DIGITAL TRUST.
ECHT GEMACHT.

digicert®

INHALTSVERZEICHNIS

1 *Einleitung: Von den Gletschern Alaskas bis ins All*

3 *Kapitel 1: Eine digitale Welt ist längst keine Science-Fiction mehr: Unsere Welt ist digital*

5 *Kapitel 2: Vertrauen sichern in allen Bereichen*

14 *Kapitel 3: Auf Basis bewährter Technologien*

16 *Fazit: Lassen Sie digitales Vertrauen für sich arbeiten*

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 Rettung war nur aus der Luft möglich. In diesem abgelegenen Gebiet gab es jedoch keinen Mobilfunkempfang und die Funkreichweite war stark eingeschränkt.

Glücklicherweise war das Flugzeug aber mit der Iridium-Satellitenkonstellation verbunden, die die Erde in 800 Kilometer Höhe umkreist. Diese empfing das Notsignal des Flugzeugs und leitete es über ein geschütztes digitales Signal mitsamt der Flugzeugposition an die Rettungsdienste weiter. Das bordeigene Iridium-Gerät hatte die Bewegungen des Flugzeugs vom Start bis zum Crash aufgezeichnet und eine Echtzeit-Spur des gesamten Flugs erstellt. Diese Funktionalität geht über das hinaus, was GPS und Funknotsignale leisten. Das war nur möglich, weil jeder der 66 Iridium-Satelliten über eine digitale Verbindung zu Geräten und zueinander verfügt. So wird die Gerätesichtbarkeit und Kommunikation jederzeit und überall auf der Welt – von der Antarktis bis nach Alaska – gewährleistet.

Die US-Küstenwache erfuhr auf diese Weise 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 für ein Interview zur 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."

Wenn wir an digitale Interaktionen denken, fällt uns zumeist erst all das ein, was wir mit dem Computer oder Handy machen, zum Beispiel Shoppen, Mailen oder Apps benutzen. In der heutigen Zeit verschwimmt die Grenze zwischen digitaler und echter Welt aber immer mehr. Praktisch alles ist vernetzt. So werden überall große Datenmengen erzeugt und verschoben sowie zahllose Geräte überwacht.

In solchen 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 hat nichts mehr mit typischen Verbindungsdefinitionen oder Datenverschlüsselung wie dem Datenverkehr auf Websites oder der Kommunikation per E-Mail zu tun. Diese Notsender müssen auf der ganzen Welt verlässlich Verbindungen herstellen und kommunizieren können. Sie müssen jederzeit und unter den schwierigsten Umständen funktionieren, um in der echten Welt leben zu retten. Darum basiert die Iridium-Satellitenkonstellation auf digitalem Vertrauen.

„DIGITALES VERTRAUEN IST DAS FUNDAMENT FÜR DIE SICHERHEIT ALLER VERNETZTEN GERÄTE – VOM MEERESGRUND BIS HOCH INS ALL.“

Brian Trzupek
Senior Vice President for Product, DigiCert

EINE DIGITALE WELT IST LÄNGST KEINE SCIENCE-FICTION MEHR: UNSERE WELT IST DIGITAL

In der heutigen Zeit ist alles mit allem vernetzt. Von der Infrastruktur im Homeoffice bis zu Kühlschränken, immer mehr der Dinge, die wir nutzen und mit denen wir interagieren, stehen mit allem anderen in Verbindung. Geräte sind das Internet, das Internet besteht aus Apps, Autos sind Computer, Arztbesuche finden virtuell statt und Unterhaltung wird gestreamt. Die Grenze zwischen digitaler und echter Welt existiert nicht mehr.

In dieser Welt der flächendeckenden Vernetzung ist Vertrauen das Fundament, das digitale Kommunikation ermöglicht. Der Austausch zwischen Systemen, Geräten und Nutzern ist vielfältig und findet gleichzeitig im realen und im virtuellen Raum als Teil eines immer komplexer werdenden globalen Netzwerks statt. Herkömmliche digitale Sicherheit ist immer noch wichtig, aber Verschlüsselung reicht allein nicht mehr aus. Damit die echte vernetzte Welt kommunizieren und funktionieren kann, brauchen wir eine viel flexiblere und verlässlichere Architektur, die Technologien, Standards und Prozesse in einem umfassenden System des digitalen Vertrauens zusammenbringt.

Was ist digitales Vertrauen?

