IoT-Sicherheitsrisiken erfolgreich meistern

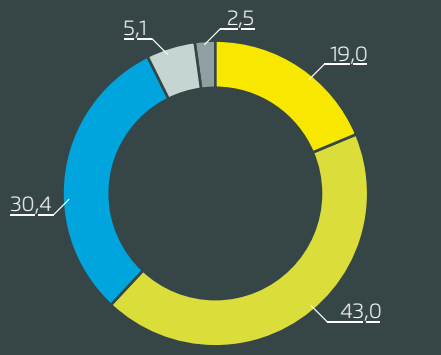
IoT-Sicherheitsrisiken erfolgreich meistern

In diesem Whitepaper setzen wir uns eingehend mit möglichen IoT-Sicherheitsrisiken und ihren Lösungen auseinander. Wir zeigen, warum IoT-Sicherheit gesondert betrachtet werden sollte und warum zahlreiche Projekte durch Sicherheitsrisiken behindert werden. Zudem erklären wir, welche Bedrohungen Projekte gefährden können und wie man sie dennoch realisiert.

IoT-Projekte bringen bedeutende Erfolge. Wie eine Studie der Lemonbeat GmbH zusammen mit IDG Research Services aus dem Jahr 2017 zeigt, sind zwei Drittel der Unternehmen mit dem Erfolg ihrer in unterschiedlichsten Bereichen durchgeführten IoT-Projekte zufrieden – besonders in Hinblick auf erhöhte Produktivität, geringere Ausfallzeiten, reduzierte Kosten, ROI, Umsatz und Verbesserung des Unternehmensimages.

Wie zufrieden sind Sie mit den Ergebnissen der durchgeführten IoT-Projekte

Angaben in Prozent. Basis: n = 81



- Sehr zufrieden
- Zufrieden
- Eher zufrieden
- Eher nicht zufrieden
- Nicht zufrieden
- Gar nicht zufrieden (keine Nennungen)

Warum hat sich Ihr Unternehmen noch nicht mit dem Thema Internet of Things (IoT) auseinandergesetzt?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n=64

Das Thema ist für unser Unternehmen nicht relevant	41,2
Derzeit andere Prioritäten	37,5
Kein Mehrwert	25,0
Fehlendes Geschäftsmodell	25,0
Fehlendes Know-how	21,9
Sicherheitsrisiko	18,8
Unsicherheit in Bezug auf künftige Entwicklung des IoT	14,1
Zu hohe Kosten	12,5
Unreife Technik	12,5
Unsicherheit in puncto künftige Kundenbedürfnisse	12,5
Keine vernünftigen Integrationsplattformen	7,8
Unbeherrschbarer Datenwust	4,7
Aus anderen Gründen	1,6

Von diesen Vorteilen profitieren natürlich nur jene, die handeln. Warum also nutzen 80 % der 385 Studienteilnehmer aus branchenübergreifenden Unternehmen in Deutschland noch immer nicht die Möglichkeiten des IoT? Wie zu erwarten gibt es mehrere Ursachen, aber immerhin 19 % nennen „Sicherheitsrisiken" als Grund für ihre Zurückhaltung bei IoT-Projekten. Welche Risiken und Gefahren sehen Unternehmen im IoT? Sind sie gerechtfertigt? Und wenn ja, wie können sie überwunden werden?

Was Sie auf den folgenden Seiten erwartet:

- Die Umfrageergebnisse zum Thema IoT-Sicherheit und Konsequenzen
- Was macht IoT-Sicherheit so besonders im Vergleich zur klassischen IT-Sicherheit?
- Häufige IoT-Bedrohungen und angemessene Gegenmaßnahmen
- Eine Anleitung zum systematischen Umgang mit IoT-Sicherheit

Welche IoT-Sicherheitsprobleme sehen Unternehmen?

„In punkto IoT stehen Unternehmen vor einer gewaltigen neuen Sicherheitsherausforderung. Unnötigerweise wird dadurch die Durchführung von Projekten behindert."

