10 Thesen zur Informationssicherheit im Zeitalter der Digitalisierung

Der technologische Fortschritt läuft in vollem Tempo und ist untrennbar mit unserem Alltag verbunden, so dass wir ihn als gegeben hinnehmen. Neuheiten aus der Welt der Technologie faszinieren die Menschen nicht mehr in dem Maße früherer Tage. So beeindruckt es bspw. kaum jemanden mehr, dass einige mobile Geräte mittlerweile so leistungsfähig sind, die Flugstrecke einer Rakete zum Mars berechnen zu können. Eine gleichsam negative wie gefährliche Nebenwirkung dieser offensichtlichen technologischen Überdosis ist der Verlust der Vorsicht in Bezug auf Informationssicherheit. Viele aktuelle und zukünftige Bedrohungen in unserem Alltag werden kaum beachtet. Je anspruchsvoller und hochentwickelter Technologien und das Internet werden, desto höher wird kurioserweise das Risiko ihrer Nutzung. Die esatus AG ist sich dieser Problematik bewusst und arbeitet aktiv an der Entwicklung neuer Konzepte, um die Zukunft für alles und alle sicherer zu machen.

Einleitung

Die Digitalisierung und die damit verbundenen Bedrohungen betreffen viele Bereiche. Dieses Whitepaper gibt einen Überblick zu den Themen Smart Home und Industrie 4.0 als Internet of Things (IoT) bzw. Industrial Internet of Things (IIoT) und es werden zehn Thesen über bestehende Bedrohungen in den Bereichen RFID, Autonomie, Wearables sowie dem Datenhandel aufgestellt und diskutiert.
Der dabei stets genommene Bezug zum aktuellen IST-Zustand sowie die Betrachtung richtungsweisender Trends ist für eine Einschätzung des Risikos auf das private und geschäftliche Umfeld essentiell.

IoT – Smart Home

1. Der Anwender muss einen lückenlosen Schutz aufbauen, der Angreifer muss hingegen nur eine kleine Schwachstelle finden.

Unter Smart Home werden allgemein computerunterstützte Haushalte verstanden, welche je nach Wunsch des Besitzers mit automatisierten Systemen ausgestattet sind. Dies können haushaltstypische Aufgaben wie das Öffnen und Schließen von Rollos, die Reinigung mit Saugrobotern und auch die Haussicherung mit Sicherheitssystemen wie Kameras, Bewegungsmeldern usw. sein. Smart Home Technologien haben aktuell ein Marktpotenzial von rund 30,2 Mrd. €. Der Umsatz belief sich bis 05/2017 bereits auf 1,296 Mrd. €[1].

In einem hochtechnischen Haus, welches dem Besitzer einen Mehrwert an Komfort und Sicherheit geben soll, müssen alle dafür vorhandenen Systeme gegen Angriffe von außen gesichert werden. Im Optimalfall fängt dies bereits bei der Planung und beim Bau des Hauses mit der Entscheidung an, welche Grundinfrastruktur – Funk oder Kabel – favorisiert wird. Beide Technologien haben Vor- und Nachteile. Aus der Sicht der Informationssicherheit ist die kabelgebundene Datenübertragung zu empfehlen, da diese durch Angreifer nicht so einfach abgehört bzw. manipuliert werden kann.
Funkübertragung ist kostengünstiger und flexibler einsetzbar, doch oft nur schlecht oder gar nicht mit einer verschlüsselten Kommunikation ausgestattet. Angreifer können mit einfachen Mitteln sensible Informationen abfangen oder den Informationsfluss mit einem Störsender komplett unterbinden. Kabelgebundene Übertragungen hingegen sind deutlich kostenintensiver und auch weniger flexibel in der Installation, bieten dafür aber ein höheres Maß an Informationssicherheit.

