MÜNCHNER KREIS - Arbeitskreis Security

Protokoll des Kick-Off-Meetings

Datum: 10. März 2016, 11:00 – 15:30 Uhr

Ort:
Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften
Seminarraum 1
Boltzmannstraße 1
85748 Garching

Teilnehmer:
Jürgen Arnold, Freiberuflicher Unternehmensberater
Dr.-Ing. Udo Bub, EIT ICT Labs Germany GmbH (telefonisch zugeschaltet)
Kai Dörnemann, genua GmbH
Prof. Dr. Michael Dowling, Universität Regensburg / MÜNCHNER KREIS
Prof. Dr. Claudia Eckert, Fraunhofer AISEC / TU München
Hartmut Fuchs, FuchsCCC GmbH / VoiceEV Verband
Dr. Magnus Harlander, genua GmbH
Dr. Detlef Houdeau, Infineon Technologies AG
Peter Köhler , FINAKI Deutschland GmbH
Stefan Maierhofer, Palo Alto Networks
Michael Montag, Nokia
Ramon Mörl, itWatch GmbH
Dr. Rolf Reinema, Siemens AG
Dr. Stefan Schiffner, ENISA
Michael Schneider , Bundesdruckerei / D-Trust
Gunther Schwarz, AIRBUS Defence & Space
Prof. Dr.-Ing. Georg Sigl, Fraunhofer AISEC / TU München
Dr. Stephan Spitz – Giesecke & Devrient GmbH
Prof. Dr. Heinz Thielmann, Emphasys GmbH / MÜNCHNER KREIS

Protokoll: Susanne Starzer und Claudia Eckert

Bem. Der Workshop orientierte sich an der vorab verteilten Agenda

Agenda:

1. **11.00 Begrüßung:** C. Eckert, H. Thielmann
2. **11.05 – 11.30 Kurze Vorstellungsrunde der Teilnehmer:** Alle
   Wer, welche Institution,
   Stakeholder: Anbieter, Anwender, FuE, Politik
3. **Ziele des AK Security und Abgrenzung**
   11.30 – 11.35 Allgemeine Ziele des MK: Intro: C. Eckert, H. Thielmann
   - Orientierungsrahmen für Politik und Wirtschaft
   - Position beziehen

   Formate, Instrumente
   - Expertenworkshops, Fachkonferenzen

- Gesprächsformate: Berliner Gespräch, Round Table
- Papiere : Positionspapiere, Handlungsempfehlungen, ‚Weck-Rufe'

11.35 – 12.00 AK-Security:

- Input von allen Teilnehmern: Ziele und priorisierte Formate/Instrumente , Abgrenzung gegenüber bekannten Initiativen zum Thema Sicherheit

4. **12.00 - 13.30 Sammlung und Diskussion der möglichen Themenfelder**
   Mittagsimbiss gegen 12.30 Uhr
   Intro: C. Eckert
   - Sammlung von Themenvorschlägen mittels Karteikarten an Flipcharts: max. 3 Vorschläge pro Teilnehmer
   - Clustern der Vorschläge durch Moderatoren (**Mittagspause)**
   - Vorstellen der Themen in den Clustern durch die Teilnehmer: warum, welche Zielvorstellung
5. **13.30 – 14.30 Priorisierung der Themen:** Alle
   Vergabe von Priopunkten für die vorgeschlagenen Themen: jeder Teilnehmer kann 5 Punkte vergeben (auch gehäuft)
   Auswertung und Erstellen einer Priorisierung: max. 5 Themen
   Festlegung von Kümmerern für Themen
6. **14.30 – 15.15** Next steps und Festlegung von ToDos
7. **15.30** Weitere Termine und Abschluss

---

1. Begrüßung

- Das Ziel des ersten Meetings: Themenfelder für den AK Security definieren und abstimmen, wie die Themen bearbeitet werden sollen.
- Großes Interesse an der Mitarbeit im AK: 40 Interessenten haben sich gemeldet, daher ist mit weiterem Zulauf zum AK Security zu rechnen.
- Vorstellung der Agenda - keine Änderungsvorschläge von Seiten der Teilnehmer.