Dr. Jens Reinelt,
CTO Lemonbeat GmbH

Die Angst der Unternehmen beim Thema IoT-Sicherheit ist nicht unbegründet: Organisationen, die bereits ein Projekt durchgeführt haben, benennen – neben generellen Hindernissen bei der Projektdurchführung – drei sicherheitsrelevante technische Herausforderungen: 43,9 % sehen die generelle Sicherheit (neues Einfallstor für Kriminelle), 39 % die Datensicherheit und Disaster Recovery und 29,7 % die Betriebssicherheit als großes technologisches Problem. 51 % der Studienteilnehmer bewerten Risiken bezüglich der Informationssicherheit als sehr hoch oder hoch. Risikobewertungen für die Sicherheit von Produktionsanlagen (49 %) und Datenschutz (48 %) fallen ähnlich aus. Und rund 45 % der Unternehmen fürchten Risiken bei der Sicherheit von Produkten, der Sicherheit von Anlagen- und Produktdaten sowie der Integrität und Korrektheit von Daten- und Servicefunktionalitäten.

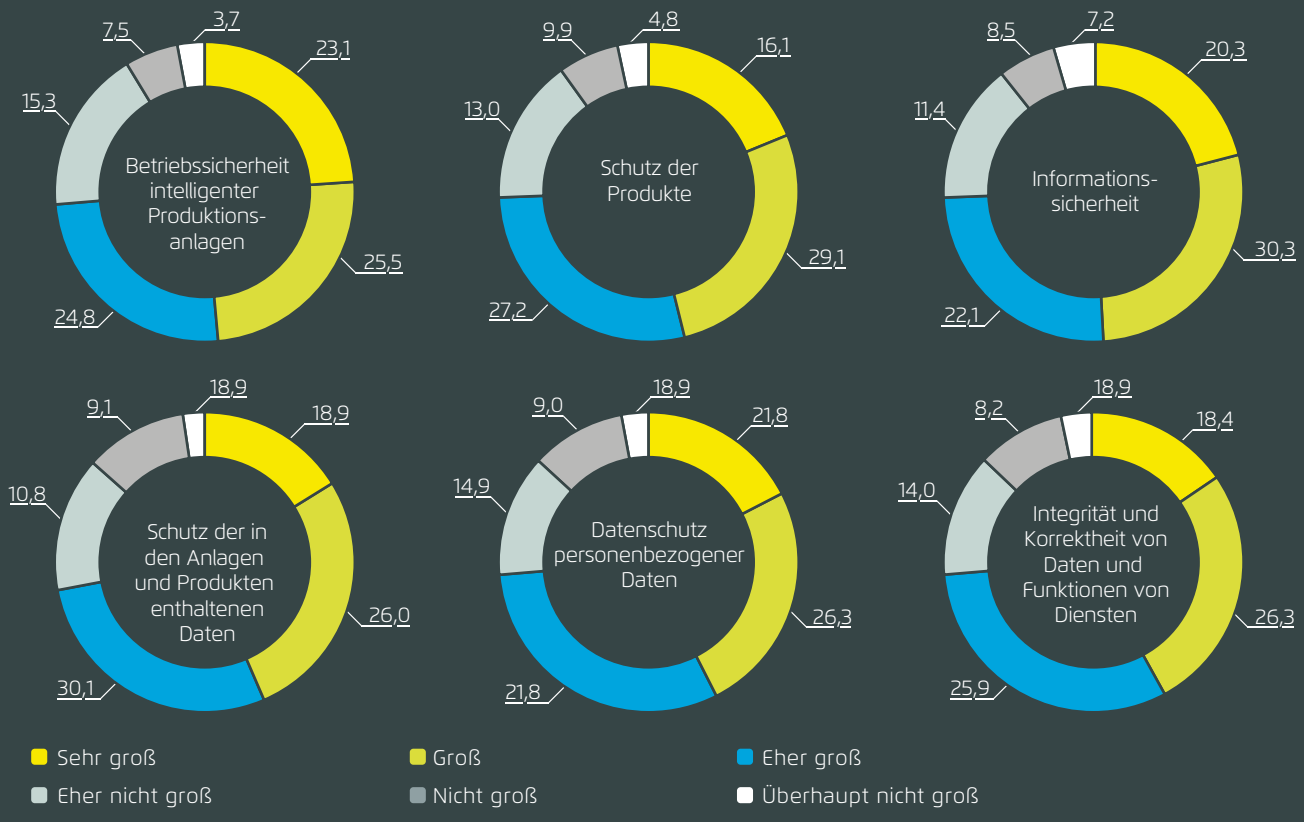
Was sind die größten technologischen Herausforderungen in Bezug auf IoT bzw. bei der Umsetzung von IoT-Projekten?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 310

