E-BOOK

WENN SIE VERTRAUEN BRAUCHEN, BRAUCHEN SIE PKI

digicert®

INHALTSVERZEICHNIS

VON DEN GLETSCHERN ALASKAS BIS INS ALL

An einem regnerischen Tag im Sommer 2013 kam ein kleines Wasserflugzeug im Tiefflug über den Bergen nahe Petersburg, Alaska ins Trudeln. An Bord saßen sechs Passagiere auf Sightseeing-Tour zum LeConte-Gletscher. Der Pilot hatte sich im Steigflug durch den Pass bei Horn Cliffs verschätzt und die Kontrolle über das Flugzeug verloren. Es krachte mit der Nase nach vorn durch die dichte Bewaldung und stürzte ab.

Die verletzten Überlebenden konnten die Unfallstelle auf einem steilen Abhang aus eigener Kraft nicht verlassen. In wenigen Stunden würde es Nacht werden, was in Alaska auch im Juni Minusgrade bedeutet. Sie waren in unwegsamem Gelände gestrandet und hatten keinen Mobilfunkempfang. Rettung war nur aus der Luft möglich.

In 800 Kilometern Höhe empfing eine Konstellation aus Iridium-Satelliten das Notsignal des Flugzeugs und leitete es mitsamt der Position an die Rettungsdienste weiter. Das bordeigene Iridium-Gerät hatte die Bewegungen des Flugzeugs vom Start bis zum Crash aufgezeichnet und eine digitale Echtzeit-Spur des gesamten Flugs erstellt. Diese Funktionalität geht über das hinaus, was GPS und Funknotsignale leisten. Dies wird durch die sorgfältig koordinierten Erdumlaufbahnen jedes einzelnen der 66 Iridium-Satelliten ermöglicht, die mit den Bodenstationen und untereinander kommunizieren und so rund um die Uhr die gesamte Erdoberfläche lückenlos abdecken. Im Netzwerk der Iridium-Konstellation ist ein funktionsfähiges Gerät überall auf der Welt jederzeit verfolgbar – von der Antarktis bis zum Nordpol.

Nicht alle Flugzeuge verfügen standardmäßig über diese Art von Tracker- und Notsignalgerät. Immer mehr Piloten und Eigentümer – insbesondere von kleinen Fliegern oder auf abgelegeneren Routen – haben es aber inzwischen installiert. Für die meisten ist diese Sicherheit einfach ein beruhigendes Gefühl, aber in manchen Fällen bedeutete sie schon die Entscheidung über Leben und Tod.

Die US-Küstenwache kannte den genauen Absturzort und konnte die Überlebenden innerhalb weniger Stunden per Helikopter in ein Krankenhaus bringen. Nach der erfolgreichen Rettung stand der Sprecher der Küstenwache, Grant DeVuyst, dem Sender Alaska Public Media[1] für ein Interview zur

[1] https://www.alaskapublic.org/2013/06/05/one-dead-six-survive-float-plane-crash-near-petersburg/

Verfügung. Zum Thema des Notsignalgeräts sagte er: „Das war der einzige Grund, weshalb wir von dem Unfall wussten und der einzige Grund, dass wir die Absturzstelle und die Überlebenden finden konnten."

In solchen seltenen, lebensbedrohlichen Notfällen muss sich der Pilot darauf verlassen können, dass das Iridium-Satellitennetzwerk den Flug verfolgt, das Notsignal auffängt und es an ein Rettungsteam weiterleitet. Das Signal muss störungssicher sein, die Identität des Notfallgeräts muss gesichert sein und das Netzwerk muss vor Unterbrechung geschützt sein. Wenn auch nur ein Teil der Iridium-Konstellation gestört ist, stehen Leben auf dem Spiel. Es handelt sich um eine sehr hohe Vertrauensstufe, auf der es keinen einzigen Fehler geben darf. Deshalb ist die Iridium-Satellitenkonstellation mittels PKI gesichert.

„PKI SICHERT VERTRAUENSWÜRDIG ALLES VOM MEERESGRUND BIS HOCH INS ALL."

Brian Trzupek
Senior Vice President for Product, DigiCert

KAPITEL 1

VERTRAUEN IST EIN DYNAMISCHES BEDÜRFNIS

Als die britischen Kryptologen James Ellis und Clifford Cocks in den 70er-Jahren die Idee der asymmetrischen Verschlüsselung entwickelten, hatten sie noch keine Vorstellung von deren zukünftigen, millionenfachen Einsatz in Websites auf der ganzen Welt. Damals war das Internet noch ein Projekt der US-Behörde DARPA und wurde gelegentlich von Wissenschaftlern zum Austausch von Daten und Forschungsergebnissen zwischen Universitäten eingesetzt.

Innerhalb weniger Jahrzehnte hat sich die Public Key Infrastructure nach Ellis und Cocks zu einem der wichtigsten Instrumente des Informationszeitalters im Kampf gegen Hacker und Betrüger entwickelt. Heute gilt eine Website dann als vertrauenswürdig, wenn sie durch PKI gesichert ist.

Aber bald nach der Erfindung des World Wide Web – das für sich alleine schon eine neue Ära der menschlichen Entwicklung einläutete –, kam es zu einer zweiten Revolution bei den vernetzten Geräten. Praktisch über Nacht wurde alles vom Kühlschrank bis zur Banking-App Teil eines Ökosystems von Netzwerken, Geräten, Anwendungen und Benutzern, die weltweit kommunizieren.

Diese Entwicklung verläuft bis heute so rasant, dass sie sich nur in Größenordnungen messen lässt. Weil hunderttausende Entwickler neue Ideen für die Verbindung von Millionen Menschen mit Milliarden Geräten auf den Markt werfen, steigt auch der Sicherheitsbedarf weiter exponentiell an.

Den vielen Vorteilen des Informationszeitalters – vom kulturellen Austausch bis zu den Fortschritten in der medizinischen Versorgung – steht die Attraktivität dieses riesigen Kommunikationsnetzwerks für Bauernfänger und Kriminelle gegenüber, die unsere Benutzer und deren Vertrauen in die Technologie für Ihre Zwecke ausnutzen.

Die Lösung dieses Bedrohungsproblems ist einfach. Man muss die höchstmögliche Sicherheit bereits in alle verbundenen Elemente integrieren. Public Key Infrastructure ist diese integrierte Sicherheit. Eine Sicherheits- und Identifizierungslösung, die zuverlässig genug ist, um selbst die sensibelsten Daten zu schützen, aber flexibel genug, um sich auch den neuesten und innovativsten Erfindungen anzupassen. Mit PKI können wir uns ganz auf die Vorteile einer fast verzögerungsfreien Kommunikation rund um den Globus – und sogar bis ins All – konzentrieren.

PUBLIC KEY INFRASTRUCTURE IST DIESE INTEGRIERTE SICHERHEIT.

Eine immer vielfältigere Bedrohungslandschaft

Jeden Tag gibt es neue, geniale Ideen zur Nutzung von Datenverbindungen für mehr Übersicht, Effizienz und Sicherheit in Computern, Apps und Geräten. Aber jede neue Verbindung ist auch eine potenzielle Sicherheitslücke, also ein Eingangstor in das Netzwerk, mit dem die App oder das Gerät kommuniziert.

Die finanziellen Risiken sind bekannt. Seit Jahren können wir beobachten, was passiert, wenn Cyberkriminelle Sicherheitslücken ausnutzen. 2017 zahlte ein großer Verbraucher-Finanzdienstleister nach einem Rechtsstreit wegen eines erheblichen Datenlecks 700 Millionen USD an Schadenersatz[2]. Eine 2019 durchgeführte Studie von Ponemon/IBM ergab, dass pro Datenleck durchschnittliche Kosten von knapp 4 Millionen USD entstehen[3]. Im selben Jahr bezifferte der Consumer Breach Report von ForgeRock[4] den diesbezüglichen Gesamtverlust im Gesundheitswesen auf 17,76 Milliarden USD. Tatsächlich war der Gesundheitssektor im Jahr 2019 mit 45 Prozent aller Fälle das beliebteste Ziel für Datendiebe.

Fast noch erschreckender als die enormen Kosten an sich ist auch die Anzahl und Art der Angriffe im Gesundheitswesen.

[2] https://investor.equifax.com/news-and-events/press-releases/2019/07-22-2019-125543228 [3] https://digitalguardian.com/blog/whats-cost-data-breach-2019 [4] https://healthitsecurity.com/news/health-sector-most-targeted-by-hackers-breach-costs-rise-to-17.76b

Die Verluste verteilten sich auf 382 einzelne Datenlecks, die durch Angriffe auf medizinische Netzwerke mit den verschiedensten Methoden entstanden sind. Während bisher in Netzwerke und Websites, vor allem bei Banken und Verbrauchertransaktionen, eingedrungen wurde, nutzen Cyberkriminelle inzwischen vermehrt Schwachstellen in Geräten sowie schlecht informierte Benutzer aus, um die reinen Daten zu stehlen.