2. Kurze Vorstellungsrunde der Teilnehmer

- Teilnehmer siehe oben. Zuordnung der Stakeholder siehe Excel-Liste.
- Erstes Meeting zeigt ein Ungleichgewicht: viele Anbieter von Sicherheitstechnologie, Anwender-Branchen sind noch unterrepräsentiert:
  To do an alle: interessierte Anwender konkret zur Mitarbeit einladen
  - Vorschläge, wer noch eingeladen werden soll (Meinungsbilder etc.), bitte an Claudia Eckert claudia.eckert@aisec.fraunhofer.de senden.
  - Anregung Dr. Schiffner: Data Protection Authority / Zertifizierungs-Authority aufnehmen

3. Ziele des AK Security und Abgrenzung

Vorstellung des MÜNCHNER KREIS durch Prof. Dr. Michael Dowling.

Hinweis auf die neue Broschüre des MÜNCHNER KREIS. Auch Nicht-Mitglieder des MÜNCHNER KREIS können an den Arbeitskreisen teilnehmen bzw. sind erwünscht

Seit eineinhalb Jahren fünf Arbeitskreise:

- Intelligente und vernetzte Mobilität
- Energie
- Digitale Infrastruktur und Basisdienste
- Arbeit in der digitalen Welt
- Neu: AK Sicherheit/Security

Keine Duplizierung von Themen in den Arbeitskreisen gewünscht. Deshalb müssen Themen identifiziert werden, die noch nicht bedient werden. Ziel: Neutrale Plattform, die Orientierung gibt.

Aufgaben des AK Security / Ziele (Dachthemen):

- Für alle Stakeholder: Unterstützung bei Einschätzung der Sicherheitslage, Reifegrad von Lösungen, Handlungsempfehlungen, Kenntnisse über Stärken der Deutschen Industrie (Sicherheitstechnologie)
- Zukunftsorientierte Szenarien: Abgrenzung gegenüber anderer Initiativen:
    - Aufgreifen und diskutieren von neue Paradigmen, deren Impakt auf existierende Geschäftsmodelle
    - Sicherheit in neuem Umfeld: Industrie 4.0, IoT Kette
    - Trends in IT und deren Auswirkungen z. B. Block-Chain-Technologie (BitCoin)
    - Security als Querschnittsthema: Synergien nutzen über Sektoren hinweg z. B. Konnektor-Technologie (eHealth, nPA, Metering, Data-Spaces)

- Bewusstsein schärfen: Stellenwert IT-Sicherheit in allen gesellschaftlichen Bereichen herausarbeiten, damit auch die wirtschaftliche aber auch politische Relevanz von Technologie-Kompetenz/Führerschaft aber auch von Aus- und Weiterbildung
    - Frühzeitige Einbringung des IT Sicherheits-Themas in die Ausbildung: politisches Agenda-Setting
    - Technikabschätzung „rote Linie“ – bestimmte Technik darf nicht miteinander kombiniert und angewendet werden (Leib und Leben in Gefahr)
- X (X=20?) Empfehlungen an die Entscheidungsträger aus Politik und Wirtschaft (alle Sektoren abbilden) erstellen
- Whitepaper für dedizierte Zielgruppen verfassen
- Format: Berliner Gespräche im September zusammen mit EICT?

- Stärken transparent machen: Deutschland ist z. B. führender Standort in der Hardware Sicherheit und auch embedded Software → Fachkonferenz anbieten (Sicherheit in der Komponente)
- Digitale Souveränität: vertrauenswürdige IT „Made in Germany“

Zusammenfassung:

1. Status Quo kritisch & konstruktiv begleiten
2. Nach vorne schauen, was kommt auf uns zu, Stakeholder darauf vorbereiten/sensibilisieren, Awareness: Politik in die Pflicht nehmen
3. Bewerten/Folgen abschätzen

Initiativen: der AK muss eine gute Abgrenzung/Positionierung finden

- VOICE: Kompetenzzentrum, Dienste/Beratung – abgrenzen: VOICE sehr gezielt, wo ist neutrale Stimme, auf welchem Level? Bestpractice-Austausch; Kooperation sinnvoll
- CERT-Verbund: Sharing
- CSSA-Verein
- Sharing-Alliances
- Verbände: Rechtsrahmen mitgestalten
- Abgrenzung zu Münchner Sicherheitsnetzwerk? → Themen werden sich schon überschneiden, aber wie diese bearbeitet werden, ist entscheidend.

