Trusted Core Network

Vernetzte Sicherheit bei IoT-Infrastrukturen

Kai-Oliver Detken

Immer mehr elektronische Komponenten werden internetfähig gemacht oder nachträglich erweitert. So wird es in Zukunft kaum noch einen nichtvernetzten Bereich geben. Autos, Häuser, Fabriken und Smartphones werden über das Internet massenhaft Daten austauschen. Die Hersteller versprechen sich davon Mehrwerte oder auch mehr Sensordaten, um Nutzerprofile besser auswerten zu können. Nur bleibt dabei häufig die IT-Sicherheit auf der Strecke. Der Ansatz Trusted Core Network (TCN) könnte die notwendige vernetzte Sicherheit im IoT-Umfeld anbieten. Er ermöglicht, die Identität von Netzknoten zu überprüfen und einen gewünschten Zustand zu etablieren. So wäre es trotz erfolgreicher Angriffe auf einzelne Komponenten möglich, den Betrieb weiter sicherzustellen.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Das Internet der Dinge bzw. Internet of Things (IoT), beinhaltet eine Verknüpfung physischer Objekte mit einer virtuellen Repräsentation in einer internetähnlichen Struktur. Dabei bestehen die Teilnehmer nicht mehr nur aus Personen, sondern ebenfalls aus Dingen. Der Begriff wurde ursprünglich von Kevin Ashton im Jahr 1999 verifiziert, der „Internet of Things" zum ersten Mal verwendete (www.rfidjournal.com/articles/view?4986).

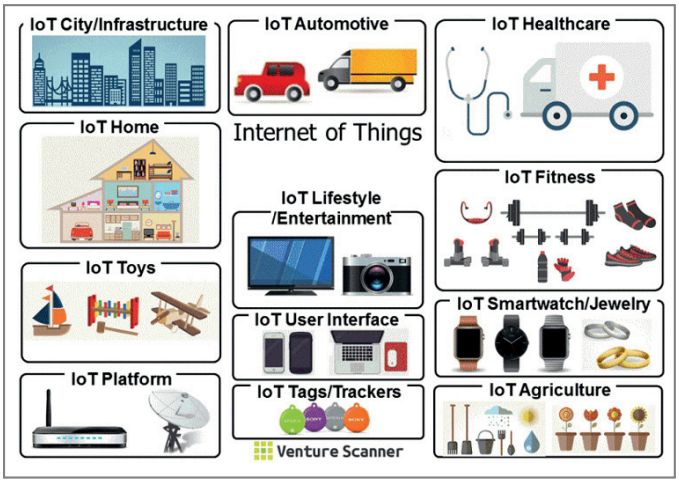

Bild 1: Unterschiedliche Schwerpunkte beim IoT-Einsatz (Quelle: www.der-bank-blog.de/15-schwerpunkte-beim-internet-der-dinge/technologie/21756/)

Ziel im IoT ist es, durch Sensoren und Aktuatoren automatisch wissenswerte Informationen aus der realen Welt zu erfassen, miteinander in Beziehung zu bringen und im Internet verfügbar zu machen. Ein Anwendungsbeispiel wäre die Abfrage von Zustandsinformationen von Bremsbelägen, die Auskunft über den aktuellen Verschleiß und die Alterung geben, so dass eine Früherkennung von notwendiger Wartung oder nötigem Austausch ermöglicht wird. Ein anderes Beispiel wäre die Abfrage eines Heizungsaggregats, das automatisiert in einen Regelkreislauf eingebunden wird, um den Energieaufwand zum Heizen oder Kühlen niedrig zu halten. *Bild 1* zeigt, in welchen Bereichen das IoT u.a. zum Einsatz kommen kann.

Um solche Anwendungsbeispiele zu ermöglichen, müssen folgende Punkte umgesetzt werden:

- Standardisierung von Komponenten und Diensten im Internet der Dinge;
- Einführung einer sicheren Netzanbindung;
- Reduktion der Kosten (Geräte, Inbetriebnahme, Anschlüsse usw.) für IoT-Komponenten;
- Entwicklung kostengünstiger, automatisierter, digitaler Dienste im Netz, die einen zusätzlichen Nutzen durch Vernetzung ermöglichen.

Speziell im Kontext von Industrie 4.0 werden immer mehr Produktionsanlagen vernetzt und mit dem Internet verbunden. Man verspricht sich dadurch verbesserte Produktionsdurchflüsse und eine Reduzierung von Lagerbeständen. Die typischen IoT-Komponenten bestehen hier aus einer schlanken, datenverarbeitenden Hardware und sind auf hohe Zuverlässigkeit ausgelegt. Dies ist im Produktionsumfeld üblich, um den Wartungsaufwand und die Ausfallrate zu begrenzen. Als Software kommen nur Betriebssysteme (u.a. Windows 10 IoT, Android Things, Contiki) mit sehr niedrigem Speicherverbrauch infrage, da es räumliche und technische Grenzen gibt.