Für Unternehmen bedeutet dies, dass sie sich vermehrt um die Sicherheit kümmern müssen, obwohl sie personell im Grunde nur schlecht dafür ausgestattet sind. Digitale Patientenakten, Online-Patientenüberwachung und intelligente Therapiegeräte revolutionieren die Patientenversorgung, aber die medizinischen Mitarbeiter sind keine Fachleute für Cybersicherheit, und die IT-Abteilungen müssen trotz Budgetkürzungen mit immer neuen Technologien sowie Gesetzen und Verordnungen arbeiten.

Es sind interessante und vielversprechende Zeiten für die Informationstechnik, und vom Endverbraucher bis hin zu multinationalen Konzernen und Regierungen sollen alle vom technologischen Fortschritt durch vernetzte Geräte profitieren können. Für die IT-Fachleute im Hintergrund ist es jedoch eine gewaltige Aufgabe, die neuen Bedrohungen zu überblicken und handhabbare Lösungen bereitzustellen, um die Risiken zu minimieren.

Im Kampf gegen wachsende Bedrohungen brauchen Sicherheitsexperten eine flexible Lösung, die sich rasch bereitstellen und einfach verwalten lässt und auch angesichts von Anpassungen an die sich wandelnden Bedürfnisse des Unternehmens jedem Angriff die Stirn bieten kann. PKI erfüllt alle diese Erfordernisse und mehr.

Im Kampf gegen wachsende Bedrohungen brauchen Sicherheitsexperten eine flexible Lösung, die sich rasch bereitstellen und einfach verwalten lässt und jedem Angriff die Stirn bieten kann.

FALLSTUDIE – FLORENCE, ALABAMA

Der Hecht im Karpfenteich

Im Juli 2019 ging die Nachricht von einem enormen Datenleck bei einer Bank um die Welt, das 100 Millionen Kunden betraf[5]. Ein weiteres Beispiel für einen enormen, grenzübergreifenden Datendiebstahl.

Noch während dieser Diebstahl stattfand, tasteten Cyberkriminelle bereits fleißig kleinere Ziele auf Schwachstellen ab und suchten nach unzureichenden Sicherheitsmaßnahmen. Vermehrt finden sich solche Schwachstellen bei kleineren Behörden, deren begrenzte Ressourcen es ihnen erschweren, alle Systeme und Benutzer zu schützen.

Also meiden Hacker inzwischen eher die gut gerüsteten Konzerne und schleusen stattdessen lieber Ransomware in die Netzwerke von kleineren Städten und Behörden ein, wo sie Lösegeldforderungen stellen wollen.

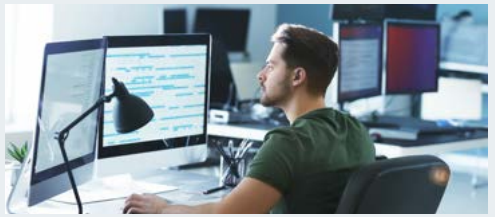
Genau das ist 2020 in Florence im US-Bundesstaat Alabama passiert. Als Ende Mai bei der 40.000-Einwohner-Kommune nahe der nördlichen Staatengrenze die Warnmeldung über ein versuchtes Eindringen einging, war es schon zu spät. Ein krimineller Hacker hatte sich anscheinend bereits einen ganzen Monat vorher Zugang verschafft und in aller Ruhe die Systeme der Stadtverwaltung übernommen. Am 5. Juni schlug er dann zu und verlangte Lösegeld in Bitcoin-Währung.

Nachdem man sich mit Sicherheitsexperten beraten hatte, die die Vorgehensweise des Verbrechers bereits kannten, entschied man sich bei der Verwaltung, die geforderten 300.000 USD zu bezahlen. Aber Florence war nicht alleine. Nur vier Monate vor dem Vorfall hatte die New York Times über Zahlen berichtet, die besagten, dass Ransomware-Angriffe zwischen 2018 und 2019 um 41 Prozent gestiegen[6] und Dutzende Städte betroffen waren.

Abseits der aufsehenerregenden großen Fälle hat sich eine Anzahl von Kriminellen eine lukrative Nische erobert und schröpft schwächere Ziele, denen nichts anderes übrigbleibt, als zu zahlen. Als Hechte im Karpfenteich nutzen hervorragend ausgerüstete Verbrecher ihren technologischen Vorsprung gegen diejenigen mit den schwächsten Verteidigungsressourcen.

Anders als andere Sicherheits- und Identifizierungslösungen ist PKI so flexibel, dass es für Netzwerke und E-Mail genauso gut funktioniert wie für das Web. PKI-Lösungen machen Sicherheitsumgebungen unkompliziert, weil Verschlüsselungs- und Authentifizierungszertifikate für die verschiedensten Systeme, Geräte und Benutzer ausgegeben und verwaltet werden können.

Die Lösung, die bereits für Ihre Website funktioniert, kann auch Ihre Netzwerke, Geräte, E-Mail, Dokumente und Benutzer sichern und dadurch sowohl Ransomware-Angriffe verhindern als auch Ihre Sicherheitsumgebung vereinfachen.



[5] https://www.capitalone.com/facts2019/ [6] https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html

KAPITEL 2

WAS SIE VIELLEICHT NOCH NICHT ÜBER PKI WISSEN

Die große Herausforderung in einer Welt, in der alles mit jedem verbunden ist, ist die Komplexität.

Entweder sind immer komplexere Angriffe abzuwehren, oder es müssen komplexe Ökosysteme geschützt werden, in denen alte und neue Technologien zusammenwirken. Oder aber es muss ein System gesichert werden, dessen Benutzer auf die immer komplexeren, raffinierteren Bedrohungen nicht vorbereitet sind.

Sicherheitsberater und Analysten hören von IT- und Sicherheitsexperten auf der ganzen Welt dasselbe Anliegen: Sie brauchen eine Lösung, die einfach einzurichten und zu verwalten ist und der sie unbedingt vertrauen können.

Hier kommt die Public Key Infrastructure ins Spiel.

Wer sich mit Internet-Sicherheit auskennt, dem ist das Konzept PKI vertraut. Das Prinzip ist schon lange im Einsatz, denn es dient bereits seit zwei Jahrzehnten als zuverlässige Website Security-Lösung – zuerst als SSL und jetzt als TLS. Es wird wie vor zwanzig Jahren noch immer zur sicheren Authentifizierung eingesetzt.

Was viele aber nicht wissen, ist, dass PKI nicht nur das Web schützt. Sondern auch Anwendungen. Und Code. Und Smart Watches, Autos, Verträge, Krankenhausbetten und Satelliten. Die Sicherheitslösung, die seit zwei Jahrzehnten zuverlässig im Web funktioniert, ist – für viele überraschend – genauso zuverlässig auf die neuesten und innovativsten Erfindungen anwendbar.

PKI ist bewährt

Trotz der täglichen Weiterentwicklung unserer vernetzten Welt ist PKI auch in der Sicherung der modernsten IoT-Geräte das bewährte Instrument, als das es vor zwanzig Jahren bei der Sicherung verschlüsselter Kommunikation begonnen hat.

Ihr Erfolg liegt in der einfachen Anwendung von Schlüsselpaaren bei der asymmetrischen Verschlüsselung. Bei der asymmetrischen Verschlüsselung kann eine Partei Daten verschlüsseln und an eine andere Partei übermitteln, ohne dass ein gemeinsamer geheimer Schlüssel vorhanden sein muss. Wird der Code für einen Schlüssel geknackt, ist dennoch die Entschlüsselung des anderen Schlüssels nicht möglich. Um die Daten zu lesen, braucht man beide Schlüssel des Paares.

Das Ergebnis ist ein Vertrauen, das seit Jahrzehnten zuverlässig fortbesteht.

PKI ist flexibel

Heutige IT-Experten brauchen ein System, mit dem sie Websites und Anwendungen absichern und sowohl Dokumente signieren als auch die Smartphones von Mitarbeitern authentifizieren können. Das eine Unternehmen braucht eine Lösung für automatisierte Fertigungsroboter, ein anderes dagegen muss die Kreditkartennummern seiner Kunden schützen. Eine Lösung, die nur bei einigen dieser Anwendungen funktioniert, belastet nicht nur das zuständige IT-Sicherheitsteam, sondern ist auch ein Risiko für das Unternehmen.

