Hohe Anforderungen an Datenschutz und Datensicherheit

Das Thema Datenschutz bedarf einer vielschichtigen Sicherheitsarchitektur, die Aspekte der Sicherheit bereits im Entstehungsprozess von Produkten integriert. NXP Semiconductors hat eine Reihe von Empfehlungen formuliert und Produkte entwickelt, die vor Cyber-Attacken schützen und die Sicherung personenbezogener Daten gewährleisten können.

Fachartikel von Marc Gebert, Johannes Berg, Janine Dobelmann

Im Jahr 2015 lag die Wahrscheinlichkeit für Unternehmen, Daten aufgrund von Cyberattacken zu verlieren, bei rund 20 Prozent. Künftig müssen Unternehmen stärker als bisher dafür Sorge tragen, solche „Datenpannen" zu vermeiden. Mit der neuen EU-Datenschutzgrundverordnung, DSGVO (englisch: GDPR), die am 25. Mai 2018 in Kraft tritt, kommen auf Unternehmen neue technische und organisatorische Anforderung in punkto Datenschutz und Datensicherheit zu. Ansonsten drohen empfindliche Strafen von bis zu vier Prozent des weltweiten Jahresumsatzes. Die Verordnung gilt für alle Unternehmen, die in der europäischen Union ansässig sind oder EU-Bürgern Waren und Dienstleistungen anbieten.

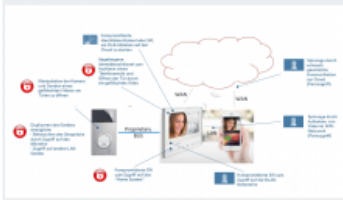

Bild 1: Geräte, Datenströme und Angriffspunkte am Beispiel einer vernetzten Türklingel.
(Bild: NXP)

Die DSGVO kommt zu einer Zeit, in der das Vertrauen in das sogenannte Internet der Dinge (IoT) aufgrund von zahlreichen Cyberattacken nachhaltig Schaden zu nehmen droht. Vor dem Hintergrund eines global wachsenden IoT-Markvolumens, das von Experten auf bis zu 40 Milliarden vernetzter Geräte bis 2020 sowie einem weltweiten wirtschaftlichen Mehrwert von bis zu 11 Billionen Dollar im Jahr 2025 taxiert wird, ist es für Unternehmen unerlässlich, die Bedenken der Nutzer ernst zu nehmen und schnellstmöglich wirksame vertrauensbildende Maßnahmen zu ergreifen. Die DSGVO ist hier ein entscheidender Meilenstein, um in einem bisher kaum regulierten IoT-Markt für ein Mindestmaß an Sicherheit und Datenschutz zu sorgen.

ECKDATEN

Um die Vorgaben der DSGVO zu erfüllen, bedarf es sicherer Hardwarekomponenten und dazu passender Softwarelösungen, die dabei helfen, intelligente Geräte und Anwendungen in den Zustand Secure by Design zu versetzen. Der Artikel geht auf die neue Verordnung ein und auf die Produkte und Aktivitäten von NXP zur Datensicherung.

Schutz persönlicher Daten

Im Mittelpunkt des neuen EU-Gesetzes steht der Schutz persönlicher Daten von natürlichen Personen, also unter anderem Kunden. Die DSGVO definiert Grundsätze, die bei der Verarbeitung dieser Daten berücksichtigt werden müssen. Dazu gehören Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Integrität und Vertraulichkeit. Das heißt zum Beispiel, dass Unternehmen, die persönliche Daten verarbeiten, künftig die Einwilligung der Betroffenen dazu einholen müssen. Darüber hinaus müssen Zweck und Dauer der Verarbeitung klar definiert werden. Das Recht an den eigenen Daten der Nutzer wird somit deutlich gestärkt.

Eine weitere Neuerung stellt insbesondere die Pflicht zu verbraucher- und datenschutzfreundlichen Voreinstellungen (Privacy by Default / Privacy by Design) bei elektronischen Geräten dar. Vernetzte Geräte wie Fitnessarmbänder, Smart-TV und -Kameras produzieren oftmals große Mengen an personenbezogenen Daten, die häufig gänzlich ungeschützt an Backend-Systeme wie Clouds weitergeleitet werden. Die DSGVO fordert nun von den Herstellern solcher Geräte die Ergreifung technischer Maßnahmen, beispielsweise die Verschlüsselung dieser Daten. Darüber hinaus umfasst die DSGVO Forderungen zu Pseudonymisierung, der sicheren Aufbewahrung der Schlüssel, sicherer Geräte-Identitäten und -Integrität sowie abgesicherten Kommunikationskanälen.