Die Vernetzung solcher relativ leistungsschwachen Komponenten ist allerdings auch mit einem gewissen Sicherheitsrisiko verbunden, da häufig Sicherheitsmechanismen nicht im Vorfeld eingeplant wurden. Auch lassen sich nicht beliebige Schutzmaßnah-

men in die ressourcenarmen IoT-Komponenten integrieren. Aus diesem Grund wird versucht, hauptsächlich *die* Komponenten vor dem Zugriff von außen abzusichern, die wenig Einfluss auf die Leistungsfähigkeit der IoT-Knoten nehmen.

Trusted Core Network (TCN)

Um Zugriffsschutz bieten zu können, lassen sich grundlegend zwei Mechanismen nennen:

- Mutural Authentication;
- Trusted Network Communications (TNC).

Die erste Variante basiert auf Zertifikaten, mit denen sich die Geräte untereinander authentifizieren und damit eine vertrauenswürdige Kommunikation gewährleisten möchten. Zusätzlich wird im Anschluss eine hybride Verschlüsselung (Kombination von asymmetrischen und symmetrischen Verfahren) ausgeführt.

Die zweite Variante kommt von der Trusted Computing Group (TCG), eine industriebetriebene Standardisierungsorganisation, die offene Standards für Trusted Computing entwickelt, und beinhaltet neben der Authentifizierung der Geräte auch die Analyse der Zugriffe innerhalb des Netzes. Zur Implementierung müssen dabei zwei Instanzen hinzugefügt werden: der Policy Enforcement Point (PEP) und der Policy Decision Point (PDP). Während der PEP die Richtlinien (Policies) für die Netzzugänge festlegt und gegebenenfalls dem Nutzer Rechte entziehen kann, trifft der PDP die Autorisierungsentscheidungen. Um optimal sicherheitstechnisch absichern zu können, wird bei TNC ein TPM-Chip (Trusted Platform Module) verwendet, der Zertifikate sicher speichern kann und bereithält sowie die Integrität – also die Vertrauenswürdigkeit der Hardwarekomponente – messen kann.

Einen Schritt weiter geht der Ansatz Trusted Core Network (TCN), der auf der TNC-Spezifikation basiert und von Fraunhofer SIT (**www.sit.fraunhofer.de**) entwickelt worden ist. Dieser prüft nicht die Richtlinien für den Nutzer, sondern die wahre Identität und den Zustand der Netzknoten. Dies wird durch eine verteilte und redundante Kontrolle der Netzknoten ermöglicht, die die Punkt-zu-Punkt-Identität sowie den Zustand der benachbarten Knoten kontrolliert (siehe *Bild 2*).

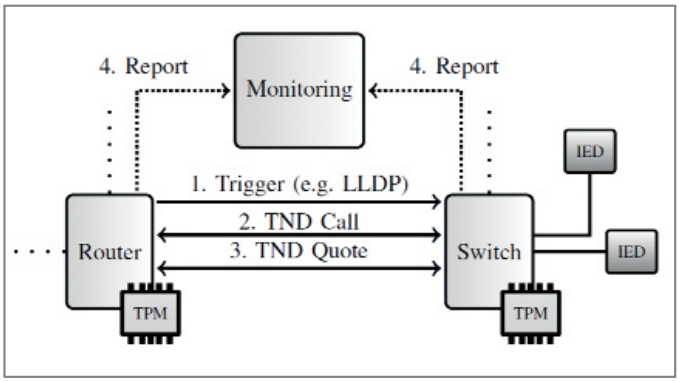

Bild 2: Überblick über die Architektur des Trusted Core Network

LLDP – Link Layer Discovery Protocol,
TND – Trusted Neighbourhood Discovery,
TPM – Trusted Platform Module,
IED – Intelligent Embedded Device

Durch das Protokoll Trusted Neighbourhood Discovery (TND) werden zunächst alle aktiven Knoten in der direkten Umgebung gefunden. Ausgelöst wird die Suche durch eine Triggernachricht, die über ein Protokoll (z.B. Link Layer Discovery Protocol – LLDP) an alle physischen Schnittstellen in periodischen Intervallen verschickt wird. Um durch diesen Mechanismus, eine Denial-of-Service-Attacke (DoS) zu vermeiden, können nur Netzknoten diesen Triggerimpuls auslösen, die einen gültigen Identitätsschlüssel und eine minimale Unterbrechung (Timeout) besitzen. Aufgrund der Verwendung des Trusted Platform Module (TPM) kann der Knoten vom System nun einwandfrei identifiziert und der Ist- mit dem Sollzustand verglichen werden. Dadurch lassen sich Manipulationen erkennen und Warnungen (Reports) an ein zentrales Monitoring weiterleiten. Die Ausbreitung von Angriffen oder das Infizieren mit Schadsoftware (Maleware) kann so effizient unterbunden werden.

