zu 15.000 Industrieanlagen aufgrund von Cyberangriffen stillgelegt werden. Es wurde außerdem hinzugefügt, dass es sich bei den meisten dieser Angriffe um Ransomware-Angriffe handelte, bei denen Computer und Daten in IT-Netzwerken verschlüsselt wurden, die jedoch auch Auswirkungen auf die OT (Operational Technology) hatten.“

Diese Angriffe lassen sich mit KI aufmotzen:
„So ermöglichen KI-Tools Hackern beispielsweise, schnell öffentlich zugängliche Informationen über Führungskräfte und Mitarbeiter der Zielorganisation zu sammeln. Anhand der Ergebnisse können sie dann eine spezifische, personalisierte Phishing-E-Mail erstellen, um ihr Ziel dazu zu bringen, auf den bösartigen Link zu klicken und einen Cyberangriff auszulösen.“

Nicht nur das: „Seit Ende Juli 2025 sieht sich die Cybersicherheits-Community mit einer neuen, noch heimtückischeren Entwicklung von Ransomware konfrontiert: Polymorphic Ransomware 2.0. Dabei handelt es sich nicht nur um ein Update, sondern um einen bedeutenden Sprung in der Komplexität, der sich fortschrittliche KI und maschinelles Lernen zunutze macht, um zu einer wirklich adaptiven und schwer fassbaren Bedrohung zu werden. Für Unternehmen, Privatpersonen und sogar kritische Infrastrukturen ist es von entscheidender Bedeutung, diese neue Generation von Ransomware zu verstehen, um wirksame Abwehrmaßnahmen zu entwickeln.“

Bild: Pixabay, Lizenz: Pixabay License

Quanten-Erpressungstrojaner sollen dagegen mit aussergewöhnlicher Geschwindigkeit beeindrucken: „Opfer haben in der Regel nur wenige Stunden zwischen der anfänglichen Infektion und der Verschlüsselung ihrer Dateien.“

Und dann wollen KI und Quantencomputer auch noch heiraten – zusammen ergibt das einen „Sicherheitsalptraum“: „Sobald die

Quantentechnologie ausgereift ist, werden Angreifer autonome KI schnell nutzen, um entschlüsselte sensible Daten mit Maschinengeschwindigkeit auszunutzen – was zu weit verbreitetem Identitätsdiebstahl, raffiniertem Spear-Phishing, dem Sammeln von Anmeldedaten und der automatisierten Ausnutzung von Infrastrukturen führen wird. Sicherheitsforscher, Geheimdienstmitarbeiter und KI-Bedrohungsmodellierer sind sich einig, dass die Frage nicht lautet, ob der Q-Day kommen wird, sondern wann.“

Carsten Stöcker Geschäftsführer der Dortmunder Spherity GmbH rät: „Defensive Maßnahmen, darunter Post-Quantum-Kryptografie (PQC), Zero-Trust-Architekturen und KI-gestützte Cyberabwehrstrategien, müssen dringend umgesetzt werden, um dieser neuen Bedrohung entgegenzuwirken.“ Zur Null-Vertrauensstrategie gehören neben quantensicherer E2EE quantensicheres FIDO2/MFA, IAM und SIEM.

Klingt für mich wie „Regelkonformität 4.0“ – Ich vermute, dass dieses Schutzniveau dem „Stand der Technik“ entspricht – das Justizministerium definiert die Vokabel so: „Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein." Die Verantwortliche haftet für dessen Nachweis. Nachzuweisen ist auch die Schulung derer, die im Auftrag der Verantwortlichen tätig sind. Soweit zum SOLL.

Derweil dauert das IST an – im Juli 2025 beklagt der TÜV-Verband einmal mehr: „Offene WLANs, schwache Passwörter oder gestohlene Geräte“. Gleichzeitig soll auch noch die Software veraltet und die Hosting-Umgebung unsicher sein.