Angesichts der drohenden, sehr hohen Strafzahlungen in Fällen von Nichteinhaltung der DSGVO-Vorgaben ist es für Hersteller ratsam, sich bereits im Entwicklungsprozess Gedanken zu machen, welche Nutzerdaten die Geräte erfassen und zu welchem Zweck diese verarbeitet werden sollen. Nur so können die Anbieter von Geräten, Lösungen und Services ihre Produkte fit für die Zukunft machen und Vertrauen für das Internet der Dinge gewinnen. Dabei können dem Stand der Technik entsprechende Security-Lösungen helfen, die Erhebung und Speicherung der Daten im Einklang mit den Anforderungen der DSGVO durchzuführen.

Nächste Seite: Smart Home, Datenökonomie & Co.

Im Zuge der zunehmenden Vernetzung und Digitalisierung von Lebens- und Arbeitsbereichen gewinnen Geschäftsmodelle, deren Grundlage die Erhebung und Analyse von Daten ist, rapide an Bedeutung. Neben intelligenten Fabriken, autonom fahrenden Fahrzeugen oder smarten medizinischen Anwendungen produziert auch das Smart Home immer größere Mengen personenbezogener, schützenswerter Daten. Dabei geht es sowohl um die Frage, wie Daten von Unternehmen genutzt werden, als auch um die Absicherung der Datenkommunikation von Geräten wie internetfähigen Kameras, Kühlschränken oder gar digitalen Türschlössern in die Backend-Systeme. Geraten diese Daten auf illegalen Wegen, zum Beispiel durch Hacks, in die falschen

Bild 2: Umsetzung von Security & Privacy by Design am Beispiel einer vernetzten Türklingel.

Hände, reichen die Konsequenzen von unerwünschter, personalisierter Werbung bis hin zu Wohnungseinbrüchen. Dazu kommt die psychologische Komponente, dass Verbraucher sich durchleuchtet und „verfolgt“ fühlen könnten.

(Bild: NXP)

Derartige Zukunftsvisionen – vom Smart Home bis zum IoT im Allgemeinen – erfordern von Unternehmen und Verbrauchern ein besseres Verständnis von möglichen Sicherheitsgefährdungen und entsprechenden Maßnahmen zum Datenschutz.

Aus der Ferne oder ganz nah

Angriffe oder Attacken auf Geräte oder Systeme – auch Cyberangriffe genannt – lassen sich zwischen Angriffen, die aus räumlicher Distanz (englisch „remote attacks“) oder vor Ort am System oder Gerät (englisch „local attacks“) ausgeführt werden, unterscheiden. „Remote attacks“ erfolgen über eine Netzwerkverbindung, der Angreifer muss dabei nicht physikalisch am Gerät oder in der Nähe sein. Diese Angriffe können sehr lukrativ sein: Durch den erfolgreichen Angriff auf einen PC oder ein IoT-Gerät hat der Angreifer die Möglichkeit, Millionen Geräte zu erreichen.

„Local attacks” hingegen erfordern einen physischen Zugang. Dadurch können Geräte sehr gezielt, aber nur in geringer Anzahl angegriffen werden. Es ist jedoch möglich, dass durch einen Angriff an einem Gerät auch ein Zugriff auf den gesamten Software-Code gelingt. Die Analyse dieses Codes führt dann möglichweise zur Aufdeckung von Schwachstellen, über die ähnliche Geräte aus der Distanz attackiert werden können. Eine Vielzahl der bekannten „remote“ Cyberangriffe lassen sich zurückführen auf den zuvor erfolgreich ausgeführten physikalischen Angriff auf ein Gerät.