Digitales Vertrauen steht für Software und eine Reihe von Prozessen, die es innerhalb eines bestimmten Rahmens ermöglichen, dass Unternehmen, Behörden, Gremien und Einzelpersonen der digitalen Welt vertrauen können. Mit digitalem Vertrauen wird hauptsächlich auf die Anforderungen der vernetzten Welt reagiert, vor Bedrohungen geschützt und das Wachstum und die Evolution digitaler Technologien prognostiziert. Zu diesem Zweck basiert digitales Vertrauen auf vier Grundpfeilern:

Standards

Führende Fachleute und Organisationen definieren die Abläufe, Technologien und Anforderungen an die Identitätsprüfung für digitale Vertrauensdienste. So legt zum Beispiel das CA/Browser Forum Standards für TLS/SSL-Zertifikate sowie einen gemeinsamen Rahmen zur Zertifizierung von Identitäten und Verschlüsselung im Internet fest.

Compliance und Betrieb

Unter Compliance sind alle Richtlinien und kontinuierlichen Audits zusammengefasst, die die fraglichen Abläufe nach den genauen Vorgaben einer Aufsichtsstelle regeln. Im Betrieb – hier am wichtigsten: Rechenzentren – wird der Zertifikatsstatus per OCSP oder anderen Protokollen verifiziert.

Verwaltung des Zertifikatslebenszyklus

Unternehmen nutzen spezielle Software (für öffentliches und/oder privates Vertrauen), um von zentraler Stelle aus den Überblick und die Kontrolle über ihre digitalen Zertifikate zu behalten.

Bereitstellung in allen Infrastrukturen und Systemen

Hierunter versteht man die Ausdehnung des Konzepts von digitalem Vertrauen auf komplexe Lieferketten, ganze Gerätelebenszyklen, den Nachweis der digitalen Rechte einer Content-Community und auf jeden anderen Bereich, in dem ein Objekt vernetzt wird.

REALES VERTRAUEN IN DER REALEN WELT

Dass sich zwei Punkte einer digitalen Verbindung gegenseitig vertrauen können, davon träumt man schon seit Beginn der digitalen Kommunikation. Technologie und Idealvorstellung lagen aber bisher oft weit auseinander. Entweder passte die Hardware nicht zur Software, um Vertrauensprinzipien umzusetzen, oder umgekehrt. Echtes digitales Vertrauen ist sowohl Konzept als auch Prozess und Werkzeug. Hier werden digitale Technologien und Ideale zusammengebracht, um Nutzen zu bringen und echte Wirkung zu erzielen.

WIR BRAUCHEN EINE ARCHITEKTUR, DIE TECHNOLOGIEN, STANDARDS UND PROZESSE IN EIN SYSTEM DES DIGITALEN VERTRAUENS EINBINDET.

VERTRAUEN SICHERN IN ALLEN BEREICHEN

Sogar die Technik- und Sicherheitsexperten, die unsere Lösungen entwickeln, sind manchmal erstaunt über die Kreativität, mit der Anwender digitales Vertrauen einsetzen. Digitales Vertrauen zieht sich wie ein roter Faden durch scheinbar grundverschiedene Technologien und Branchen und ist ein bedeutender Bestandteil davon, wie wir in der echten Welt kommunizieren, uns bewegen und arbeiten.

LUFTFAHRT

Sanfter Start, sichere Landung

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

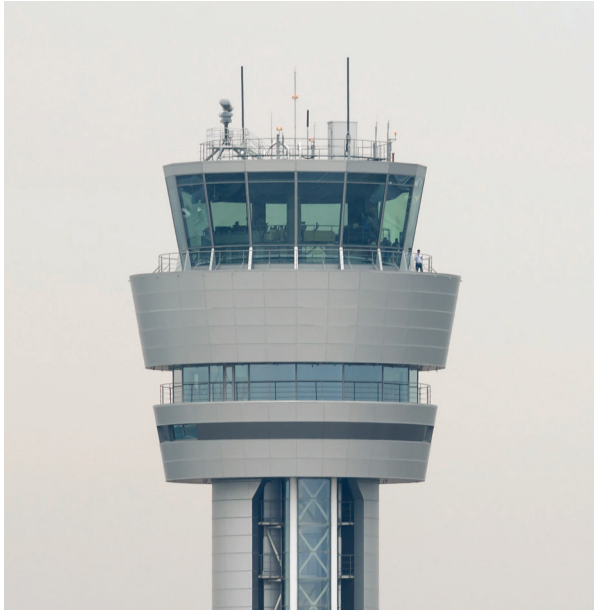
Unter dem Schutz dieser Geräte und ihrer Daten durch digitale Vertrauenslösungen können Piloten und Fluglotsen unabhängig vom jeweiligen Flugzeug oder Flughafen zuverlässig und sicher die verschiedenen Daten erfassen, weiterleiten und nutzen, die zum sicheren Starten und Landen gebraucht werden. Über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

Einsatz: weltweit

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

Grundbedürfnis: Authentifizierung

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



SEIT 2016 ERFOLGT DIE ÜBERMITTLUNG DIESER LEBENSWICHTIGEN INFORMATIONEN AN TOWER UND FLUGZEUGE WELTWEIT DURCH IoT-SENSOREN, DIE DURCH DIGITALES VERTRAUEN GESICHERT SIND.