Security (neues Einfallstor für Kriminelle)	43,9
Datensicherheit/Disaster Recovery	39,0
Safety/Betriebssicherheit	29,7

Als wie hoch stufen Sie die Sicherheitsrisiken durch IoT ein?

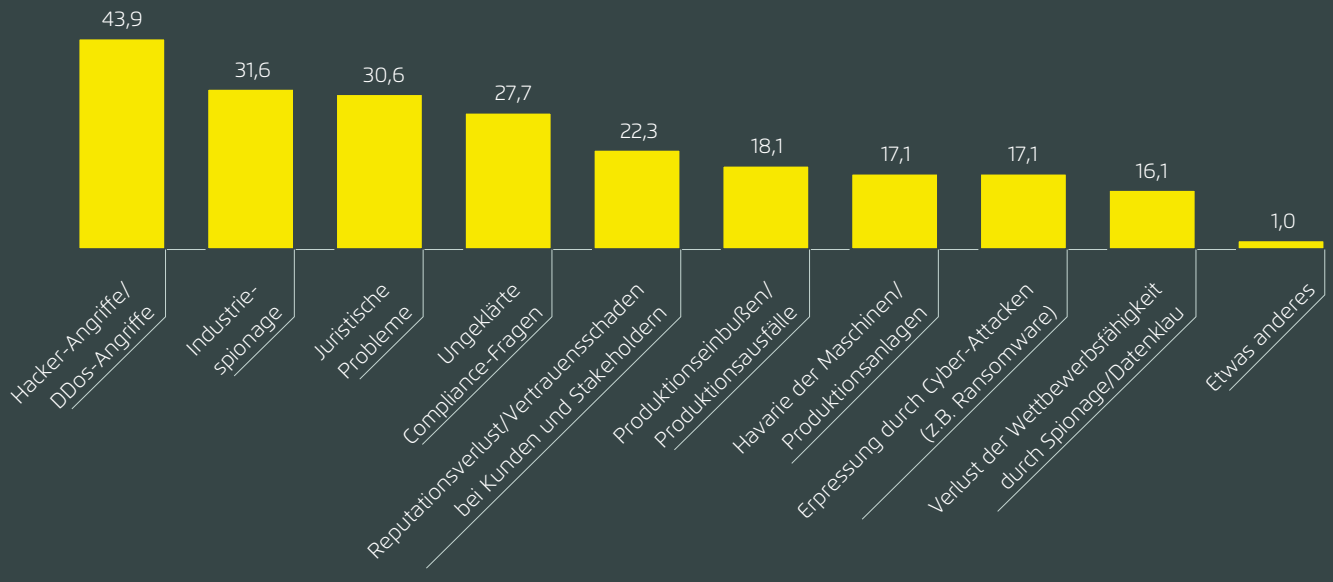
Angaben in Prozent. Bewertung auf einer Skala von 1 (Sehr groß) bis 6 (Überhaupt nicht groß). Basis: n = 309



Welche Ängste speisen diese Risikobewertungen? Die größte Angst besteht vor DDoS- und anderen Hackerangriffen (43,9 %) sowie vor Industriespionage (32 %). Juristische Probleme (31 %) und Compliance-Fragen (28 %) sind dicht auf, gefolgt von Reputationsverlust (22 %), Produktionsausfall (18 %) und Erpressung durch Cyber-Attacken (17 %).

Sicherheit gilt als eines der Hemmnisse beim Thema IoT. Was fürchten Sie für Ihr Unternehmen am meisten?

