Positionierung

- Wen adressieren wir mit dem Papier: die Politik, CxO-Ebene im Mittelstand, IT-Sicherheitsverantwortlichen, interessierte Laien?
  - ➔ *Im Prinzip alle genannten Gruppen, am wenigsten sind aber die „interessierten Laien" als Zielgruppe im Fokus (soweit nicht CxO-Ebene und Politik auch zur „Laiengruppe" zugehörig gesehen werden können). Technische Details stehen nicht im Mittelpunkt. Dennoch sollte eine Tiefe der Betrachtung und Neuigkeitswert erreicht werden, der das Papier auch für z.B. Sicherheitsverantwortliche interessant macht.*
- Was ist der Nutzen für die Leser:
  - o Bewusstsein für eine neue Problematik
  - o Beschreibung der Stand der Kunst
  - o Handlungsempfehlungen
  - o …
  - ➔ *Im prinzip alle aufgelisteten Punkte. Stand der Kunst auch aus der Perspektive der „Angreifer". Im Mittelpunkt steht eher das Aufzeigen möglicher Szenarios, deren Konsequenzen (z.B. auch bezüglich Haftungsfragen) und Handlungsmöglichkeiten. Es geht eher darum den Raum der Handlungsmöglichkeiten/Optionen aufzuzeigen und weniger direkt konkrete/AK-offizielle Handlungsempfehlungen auszusprechen.*
- Daraus abgeleitet: wie detailliert und wie umfangreich soll das Papier werden?
  - ➔ *Es werden 8-10 Seiten angepeilt.*
- Bis wann soll eine erste Version entstehen und wie erfolgt die Veröffentlichung (etwa im Rahmen einer Veranstaltung)?
  - ➔ *Eine Veröffentlichung in 2016 sollte das Mindestziel sein. Es soll aber auch versucht werden für die Oktober-Veranstaltung des AK in Berlin zumindest verwertbare Zwischenergebnisse beitragen zu können. Das geplante Vorgehen sollte auch eine Fertigstellung einer ersten Version des Pappiers zu dieser Veranstaltung nicht von vorneherein ausschließen (allerdings kann dies nicht zugesagt werden).*
- In welchem Bezug steht das Papier zu den anderen Aktivitäten des AK Security?
  - ➔ *Dies ist im AK zu klären. Eher kein Bezug zur „Blueprint"-Aktivität, aber evtl. zur Berlinveranstaltung im Oktober (siehe vorherige Frage).*

Vorschlag an den AK (Meeting 18.7.16) für das weitere Vorgehen:

<<Note: Dieses Vorgehen sollte so geplant werden, dass die Option eines relevanten Beitrages für die Oktober-Veranstaltung in Berlin möglich bleibt>>

Die Arbeitsgruppe hat sich dazu entschieden, als erstes Trendpapier ein Grundlagenpapier mit den Themen "eindeutige Identifizierung" und "trusted data" zu erstellen. Ein erster Entwurf dazu liegt bei. Für die Bearbeitung dieses vielschichtigen Papiers wird folgendes Vorgehen vorgeschlagen:

1. ein Workshop im Herbst mit ca 6-8 Teilnehmern aus dem Arbeitskreis Sicherheit und/oder weiteren sachkundigen Personen, bei dem auf der Grundlage des beiliegenden Papiers die Inhalte vertieft werden

2. anschließend Ausarbeitung des Trendpapiers durch einen erweiterten Autorenkreis

Entwurf

Gliederung des Papiers „eindeutige Identifizierung" und „trusted data"

Einleitung: Motivation und Scope

Im „wirklichen Leben“, sei es bei sensiblen Geschäften, sei es bei der Anbahnung von Verträgen mit Geschäftspartnern, oder sei es, wenn wir persönliche Beziehungen eingehen, stellen wir uns immer diese Fragen: mit wem habe ich es zu tun ? Was ist das für eine Person ? Wer steckt hinter diesem Unternehmen, dieser Organisation, diesem potenziellen Partner ? Was sind ihre/seine Motivationen, seine Absichten ? Ist sie/er ehrlich und vertrauenswürdig, kann ich ihm glauben ? Kann und will ich ihr/ihm vertrauen ? Inwieweit will ich mich auf sie/ihn verlassen ? Wieviel Transparenz, wieviel Kontrolle benötigen wir, wenn wir zusammenarbeiten, etwas zusammen unternehmen, uns zusammentun ? Wie stehen die Chancen, dass wir immer offen und ehrlich miteinander umgehen ? Wie halten wir das gegenseitige Vertrauen auch dann aufrecht, wenn es zu Konflikten und Störungen kommt ? Was geschieht im Falle der Trennung ? Wir entwickeln im Umgang von Mensch zu Mensch auf der Grundlage unserer Erfahrungen recht gute Sensoren, die uns frühzeitig signalisieren, wenn Dinge nicht „glatt“ laufen, wir agieren sehr sensibel, wenn wir meinen, getäuscht worden zu sein oder einen Vertrauensbruch zu v erspüren, und wir gehen dieser Vermutung nach.