LIEFERKETTEN

Identitätsprüfung für jedes Kettenglied

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.

Digitale Sicht

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 von Containern. 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 digitalem Vertrauen können Frachtcontainer auf dem gesamten Transportweg von der Verladung bis zum Zielhafen sicher verfolgt werden, unabhängig von der Anzahl der Transporte oder wo in der Welt sie sich befinden. Dadurch sinkt das Diebstahl- oder Verlustrisiko und steigt die Effizienz des Warenverkehrs von Hafen zu Hafen.

Einsatz: weltweit

Als Rückgrat der Lieferkette werden Güter und Rohstoffe in vernetzten Containern zu jedem Kontinent unseres Planeten transportiert.

Grundbedürfnis: Authentifizierung

Die Lösungen von DigiCert leisten 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 DIGITALEM VERTRAUEN KÖNNEN FRACHTCONTAINER AUF DEM GESAMTEN TRANSPORTWEG VON DER VERLADUNG BIS ZUM ZIELHAFEN SICHER VERFOLGT WERDEN.

GLOBAL ARBEITEN

Für jeden Nutzer, überall, zu jeder Zeit

Manchmal ist das Personalmanagement eines großen Unternehmens genauso kompliziert wie das Management der Produktionsabläufe. Wie sichert beispielsweise ein Unternehmen einzelne Benutzer, die nicht nur in internationalen Niederlassungen verschiedenen Aufgaben nachgehen, sondern dabei auch noch unterschiedliche Geräte mit jeweils anderen Betriebssystemen und Anwendungen nutzen – oftmals in Form von BYOD?

Für IBM war das nicht nur eine Denksportübung. Es war ein echtes Problem, mit dem sich das Unternehmen schon beschäftigen musste, lange bevor die COVID-19-Pandemie viele weitere Unternehmen zwang, Lösungen für die Telearbeit zu finden.

Bring-your-own – ja, was eigentlich?

Die Aufgabe: Authentifizierung, Identifizierung 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 digitalen Vertrauenslösung 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, Anbieter 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.

In solchen Fällen sind Flexibilität und Skalierbarkeit ausschlaggebend, d. h. die Eigenschaften, die grundlegender Teil von digitalem Vertrauen sind. Mit digitalen Vertrauenslösungen war IBM in der Lage, nicht nur beliebig viele Geräte unabhängig von deren Eigentümer und den darauf laufenden Anwendungen zu authentifizieren, sondern konnte dies gleichzeitig mit Hunderttausenden von Benutzern und ihren jeweils mehreren Geräten an beliebigen Standorten tun. Für alle 500.000 Benutzer fühlt sich dies vollständig reibungslos an.