Angaben in Prozent. Mehrfachantworten möglich, Basis: n = 310



Die oben aufgeführten Umfrageergebnisse zeigen, dass Sicherheit (security), Produktsicherheit (safety) und Datenschutz Themen sind, die bei einer merklichen Anzahl an Projekten die Durchführung verhindern. Aber warum spielen diese Themen eine so große Rolle in einem Umfeld, das sich seit Jahrzehnten mit Computernetzwerken und somit auch mit IT-Sicherheitsmaßnahmen auskennt? Auf den nächsten Seiten finden Sie die wichtigsten Fakten über die besondere Komplexität der IoT-Sicherheit und einen Leitfaden zum Umgang damit.

Warum IoT-Sicherheit neue Fragen aufwirft

Seit Jahrzehnten ist die IT-Sicherheit ein Schlachtfeld, auf dem Kriminelle den Antivirenprogrammen und Sicherheitsspezialisten oft einen Schritt voraus sind, während Administratoren und Entwickler versuchen, sich vor den nie endenden Angriffen zu schützen. Wie groß müssen die Herausforderungen daher im IoT-Bereich sein, wo virtuelle und physische Welt verschmelzen und somit oft noch ungeschützte Flanken existieren? Hier treffen zwei unterschiedliche Welten mit ganz eigenen Herausforderungen aufeinander. Die entscheidende Frage ist: Haben die Experten beider Welten genügend Wissen über den jeweils anderen Bereich, um im Kampf gegen kriminelle Eindringlinge gut positioniert zu sein.

Auf der einen Seite stehen IT-Sicherheitsexperten, die zumeist über herausragende Kenntnisse auf ihrem Gebiet verfügen. Die Sicherung von Netzwerken und das Einhalten von grundlegenden Sicherheitsprinzipien wie Vertraulichkeit, Integrität und Nachweisbarkeit sind für sie keine Herausforderung. Wenn es bei physischen IoT-Geräten jedoch um Aspekte wie Sicherheitsdesigns und Fehlertoleranz im Sinne des Produktsicherheitsgesetzes geht, sind sie mehr oder weniger Anfänger. Auf der anderen Seite stehen Ingenieure verschiedener Disziplinen (Chemie, Elektronik, Mechanik, Automotive usw.), die Experten darin sind, ihre Produkte gemäß dem Produktsicherheitsgesetz für Kunden sicher zu gestalten. Gerätesteuerung sowie Datenerfassung und -übertragung über das Internet und die damit verbundenen Sicherheitsprobleme sind für sie jedoch häufig Neuland.

Sicherheitsexperten könnten natürlich versuchen, das notwendige Wissen aus der Ingenieurswelt zu erlangen. Aber diese Welt ist so vielfältig, dass dies ein aussichtsloses Unterfangen wäre. Vielmehr ist eine enge Zusammenarbeit beider Seiten sinnvoll, um Ingenieure mit den notwendigen Instrumenten der Sicherheitsbranche vertraut zu machen, damit sie beim Planen von Produkten von Anfang an beides, IT-Sicherheit und Produktsicherheit, im Blick haben. Frühzeitig auf mögliche Sicherheitsprobleme vorbereitet zu sein und solide und ökonomisch sinnvolle Maßnahmen zu ergreifen, ist der einzige Weg, um eine effektive, aber auch bezahlbare Sicherheit im IoT zu erreichen. Welche Maßnahmen bezahlbar und vernünftig erscheinen, hängt jedoch stark davon ab, welche intelligenten Dinge in welchem technischen Bereich produziert werden.

Am Ende ist jedes Gerät oder System nur so stark wie sein schwächstes Glied. Daher müssen alle am Lebenszyklus eines IoT-Geräts beteiligten Parteien bedenken, dass Sicherheit im IoT nur machbar ist, wenn sich alle verantwortlich fühlen – vom Drittanbieter über den Produkthersteller bis zum Cloud-Anbieter. Zudem wäre eine engere Zusammenarbeit der unterschiedlichen Ingenieursdisziplinen hilfreich. Die Gefahren, die der IoT-Welt und ihren Geräten drohen, richten sich nicht gegen ein bestimmtes Gerät oder Unternehmen oder eine einzelne Disziplin. Zumeist betrifft die Bedrohung eine größere Gruppe.