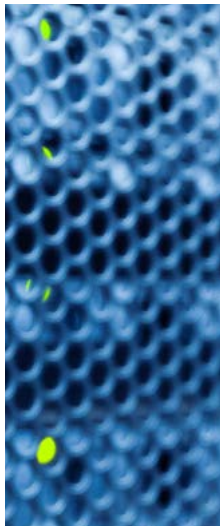
Im Gegensatz zu anderen Sicherheitslösungen ist PKI unglaublich flexibel. Da sie auf asymmetrischen Schlüsselpaaren basiert und der Sicherheitsprozess sowohl für die Validierung als auch für die Verschlüsselung ganz einfach funktioniert, kann PKI in den verschiedensten Umgebungen für ganz unterschiedliche Verbindungen Anwendung finden. PKI-Lösungen können abwärts oder aufwärts skaliert werden, in der Cloud, On-Premises oder in hybriden Umgebungen ausgeführt werden und heute Web und E-Mail genauso sichern wie morgen BYOD und IoT. Sie bieten also eine Lösung für alle Sicherheitsanforderungen.

PKI schafft öffentliches und privates Vertrauen

Zusätzlich zur Verschlüsselung verbindet PKI über einen Signiervorgang eine Identifizierung mit dem Schlüssel. Die Signatur wird von der Stamminstanz (Root) ausgegeben, sodass jeder, der über den öffentlichen Schlüssel zu dieser Root verfügt, sicher sein kann, dass das damit verbundene PKI-Zertifikat gültig und vertrauenswürdig ist.

In manchen Fällen ist das Root-Zertifikat öffentlich: Es wurde in einem Trust Store hinterlegt, der Bestandteil eines Web-Browsers wie Chrome oder Firefox oder eines Betriebssystems wie Microsoft Windows oder Apple MacOS ist. In anderen Fällen ist das Root-Zertifikat privat: Es ist Teil eines Systems, das ein Unternehmen oder eine Unternehmensgruppe intern verwenden will. Die Verschlüsselung funktioniert in beiden Fällen gleich, aber es ist die Fähigkeit zur Ausstellung sowohl öffentlicher als auch privater Zertifikate, die PKI so vielseitig macht.

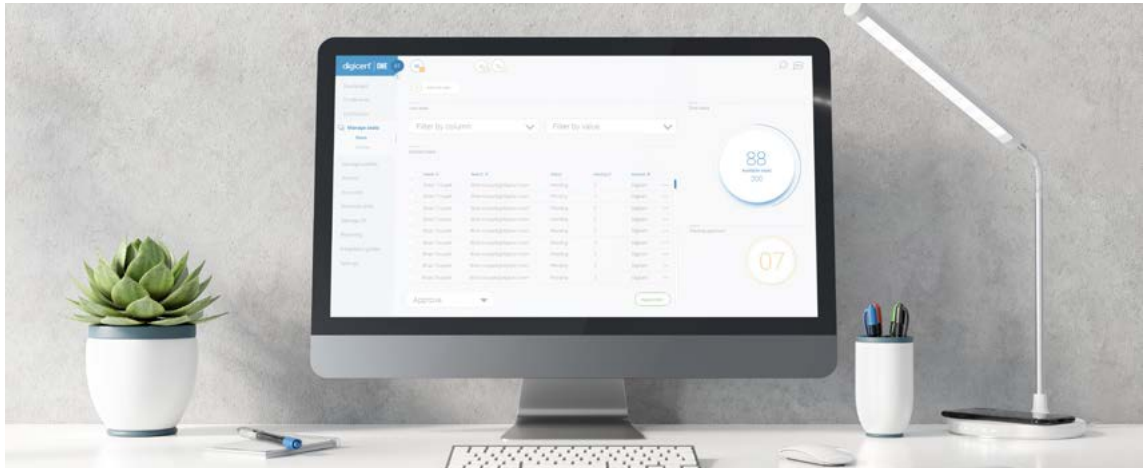
Aufgrund dieser Flexibilität schließt PKI die Lücke zwischen öffentlichen und privaten vertrauenswürdigen Anwendungen. Sie ist leistungsstark und sicher genug, um als private Verschlüsselungs- und Identifizierungslösung für viele Behörden zu dienen, aber auch als öffentliche Lösung für die IoT-Geräte von Verbrauchern.



PKI kann einfach sein

Früher war PKI kompliziert. Ohne Fachleute und ohne einfache Management-Plattformen und Tools mussten einzelne unternehmensinterne IT-Fachleute PKI-Lösungen selbst entwickeln, was ohne das richtige Spezialwissen ein Risiko war. Wenn sie erst einmal lief, war PKI dank ihrer Zuverlässigkeit die ideale Lösung, aber auf dem Weg dorthin schaffte sie mehr Probleme als sie löste.

Dies alles gehört der Vergangenheit an. Heute ist PKI, wenn man richtig ansetzt, ganz leicht einzurichten und anzuwenden. Smarte Tools für die Bereitstellung und Überwachung von PKI-Lösungen laufen heute auf einer Single-Sign-On-Plattform ab. Und weil PKI so vielseitig ist, lassen sich Lösungen für viele verschiedene Sicherheitsaufgaben an einer zentralen Stelle bündeln. Anstatt anwendungsspezifisch jeweils eine einzelne PKI-Lösung entwickeln zu müssen, können Sie heute mehrere Sicherheitslösungen an einem Ort bereitstellen und verwalten – und zur Einrichtung und Ausführung Ihrer PKI-Umgebung brauchen Sie kein Spezialwissen mehr.



Vier Missverständnisse über PKI

Was – PKI wird immer noch genutzt?

Manche Dinge kommen nie aus der Mode. PKI wird nicht nur immer noch genutzt, sondern entwickelt sich evolutionär weiter. Der Wert von PKI liegt in ihrer Flexibilität und in ihrer bewährten Vertrauenswürdigkeit. Bei immer mehr Verbindungen zeigt sich, dass PKI die beste Lösung für Sicherheit und Identifizierung ist und aufgrund ihrer bekannt robusten Schutzwirkung gerne implementiert wird.

Aber es gibt doch da dieses Problem mit Chrome?

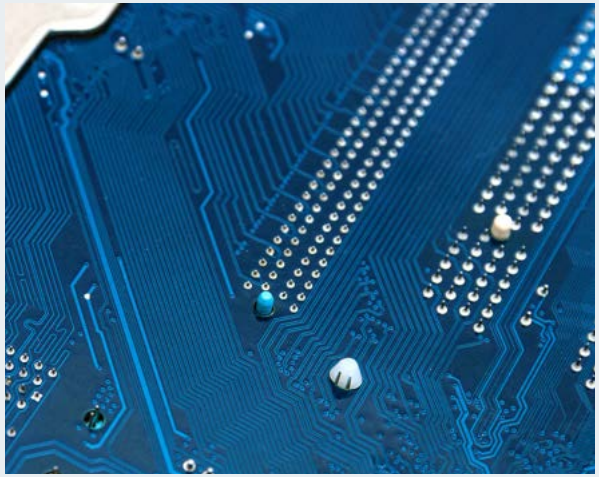
PKI hat eine unglaubliche Erfolgsbilanz in Sachen Sicherheit. Ihre Umsetzung liegt jedoch in der Hand der ausgebenden Stelle. 2017 gab Google bekannt[7], dass es eine Reihe von Symantec ausgestellter Zertifikate als nicht vertrauenswürdig einstufen würde, weil diese Zertifikate den Baseline Requirements des CA/Browser Forum nicht mehr genügten.

Dies ist ein bedauerliches Beispiel einer überholten Vorgehensweise, und die Auswirkungen waren spürbar. Aufgrund der Möglichkeit einer

[7] https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html

erheblichen Lücke im weltweiten Sicherheitsnetz suchten Symantec und Google nach einer Zertifizierungsstelle, die für eine umfangreiche Neuausstellung vertrauenswürdig genug war und eine ausreichend leistungsstarke Infrastruktur hatte. Man entschied sich für DigiCert und ließ die Zertifikate von Symantec zu den vertrauenswürdigen Roots von DigiCert transferieren, sodass es für Chrome-Nutzer keine Unterbrechung beim Zugang zu PKI-gesicherten Websites gab.

Wie vor zwanzig Jahren ist PKI auch heute noch die vertrauenswürdige Lösung für die Sicherung von Kommunikation über das Internet, auch mit Chrome.



PKI funktioniert auf vielen Geräten nicht

Korrekter wäre es, zu sagen: PKI funktioniert auf jedem Gerät, das genug Power dafür hat. Für asymmetrische Schlüsselpaarungen wird eine ausreichende Verarbeitungsgeschwindigkeit, genug Arbeitsspeicher und Festplattenplatz gebraucht. Da es PKI seit über 20 Jahren gibt, müsste jedes moderne Gerät eigentlich in der Lage sein, das zu leisten, was bereits mit den Prozessoren der späten Neunziger möglich war. In einigen Fällen ist trotz der Fortschritte in der Mikroprozessortechnik die Leistung mancher IoT-Geräte so rudimentär, dass sie nicht schnell genug die Schlüssel erzeugen oder den Kommunikationskanal signieren können.