Im Gegensatz zur TNC-Spezifikation, die auf Authentifizierung und Zugriffskontrolle achtet, basiert dieser Ansatz demnach auf einer Integritätsüberprüfung aller Netzknoten (z.B. Router, Switche). Auf Basis eines TPM-Chips überprüft so jeder Knoten seinen eigenen Gesundheitszustand sowie im Anschluss daran den Gesundheitszustand seiner Nachbarknoten. Dies wird durch das TND-Protokoll umgesetzt, das zu den Link-Layer-Netzprotokollen gehört und Anomalien erkennen kann. TND verwendet Trusted-Computing-Technik zur sicheren Identifizierung von Endknoten bzw. Geräten und verteilt die verfügbare Statusinformation über die TNC-Funktion Remote Attestation (entfernte Beglaubigung). Damit kann der Sicherheitsstatus eines Nachbarknotens über dessen TPM-Chip abgefragt werden, bevor eine reguläre Kommunikation darüber stattfindet.

Bei der Integration neuer Geräte wird eine Zero-Touch-Konfiguration angewandt, die Fraunhofer SIT ebenfalls für diesen Fall entwickelt hat. Hierbei handelt es sich um das gleichnamige Protokoll, das ebenfalls auf den Sicherheitsfunktionen des TPM-Chips basiert. Die Registrierung der Geräte benötigt lediglich eine eindeutige Geräteerkennung, die beispielsweise über einen QR-Code durch einen automatisch eingelesenen Fingerprint eines kryptografischen Schlüssels umgesetzt werden kann. Bei Anschluss eines solchen Geräts würden u.a. Konfiguration und Registrierung komplett automatisch ablaufen. Laptops oder USB-Sticks werden nicht mehr benötigt. Nur für den Fehlerfall muss eine Nutzerschnittstelle vorhanden sein (**www.sit.fraunhofer.de/de/tcn/**).

Notwendigkeit zusätzlicher Absicherungsmaßnahmen

Die Notwendigkeit dieser zusätzlichen Absicherungsmaßnahmen macht die Situation von sog. kritischen Infrastrukturen (Kritis) deutlich (siehe auch NET 7/2017, Seite 17). Hier werden Produktionssysteme genutzt, die kaum auf dem neuesten Stand gehal-

ten werden (z.B. Nutzung von abgekündigten Betriebssystemen wie Windows XP oder Embedded-Betriebssystemen in Routern mit altem Firmwarestatus). Hier steht noch die Verfügbarkeit, im Gegensatz zur sog. Office-IT, vor der IT-Sicherheit, obwohl man beides eigentlich nicht separat betrachten sollte. Durch die Vernetzungsstrategie im Industrie-4.0-Kontext sind diese Systeme nun auf einmal auch über das Internetprotokoll (IP) erreichbar und ermöglichen ganz neue Angriffsvektoren für Hacker. Die sind jetzt schon bereits sehr rege, wie die Studie „Industrie im Visier von Cyberkriminellen und Nachrichtendiensten" des Bitkom im letzten Jahr ausmachte. Es wurde ermittelt, dass 69 % der deutschen Industrieunternehmen bereits Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden waren. Dabei entstand ein Gesamtschaden von ca. 22 Mrd. € pro Jahr. Durch die Vernetzung von Maschinen über das Internet und der Trend zur digitalen Fabrik verschlimmert sich diese Situation noch. Um diese neuen Herausforderungen meistern zu können, sollte man sich über neue Sicherheitsmechanismen in jedem Fall Gedanken machen. Ein zentrales Monitoring über den Gesundheitszustand von Netzknoten könnte dabei helfen.

Generell kann der TCN-Ansatz für verschiedene Szenarien verwendet werden, die eine Überprüfung des Gesundheitszustands von IT-Systemen beinhalten. Ein wichtiger Anwendungsfall ist sicherlich im industriellen Zusammenhang zu sehen, der die gegenseitige Absicherung von Netzkomponenten vorsieht und Anomalien erkennt, um diese an ein Security-Event-Management-System (SEM) weiterleiten zu können. Wurde der TCN-Ansatz implementiert, kann das Unternehmen davon ausgehen, dass keine bösartige Manipulation (z.B. umgeleiteter Datenverkehr) oder verletzte Sicherheitsrichtlinien für die verwendete IT-Infrastruktur vorliegen.