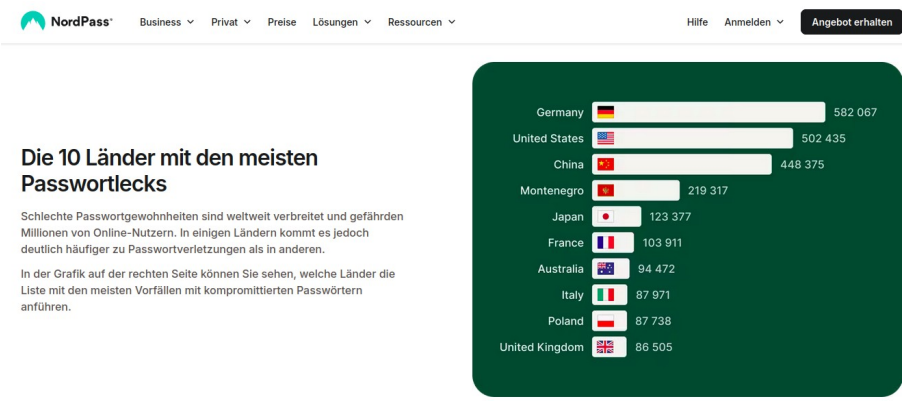

Bild: Nordpass

Kein Wunder, dass Deutschland dreimal so viel Passwort-Verluste zu beklagen haben soll wie Frankreich und Italien – zusammen! Das jedoch ändert nix am Selbstvertrauen der Verantwortlichen: „Neun von zehn Unternehmen bewertet eigene Cybersicherheit als gut“, meldet der TÜV-Verband. Die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI) hält das für ein „Wunschdenken“ – und meint, die meisten Firmen hätten „noch nicht einmal Seepferdchen, um sicher an den Beckenrand zu kommen.“

Wer nicht schwimmen kann, muss damit rechnen, unterzugehen:
Für das Jahr 2020 hat dsgvo-portal.de 23 Deutsche Datenpannen erfasst. Im Jahr 2024 waren es 308. In den ersten sieben Monaten 2025 sind die Firmen Fasana, Kreisel, Eu-Rec, Scoop Aalen und die Einhaus Gruppe wegen solcher Pannen insolvent gegangen. Nicht einmal Konzerne sind vor Cyber-Insolvenzen gefeit: „23andMe: Einst 5,8 Mrd. Dollar wert, jetzt um nur 256 Mio. Dollar verkauft“ hieß es im Mai 2025.

Interessant ist: Zum Pleitegehen sind nicht zwingend Geldbußen der Aufsichtsbehörden noch Schadenersatzforderungen seitens der Kundinnen erforderlich. Die könnten aber noch obendrauf

kommen; zuletzt hatte der Europäische Gerichtshof im Februar 2025 bestätigt, dass Geldbußen nach Datenschutzgrundverordnung (DSGVO) „wirksam und abschreckend“ zu sein hätten.

Ein Viertel Jahr später kassierte Vodafone eine Geldbuße in Höhe von 45 Millionen Euro, weil die Aufsichtsbehörde Mängel bei der Authentifizierung und der Überwachung der Dienstleisterinnen festgestellt haben will.

Bild: n-tv.de

Mit Peanuts wollen sich die Verbraucheranwälte nicht herumschlagen: „Meta unter Druck: Bis zu 10.000 Euro DSGVO-Schadensersatz wegen Meta Pixel möglich“, titelt die Dr. Stoll & Sauer Rechtsanwaltsgesellschaft mbH. Und hofft auf ein dickes Geschäft: „Betroffen sind Millionen Internetnutzer“. Ach?! Sie sind aber kein internationaler Konzern, sondern nur ein Mittelständler mit ein paar Hundert Mitarbeiterinnen? Gut – Mittelständlerinnen müssen nur halb so viel Schadenersatz wie Meta zahlen.

Die Digitalisierung geht mit Risiken und Rechtsfolgen einher – die Risiken steigen einmal mit der Anzahl der vernetzten Geräte: "Je mehr vernetzte Geräte in den unterschiedlichsten Branchen zum Einsatz kommen, desto mehr Sicherheitslücken tun sich auf. Laut Statista sind 2025 bereits über 19,8 Milliarden IoT-Geräte online. Prognosen zufolge wird diese Zahl bis 2030 auf über 29 Milliarden steigen. Damit wächst die potenzielle Angriffsfläche rasant.
Und je mehr Verantwortung diese Geräte übernehmen, desto höher sind die Risiken. So steuern industrielle Router heute ganze Produktionslinien. Vernetzte Sensoren überwachen Infrastrukturen. Intelligente Kameras sichern öffentliche Räume. Ein Sicherheitsverstoß bedeutet hier also nicht nur ein Datenschutzproblem, sondern kann auch Produktionsausfälle, Risiken für die öffentliche Sicherheit oder Compliance-Verstöße nach sich ziehen."

Hinzu kommt die Geschwindigkeit, mit der die Geräte angeschlossen werden: "5G ermöglicht komplexere Angriffsvektoren. Angreifer können die höhere Geschwindigkeit und geringere Latenz ausnutzen, um schnellere und komplexere Angriffe durchzuführen. Distributed-Denial-of-Service-Angriffe (DDoS) können beispielsweise aufgrund der erhöhten Durchsatzkapazitäten an Wirksamkeit gewinnen."