[1] https://www.splendid-research.com/smarthome.html (17.08.2017)

2. Wenn alles vernetzt ist, ist alles angreifbar.

Doch auch die sicherere kabelgebundene Übertragung eines Smart Home ist nicht gänzlich vor Angriffen aus dem Internet gefeit. Jedes sich im Netzwerk befindende smarte Gerät hat eine eigene öffentliche IP-Adresse und ist darüber angreifbar. Dies betrifft gleichermaßen Kühlschränke, Staubsaugroboter oder Thermostate. Die Bandbreite der möglichen Angriffe – von einer einfachen DDoS-Attacke (Distributed Denial of Service) bis hin zu einer Ransomware-Infizierung – machen ein voll digitalisiertes Smart Home zu einem gefährdeten Angriffsziel. Jedoch zeigten über 50% der zentralisierten Sicherheitssysteme schwerwiegende Mängel in der Verschlüsselung und Authentifizierung[2]. Hier ist ein Umdenken der Hersteller notwendig, um standardisierte Sicherheitsmaßnahmen effektiv einzusetzen und den Einsatz mangelhafter Sicherheitssysteme auszuschließen.

IIoT – Industrie 4.0

Industrie 4.0 – auch Smart Factory genannt – setzt höhere Anforderungen an die Digitalisierung voraus. Daher wird hier auch nicht mehr von IoT gesprochen, sondern von „Industrial Internet of Things", kurz IIoT. Im IIoT muss eine Kombination aus komplexen Maschinen, Sensoren und Big-Data Analysen mit M2M-Technologien (Machine-to-Machine) miteinander vernetzt werden, um effektiv Produktionsprozesse zu optimieren, Geräte zu überwachen sowie neue Geschäftsmodelle generieren zu können. Der Fokus liegt dabei auf der Effizienzsteigerung sowie der Einbindung von Kundenwünschen in die Supply-Chain. Es wird eine Effizienzsteigerung von mehr als 18% sowie eine Umsatzsteigerung von 2-3% durch IIoT pro Jahr erwartet.[3]

3. IIot führt zu einer menschenfreien Produktion.

Die fortschreitende Digitalisierung hat eine disruptive Wirkung auf bestehende Systeme sowie Geschäftsmodelle, da diese mit der (technologischen) Entwicklung Schritt halten müssen. Eine nahezu vollständige Transformation hin zur menschenfreien Umgebung ist in den Abteilungen Produktion, Personalwesen sowie der Organisation abzusehen. Viele Arbeitsaufgaben, welche bereits heute maschinell unterstützt werden, können in diesen Bereichen zukünftig vollständig autonom durch den Einsatz von Software und/oder Maschinen durchgeführt werden. Dies wird jedoch den Einsatz von Menschen in diesen Abteilungen nicht gänzlich ausschließen. Stattdessen besteht die Herausforderung darin, die bestehenden Mitarbeiter für die neuen Technologien umzuschulen und neue Mitarbeiter, die bereits über die erforderlichen Kenntnissen verfügen, einzustellen.

Eine Hand-in-Hand Entwicklung von Mensch und Maschine wird die nächsten Jahre prägen. Es ist jedoch davon auszugehen, dass ab gewissen Entwicklungsständen die angesprochene disruptive Wirkung dazu führen kann, dass humanoide Robotik sowie die künstliche Intelligenz den Einsatz von menschlichem Personal unnötig machen. Sobald dies der Fall ist, wird die menschliche Kompetenz zentralisiert für Konfigurationen und Sicherheitsmaßnahmen benötigt. Um dies umsetzen zu können, wurden bereits 2016 weltweit rund 4,3 Milliarden Euro investiert. Tendenz steigend. Experten schätzen, dass die vollständige Ablösung ab dem Jahr 2062 mit dem Eintritt der sog. Singularität einhergehen wird.

4. Die Industrie besteht unter Beschuss.

Jedoch ist die Vermutung, dass die technologische Weiterentwicklung die Gefahr von gezielten Angriffen mindert, ein Trugschluss. Wirtschaftsspionage/-schädigung, gezielte nachrichtendienstliche Überwachung sowie geheimdienstliche Manipulation sind und bleiben für deren Initiatoren erstrebenswerte bzw. lukrative Mittel. Das Beispiel Stuxnet zeigt, wie gefährlich ein Angriff dieser Form sein kann.