Auf den Punkt gebracht lauten die Kernfragen, von denen alles andere abhängt: mit wem habe ich es zu tun, ist mein Gegenüber wirklich der, der er zu sein vorgibt ? Kann ich mich darauf verlassen, dass das, was diese Person mir gegenüber äußert, wahr ist ?

Die Digitalisierung von Prozessen, Produkten und Dienstleistungen trägt als charakteristisches Merkmal in sich, dass die Kommunikation von Mensch zu Mensch durch die Kommunikation von Menschen mit Maschinen und Maschinen mit Maschinen erweitert und sogar ersetzt wird. Das Verhalten der Maschinen wird durch Algorithmen definiert und determiniert, die in Systemen und Systemverbünden organisiert sind. Das Verhalten der Systeme / Algorithmen wird durch die eingehenden Informationen / Daten beeinflusst, der Output der Systeme/ Algorithmen besteht seinerseits in Informationen / Daten, die je nach Zweck und Einsatz des Systeme/Algorithmus das Verhalten von Menschen oder anderen Systemen / Maschinen beeinflussen.

In diesem Kontext stellen sich die gleichen Fragen wie im „wirklichen Leben“: ist das System, mit dem ich (als Mensch oder als System) kommuniziere, dasjenige, das es zu sein vorgibt, und mit dem ich kommunizieren möchte ? Sind die Daten/Informationen, die ich von ihm bekomme, wahrhaftig, so dass ich mein Verhalten darauf stützen kann ?

Eindeutige Identität und Verlässlichkeit der Daten sind folglich die entscheidenden Basisparadigmen für jede zuverlässige Kommunikation. Dies gilt erst recht für eine von Menschen nur noch bedingt kontrollierte Kommunikationen von Maschinen mit Maschinen.

Konzepte wie Industrie 4.0 sind in hohem Maße risikobehaftet, wenn diese Basisparadigmen in der Kommunikation nicht zweifelsfrei gegeben sind. Das Vortäuschen einer Identität und das Vortäuschen von manipulierten Daten/Informationen als wahrhaftig sind die zentralen Angriffspunkte, die die Robustheit, Safety und Security von Systemen, Prozessen und Produkten verletzen.

Deshalb befasst sich dieses Trendpapier mit den Kernthemen „eindeutige Identifizierung“ und „trusted data“.

Teil 1: Grundlagen

1.1 und 1.2 Definition und Abgrenzung: Was ist (trusted) Identity ? und was ist „trust in data“

Der Duden definiert Identität unter Anderem als "Echtheit einer Person oder Sache; völlige Übereinstimmung mit dem, was sie ist oder als was sie bezeichnet wird".

Neben natürlichen Personen und Organisationen, sogenannten "juristischen Personen", existieren in der modernen Welt viele weitere Entitäten mit einer Identität.

Durch Software gesteuerte komplexe Maschinen übernehmen Aufgaben in der realen Welt. Neben einfachen und weitgehend ungefährlichen Tätigkeiten wie dem Staubsaugen oder Rasenmähen sind in der jüngeren Vergangenheit zunehmend verantwortungsvolle Aufgaben, z.B. das Fahren eines Autos oder die automatischen Ausführung von Finanztransaktionen, hinzugekommen. Die Verantwortung für die handelnde Software wird dabei in fast allen Fällen dem Benutzer übertragen. Durch die Software ausgeführte Handlungen werden als Handlungen des Benutzers interpretiert, somit übernimmt die Software dessen Identität.