Im schlimmsten Fall kann ein einziger angreifbarer intelligenter Sensor in einer Schule, einem Krankenhaus oder sogar einem Atomkraftwerk Zugang zum Netzwerk bieten und somit potenzielle Risiken und Gefahren mit sich bringen.

Angriffe auf das IoT

Häufige Angriffe gegen IoT-Geräte und geeignete Gegenmaßnahmen.

Kabelloses und -gebundenes Scanning und Mapping

Angriffsmethode:

Dabei werden dieselben Paradigmen wie bei regulären Netzwerk-Scanangriffen verwendet, um drahtlose Kommunikationsprotokolle anzugreifen und so Informationen über IoT-Geräte zu erlangen.
Risiko: Kontrollübernahme, z. B. über Licht, Türöffner usw.

Gegenmaßnahmen:

- Präventiver Netzwerkport-Scan
- Präventive Schwachstellenüberprüfung

Protokollbezogene Angriffe

Angriffsmethode:

Jedes Protokoll hat seine Sicherheitsbeschränkungen. Ein mögliches Schlupfloch ist beispielsweise der Pairing-Prozess, bei dem Netzwerkschlüssel während des Austauschs anfällig für Sniffing sind.
Risiko: Verlust von Vertraulichkeit.

Gegenmaßnahmen:

- Wissen um die Beschränkungen jedes verwendeten Protokolls
- Implementierung oder Verstärkung von ergänzenden Maßnahmen auf anderen Ebenen

Kryptographische Algorithmen und Schlüsselmanagement-Angriffe

Angriffsmethode:

Zugriff auf Computer, Geräte oder Netzwerke durch kompromittierte Schlüssel.
Risiko: Entschlüsselung und somit Änderung von Daten.

Gegenmaßnahmen:

- Starke Verschlüsselung basierend auf Kryptographie
- Zählermodi
- Digitale Signaturen
- Zufallszahlenerzeugung
- Blockchain-Modi

Lauschangriff

Angriffsmethode:

Abhören des Datenverkehrs zwischen Geräten oder Geräten, Gateway und Cloud um Zugang zum Netzwerk zu erlangen.
Risiko hier: Verlust der Vertraulichkeit.

Gegenmaßnahmen:

- Prüfung der wichtigsten Binärdateien
- Entfernung ungenutzter Services
- Vollständig verschlüsselte Kommunikation

Denial of Service und Blockieren

Angriffsmethode:

Der Versuch, das Verhalten von Computern, Applikationen und Services zu stören oder diese zum völligen Stillstand zu bringen, indem sie mit einer Welle ungültiger Daten geflutet werden. Desweiteren das Blockieren des Datenverkehrs, um autorisierten Nutzern den Zugriff zu verwehren.

Gegenmaßnahmen:

- Kontinuität bei der Betriebsplanung (COOP)
- Ausreichenden Datendurchsatz für jeden Knotenpunkt gewährleisten, um DoS Attacken zu widerstehen
- Sicherheitslücken in der Nachrichten- und Dateninfrastruktur sowie bei der Nutzung von Variablen schließen

Physische Sicherheitsangriffe

Angriffsmethode:

Diebstahl und Zerstörung physischer Geräte, um Zugang zu Prozessor, Speicher usw. zu erhalten.
Risiko: Erlangung sensibler Daten wie Schlüsselmaterial, Passwörter und Konfigurationsdaten.

Gegenmaßnahmen:

- Manipulationserkennung
- Manipulationsreaktionsmechanismus (z. B. automatische Speicherlöschung)
- Kryptographische Module zum Schutz kryptografischer Variablen
- Vermeidungsplanung
- Passwortgeschützte Debug-Ports
- Keine fest codierten Passwörter
- Implementierung nur absolut wichtiger physikalischer Ports (z. B. USB)

Zugriffskontrollangriffe

Angriffsmethode:

Rechteausweitung durch Social Engineering und Rechteerhöhung sowie gefälschte Identitäten mithilfe gefälschter IP-Adressen und Phishing.
Risiko: Modifizieren, Umleiten oder Löschen von Daten.