Die Digitalisierung der Industrie ermöglicht darüber hinaus Angriffe, denen auch der Smart Home Bereich ausgesetzt ist. Der Grund ist einfach: Die smarten Geräte des IIoT sind ähnlich schlecht geschützt, wie die des IoT-Bereichs. Der CEO von Endian, Raphael Vallaz-

[2] https://www.av-test.org/fileadmin/pdf/avtest_2014-04_smart_home_deutsch.pdf (17.08.2017)
[3] https://www.strategyand.pwc.com/media/file/Industrie-4-0.pdf (17.08.2017)

za, sagt dazu: „Jedes Gerät, das mit dem Netz verbunden ist, kann angegriffen oder – schlimmer noch – ferngesteuert werden". Viele smarte Geräte werden innerhalb des internen IIoT genutzt und verwaltet. Jedoch sind einige direkt mit dem öffentlichen Internet verbunden, um Monitoring sowie Fernwartung zu ermöglichen.
Aus diesen und weiteren Schwachstellen resultieren große Risiken, welche die Unternehmen mit gezielten Sicherheitsmaßnahmen begegnen müssen, um nicht schutzlos – u. U. sehr kostenintensiven – Angriffen ausgesetzt zu sein. Unternehmen von höherer Bekanntheit müssen sich darüber hinaus auch gegen Angriffe von weiteren Interessengruppen wie Hacktivisten, Blackhat Hackern bis hin zu Skript Kiddies wappnen.

RFID

Radio-frequency identification, kurz RFID, bezeichnet die kontaktlose und automatische Identifizierung von Personen, Tieren, Waren sowie Gütern. Die Technologie findet heutzutage, besonders aufgrund der geringen Kosten, breiten Einsatz in vielen privaten und geschäftlichen Bereichen und Anwendungen.

5. In Zukunft werden wir gechippt wie Schafe.

Die RFID-Technologie zeichnet sich dadurch aus, keine Batterie zu benötigen. Dies prädestiniert die RFID-Chips im geschäftlichen Bereich u. a. für den Einsatz in der Lagerhaltung, der Produktionsüberwachung und auch zur Zugangsauthentifizierung.

Im privaten Bereich wird RFID bspw. in Personalausweisen/Pässen, EC-/Kreditkarten uvm. eingesetzt. Der Einsatz von Chips für Marktforschungszwecke in Konsumartikeln, wie z. B. in Kleidung, verbreitet sich ebenfalls stark. Dabei werden die Chips in Etiketten eingearbeitet und können von entsprechenden Lesegeräten erkannt werden. Sinn und Zweck dieses Einsatzes sind zum einen der Diebstahlschutz und zum anderen das Sammeln von weiterführenden Daten über die Kunden. Um das Auslesen der Daten zu ermöglichen, existieren mehrere öffentliche Lesegeräte, welche die Daten aufzeichnen und mit allen weiteren verfügbaren Informationen in einer Datenbank verbinden. Ziel ist es, Informationen über bevorstehende Trends, Zugehörigkeit zu bestimmten Bevölkerungsschichten, Herkunft, Berufstätigkeit uvm. zu erhalten.

Es existieren bereits Patentanträge, wie mit dieser Technik einzelne Personen getrackt werden können. Dies wirft verstärkt Fragen bzgl. des Datenschutzes und der Sicherheit dieser Technologie auf.
Beispielsweise können aufgrund geringer Speicherkapazitäten die RFID-Chips, welche z. B. für die Zugangs-Authentifikation eingesetzt werden, schnell im Vorbeigehen kopiert werden. Dies birgt ein Sicherheitsrisiko, denn der 24 – 48 Bit lange Schlüssel kann schnell geknackt werden und der Angreifer kann auf diese Weise Zutritt zu den gewünschten Räumlichkeiten erlangen. Solange kein effektiver Schutz gegen permanentes Auslesen existiert, ist der Einsatz von RFID in sicherheitsbeschränkten Bereichen risikobehaftet.

Autonomie

Autonomie ist ein Begriff, welcher bislang nur in der Industrie zum Einsatz kam. Doch mit der Entwicklung von Smart Cars drängen autonome Technologien verstärkt in den Automotive-Bereich.