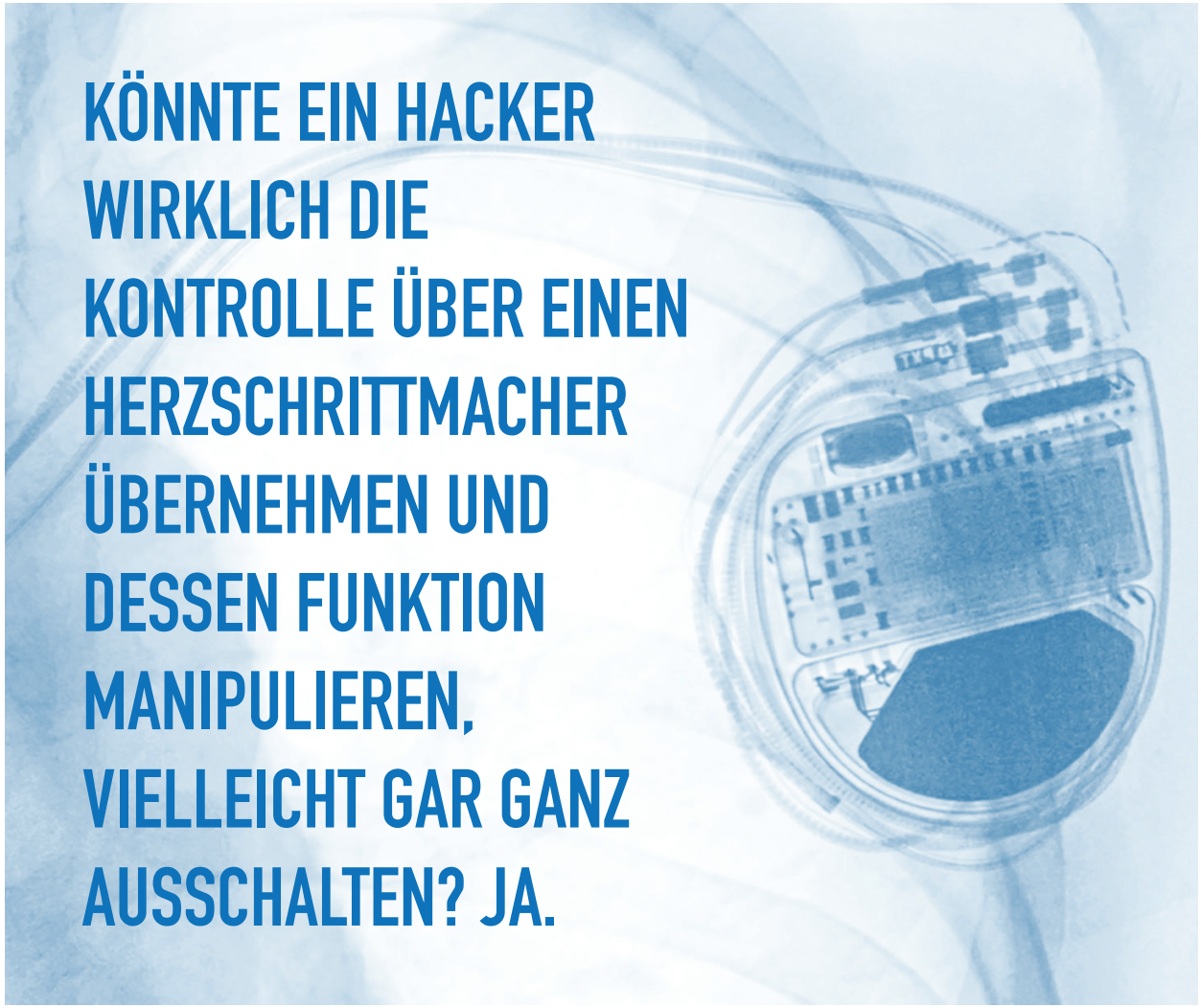
Einsatz: weltweit

Ein global führendes Traditionsunternehmen für Hardware und Software arbeitet über weltweit Tausende Standorte verteilt.

Grundbedürfnis: Flexibilität und Skalierbarkeit

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

IN EINER UMGEBUNG, IN DER SYSTEME, ARBEITNEHMER, ANBIETER UND ZULIEFERER MITEINANDER VERNETZT SIND, BRAUCHT ES EIN ANPASSUNGSFÄHIGES UND ROBUSTES SICHERHEITSSYSTEM.



GESUNDHEITSWESEN

Vertrauen als Mittelpunkt der medizinischen Versorgung

Digitale Geräte erleichtern unseren Alltag. 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. Diese Vernetzung ist für uns angenehm und praktisch, aber notfalls könnten wir auch darauf verzichten. Doch für manche Menschen stellt die Vernetzung den Unterschied zwischen Leben und Tod dar.

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 Funktionalität 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. Für Menschen mit diesen Herzschrittmachern ist digitales Vertrauen eine echte Notwendigkeit.

Wenn „Leben und Tod“ wörtlich zu nehmen ist

Im August 2017 tauchte in den Nachrichten eine ungewöhnliche Meldung 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 Handlung 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 Medizingeräten, vom smarten 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 hatten Hacker einen Angriffspunkt zum Eindringen in Herzschrittmacher gefunden. Die Hersteller hatten 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 digitale Vertrauenslösungen.

Heute können Tausende von 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 das digitale Vertrauen.

Einsatz: viele Länder weltweit

Genutzt werden diesen Technologien sowohl durch Dienstleister als auch durch Patienten in Tausenden Krankenhäusern und Pflegeeinrichtungen, von 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.

AUF BASIS BEWÄHRTER TECHNOLOGIEN

Ohne die zugrunde liegende Technologie ist „digitales Vertrauen“ nur eine leere Hülle. Für den Einsatz von digitalem Vertrauen in der echten Welt sind Software und Systeme nötig, die in dieser weiten und komplexen Landschaft eine sichere Vernetzung ermöglichen. Das darf nicht einfach nur irgendeine Technologie sein. Damit Vertrauen auch in der realen Welt entsteht, müssen Verbindungen bestimmte Merkmale aufweisen, die auf bewährter Sicherheitssoftware und entsprechenden Abläufen basieren.