Gegenmaßnahmen:

- Sensibilisierung der Mitarbeiter
- Assets auf ungewöhnliches Verhalten überprüfen
- Sensible Authentifizierungsstufen
- Sinnvolle Stufen für Administratorkompetenzen
- Trennung von administrativen Funktionen und Funktionen auf Benutzerebene

14 Punkte, die beim Erstellen vertrauens-würdiger IoT-Netzwerke beachtet werden sollten

Beim Planen und Entwerfen von IoT-Geräten und IoT-Systemen empfiehlt es sich, nicht nur IT-Sicherheit, sondern auch Produktsicherheit und Datenschutz im Blick zu haben. Zudem sollten alle Beteiligten immer alle Teile des Systems bedenken und dabei stets einen Gedanken im Hinterkopf haben: Beim Thema IoT-Sicherheit geht es nicht nur um den Verlust von Daten und Vertraulichkeit, sondern auch um Gefahren für den Menschen. Nicht nur Garagentore, sondern auch Herzschrittmacher können manipuliert werden.

Produktsicherheit ist ein klassischer Designaspekt in der Maschinenbauwelt. Da IoT-Geräte physische Dinge sind, ist es wichtig, ihre Produktsicherheit durch eine Risikobeurteilung zu gewährleisten, um mögliche Gefahren für Leib, Leben und Eigentum frühzeitig zu erkennen. Auf der anderen Seite werden IoT-Geräte oft verwendet, um Daten von verschiedenen Geräten zu aggregieren, die dann auf einem Gateway gesammelt und beispielsweise in die Cloud gesendet werden. Deswegen muss unbedingt an beiden Enden, den IoT-Geräten und dem Backend, eine sichere Kommunikationskonfiguration vorhanden sein. Hinsichtlich der IoT-Sicherheit ist es daher eine gute Idee, von Anfang an Bedrohungsmodellierung kombiniert mit Fehlerbaumanalysen einzusetzen. Beim Entwerfen eines Geräts oder Systems bedeutet Bedrohungsmodellierung, alle potenziellen Bedrohungen für einen Dienst oder ein System aufzuspüren und aufzulisten. Eine ergänzende Methode bieten Angriffsbäume, bei denen die Ausgangsfrage an anderer Stelle ansetzt: Wie würde ein Angreifer versuchen, Zugang zum Gerät oder System zu erlangen? Wie würde er es manipulieren oder beschädigen?

Bei der Planung für das IoT sollten Unternehmen Sicherheitsmaßnahmen daher von Anfang an in angemessenem Umfang planen. Was vernünftig erscheint und wie umfassend, tiefgreifend und ausgeklügelt Gegenmaßnahmen sein müssen, muss von Fall zu Fall diskutiert werden – abhängig von der Ingenieursdisziplin sowie den produzierten smarten Dingen und den damit verbundenen Sicherheitsproblemen und gefahren. Je größer die Risiken und potenziellen Schäden und je sensibler der industrielle Sektor oder das mögliche Einsatzgebiet, desto sorgfältiger sollten vorausschauende Planung und mögliche Gegenmaßnahmen durchdacht und angewendet werden.

Beachten Sie, dass die folgenden Empfehlungen nur einen Modellansatz für die Planung sicherer IoT-Projekte darstellen – wobei Sicherheit hier IT- und Produktsicherheit umfasst. Welche Aspekte relevant sind, muss in der Praxis für jeden Fall individuell entschieden werden.

Hardware-Design und Planung:

1. Drittanbieter in die Planung einbeziehen.
   Zusammenarbeit mit Drittanbietern über SLA und Datenschutzvereinbarungen sowie eine genehmigte Liste für Soft- und Hardware von Drittanbietern.