Zum Glück haben sich clevere PKI-Experten Tricks ausgedacht, das Problem zu umgehen, ohne Kompromisse bei der Sicherheit zu machen. Dabei wird der Inhalt der PKI-Zertifikate so reduziert, dass sie mit der geringen Bandbreite und schwächeren Prozessorausstattung einiger IoT-Geräte bearbeitet werden können. Einige Softwarefirmen bieten auch Systeme für die Schlüssel- oder CSR-Generierung auf schlechter bestückten Geräten an.

Wir gehen davon aus, dass die Anzahl der Geräte mit PKI-Kompatibilitätsproblemen in Zukunft abnehmen wird. Neue Fertigungsprozesse erlauben mittlerweile den hardwareseitigen Einbau von Schlüsseln. Damit ist integrierte Sicherheit gleich zu Beginn der Lieferkette möglich. So werden nicht nur Kompatibilitätsprobleme gelöst, auch die Fertigung wird beschleunigt, während gleichzeitig die Sicherheit und Identifizierung gleich von Beginn des Lebenszyklus an gewährleistet ist.

Aber PKI ist doch nur SSL fürs Web?

Wenn Sie in Sachen Netzwerksicherheit schon einige Jahre Erfahrung haben, kennen Sie PKI vermutlich als den Schutzmechanismus Secure Sockets Layer (SSL). SSL gibt es seit 1995, als die erste funktionsfähige Version als Verschlüsselungsprotokoll für Netscape genutzt wurde. Seit 1999 gibt es einen Nachfolger für SSL, nämlich Transport Layer Security (TLS). TLS ist und bleibt bis heute das vertrauenswürdige Verschlüsselungsprotokoll im Web.

TLS/SSL ist sicherlich die bekannteste Umsetzung des PKI-Prinzips, aber es gibt noch Dutzende weitere Anwendungen. In der Praxis stößt man überall auf PKI; sie kommt in so gut wie jeder Vernetzungstechnologie vor, die weltweit erfunden wurde. Tatsächlich nutzt man PKI heute zur Sicherung der verschiedensten Dinge, die sich vor einem Vierteljahrhundert, als Netscape mit SSL begann, noch kaum jemand vorstellen konnte.

VERTRAUEN SICHERN IN ALLEN BEREICHEN

Sogar die Technik- und Sicherheitsexperten, die PKI-Lösungen entwickeln, sind manchmal erstaunt über die Kreativität, mit der Anwender diese zur Sicherung ihrer Erfindungen einsetzen. PKI zieht sich wie ein roter Faden durch ein schier unübersichtliches Labyrinth der unterschiedlichsten – und manchmal überraschendsten – Technologien und Branchen. Aber eines verbindet alle diese verschiedenen Anwendungsfälle miteinander – der Bedarf an kompromissloser Vertrauenswürdigkeit.

ERSTE FALLSTUDIE

AeroMACS

Vertrauenswürdig in großen Höhen

Piloten der zivilen Luftfahrt nutzen heutzutage bei jedem Flug mehr Sensordaten, als den Astronauten Young und Crippen im Jahre 1981 beim Jungfernflug der *Columbia* zum Verlassen des Orbits zur Verfügung standen.

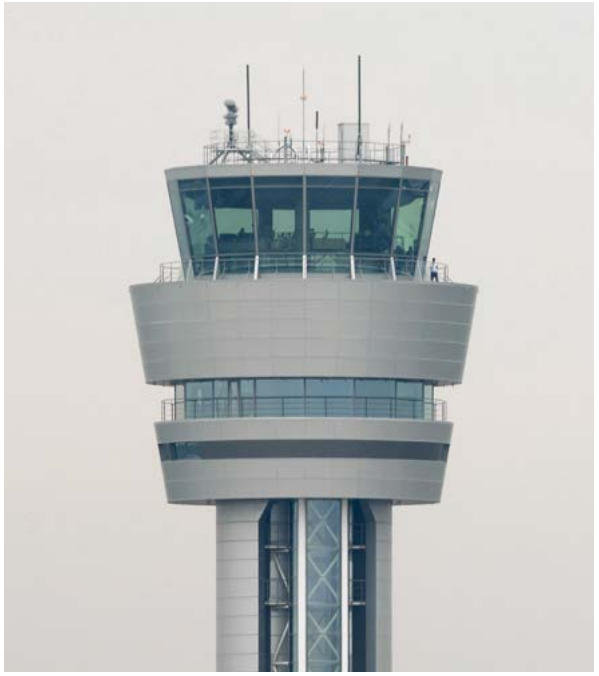
Dennoch bleibt heute wie damals der menschliche Faktor in der Luft- und Raumfahrt entscheidend. Die Person am Steuerknüppel braucht so viele exakte Daten wie möglich, um das riesige Luftfahrzeug sicher wieder auf den Boden zu bringen.

Die meisten Unglücksfälle mit Flugzeugen passieren im Rahmen von Start und Landung. In diesen Situationen ist das Flugzeug am angreifbarsten für die – physikalischen und menschlichen – Einflüsse, die den komplizierten Vorgang stören können, der 60 Tonnen Metall, Treibstoff, Fracht und Passagiere in die Luft bringt. Eine unerwartete Windbö, falsches Timing, schlechte Sichtverhältnisse.

Beim Start und im Landeanflug nutzen Airline-Piloten unerlässliche Informationen, die von Sensoren erfasst und im Cockpit angezeigt sowie an den Tower weitergeleitet werden, um die für sicheres Fliegen notwendigen Entscheidungen treffen zu können. Seit 2016 erfolgt die Übermittlung dieser lebenswichtigen Informationen an Tower und Flugzeuge weltweit durch IoT-Sensoren, die per PKI gesichert sind.

Die meisten Unglücksfälle mit Flugzeugen passieren im Rahmen von Start und Landung. In diesen Situationen ist das Flugzeug am angreifbarsten für die – physikalischen und menschlichen – Einflüsse, die den komplizierten Vorgang stören können, der 60 Tonnen Metall, Treibstoff, Fracht und Passagiere in die Luft bringt.

SEIT 2016 WERDEN LEBENSWICHTIGE INFORMATIONEN AN TOWER UND FLUGZEUGE WELTWEIT VON IoT-SENSOREN ÜBERMITTELT, DIE PER PKI GESICHERT SIND.



Mehr Effizienz mit weniger Aufwand

Es wird erwartet, dass sich die Zahl der Flugzeuge, die weltweit unterwegs sind, bis 2025 verdoppelt haben wird. Beispielsweise hat sich das Flug-gastaufkommen am Flughafen Beijing-Daxing von 2017 bis 2018 um 5 Prozent vergrößert und am US-Flughafen Dallas Love Field betrug die Stei-gerung 90 Prozent zwischen 2010 und 2020.

AeroMACS IST EINE BREITBAND-HOCHKAPAZITÄTS-DATENFUNKVERBINDUNG, ÜBER DIE IoT-SENSORDATEN VON FLUGHÄFEN ZU DEN KONTROLLTÜRMEN UND FLUGZEUGEN ÜBERMITTELT WERDEN.

Obwohl weltweit neue Flughäfen gebaut werden, haben die vorhandenen Einrichtungen angesichts der steigenden Zahl der Flüge keine andere Wahl, als die Effizienz ihrer Flugverkehrskoordination zu steigern und den reibungslosen Ablauf von Starts und Landungen zu gewährleisten.

Was ist AeroMACS?

Das Aeronautical Mobile Aviation Communication System (AeroMACS) ist eine Breitband-Hoch-kapazitäts-Datenfunkverbindung, über die IoT-Sen-sordaten von Flughäfen zu den Kontrolltürmen und Flugzeugen übermittelt werden. Von Tem-peraturen und Windstärken bis zur Fluginforma-tionsanzeige werden alle Daten von Flugfeld- und Airport-Geräten, sogar die Gepäckabfertigung, per AeroMACS kommuniziert.

AeroMACS ist mehr als die Summe seiner Geräte. Dieses System aus Augen und Ohren am Boden ist aus der Koordination von Flugplänen nicht mehr wegzudenken. Es bildet das Herzstück des Flughafenbetriebs. Unbefugte könnten es missbrauchen, um falsche Informationen an das Flugzeug und die Piloten zu senden. Darum ist es für die vielen Flüge und Passagiere bei Start, Flug und Landung lebenswichtig, die Informationen in AeroMACS gegen Manipulationen zu schützen.

PKI gehört auf die Cockpit-Checkliste

In Branchen mit komplexen IT-Landschaften, in denen viele Elemente die Leistungsfähigkeit der unterschiedlichsten Gerätetypen strapazieren, besteht ein Bedarf an einer anpassbaren, zuverläs-

sigen Sicherheitslösung. Im Fall des Flugverkehrs treffen alle diese Faktoren zu, zusätzlich sind die Daten aber auch vertraulich. Sowohl die zwischen dem Boden und dem Flugzeug übermittelten Informationen als auch die Geräte müssen gesichert sein, um potenziell katastrophale Manipulationen zu verhindern.