Ein anderer Anwendungsfall wäre es, wenn ein Trust-Bereich zwischen den Substationen eines Power Grids etabliert würde, um Manipulationen der Geräte auszuschließen. Hierbei handelt es sich um Intelligent Embedded Devices (IED, Bild 2), deren Instabilität kritische Stromausfälle zur Folge haben könnte. TCN würde hier helfen das geplante Verhalten der IED weiter sicherzustellen, auch wenn eine Attacke auf das Stromnetz erfolgte.

Der TCN-Ansatz wurde vom Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Zusammenarbeit mit Industriepartnern für zwei Einsatzumgebungen prototypisch umgesetzt. Für die Industrieumgebung wurden handelsübliche Eagle-Router der Firma Hirschmann verwendet, die um einen TPM-Chip am I^2C-Bus erweitert wurden. Diese Router waren nun in der Lage, alle Geräte in der direkten Nachbarschaft zu prüfen und das Ergebnis über das Protokoll IF-MAP (IF-MAP – Interface for a Metadata Access Point, standardisiertes Protokoll der TCG) an einen MAP-Server zu berichten. Der MAP-Server ist in der Lage, die Informationen über den aktuellen Zustand des Netzes zu sammeln und visuell aufbereitet darzustellen. So können Schwachstellen oder unerlaubte Zugriffe sofort erkannt werden.

Aber auch in drahtlosen Umgebungen, in sog. Manet-Netzen (Mobile Ad-hoc Networks, drahtloses Ad-hoc-Netz, das sich selbstständig aufbaut und konfiguriert), kann TCN verwendet werden, indem eine Prüfung der Netzknoten durchgeführt wird, bevor diese in das Netz aufgenommen werden. Diese Prüfung muss natürlich kontinuierlich wiederholt werden. Aber so lassen sich auch Wireless LANs, die von Haus aus einfacher zugänglicher sind, besser absichern.

Fazit

Um die IT-Sicherheit auf einem möglichst hohen Niveau zu halten, müssen die Unternehmen erst einmal ihre Hausaufgaben im Bereich IT-Sicherheit machen. Das heißt, Basiskomponenten wie Virenscanner, Firewalls, regelmäßige Patche sowie aktuelle Betriebssysteme sollten zum Einsatz kommen und kontinuierlich aktualisiert und überprüft werden. Des Weiteren sollte man sich über Systeme Gedanken machen, die zusätzlichen Schutz bieten, wie beispielsweise NAC- oder SIEM-Systeme zum Erkennen und zur Abwehr von Hackerangriffen, sowie die sichere Authentifizierung und Verschlüsselung sensibler Daten vornehmen. Zudem sollte die organisatorische Sicherheit erhöht werden, um Richtlinien (Policies) für die zu nutzenden Dienste zu definieren und deren Einhaltung zu überprüfen. Dazu gehört auch, die Mitarbeiter zu sensibilisieren und regelmäßig auf falsche Nutzung (z.B. den Umgang mit E-Mail-Anhängen) hinzuweisen.

Durch die komplette Vernetzung im Rahmen des Internet der Dinge reicht es heute nicht mehr aus, Systeme isoliert voneinander zu betrachten. Hat ein Hacker erst einmal eine Lücke gefunden, könnte er sich so ungehindert im Netz ausbreiten, da er damit auch die anderen Sicherheitssysteme umgeht. Dies ist nur zu verhindern, wenn die verschiedenen Sicherheitssysteme miteinander interagieren. Erst dann kann eine automatisierte Reaktion erfolgen, die einer langsamen manuellen Handlung überlegen ist. Noch besser wäre es allerdings, wenn sich die Netzknoten selbst gegenseitig im Vorfeld einer Kommunikation überprüfen würden, um dann eine sichere Kommunikationsplattform anbieten zu können, wie es der TNC-Ansatz vorsieht.

Der TNC-Ansatz ist allerdings schwierig umzusetzen, da er fordert, dass alle Netzknoten mit entsprechenden TPM-Chips ausgestattet sein müssen. Dies wurde zwar bereits prototypisch für Eagle-Router der Firma Hirschmann in Zusammenarbeit mit Infineon und Fraunhofer SIT realisiert, gehört aber derzeit nicht zur Standardausrüstung. Hinzu kommt, dass heute in der Netzumgebung zumeist amerikanische Komponenten (Cisco, HP) verbaut werden, die keine nachträgliche TPM-Integration gestatten. Trotzdem bleibt zu hoffen, dass die Hersteller IT-Sicherheit in ihre Komponenten integrieren, damit möglichst wenig Angriffsvektoren in einer IoT-Infrastruktur verfügbar sind. Der Trusted-Core-Network-Ansatz ist dafür geeignet, als entsprechende Lösung zu dienen. *(bk)*