2. Wählen Sie gute und geeignete MCU und RTOS.
   Eine gute MCU beinhaltet u. a. bereits einen kryptografischen Bootloader, sicheren Speicherschutz, Manipulationsschutz, Schutz vor Reverse Engineering. Ein gutes RTOS sollte für die spezifische Ingenieursdisziplin oder Industrie geeignet sein.

Prozessmodelle und Testing:

3. Verwenden Sie Risikobeurteilung, Bedrohungsmodellierung und Fehlerbaumanalyse/Angriffsbaum-Methoden, um Gefahren, Risiken, Schwachstellen und Fehler zu erkennen.

4. Erstellen Sie klare und sichere Programmierrichtlinien und prüfen und analysieren Sie Code durch eine Kombination aus frühzeitigem Peer-Review und Analysetools.

5. Führen Sie Penetrationstests durch, z. B. Grey-Box-Tests für Software, Firmware, Hardware, Protokollkonfiguration und, falls verwendet, Funkfrequenz (RF), um Sicherheitslücken zu erkennen.

Authentifizierung/Datenschutz/ Zertifizierung:

6. Weisen Sie jedem IoT-Gerät eine eindeutige Kennung zu, z. B. eine elektronische Seriennummer (ESN) oder serialisierte globale Handelsartikelnummer (SGTIN). Stellen Sie Zertifikate für die Authentifizierung und Autorisierung bereit und nutzen Sie einen sicheren Update-Prozess.

7. Verwenden Sie ein starkes Passwort, verschlüsselte Daten und sicheres Schlüsselmaterial und speichern Sie Zertifikate bei vertrauenswürdigen Stellen.

8. Registrierung und Anmeldung durch sicheres Bootstrapping für die Erstbereitstellung von sicheren Passwörtern, Anmeldeinformationen, Netzwerkinformationen usw.

9. Planen Sie ein gutes Identitätsmanagement, indem Sie Identitäten pflegen und Anmeldedaten regelmäßig aktualisieren.

10. Gewährleisten Sie Vertraulichkeit und erfüllen Sie die Datenschutzanforderungen, indem Sie sicheres Data Mining planen und Compliance-Vorschriften einführen.

11. Wahren Sie die Privatsphäre Ihrer Kunden.
    IoT-Geräte wie Sensoren sammeln eine große Menge an Daten. Diese Daten sowie Metadaten (z. B. das Verfolgen von Personen über MAC-Adressen in Wearables) können Informationen enthalten, die datenschutzrechtlich relevant sind. Daher muss Ihr System in der Lage sein, zwischen normalen und sensiblen Daten zu unterscheiden.

Laufende Wartung:

12. Stellen Sie Patches und Updates über einen sicheren Update-Prozess bereit.

13. Überwachen Sie Hosts und Netzwerke sowie Accounts und Anmeldedaten auf Anomalien. Planen Sie eine sinnvolle Kontosperrung (für Analysezwecke) oder Löschung.

14. Berücksichtigen Sie die Sicherheit des physischen IoT-Geräts im Feld – ist der Standort sicher; kann das Gerät leicht gestohlen werden; ist eine Manipulation oder ein Speicherabbild möglich; kann ein Eindringling die Firmware aktualisieren usw.

Die obige Anleitung soll Ihnen den Einstieg in die IoT-Projektdurchführung erleichtern. Sie vermittelt Ihnen ein grundlegendes Verständnis für den Themenkomplex IoT-Sicherheit und zeigt Ihnen, was Sie mit Ihren IT- und Serviceprovidern besprechen sollten.

So hoffen wir, sowohl Ihr gefühltes als auch das tatsächliche IoT-Sicherheitsrisiko deutlich zu verringern. Denn erst das Überwinden dieser Hindernisse ermöglicht es Ihnen am profitablen IoT-Markt teilzunehmen.

Interesse an einer sicheren IoT-Lösung?

Sprechen Sie mit Dr. Jens Reinelt,
dem Sicherheitsexperten bei Lemonbeat: j.reinelt@lemonbeat.com

lemonbeat GmbH
Deutsche Straße 5
44339 Dortmund
Tel.: +49 (0)231 – 586 937 0
Mail: info@lemonbeat.com
Web: www.lemonbeat.de