Die drei Prinzipien einer sicheren Verbindung

Identität

Personen, Unternehmen, Maschinen, Workloads, Container, Services (und alles, was sonst noch vernetzt ist) müssen sich mit einer kryptografisch eindeutigen Identität authentifizieren.

Integritätsschutz

Objekte müssen mit Manipulationsabwehr ausgestattet sein, damit sie während der Nutzung und Übertragung geschützt sind, während Tools überprüfen, dass ein Objekt nicht manipuliert wurde.

Verschlüsselung

Daten müssen während der Übertragung geschützt werden.

DAMIT VERTRAUEN AUCH IN DER REALEN WELT ENTSTEHT, MÜSSEN VERBINDUNGEN AUF BEWÄHRTER SICHERHEITSSOFTWARE UND ENTSPRECHENDEN ABLÄUFEN BASIEREN.

PKI ALS FUNDAMENT

Public Key Infrastructure (PKI) bewährt sich bei der Absicherung von Websites schon seit Jahrzehnten. Während sich die vernetzte Welt entwickelte, erkannten Experten für digitale Sicherheit, dass dieselbe Technologie, die sich auch bei der Verschlüsselung von Websites bewährt hatte, auch für die Verifizierung digitaler Identität bei der Datenauthentifizierung genutzt werden kann. Diese Zertifikate können für fast alle digitale Objekte – von Netzwerken bis E-Mails, Codes bis Dokumenten und selbst Benutzern und Geräten – ausgestellt werden. PKI bietet Verschlüsselung, Integritäts- und Identitätsschutz für digitale Verbindungen und ist daher grundlegender Bestandteil des digitalen Vertrauens. Als dieser ist sie in der Lage, jede Herausforderung zu meistern.

Flexibilität

Heutige IT-Experten brauchen ein System, mit dem sie Webseiten 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 die Technologie auf asymmetrischen Schlüsselpaaren basiert und der Sicherheitsprozess sowohl für die Verschlüsselung als auch für die Validierung 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, lokal 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.

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. PKI 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.

LASSEN SIE DIGITALES VERTRAUEN FÜR SICH ARBEITEN

Die wichtigste Eigenschaft von digitalem Vertrauen wird meist übersehen. Digital bedeutet nicht mehr digital. Im Zentrum des digitalen Vertrauens befindet sich etwas, das schon seit jeher die Grundlage von Geschäften, Verträgen, gesellschaftlichen Übereinkünften und einfachen menschlichen Interaktionen bildet. Egal, in welchem Raum – ob physisch oder virtuell – wir uns bewegen, wir müssen wissen, dass unsere Interaktionen authentisch sind, unsere Kommunikation sicher ist und die Informationen, die wir austauschen, echt und unverändert sind.

Digitales Vertrauen ist mehr als eine intellektuelle Übung und auch mehr als eine Sicherheitssoftware. Es ist das Vertrauen in Interaktionen zwischen allem und allen Vernetzten. Es ist also wichtiger, wie digitales Vertrauen genutzt werden kann, als was es ist.

Über DigiCert

Als einer der führenden Anbieter digitaler Vertrauenslösungen sorgt DigiCert dafür, dass Einzelpersonen, Unternehmen, Behörden und Gremien digitalen Interaktionen in dem Wissen vertrauen können, dass ihre digitale Infrastruktur und ihre Anbindung an eine Welt voller Online-Transaktionen sicher und geschützt sind.

DigiCert® ONE, das Fundament für digitale Vertrauensdienste, bietet Unternehmen eine zentrale Anlaufstelle für Einblicke und die Kontrolle über eine Vielzahl von digitalen Anwendungsbereichen, in der das Vertrauen eine wichtige Rolle spielt. Dazu gehören der sichere Zugriff auf Unternehmenssysteme, sichere Business-Kommunikation sowie der Schutz von Websites, Software, Identitäten, Inhalten und Geräten. Wir bei DigiCert bieten nicht nur preisgekrönte Softwarelösungen an, sondern haben uns nicht zuletzt auch durch unsere branchenweite Führungsrolle bei Standards, Support und Betrieb als bevorzugter Anbieter bei Unternehmen auf der ganzen Welt einen Namen gemacht, die Vertrauen für sich arbeiten lassen.

Wie können Sie digitales Vertrauen für Ihr Unternehmen arbeiten lassen? Weitere Informationen erhalten Sie per E-Mail an sales@digicert.com.