Relevante Handlungen werden sowohl im Alltag als auch für sichere Softwaresysteme autorisiert, nachdem eine erfolgreiche Authentifizierung der handelnden Person erfolgt ist. Die Genauigkeit und Aufwendigkeit der Authorisierung richtet sich dabei nach dem zu erwartendem Schaden durch die Handlung. Wichtige Verträge werden so z.B. im Beisein eines Notars nach vorheriger Kontrolle der Ausweispapiere unterzeichnet. Der Besitz eines Schlüssels autorisiert automatisch zum Öffnen der zugehörigen Tür. Durch eine erfolgreiche Authentisierung wird die Identität der Person überprüft, sie erhält eine "Trusted Identity".

In der realen Welt besteht ein Authentifizierungsvorgang üblicherweise aus einer Kette von Einzelnachweisen, die wie die Ausweiskontrolle bewusst formal, oft aber auch intuitiv erfolgen. Jemand, der durch einen Pass vorgibt, deutscher Staatsbürger zu sein und die Landessprache nicht korrekt beherrscht, wird z.B. bei einer Kontoeröffnung Misstrauen erregen. In technischen Systemen gibt es hierzu Analogien: In Computernetzwerken reicht neben den schwierig zu unterlaufenden kryptographischen Authentifizierungsmethoden z.B. oft eine Prüfung der IP-Adresse für Zugriff auf weniger kritische Daten.

Daten umfassen neben klassischen Texten, Bildern oder Audiodateien heutzutage auch Steueranweisungen für Maschinen oder Programmcode. Wann sind Daten nun als "vertrauenswürdig", als "Trusted Data" zu bezeichnen? Zum einen muss man die Daten/den Programmcode einer eindeutigen, authentifizierten Quelle zuordnen können. In der "analogen" Welt wird die Zuordnung zur Quelle z.B. durch eine Unterschrift und den ausgedruckten Text auf Firmenpapier hergestellt. In der digitalen Variante ist die Quelle als auch die Integrität der Daten mit kryptografischen Verfahren prüfbar.

Spätestens auf dem Weg zur Vollautomatisierung, der sogenannten "Industrie 4.0", fällt der Mensch als Kontrollinstanz weg. Maschinen reden mit Maschinen -- den früher am Prozess direkt beteiligten Menschen fallen ungewöhnliche Daten, Nachrichten oder Verhaltensweisen erst viel später auf, im Extremfall erst dann, wenn die Maschinen Schaden in der physischen Welt angerichtet haben. Die kryptographische Kopplung an die Datenquelle als auch der Integritätsschutz gegen Manipulationen auf dem Übertragungsweg (Internet!) ist somit als Mindestforderung einzustufen.

Ein anderer Aspekt betrifft die Erzeugung der Daten oder Steuerbefehle an sich: Diese werden mit immer komplexerer Software erstellt, die mit den heute verwendeten Entwicklungsmethoden mit

ziemlicher Sicherheit Fehler enthalten wird. Sind die erzeugten Daten/Steuerkommandos noch vertrauenswürdig, wenn der Mensch gar nicht mehr die Algorithmen zur Erzeugung versteht und ihn in komplexen Systemen auch nicht mehr ausreichend prüfen kann?

1.3 Vereinfachtes Kommunikationsmodell (Grafik mit Erläuterung)

1.4 Relevanz von „eindeutige Identifizierung“ und „trust in data“ für Information Security / Cyber Security

Ein momentaner Trend ist der zunehmende Einsatz von von Decision-Support-Systems auf der Basis umfangreicher und komplexer Datenanalysen, auf deren Grundlage automatisierte Reaktionen veranlasst werden. Genau dieser Aspekt wird ein sehr relevantes Einfallstor für zukünftige Angriffe werden. Nicht das IT-System selber wird direkt angegriffen, sondern durch die Manipulation der eingehenden Daten wird indirekt Einfluß auf die automatisierten Reaktionen genommen. Die dadurch realisierbaren Bedrohungen sind sehr vielfältig, von individuellen finanziellen Vorteilen (z.B. durch die Manipulation von Verbrauchsdaten) bis hin zur Sabotage kritischer Infrastrukturen in der realen Welt (z.B. Vorspiegelung von Komponentenausfällen um das Anlaufen eines Notfallplanes zu provozieren). Erste Angriffe dieser Art werden bereits berichtet.