Unter dem Schutz dieser Geräte und ihrer Daten durch PKI können Piloten und Fluglotsen unabhängig vom jeweiligen Flugzeug oder Airport zuverlässig und sicher die verschiedenen Daten erfassen, weiterleiten und nutzen, die zum sicheren Starten und Landen gebraucht werden. Über AeroMACS läuft beispielsweise auf einem kleinen Flugplatz in den USA alles genauso zuverlässig wie in einem Hauptstadt-Airport in Australien.

Einsatz: weltweit

PKI-Lösungen schützen das AeroMACS-Netzwerk, das in naher Zukunft der flugtechnische Kommunikationsstandard auf fast jedem Flughafen der Welt sein wird.

Grundbedürfnis: Vertrauen

Angesichts der täglich tausenden gleichzeitig stattfindenden Flüge müssen sich Flughäfen, Airlines und Piloten für die Sicherheit und Pünktlichkeit von Millionen Reisenden auf AeroMACS verlassen können.

ZWEITE FALLSTUDIE

GATEKEEPER IN AUSTRALIEN

Behörden vertrauen auf den Schutz ihrer Bürger

Die meisten Australierinnen und Australier wissen vermutlich nichts von der Sicherheits- und Identifizierungslösung, die ihre Daten und ihre wichtigsten Transaktionen schützt. Wer kürzlich in Australien ein Haus gekauft hat, hat Gatekeeper benutzt.Wer Güter importiert hat, hat Gatekeeper benutzt.

Das Gatekeeper Public Key Infrastructure Framework regelt nunmehr im dritten Jahrzehnt „die Nutzung digitaler Schlüssel und Zertifikate durch australische Behörden zur Sicherstellung der Identität von Nutzern gegenüber den Authentifizierungsdiensten".Vom wichtigen Rechtsakt über Vertragsdokumente und Grenzschutz bis hin zum Bankwesen läuft die Verschlüsselung und Authentifizierung vieler besonders sensibler, vertrauensbasierter öffentlicher Vorgänge über PKI-Lösungen.

Ein ganzes Land wird gesichert

Am Ende des vergangenen Jahrhunderts begann die australische Regierung mit der Suche nach einem Mechanismus, der zuverlässig die Informationen in den immer zahlreicher werdenden digitalen Dokumenten und Transaktionen schützen könnte. Zunächst entwickelten einzelne Behörden jeweils eigene Lösungen, aber sie erkannten schnell, dass die interne Verwaltung des gewünschten, hohen Sicherheitsstandards schwierig, zeitaufwändig und riskant war.

Aus diesem Grund definierte eine Rahmenkommission eine Lösung, die imstande war, eine ganze Nation zu sichern und gleichzeitig so wenig Zeit und Ressourcen wie möglich für ihre Verwaltung beanspruchte.Es entstand das Gatekeeper Framework, das heute „für Integrität, Interoperabilität, Authentifizierung und Vertrauen zwischen Behörden und ihren Kunden sorgt".

IN AUSTRALIEN HAT DAS VERTRAUEN AUF PKI NATIONALE TRAGWEITE – KEIN PROBLEM FÜR PKI.

Unsichtbar – aber immer da

Oftmals haben die Technologien, die wir nicht sehen, in unserem Leben den größten Einfluss. Stromnetze. Wasserversorgungsnetze. Bankennetzwerke. Wir nehmen die Zuverlässigkeit dieser „dienstbaren Geister“ als Selbstverständlichkeit hin. Für die Australierinnen und Australier ist Gatekeeper ein solches System, von dessen Zuverlässigkeit sie abhängen. Nicht nur sorgt es für Effizienz und Komfort, sondern es ist auch unverzichtbar für viele kritische Behördenabläufe. Ohne die starke Sicherheit von PKI könnten die personenbezogenen Daten von Millionen australischer Bürger gestohlen, wichtige Transaktionen und Rechtssachen verzögert oder verhindert oder Zoll- und Gewerbebehörden infiltriert werden. In Australien hat das Vertrauen auf PKI nationale Tragweite – kein Problem für PKI.

ALLES MUSS STETIG UND STÄNDIG FUNKTIONIEREN.

Einsatz: Australien

Eine landesweite Sicherheits- und Identifizierungslösung für zahlreiche Behörden, mit der viele äußerst sensible Belange des öffentlichen Lebens geschützt werden.

Grundbedürfnis: Integrität

Das Bankwesen, die Immobilienwirtschaft oder der Grenzschutz können sich Fehler oder Schwachstellen nicht leisten. Alles muss stetig und ständig funktionieren.

DRITTE FALLSTUDIE

WELTWEITER SEEHANDEL

Vertrauen auf globaler Ebene

Stellen wir uns einmal vor, wir müssten einen einzelnen Frachtcontainer auf seinem Weg zwischen zwei Häfen, zwischen Kontinenten und Weltmeeren unter Millionen anderen auffinden. Was wäre, wenn wir versuchen würden, ihn mithilfe von Datenbanken und Frachtlisten zu finden?

Die globalen Lieferketten sind wie eine komplizierte Uhr: Jedes kleinste Rad, jede Feder und jeder Draht muss an seinem Platz sein und ordnungsgemäß arbeiten, damit das Ganze funktioniert. Transportverzögerungen bringen Störungen in die Kette. Fehlende Lieferungen können die Kette sogar unterbrechen und bedeuten Verluste an Material und Umsatz für die betroffenen Unternehmen.

Jährlich werden mehr als 11 Milliarden Tonnen Güter auf dem Seeweg umgeschlagen. Derzeit gibt es weltweit über 50.000 Containerschiffe.

Digitale Transparenz

Jährlich werden mehr als 11 Milliarden Tonnen Güter auf dem Seeweg umgeschlagen. Derzeit gibt es weltweit über 50.000 Containerschiffe. Der Seehandelsverkehr ist gigantisch, aber auch dynamisch. Jeder Frachter ist ein Punkt auf einer Seekarte, der ständig in Bewegung ist.

Auf jedem dieser vielen Schiffe befinden sich wiederum tausende Container. Das – sichere – Auffinden und Verfolgen jedes einzelnen Containers in Echtzeit ist ein enormes Unterfangen.

Die Herausforderung angesichts der riesigen Frachtmengen ist die gegenseitige Authentifizierung von Geräten auf See in der Cloud, wo die Verfolgung von Gütern stattfindet. Bei einer Störung kann der Frachtführer den Aufenthaltsort der Container aus den Augen verlieren oder falsche Daten erhalten. Um effektiv zu sein, muss eine Sicherheitslösung nicht nur das Endgerät, sondern auch die Daten während der Übertragung sichern. Sie muss außerdem skalierbar sein und fehlerfrei zehntausende Geräte auf einmal sichern können.

Jeder Seeweg überall in der Welt

Mit PKI-Authentifizierung können Frachtcontainer auf dem gesamten Transportweg von der Verladung bis zum Zielhafen sicher verfolgt werden. Und weil im Transportwesen die Zahl der benötigten Geräte und zu sichernden Ladungen von Jahr zu Jahr steigt, steigt auch der Sicherheitsbedarf. Dank seiner Skalierbarkeit kann PKI die Nachfrage decken.

Die Daten werden also unabhängig von der Anzahl der Transporte immer gesichert und die Container sind überall in der Welt verfolgbar. Dadurch sinkt das Diebstahl- oder Verlustrisiko und steigt die Effizienz des Warenverkehrs von Hafen zu Hafen. Dank einer ununterbrochenen Lieferkette profitieren sowohl Unternehmen als auch Verbraucher von der höheren Güterverfügbarkeit zu niedrigeren Kosten.

Einsatz: weltweit

Als Rückgrat der Lieferkette transportieren vernetzte Container Güter und Rohstoffe zu jedem Kontinent unseres Planeten.

Grundbedürfnis: Authentifizierung

PKI leistet hier mehr als nur einfache Verfolgung, nämlich eine gesicherte Authentifizierung in Echtzeit, damit Unternehmen jedes in einem Frachtcontainer angebrachte Gerät auffinden und identifizieren können.

MIT PKI KÖNNEN FRACHTCONTAINER AUF DEM GESAMTEN TRANSPORTWEG SICHER VERFOLGT WERDEN.

IBM

Führende Tech-Firmen vertrauen auf PKI

Oftmals sind es die größten Unternehmen, die vor den größten Herausforderungen stehen. Manchmal ist die Größe des Unternehmens an sich die Herausforderung. Wie sichert beispielsweise ein Unternehmen einzelne Benutzer, die nicht nur in unterschiedlichen Büros überall auf der Welt verschiedenen Aufgaben nachgehen, sondern dabei auch noch verschiedene Geräte mit unterschiedlichen Betriebssystemen und Anwendungen nutzen?