Im Haus installierte IP-Kameras könnten aufgrund mangelnder Verschlüsselung der Videodaten oder bekannter Passwörter angegriffen beziehungsweise gehackt werden. Die daraus gewonnenen Daten könnten benutzt werden, um An- und Abwesenheiten zu protokollieren und somit eventuelle Einbrüche vorzubereiten. Ein weiteres Einfallstor für einen Angriff stellt die zentrale Steuereinheit des Hauses dar. Durch das Einbringen einer Schadsoftware, entweder durch einen nicht vertrauenswürdigen Auftragsfertiger des Herstellers oder durch ein manipuliertes Software-Update, könnten diverse Angriffe auf das Steuerungssystem des Hauses oder sogar auf die Cloud-Infrastruktur des Herstellers erfolgen. Eine Komponente, ein Gerät oder System kann während seines kompletten Lebenszyklus angegriffen werden, und zwar aus der Entfernung oder lokal.

Die unterschiedlichen Angriffsszenarien lassen sich vom Smart Home auch ohne weiteres auf eine Vielzahl von weiteren IoT-Anwendungen erweitern. Dieser Umstand sowie auch die unterschiedlichen Zeitpunkte für einen Angriff zeigen, dass das Thema Datenschutz einer vielschichtigen Sicherheitsarchitektur bedarf, die Aspekte der Sicherheit bereits im Entstehungsprozess von Produkten integriert.

Wie Security by Design zum Schutz vor Angriffen beiträgt

NXP Semiconductors hat eine Reihe von Empfehlungen formuliert und Produkte entwickelt, die vor den oben skizzierten Angriffen schützen und die Sicherung personenbezogener Daten gewährleisten können. Zum einen sollten bei der Systemarchitektur die jeweiligen Schlüssel und Kryptofunktionen von den nicht sicherheitskritischen Operationen isoliert werden. Sie müssen in einem manipulationssicheren („tamper resistant“) Speicher (zum Beispiel Sicherheitschip) abgelegt werden (Bild 2).

Um Geräte über die Cloud zu aktualisieren, sollte die Kommunikation zwischen der Cloud und den verbundenen Geräten gegen Manipulation geschützt (Gewährleistung der Integrität) und verschlüsselt sein. Darüber hinaus sollte sowohl eine sichere Geräte-Identifikation als auch eine sichere Benutzer-Authentifizierung vorhanden sein. Die Authentifizierung von Benutzer und Gerät sollte jedoch aus datenschutzrechtlichen Gründen voneinander unabhängig erfolgen. Zudem ist es zu vermeiden, denselben privaten oder symmetrischen Schlüssel in mehr als einem Gerät zu verwenden oder für mehr als einen einzigen Zweck zu nutzen. Geräte sollten in der Lage sein, sich selbst zu schützen, indem sie sich nur mit authentifizierten und damit vertrauenswürdigen Hosts oder Gateways verbinden können. Derartige Gateways werden von NXP beispielsweise in intelligenten Stromzählern (Smart Metern) eingesetzt und tragen schon heute dazu bei, dass diese Geräte den höchsten regulatorischen Anforderungen an Sicherheit und Datenschutz gerecht werden.

Können nicht alle gewünschten Gegenmaßnahmen implementiert werden, sollten die Geräte keine eingehende Netzwerkverbindung akzeptieren, sondern den Server oder das Gateway aus eigener Initiative abfragen. Dies reduziert die Angriffsfläche für „Remote“-Angriffe. Dies setzt natürlich voraus, dass die Geräte über ausreichende Kapazitäten verfügen, um eine sichere Verbindung zum Server oder Gateway aufzubauen. Und schlussendlich müssen Geräte während ihrer Lebensdauer Sicherheitsupdates erhalten. Wenn dieser Service beendet wird, ist das Lebensdauerende des Gerätes erreicht.

Nächste Seite: Datenverschlüsselung: Ein wichtiger Baustein zur Einhaltung der DSGVO

Neben der beschriebenen, hardwareseitigen Absicherung eines Systems sind auch Praktiken zur Datenverschlüsselung unabdingbar. Wie bereits beschrieben, fungiert die DSGVO hier als eine Art Katalysator, um Datenschutzprobleme bei der Gestaltung von neuen Produkten und Lösungen direkt und wirksam anzugehen. Authentifizierung in Kombination mit Verschlüsselung ist eine Möglichkeit, die Daten und die Kommunikation zu sichern. Im Falle des Smart Home heißt dies, dass zum Beispiel nur das für die Abrechnung zuständige Energieversorgungsunternehmen die Abrechnungsdaten der Kunden entschlüsseln kann. Ebenso sollte eine Produktionsmaschine nur die für ihren Produktionsschritt notwendigen Daten „lesen“ und nutzen können. Die für die Umsetzung

solcher Anforderungen erforderlichen Technologien gibt es bereits: Sie basieren fast immer auf dem Einsatz von kryptographischen Protokollen in Verbindung mit sicherer Hardware (beispielsweise der IEEE 1609.2-Standard für Fahrzeugkommunikation).