<<Note: Hier sollten aktuelle konkrete Angriffsbeispiele aufgeführt werden>>

Für die Angemessenheit und das Vertrauen in die automatischen Reaktionen ist die Sicherstellung der Qualität, Zuverlässigkeit, Authentizität und Integrität der Datenbasis des Entscheidungsprozesses essentiell. Unabdingbare Voraussetzung für das Vertrauen in die Datenbasis („trust in data“) und letztendlich in die ausgeführten Reaktionen sind Sicherheitsmechanismen, die dies nachweisbar gewährleisten. Sowohl für die von einfachen Sensoren generierten „Rohdaten“, als auch für akkumulierte Daten.

Aspekte, die in diesem Zusammenhang zu diskutieren sind:

- Grundlage aller Schutzmaßnahmen ist die Sicherstellung einer nachweisbaren eindeutigen Identität für alle beteiligten Komponenten. Vom einfachsten Sensor bis hin zu komplexen IT-Systemen, die diese Daten aggregieren. Die Möglichkeit von „faked Identities“ muss verhindert werden.
- Idealerweise ist die Überprüfbarkeit der Authentizität (Quelle) und Integrität jeder einzelnen Datentransaktion sicherzustellen. Insbesondere auch für den Fall von aus verschiedenen Quellen bereits akkumulierten Daten.
- Diese Bedrohungen machen das Zusammenwachsen des Cyberspace und des Physicalspace deutlich (manipulierter Sensor → Beeinflussung der IT-basierten Entscheidungsfindung → automatische Reaktion mit Einfluß auf den Physicalspace). Oft mit direkter Auswirkung auf Safety-Aspekte.
- Die Notwendigkeit die Verfahren zur Risikobewertung so zu erweitern, dass der Einfluss bestimmter Daten im Allgemeinen und speziell auf automatische Reaktionen angemessen modelliert und berücksichtigt wird.
- Transparenz der Datenwege und –verarbeitung. Einerseits kann dies Angreifern die Identifizierung von Angriffspunkten erleichterm, andererseits ist dies aber für das Vertrauen in die Prozesse und Reaktionen sowie die Risikobewertung (für Organisationen und Individuen) unbedingt notwendig. Hier wird man sich in Analogie zu der Regel „no security by obscurity“ in der Regel für die Priorisierung der Transparenz entscheiden müssen.
- …

Teil 2: Anwendungsbeispiele und Einsatzszenarien

<<Note: Dieser Abschnitt sollte den Bezug zu Trend/Vision und Security angemessen herausstellen>>

Sicherheitsbezogene Herausfodrerungen von eindeutiger Identität und Trusted data in:

- E-government
- E-commerce und Zahlungsverkehr
- Übergreifende Logistik / Lieferketten / Supply Chains
- I 4.0-Produktion / mit Link zu Robotik
- KI-gestützte Entscheidungssysteme, evtl. Optimierungsprozesse, evtl. Gesundheitssystem ?
- Fernwartungsprozesse für Produkte im Endkundeneinsatz mit automatisierter Analyse-Unterstützung, Link zur Sensorik, weiterer Akzent: Link zu Firmware-/Software-Updates
- ….

Teil 3: Schlussfolgerungen:

1. Anforderungen für die technische Umsetzung

Aktive Seite:

- Physisches Netz (Netzwerkprotokoll, Zonierung, Zulassungsbeschränkungen, -prüfungen, Trusted identity“, usw.)
- Übertragungsverfahren und Kryptographie, Schutzmechanismen gegen Fälschung und Verfälschung (im internen und intern-externen Kommunkationskontext)
- Transparency
- Redundanz
- Plausibilitätsprüfungen und evtl. explizite manuelle Freigabe als Prozeßschritt
- ….

Passive Seite:

- IT-„Ecosysteme“ im übegreifenden verbund als Teilenehmer im Kommunikationsverkehr – kontrollierte und überprüfbare Zugänge, KI/Plausibilitäten und Verhaltensmuster-Prüfungen; Maschinenverhalten in sicheren Produktionsumgebungen
- Differenzierung zwischen verschiedenen Einsatz-Szenarien – high vs.low level Security (Link zu den Risiken in Kapitel 1)

2. Minimal-Anforderungen für Sicherheitsstandards

<<Note: soweit nicht im vorhergehenden Abschnitt oberflächlich behandelt, sollten wir in dem Papier evtl. nicht soweit gehen Minimal-Anforderungen für Standards zu definieren. Das wäre evtl. zu ambitoniert, oder ?>>

3. Anforderungen an die regulatorische Ebene – Optionen und Grenzen

4. Empfehlungen / Denkanstöße des Münchner Kreises