Daher sind angemessene Maßnahmen erforderlich, um die Bedrohung zu begrenzen:
„KI automatisiert bereits Compliance-Aufgaben und analysiert komplexe Datensätze, wodurch traditionelle Rollen in den Bereichen Cybersicherheit und Compliance neu definiert werden. In Kombination mit der Leistungsfähigkeit des Quantencomputings kann KI Echtzeit-Compliance-Architekturen, Notfallwiederherstellungspläne, optimale Konfigurationen von Sicherheitstools, fortschrittliche Bedrohungserkennung und intelligenteres Risikomanagement liefern und damit die Möglichkeiten der Cybersicherheit neu definieren.“

Der Nachweis der Regelkonformität gelingt leichter, wenn die Verantwortliche Zugang zum Quellcode hat:
„Die Transparenz von Open-Source-Software ist einer ihrer größten Vorteile in Bezug auf die Einhaltung gesetzlicher Vorschriften. Da der Quellcode für alle zugänglich ist, lässt sich leichter sicherstellen, dass die Software ohne versteckte Funktionen den Compliance-Standards entspricht. Diese Transparenz fördert das Vertrauen, eine entscheidende Komponente im regulatorischen Kontext, insbesondere beim Umgang mit sensiblen oder kritischen Daten. Darüber hinaus erhöht der gemeinschaftliche Charakter von Open-Source-Projekten die Zuverlässigkeit und Sicherheit der Software, da eine große Entwicklergemeinschaft den Code kontinuierlich testet, verfeinert und validiert."

Das bedeutet: „Sicherheit hat oberste Priorität […] Da Quantencomputer bald Realität werden, kann die Bedeutung von Open Source gar nicht hoch genug eingeschätzt werden. Die Transparenz, die Sicherheit durch die Kontrolle durch die Community und die Flexibilität, die Open-Source-Software auszeichnen, machen sie zur idealen Wahl für die Entwicklung von Kommunikationsdiensten mit maximaler Sicherheit und Post-Quanten-Verschlüsselung."

Vor einem Jahr gab Apple „die bedeutendste Verbesserung der kryptografischen Sicherheit in der Geschichte von iMessage bekannt: die Einführung von PQ3, einem bahnbrechenden Post-Quanten-Kryptografieprotokoll, das den Stand der Technik im Bereich der sicheren End-to-End-Kommunikation weiter vorantreibt."

Genauso geht „ein Aufruf zum Handeln" an die KMU:
„Es ist jetzt Zeit zu handeln. Auch wenn es noch Jahre dauern kann, bis Quantencomputer in der Lage sind, Verschlüsselungen zu knacken, müssen die Grundlagen für quantensichere Sicherheit schon heute gelegt werden. KMU, die frühzeitig auf PQC setzen, schützen sich nicht nur selbst, sondern verschaffen sich auch einen Wettbewerbsvorteil in einem zunehmend digitalen und sicherheitsbewussten Markt."

Bild: ChatGPT

Um das zu erreichen, ist Schulung auf allen Ebenen wichtig: „Entwickler und IT-Teams müssen die Unterschiede zwischen PQC-Algorithmen verstehen und wissen, wie diese korrekt implementiert werden. Der Missbrauch eines Algorithmus (unabhängig davon, ob er quantenresistent ist oder nicht) kann E2EE untergraben. Darüber hinaus werden eine robuste Schlüsselverwaltung und -speicherung noch wichtiger, wenn neue Algorithmen größere Schlüssel oder eine zustandsbehaftete Verwaltung erfordern (wie bei hashbasierten Signaturen)."

Und was hat das mit Freier Software zu tun?
Stefan-Lukas Gazdag, Kryptoforscher bei genua ist der Ansicht:

„Die Migration auf Post-Quanten-Kryptographie ist nicht nur eine rein technologische Herausforderung, sondern auch eine organisatorische. Behörden,

Standardisierungsgremien, Universitäten, Hersteller und auch Anwender weltweit müssen nicht nur gemeinsam Lösungen erarbeiten, damit diese eine Chance auf praktische Nutzung haben, sondern diese Lösungen müssen auch tatsächlich in die Praxis gelangen. Bei der ganzheitlichen Untersuchung und Bearbeitung einer Thematik sind insbesondere Abhängigkeiten durch proprietäre Lösungen schwierig, da man auf die entsprechenden Hersteller und ihre zeitnahe Kooperation angewiesen ist. Umso praktischer ist es wie im CI/CD-Kontext, wenn wichtige Systeme als Open-Source vorliegen. So können direkt potentielle Lösungen eingearbeitet und ausgetestet werden. Sollten sich Lösungen mit der Zeit als sicher und praxistauglich erweisen, können diese den Open-Source-Projekten angeboten werden, um direkt einen Mehrwert für die Allgemeinheit zu generieren.“