4. Sammlung und Diskussion der möglichen Themenfelder

Teilnehmer haben ihre Themen auf Kärtchen geschrieben und ordnen sie den Themenfeldern wie folgt zu:

Anwendungsdomäne

- Branchenübergreifende Konzepte & Lösungen
- IT-Plattform-Architekturen für alle kritischen Infrastruktur-Sektoren
- IT und OT brauchen unterschiedliche Lösungen, was machen wir an der Schnittstelle?
- Stärken: Was können wir tun?
- Vertrauenskette in Robustheit verankern: Vertrauen wird durch Marketing in der Bevölkerung aufgebaut, ohne tatsächlichen/echten Schutz

Technologie Souveränität

- Technologie Souveränität vs. Protektionismus: Wir brauchen Lösungen für globalen Markt
- Security-bezogene Kern-Paradigmen für neue/künftige Entwicklungen (Industrie 4.0 etc.)

- Sichere ID/Blueprint einer bewussten/robusten Sicherheitsarchitektur: Besonders gut geschützte ID/Sicherheitsarchitektur
- Metrik für die Robustheit von IT-Sicherheit: Sicherheitsarchitektur
- Deutsche Sicherheitskerntechnologie
- IT Security und funktionale Sicherheit
- Wie kann man 100% sichere IT-Systeme herstellen? Sicherheit im Gesamtsystem
- Block-Chains sicher? Wozu?
- Fachkonferenz: Stärke HW- und Embedded Security, Sichtbarkeit erzeugen, Wie kann man diese Stärke nutzen?
- Security-Labels unterhalb CC EAL 4+: Komplexe Komponenten & vertrauenswürdige Lieferanten (unterschiedliche Sicherheitsniveaus)

Standards

- Verbindung der Safety mit der Security Welt
- Politik – Standards – Normen: Reichen diese aus? Kreativität der Bedrohungen nimmt zu!
- Beurteilung von Referenzarchitekturen – positiv / negativ
- Technische Reife / Sicherheitsqualität / Produktreife: Was ist technisch machbar? → ist dann der Standard
- Security Info Sharing / Common Threat Intelligence: Awareness schaffen, wie könnte es in der Zukunft aussehen?
- Cyber Security Versicherung: Standard werden verlangt werden. Technologie-Folgen Abschätzung

Trends / Neue Herausforderungen

- Vorausschauend die Rolle von IT Sicherheit bei neuen Themen (z. B. IoT, Industrie 4.0, Connected Cars): Themen setzen
- Orientierung: Trends und alternative Szenarien inkl. sozio-ökonomischer Aspekte z. B. Safety, Block-Chain
- Was passiert nach Erfindung der Block Chain?
- By Design Paradigma: Auf den Prüfstand stellen
- Useable Security: Sicherheit wird als Bremse begriffen
- End-to-End Sec: Referenzarchitekturen/Sec Index/Sec Standards → Management!

Aus-/Weiterbildung

- Lehrpläne / Studienpläne / Interdisziplinarität
- Vorschule, Schule, Uni – auch restl. Bevölkerung (Fortbildungsmaßnahmen anbieten), Kultusministerium, VHS
- Ausbildung
- Politik in die Pflicht

Awareness Gesellschaft

- Status Quo: Was ist der Status Quo? Womit müssen wir uns eigentlich auseinandersetzen? Strukturieren & Darstellen
- Gesellschaftliche Diskussion anstoßen: Wo akzeptieren wir welche Überwachung? Oder: Wo müssen wir Daten wie schützen?
- Dialog mit Politik, Verwaltung & Bevölkerung
- Sensibilisierung für die Problematik – Zukunftsszenarien (bisher haben wir noch Glück gehabt bzw. Vorfälle werden nicht publik gemacht)

Ordnungsrahmen/Gesetze

- Beurteilung des rechtlichen und regulatorischen Rahmens
- Schutz der digitalen Identität
- Kritis Schutzziele auf Metrik abbilden: Mindeststandards/Mindestschutz
- Gesetzgeber: Mindeststandards fordern, nicht nur dem Markt überlassen