6. Automobile werden zu Computern auf Rädern.

Das autonome Fahren ist eine Kombination aus vielen bereits eingesetzten Fahrassistenzsystemen, wie z. B. Spurhalteassistent, Tempomat, usw. Das vollständige Ersetzen des Fahrers durch einen Computer ist bislang jedoch nur teilweise möglich (Teil-Autonomie). Viele Automobilhersteller beschäftigen sich aber verstärkt mit der Entwicklung voll-automatisierter Autos und insbesondere Tesla scheint mit dem Einsatz der Funktionalität in seinen Modellen bereits relativ weit zu sein. Eine Masseneinführung wird für das Jahr 2020 prognostiziert.
Im Güterverkehr ist aktuell Daimler der führende Entwickler und sagt: „In den kommenden zehn Jahren werden wir bei LKWs mehr Veränderungen erleben, als in den vier Jahrzehnten davor". Fast alle modernen Autos besitzen bereits vernetzte Komponenten (ECUs),

um die technischen Anforderungen für Fahrassistenzsysteme umsetzen zu können.

7. Das Auto wird zur Waffe.

Die Vernetzung der Komponenten sowie die Verbindung mit dem Internet ermöglichen zukünftig Angriffe, wie sie vorher noch nicht existiert haben. Bereits 2014 musste der Jeep Cherokee zurückgerufen werden, da dieser aus der Ferne kontrolliert werden konnte. Eingriffe in das Bremssystem sind bei einem Auto besonders gefährlich. Auch immer hochentwickeltere Entertainmentsysteme umfassen viele Funktionen, die potenziell für Angriffe missbraucht werden können (bspw. die Verbindung mit App und Internet). Die University of Wisconsin in San Diego hat in einer Untersuchung festgestellt, dass viele Komponenten, die standardmäßig verbaut werden, Schwachstellen aufweisen. Den Forschern der Universität war es möglich, ein Großteil der Funktionalität aus der Ferne zu kompromittieren. Derzeit ist die Entwicklung von Schadcode für den „normalen" Angreifer noch zu kostspielig, doch mit der weiteren Entwicklung hin zu voll-automatisierten Autos kann sich dies ändern. In Wikileaks-Berichten wird diese Entwicklung bereits angedeutet. Eine Infrastruktur voller autonom agierender Fahrzeuge wäre somit ebenfalls ein Ziel vieler Interessensgruppen, womit die Gefahr von schwerwiegenden Angriffen durch diese Technologie steigen könnte.

Wearables

Wearables, kurz beschrieben als tragbare Computersysteme, sind aktuell stark im Aufschwung. Vor allem in Form der Smart Watch besitzen solche Geräte viele neue Funktionen wie Pulsmesser, Schrittzähler usw., die den Besitzern das Leben komfortabler machen sollen.

8. Der Mensch wird zum Datensammler.

Der Einsatz ist derzeit vorwiegend im Sport- und Gesundheitsbereich angesiedelt, um den Körper besser überwachen zu können. Ausgewertet werden die gesammelten Daten mit einer auf dem Smartphone installierten App. Entwicklungen in diesem Bereich bieten ständig neue Produkte und Funktionen, die die körperliche Überwachung optimieren. So befinden sich smarte Textilien wie T-Shirts/Shorts und Schuhe bereits in der Entwicklung. Ziel ist die Überwachung so zu optimieren, dass der Nutzer maximalen Komfort genießen kann, aber auch bei gesundheitlichen Problemen stets über aktuelle Körperdaten informiert ist bzw. bei Anzeichen von Verschlechterungen gewarnt wird. Ebenso ist der präventive Einsatz besonders im Sport gefragt, da Tipps zur korrekten Haltungen sowie weiteren Verbesserung gegeben werden können. Problematisch an dieser Thematik ist, dass die gesamten Informationen sehr sensibel sind und bis vor nicht allzu langer Zeit nur dem der Schweigepflicht unterliegenden Arzt zugänglich waren. Eine aktuelle Untersuchung von sieben deutschen Datenschutzaufsichtsbehörden (BfDi) besagt, dass alle bereits verfügbaren Geräte Mängel bei der Erfüllung von datenschutzrechtlichen Anforderungen aufweisen. Die Daten werden von den Herstellern gesammelt und auf dem Markt offen verkauft. Einige gaben zu, dass über 50% der bestehenden Einnahmen aus dem Verkauf von Daten an Versicherungsunternehmen ausmachen. Versicherungen sind insbesondere deswegen an den Daten interessiert, da sie damit eine Aufstufung der Bezüge bzw. eine Kündigung in Betracht ziehen zu können, sollte der Versicherungsnehmer sich ungesund verhalten oder Symptome einer kostenintensiven Erkrankung zeigen.