Eine grundsätzliche Eigenschaft dieser herkömmlichen Verschlüsselungsverfahren ist, dass Daten erst entschlüsselt werden müssen, bevor sie verarbeitet werden können. Die Kontrolle der Privatsphäre liegt also in den Händen des Empfängers der verschlüsselten Daten.

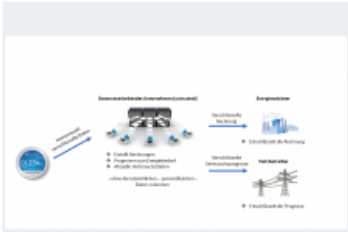

Bild 3: Homomorphe Verschlüsselung ermöglicht die Verarbeitung von verschlüsselten Daten.
(Bild: NXP)

Ein grundlegend anderer Ansatz ist es, sich auf die vollständig homomorphe Verschlüsselung zu verlassen. Der Empfänger kann dabei mit verschlüsselten Daten operieren, ohne diese vorab entschlüsseln zu müssen. NXP engagiert sich im Rahmen mehrerer Forschungsprojekte, unter anderem dem Homomorphic Encryption Applications and Technology sowie dem Projekt Flex4Apps, auf EU-Ebene zu diesem Thema. Als Projektpartner untersucht NXP, wie der Schutz empfindlicher Smart-Meter- und Sensormesswerte durch homomorphe Verschlüsselungsverfahren erreicht und gleichzeitig bestehende Systemvoraussetzungen gewährleistet werden können. Der vorgeschlagene Ansatz ermöglicht es den Netzbetreibern, den Energiebedarf durch die Berechnung verschlüsselter Daten zu kalkulieren, sodass sie den Energiebedarf für den Lastausgleich genau prognostizieren können. Informationen über individuelles Verbraucherverhalten sind dazu nicht notwendig (Bild 3) Dieses neue Verschlüsselungsverfahren ist ein weiterer Schritt, um IoT-Geräte gegen Angriffe abzusichern und personenbezogene Nutzerdaten besser zu schützen.

Sichere Hardware- und Softwarelösungen

Um die Vorgaben der DSGVO zu erfüllen, bedarf es sowohl sicherer Hardwarekomponenten als auch dazu passender Softwarelösungen, die dabei helfen, intelligente Geräte und Anwendungen in den Zustand Secure by Design zu versetzen. Darüber hinaus sind die sichere Aufbewahrung von Schlüsseln, zum Beispiel in manipulationssicheren Hardwarebausteinen, die Erstellung einer individuellen Geräteidentität, die Möglichkeit sicherer Benutzeridentitäten unter Wahrung der Privatsphäre-Einstellungen des Benutzers sowie die Gewährleistung sichere Kommunikationskanäle durch Datenverschlüsselung wichtige Maßnahmen.

NXP Semiconductors bietet die dafür notwendigen Technologien – von Mikrocontrollern und Prozessoren mit sicheren Hardware- und Softwarekomponenten über hochsichere Mikrocontroller für IoT-Geräte bis hin zu RFID-Produkten, fortschrittlichen Smartcards, NFC-Technologien und Software, die dabei helfen, die regulatorischen Vorgaben der DSGVO zu erfüllen und das Vertrauen in vernetzte Geräte zu stärken.

(ah)

ÜBER DIE AUTOREN

Marc Gebert
Senior Director, IoT Security Business Development Global Sales & Marketing bei NXP Semiconductors

Johannes Berg
Senior Project Manager Cooperative Innovation Projects bei NXP Semiconductors

Janine Dobelmann
Manager Political Affairs bei NXP Semiconductors

● WEITERE INFOS

NXP Semiconductors Germany GmbH

Schatzbogen 7

81829 München

Deutschland

Zum Firmenprofil ›