Für IBM war das nicht nur eine Denksportübung, sondern ein echtes Problem. Ein Problem, das eine halbe Million Mitarbeiter betrifft.

Bring-your-own – ja was eigentlich?

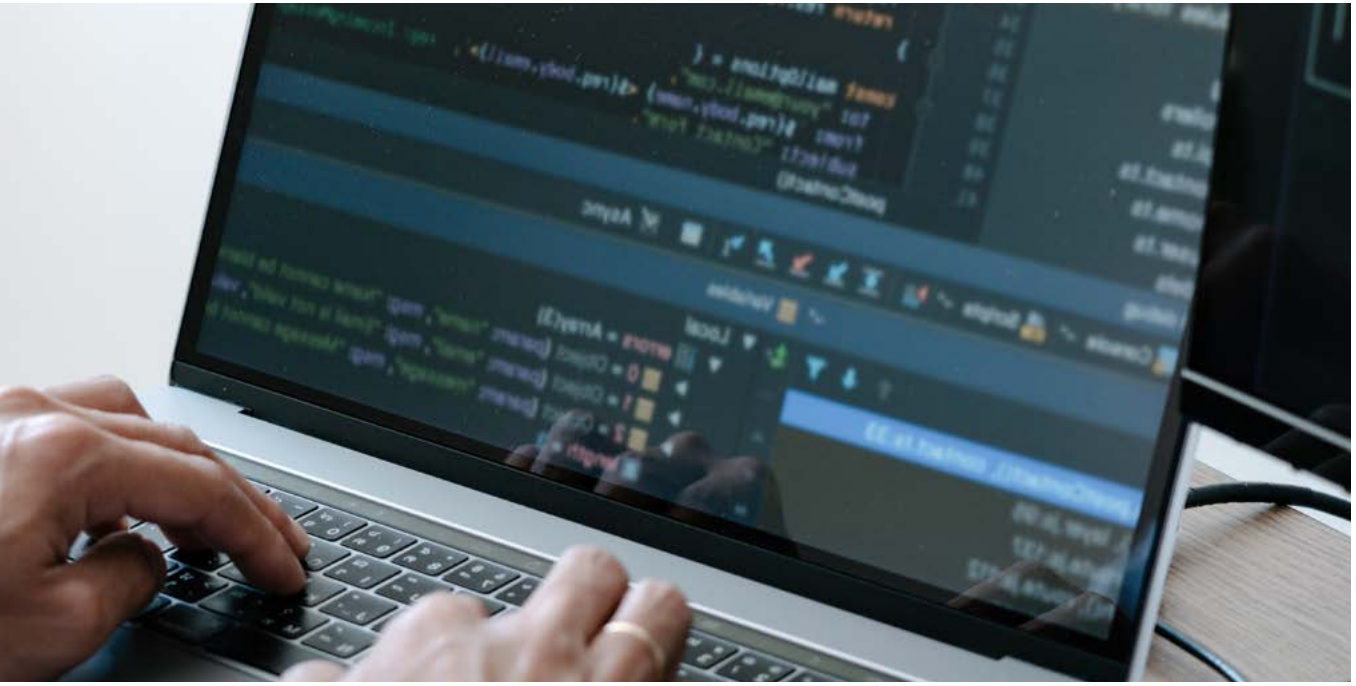
Authentifizierung, Identifikation und Sicherheit für über 500.000 Benutzer.

Hier fällt der Anspruch „flexibel und skalierbar" aus der Höhe einer theoretischen Beschreibung auf den harten Boden der Realität und muss in einer PKI-Lösung funktionieren. Die größte Herausforderung ist hierbei nicht einmal die schiere Anzahl der Benutzer, sondern die Verschiedenheit der Geräte und Anwendungen, die diese Benutzer verwenden und mit zur Arbeit bringen. Der vom Unternehmen zur Verfügung gestellte Laptop. Das persönliche Smartphone. Das alte iPad. Wenn Ihre Mitarbeiter und Zulieferer so flexibel wie möglich arbeiten und dazu die am besten geeigneten Geräte einsetzen sollen, Sie aber keine Schwachstellen in Ihrem Netzwerk dulden können, brauchen Sie eine anpassungsfähige, aber robuste Sicherheitslösung.

PKI ist nicht nur flexibel, sondern auch skalierbar. Mit Public Key Infrastructure kann man nicht nur beliebig viele Geräte unabhängig von deren Eigentümer und den darauf laufenden Anwendungen authentifizieren, sondern man kann dies gleichzeitig mit hunderttausenden Benutzern und ihren jeweils mehreren Geräten an beliebigen Standorten tun. Für alle 500.000 Benutzer fühlt sich dies vollständig reibungslos an.

Vertrauen heißt Zuverlässigkeit

Seit mehr als einem Jahrzehnt laufen PKI-Identifizierungslösungen ununterbrochen in über 170 Ländern alleine in diesem Unternehmen.



PKI IST NICHT NUR FLEXIBEL, SONDERN AUCH SKALIERBAR.

Zusätzlich zur vertrauenswürdigen Sicherheit wird dabei vor allem Zuverlässigkeit gebraucht. In dieser Größenordnung muss eine Software-as-a-Service-Authentifizierung robust genug sein, um ständig und überall zu funktionieren. 24 Stunden am Tag, 7 Tage die Woche haben überall auf der Welt hunderttausende Benutzer unabhängig vom verwendeten Gerät sicheren Zugriff auf das IBM-Netzwerk. Es funktioniert so sicher und reibungslos, dass die Benutzer nicht darüber nachdenken müssen und das Unternehmen sich über Schwachstellen keine Sorgen machen muss.

Einsatz: weltweit

Ein global führendes Hardware- und Software-Traditionsunternehmen arbeitet über weltweit tausende Standorte verteilt.

Grundbedürfnis: Flexibilität

Eine PKI-basierte Lösung dient der Authentifizierung, Sicherung und Identifikation einer halben Million Mitarbeiter auf dem gesamten Globus, die unternehmenskritische Arbeiten ausführen.

FÜNFTE FALLSTUDIE

GESUNDHEITSWESEN

Vertrauenswürdig auch in lebenserhaltenden Anwendungen

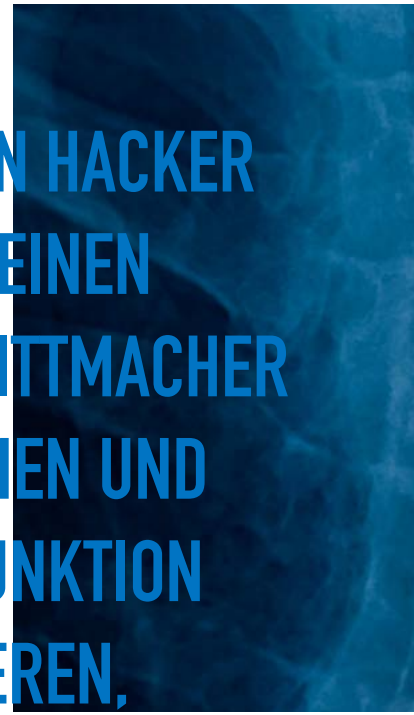
Für die meisten von uns sind vernetzte Komponenten eine nützliche Sache. Über eine Bluetooth-Verbindung prüfen wir die Außentemperatur und Luftfeuchtigkeit auf unserer Terrasse. Die WLAN-Verbindung zwischen dem iPad in der Küche und dem Smart-TV im Wohnzimmer erlaubt es uns, beim Abendbrot die spannende Serie weiterzuschauen. Vernetzung ist für uns angenehm und praktisch, aber notfalls könnten wir auch darauf verzichten. In manchen Fällen ist eine Vernetzung aber viel mehr als nur nützlich oder komfortabel. Für manche Menschen bedeutet vernetzt zu sein den Unterschied zwischen Leben und Tod.

Vor einigen Jahren kam ein neuer Typus von Herzschrittmacher auf den Markt. Es handelte sich um ein „intelligentes" Modell. Dank einer Bluetooth-Verbindung zu einem externen Monitor und einer App auf dem Smartphone des Patienten konnte der Schrittmacher nicht nur die lebensnotwendigen Signale an das Herz des Patienten abgeben, sondern auch dem Patienten und dem Arzt Auskunft über seine Funktion geben. Funktioniert der Schrittmacher ordnungsgemäß? Wie lang reicht die Batterie noch? Bislang musste der Patient zur Feststellung oder Korrektur dieser Daten das Krankenhaus aufsuchen oder sich sogar einem Eingriff unterziehen. Nun konnten alle diese Informationen automatisch und stetig überwacht, aufgezeichnet und übermittelt werden.