Freie Themen

- Geschäftsmodelle für Sicherheit
- Stellenwert der IT Sicherheit

5. Priorisierung der Themen

Jeder Teilnehmer erhält 5 Klebepunkte und darf diese vergeben (auch gehäuft). Daraus ergeben sich folgende Schwerpunkte:

Anwendungsdomäne

- Branchenübergreifende Konzepte & Lösungen
- IT-Plattform Architekturen für alle kritischen Infrastruktur-Sektoren

Technologie Souveränität

- Sichere ID/Blueprint einer bewussten/robusten Sicherheitsarchitektur: besonders gut geschützte ID/Sicherheitsarchitektur, Wie bewertet man das?
- Security & Safety: Wechselspiel, Zusammenspiel, Auswirkungen

Standards

- Beurteilung von Referenzarchitekturen – positiv / negativ

Trends / Neue Herausforderungen

- Orientierung: Trends und alternative Szenarien inkl. sozio-ökonomischer Aspekte z. B. Safety, Blog-Chain; Welche Bedeutungen hat das auf verschiedene Bereiche? Referenzarchitekturen

Awareness Gesellschaft

- Gesellschaftliche Diskussion anstoßen: Wo akzeptieren wir welche Überwachung? Oder: Wo müssen wir Daten wie schützen?
- Sensibilisierung für die Problematik – Zukunftsszenarien (bisher haben wir noch Glück gehabt bzw. Vorfälle werden nicht publik gemacht)

6. Next Steps und Festlegung von ToDos

Diskussion der Teilnehmer über die weitere Vorgehensweise. Themenabstract soll zu den einzelnen Themen verfasst werden.

Folgende Aspekte sollen dabei erarbeitet werden:

- Herausforderung
- Status Quo
- Ziel / Nicht-Ziel
- Umsetzung

Erstellung von Abstracts: Themen und Kümmerer, bis zum 1.4.2016

1. Architektur: Kümmerer: Ramon Mörl und Michael Schneider

2. Neue Trends: Kümmerer: Michael Montag und Hartmut Fuchs

3. Gesellschaftliche Diskussionen: Kümmerer: Georg Sigl und Stefan Schiffner

Folgende Überlegungen wurden angestellt:

- Was ist Inhalt, was nicht? Was verstehen wir unter dem Thema?
- Wird das den unterschiedlichen Themenfeldern gerecht? Für jeden Themenblock überlegen, wie es bearbeitet werden muss.
- Wer ist die Zielgruppe? Wen wollen wir adressieren? Beratung der Politik, Industrieunternehmen, Anwender?
- Welche Formate stellen wir uns vor? Konferenz? Beiträge?

- Ist für dieses Jahr noch eine Veranstaltung geplant? Falls ja, alle drei Themen für Veranstaltung?

Mögliche Veranstaltung: Berliner Gespräch

Max. 100 Teilnehmer, Thema „Ordnungsrahmen“ denkbar

Weiteres Vorgehen:

- Protokoll wird an alle, die auf der Liste stehen, versendet.(auch an die eingeladenen, verhinderten auf der Liste
- Zudem wurde mehrfach der Wunsch geäußert, eine Teilnehmerliste mit den Angaben Name, Firma und E-Mail zu haben. Die anwesenden Teilnehmer stimmen der Weitergabe Ihrer Daten zu. Eine entsprechende Liste wird vorbereitet und den Teilnehmern des Kick-Off-Meetings per Mail gesendet.
- Um Ausarbeitung der Themenabstracts wird bis 1. April 2016 gebeten
- Bei nächstem Meeting: Themenabstracts diskutieren und weiteres Vorgehen festlegen

7. Weitere Termine und Abschluss

Nächstes Meeting AK Security des MÜNCHNER KREIS ist für

- Dienstag, den 19. April 2016 11 - 14 Uhr geplant
- Gastgeber: Firma Siemens, Neuperlach, München
  vielen Dank an Dr. Rolf Reinema
- Eine Einladung wird an alle Teilnehmer und Interessenten an einer AK-Mitarbeit versendet.
- Vorschläge, wer noch eingeladen werden soll (Meinungsbilder etc.) bitte an Claudia Eckert, claudia.eckert@aisec.fraunhofer.de, senden.