Ein personalisierter Krankenversicherungsvertrag ist mit dieser Entwicklung möglich. Erste Schritte dahin wurden bei den gesetzlichen Krankenkassen durch Bonusprogramme (TK) bereits gemacht. Die Entwicklungen können jedoch kritisch gesehen werden, denn die damit einhergehende Verflechtung von Daten mit Bereichen des täglichen Lebens können bei Manipulation der Daten zu schwerwiegenden Problemen führen. Eine plötzliche Schufa-Herabsetzung wäre ein Beispiel hierfür.

Datenhandel

Jedes digitale (smarte) Gerät sammelt Informationen, welche wiederum auf Servern im Internet gespeichert werden. Doch was passiert den gesammelten Daten?

9. Daten sind das neue Öl.

Es existiert ein weltweit agierender Informationsmarkt mit einem Volumen von 122 Milliarden €, welche laut dem Tagesspiegel im Jahr 2016 umgesetzt wurden. Auch hier ist die Tendenz steigend. Der deutsche Ableger des Datenhandels Acxiom Corp. besitzt nach eigenen Angaben rund 1.500 Datensätze pro Person. Genutzt werden diese, um jede Art von Frage- bzw. Problemstellung beantworten zu können, wie z. B.:

- Welche Personen würden dieses Produkt kaufen?
- Bestehen Gefahren für Krankheiten bzw. treten bereits Symptome auf?
- Personalentscheidungen wie Einstellungen und Entlassungen

Dabei stützen sich die Unternehmen auf eine große Bandbreite von Informationen, welche mittels Big-Data Analysen ausgewertet und die Ergebnisse verkauft werden. Die weitere Zunahme der Digitalisierung ermöglicht darüber hinaus die Erstellung präziserer Daten, welche die bereits bestehenden Profile und Prognosen verbessern können.

10 Die Digitalisierung führt zu einer DDR 2.0.

Eine Nutzung der Daten durch Behörden könnte zu einer indirekten totalen Überwachung führen. Personen, welche sich dieser Technik entziehen, könnten dabei als potenzielle Bedrohung angesehen werden. Zieht man den Vergleich von den damaligen Methoden der Stasi zur NSA, befinden wir uns bereits in einer totalen Überwachung. Die Stasi füllte mit den gesammelten Daten insgesamt 48.000 Aktenschränke. Die NSA hat fünf Zettabyte an Daten gespeichert, was umgerechnet etwa 42.000.000.000.000 Aktenschränke füllen würde. Darüber hinaus zeichnet sich auch in der Politik eine Entwicklung dahingehend ab, Daten offiziell und aktiv für das Strafrecht zu sammeln und nutzen zu können, u. a. mit der Begründung der Terrorabwehr.

Die **esatus** AG ist ein mittelständisches IT-Beratungsunternehmen. Getreu der Unternehmensmission „Enforcing Information Security" ist die esatus AG der qualifizierte, erfahrene und flexible Ansprechpartner für Projekte rund um das Thema Informationssicherheit. Für Kunden werden optimale und individuell gestaltete Lösungen für Herausforderungen in den Bereichen Identity & Access Governance, IT Security, sowie Governance, Risk und Compliance angeboten. Zudem bietet die **esatus** AG eine umfassende Beratung zur Thematik des IT-Sicherheitsgesetzes an, beispielsweise zur Einrichtung einer Meldestruktur. Die Zufriedenheit von Kunden ist der Leitfaden, nachdem sich das gesamte Handeln des Unternehmens richtet.

Herausgeber **esatus** AG

Weitere Informationen zum Thema „10 Thesen zur Informationssicherheit im Zeitalter der Digitalisierung" bei der **esatus** AG finden Sie unter: esatus.com

Stand der Informationen im vorliegenden Whitepaper: August 2017