Vernetzte Schrittmacher sind mehr als nur komfortabel. Tausende Patienten vertrauen ihrem Gerät ihr Leben an. Wie bei jeder Verbindung besteht aber auch hier die Gefahr von Störungen. Wie jedes andere IoT-Gerät braucht auch ein vernetzter Herzschrittmacher eine sichere, lückenlose Verschlüsselung.

Wenn „Leben und Tod" wörtlich zu nehmen ist

Im August 2017 tauchte in den Nachrichten eine ungewöhnliche Meldung[8] auf – ungewöhnlich zumindest für diejenigen, die nicht im IoT-Bereich arbeiten. Die US-Gesundheitsbehörde FDA rief aufgrund einer Cybersicherheitsbedrohung einige Herzschrittmacher zurück. In der Meldung warnte die FDA, dass bestimmte Schrittmacher „anfällig für Cyberangriffe und Exploits" sein könnten. Die Ähnlichkeit der Terminologie mit bekannten Meldungen über Hackerangriffe war frappierend. Man war befremdet und fühlte sich an die Hand-



KÖNNTE EIN HACKER WIRKLICH EINEN HERZSCHRITTMACHER ÜBERNEHMEN UND DESSEN FUNKTION MANIPULIEREN, VIELLEICHT GAR GANZ AUSSCHALTEN? JA.

[8] https://thehealthcareblog.com/blog/2019/07/29/security-crisis-of-cardiac-pacemakers-paves-the-way-for-iot-security-evolution-in-cardiology/

lung eines Science-Fiction-Films erinnert. Könnte ein Hacker wirklich die Kontrolle über einen Herzschrittmacher übernehmen und dessen Funktion manipulieren, vielleicht gar ganz ausschalten? Ja.

Immer mehr neuartige Technologien zur Vernetzung von Geräten vom Krankenhausbett bis zum Blutzuckerüberwachungsgerät wurden erfunden und führten zu einer sprunghaften Verbesserung der Patientenversorgung. Gleichzeitig wurden aber auch warnende Stimmen über den Schutz von Patientendaten auf vernetzten Geräten laut, über die Möglichkeit von Angriffen auf Geräte, die zu deren Ausfall führen könnten.

Tatsächlich haben Hacker inzwischen einen Angriffspunkt zum Eindringen in Herzschrittmacher gefunden. Die Hersteller haben zwar die Kommunikation zwischen dem Gerät und dem Patientenmonitor verschlüsselt, aber der Monitor selbst war nicht gesichert. Über den Zugriff auf den Monitor konnten die Hacker wiederholt Befehle an den Schrittmacher senden und dadurch die Batterieladung aufbrauchen. Es war sogar möglich, dem Schrittmacher den Befehl zu erteilen, den Patienten zu defibrillieren. Auf der Suche nach einer Lösung für die Sicherheit des Geräts und des Patienten entdeckten viele Hersteller PKI.

Der Wert der Anwendung von PKI bei medizinischen Geräten steckt nicht nur in ihrer langjährig bewährten, starken Verschlüsselung, sondern auch in der integrierten Identitätsprüfung.

EINE SICHERHEITS-LÖSUNG, DIE DIE INTEGRITÄT DES GERÄTS UND DER PATIENTENDATEN SCHÜTZT UND ZU-VERLÄSSIG GENUG IST, IHR EIN LEBEN ANZUVERTRAUEN.

Medizingeräte werden kleiner und smarter, aber die Sicherheitslösung, die die Daten – und das Leben – von Patienten sichert, ist weiterhin PKI.

Mit PKI können Gerätedaten ganz einfach gesichert und die Geräte mit einer verschlüsselten ID authentifiziert werden. Auf diese Weise wird das Gerät bereits bei der Herstellung gesichert, und diese Sicherheit wird über das Krankenhaus an den Patienten weitergegeben. Obwohl das Gerät in seinem Lebenszyklus verschiedene Phasen durchläuft und durch verschiedene Hände geht, bleibt die Sicherheit zu jeder Zeit intakt und ununterbrochen.

Die Zukunft medizinischer Geräte wird noch intelligenter

Seit einiger Zeit wird wieder verstärkt in die Forschung und Entwicklung kleinerer, noch intelligenterer Geräte investiert, und einige Projekte haben bereits die behördliche Zulassung erhalten. Inzwischen sind bereits elektrodenlose Schrittmacher im praktischen Einsatz, die klein genug sind, um minimalinvasiv über einen Katheter direkt ins Herz implantiert zu werden. Die Operation wird dadurch kleiner und die Gefahr eines Verschleißes von Elektroden durch millionenfache Mikrobewegungen mit dem Herzschlag ist damit ausgeschaltet.

Die nächste Generation von Herzschrittmachern ist elektrodenlos und noch intelligenter. Sie sind mit kleinen Defibrillatoren vernetzt und überwachen nicht nur ihren eigenen Zustand, sondern auch die Herzgesundheit und teilen dem Defibrillator per Bluetooth mit, wenn das Herz einen lebensrettenden Impuls braucht. Sie können Daten an den zuständigen Kardiologen senden und sind in Echtzeit ohne operativen Eingriff umprogrammierbar, sodass der Arzt auf die Herzgesundheit des Patienten Einfluss nehmen kann, während dieser ganz normal sitzt.

Heute können Tausende Herzpatienten sicher sein, dass ein automatisches, gesichertes Überwachungssystem die Funktion ihres Schrittmachers gewährleistet und sie gegebenenfalls alarmiert, falls es zu Problemen kommt. Schon bald können noch mehr Patienten und ihre Ärzte von den erweiterten Möglichkeiten der Kardiotechnik profitieren und ohne Eingriff und Krankenhausaufenthalt bessere Daten und sofortige Hilfe erhalten. Die Medizingeräte werden kleiner und smarter, aber die Sicherheitslösung, die die Daten – und das Leben – von Patienten sichert, ist weiterhin PKI.

Einsatz: viele Länder weltweit

Zur Nutzung sowohl durch Dienstleister als auch durch Patienten in tausenden Krankenhäusern und Pflegeeinrichtungen für Millionen Menschen unter verschiedenen Zulassungs- und Implementierungsstandards.

Grundbedürfnis: Zuverlässigkeit

Eine Sicherheitslösung, die die Integrität des Geräts und der Patientendaten schützt und zuverlässig genug ist, ihr ein Leben anzuvertrauen.

KAPITEL 3

UNWISSENHEIT SCHÜTZT VOR SCHADEN NICHT.

Ja, PKI ist bereits seit Jahrzehnten vertrauenswürdig. Aber dieses Vertrauen braucht Fachwissen. Schließlich stellen bei einer unsachgemäß eingerichteten PKI-Lösung die Schwachstellen ein genauso großes Risiko dar wie ein ungesichertes System.

Aufgrund der langen Geschichte von PKI haben Techniker und Computerwissenschaftler genügend Zeit gehabt, ihre praktische Anwendung zu studieren. Es gibt Beispiele smarter, innovativer Einsätze, aber auch Fälle von Fehlschlägen, bei denen Konzeptionsfehler oder falsche Betreuung ein ansonsten fast perfektes System geschwächt haben.

Jede Implementierung einer PKI bietet eine neue Chance, ihre Funktion zu beobachten, insbesondere wenn es sich um eine neuartige Einsatzumgebung oder eine neue Technologie handelt. Und jedes Mal, wenn etwas gut klappt, lernen PKI-Techniker etwas über die intelligentesten und sichersten Nutzungsweisen der Technologie dazu.

Einige PKI-Tipps von Sicherheitsexperten

Richtiger Schutz für die Schlüssel

PKI ist nur so gut wie der geheime Schlüssel, mit dem die Zertifikatskette signiert wird. Dies ist im Allgemeinen ein Schlüssel für die Zertifizierungsstelle und einer für die ausstellende CA (ICA). Wird mindestens einer dieser Schlüssel auf unsichere Weise erstellt oder aufbewahrt, sind die ausgestellten PKI-Zertifikate nicht sehr vertrauenswürdig. Dies kann in einem Unternehmen passieren, wenn beispielsweise IT-Techniker Schlüssel im Klartext auf einem von ihnen verwalteten Server erstellen, dabei Software verwenden, die sie vom Internet heruntergeladen haben und die Schlüssel dann auf ihre CA übertragen, die im Netzwerk abläuft, um ein Backup zu haben. In diesem Fall ist das PKI-System extrem unsicher, denn die Schlüssel – die zu keinem Zeitpunkt geschützt waren – können ganz einfach gestohlen werden. Nur durch geeigneten Schutz ist die Vertrauenswürdigkeit der gesamten PKI-Hierarchie gewährleistet.

Zertifikatstatus

PKI-Systeme sollen einem Gerät oder Browser eine Methode an die Hand geben, mit der sie feststellen können, ob das Zertifikat noch gültig und nutzbar ist. Wenn PKI nicht korrekt implementiert ist, fehlt in der Hierarchie oftmals die Information, die für eine Sperrung notwendig ist, oder es fehlt jede Information. In manchen Fällen ist die Information zwar vorhanden und richtig, aber das System verwaltet die Anfragen nicht richtig. Unabhängig von der Ursache ist das Ergebnis ein nicht vertrauenswürdiges System.

Falsche Konfiguration

Außer einer korrekten Einrichtung des Systems müssen Konfigurationen innerhalb des Zertifikats oder der Zertifikatskette oftmals auf spezielle Weise erfolgen, damit PKI Software und Hardware schützen kann. Im Falle „selbstgestrickter" Implementierungen finden sich nicht selten Behelfskonfigurationen, die in einem Fall ein Problem lösen, das Zertifikat aber anderen Risiken durch Umgehung, Aneignung oder Missbrauch aussetzen.

JA, PKI IST BEREITS SEIT JAHRZEHNTEN VERTRAUENSWÜRDIG. ABER DIESES VER-TRAUEN BRAUCHT FACHWISSEN.

Vier Fehler bei der Einrichtung einer PKI-Verschlüsselung

Zukünftige Iterationen werden nicht eingeplant

Oftmals vergessen Sicherheitsbeauftragte beim Einrichten einer „selbstgebastelten" PKI-Lösung, später notwendig werdende Veränderungen mit einzuplanen. Unternehmen verändern sich, Geschäftsziele entwickeln sich, neue Produkte oder Teams kommen hinzu. Wenn eine PKI-Lösung da nicht anpassbar ist oder keine neuen Bereitstellungen ermöglicht, veraltet sie oder wird zur Gefahr.

Man versucht, eine PKI-Landschaft intern zu verwalten

Die einfache Zuverlässigkeit von PKI kann trügen. Natürlich ist sie flexibel, skalierbar, schnell und zuverlässig – aber nur wenn sie ordnungsgemäß integriert und bereitgestellt wird. Intern errichtete Lösungen tendieren dazu, unhandlich zu werden und unnötig Ressourcen zu verbrauchen. Ohne fachgerechte Installation und Aufsicht wird es schwer nachzuvollziehen, wo PKI implementiert wurde, wie ihr Status ist und wo eventuell noch Fehler oder Lücken sind. Managed-PKI und zentrale Plattformen sind hier die Lösung, sparen Zeit bei der Überwachung und befreien von Sorgen über Sicherheitsfehler, abweichende Schlüssel oder Benutzerfehler.

Die Einhaltung von Vorschriften wird nicht beachtet

Eine der herausragenden Eigenschaften von PKI – und eine ihrer größten Vorteile – ist die Option für flexible Bereitstellung. Die möglichen Modelle reichen von On-Premises bis cloudgestützt. Es ist nicht nur wichtig, zu wissen, welche Option für die Geschäfte, Sicherheit und Benutzerbedürfnisse des Unternehmens die richtige ist, sondern auch, welche im Einklang mit den örtlichen, regionalen oder nationalen Vorschriften ist. Auch die Stellung der PKI-Lösung in der übergeordneten Sicherheitsstrategie des Unternehmens und der Branche muss durchschaut werden.

Man ist nicht vorbereitet auf die kommende PQC-Revolution

Post-Quantum-Computing, also Quanteninformatik, ist nicht mehr nur Science Fiction, sondern könnte bald technologische Realität werden. Neben den Vorteilen von Quantencomputern sind auch entsprechende Nachteile zu erwarten. Das volle Potenzial von Quantencomputern beim Knacken von mathematisch unmöglichen Codes ist noch nicht absehbar. Sicherheitsfachleute sollten nicht den Fehler machen, auf die praktische Einsetzbarkeit der Quanten-IT zu warten, sondern ihre Umgebungen bereits heute gegen die möglichen Bedrohungen rüsten. Die Grundlagen für die Sicherung von Systemen in der Welt des Post-Quantum-Computings sind bereits gelegt, und gut informierte Sicherheitsfachleute wissen um die Notwendigkeit, Systeme zu verstehen und zu testen, die ihre Ressourcen auch im kommenden Quantenzeitalter schützen können.

FAZIT

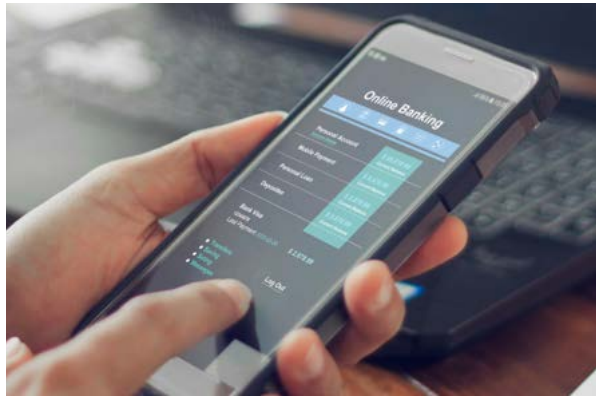
ÜBERDENKEN SIE ALTE ANNAHMEN. PKI IST TEIL DER MODERNEN WELT.

Wie kann eine Jahrzehnte alte und als zuverlässig bekannte Technologie sich den heutigen Verhältnissen anpassen? Dazu muss nicht die Technologie, sondern ihre Anwendungsweise angepasst werden.

PKI funktioniert. Diese Sicherheits- und Identifizierungslösung ist seit den Zeiten von Netscape und 33.6-k-Modems erprobt und vertrauenswürdig. Trotz einiger Updates und kleinerer Anpassungen an Entwicklungen der IT-Branche ist das Prinzip von PKI im Lauf der Jahre unverändert geblieben.

1996 konzentrierte sich die Arbeit mit PKI beispielsweise auf den Schutz von Suchergebnissen in Excite und sichere Einkäufe bei eBay. Deshalb denken viele beim Stichwort PKI auch heute noch in diesen Begriffen. Woran man nicht sofort denkt, ist, dass PKI heute auch zum Schutz vor Unfällen im Zugverkehr oder zum Aussperren von Hackern aus der Übertragung personenbezogener Daten mittels Smart Watches zum Einsatz kommt. Und auch immer noch zur Verschlüsselung auf eBay.

Die moderne PKI hat sich mit anderen Technologien weiterentwickelt und erfüllt inzwischen Sicherheitsanforderungen auf der ganzen Welt, in allen Branchen, in Unternehmen und Behörden und auch im privaten Bereich. Die Bedeutung von PKI für Flugzeug-Notsignalgeräte ist vielleicht nicht geringer als für Millionen von Menschen, die täglich auf die Sicherung von Banktransaktionen und den Schutz vor dem Diebstahl von Kreditkartendaten durch PKI vertrauen. In allen Fällen kann die Bedeutung von Vertrauen nicht hoch genug eingeschätzt werden. PKI ist gleichzeitig eine bewährte Technologie und eine Lösung, die für die Sicherheit und Identifizierung der Erfindungen von heute und morgen eingesetzt werden kann. Ganz gleich, was auf uns zukommt – PKI sorgt nachvollziehbar und flexibel für Vertrauen.



DIE MODERNE PKI HAT SICH MIT ANDEREN TECHNOLOGIEN WEITERENTWICKELT UND ERFÜLLT INZWISCHEN SICHERHEITSANFORDERUNGEN AUF DER GANZEN WELT.

Sie haben Kenntnis von einer innovativen Anwendung von PKI? Wir möchten gerne darüber berichten. Sie möchten gerne mehr über die PKI-Lösungen von DigiCert erfahren?
Wir helfen gern. PKI_Info@digicert.com

Über DigiCert

Wir finden die bessere Lösung und machen sie zum Standard.

DigiCert steht für mehr Sicherheit im Internet. Dieses Ziel zieht sich als roter Faden durch unsere gesamte Unternehmensgeschichte. Deshalb genießen unsere TLS/SSL-Zertifikate tagtäglich und millionenfach das Vertrauen von 89 % der Fortune 500-Unternehmen, 97 der 100 größten internationalen Finanzinstitute und 81 % aller weltweit tätigen Online-Händler. Nicht umsonst erhalten wir von unseren Kunden branchenweit die meisten Fünf-Sterne-Bewertungen für Service und Support. Mit der Plattform DigiCert ONE und mit unseren Verwaltungstools modernisieren wir die Public Key Infrastructure und unterstützen Unternehmen und Behörden beim Schutz von Identitäten, Zugriffen, Servern, Netzwerken, E-Mails, Codes, Signaturen, Dokumenten und IoT-Geräten. So stellen wir sicher, dass DigiCert auch in Zukunft eine Vorreiterrolle bei der Entwicklung innovativer SSL-, IoT- und PKI-Lösungen einnimmt.