

MÜNCHNER KREIS - Arbeitskreis Security

Aktionsliste

Themenfeld	Aufgabe	Kümmerner	Deadline
<u>Gesellschaftliche Diskussion</u>	Aufbereiten und vertiefen der Themen: Grundverordnung, Krypto-Debatte und Lebenszyklus der Daten; Ziel/Ergebnis: Agenda für Fachkonferenz, Expertenworkshop	Prof. Dr. Udo Helmbrecht/ENISA, Prof. Dr.-Ing. Georg Sigl, (Dr.-Ing. Udo Bub)	Juni
<u>Trendbeurteilung</u>	Analyse existierender Reports, Prüfen der vorgeschlagenen Themen, Plan für weitere Vorgehensweise	Michael Montag, Kai Dörnemann, Jamie Wilkie, Hartmut Fuchs	Juni
<u>Architektur</u>	Erstellen einer Studie: Fragenkataloge für Stakeholder entwickeln Ggf. Thema für eine Podiumsdiskussion, Kammingespräch Was wollen Anwender an Sicherheit (messbar)	Dr. Kim Nguyen, Kai Dörnemann, Stefan Maierhofer, Ramon Mörl , (Dr.-Ing. Udo Bub)	Juni
<u>Berliner Gespräch</u>	Thema für Berliner Gespräch: • Krypto-Debatte: Freie vs. regulierte Kryptografie, Exportkontrolle, organisierte Kriminalität • Trend-Thema auch denkbar? Bitte prüfen und Feedback geben	Dr.-Ing. Udo Bub, Prof. Dr.-Ing Georg Sigl, Prof. Dr. Udo Helmbrecht, Klaus-Dieter Wolfenstetter	April/Mai

Protokoll des zweiten Arbeitstreffens

Datum: 19. April 2016, 11:00 – 14:45 Uhr

Ort:

Siemens AG
Otto-Hahn-Ring 6
81739 München

Teilnehmer:

Dr.-Ing. Udo Bub, EIT ICT Labs Germany GmbH
Kai Dörnemann, genua GmbH
Prof. Dr. Claudia Eckert, Fraunhofer AISEC / TU München: Moderation
Prof. Dr. Udo Helmbrecht, ENISA
Stefan Maierhofer, Palo Alto Networks
Michael Montag, Nokia
Ramon Mörl, itWatch GmbH
Dr. Rolf Reinema, Siemens AG

Prof. Dr.-Ing. Georg Sigl, Fraunhofer AISEC / TU München
Jamie Wilkie, Fujitsu Technology Solutions GmbH
Klaus-Dieter Wolfenstetter, Deutsche Telecom AG

Protokoll: Prof. Dr. Claudia Eckert, Susanne Starzer

Bemerkung: Das Arbeitstreffen orientierte sich an der vorab verteilten Agenda.

Agenda:

1. **Begrüßung**
2. **Kurze Zusammenfassung des Standes nach dem Kick-off Workshop**
3. **Vorstellen und Diskussion der drei priorisierten Schwerpunktthemen**
4. **Konferenz im September in Berlin:** Thema, Format, Zielgruppe
5. **Weitere Schritte**

1. Begrüßung

- Das Ziel des zweiten Arbeitstreffens: Erarbeiten eines abgestimmten Bildes der jeweiligen Schwerpunktthemen sowie das Festlegen weiterer Schritte.
- Vorstellung der Agenda: Keine Änderungsvorschläge von Seiten der Teilnehmer
- Kurze Vorstellungsrunde der anwesenden Teilnehmer

2. Kurze Zusammenfassung des Standes nach dem Kick-off Workshop

- Schwerpunkt des Kick-Off Workshops: Ziele des neu gegründeten AK Security im Rahmen des MÜNCHNER KREIS und Identifikation der Themenfelder, die im Rahmen des AK Security bearbeitet werden sollen.
- Die Ergebnisse wurden in einem Protokoll erfasst, welches an alle Teilnehmer und Interessenten versandt wurde. Alle erarbeiteten Themenfelder sind dort nachzulesen.
- Nach der Priorisierung der Themenfelder ergaben sich drei Schwerpunktthemen, die weiter erarbeitet werden sollen:
 - (1) Gesellschaftliche Diskussion
 - (2) Trendbeurteilung
 - (3) Robustheit von IT-Sicherheitsarchitekturen

3. Vorstellen und Diskussion der drei priorisierten Schwerpunktthemen

Ziel: Erarbeiten eines abgestimmten Bildes der Teilnehmer pro Schwerpunktthema zu den vier Fragen:

- Herausforderung?
- Status Quo?
- Ziel/Nicht-Ziel?
- Umsetzung? Welche Zielgruppe, welche Formate für den Transfer?

3.1 Gesellschaftliche Diskussion (Kümmerer: Prof. Dr.-Ing. Georg Sigl & Dr. Stefan Schiffner)

Vorstellen der Ergebnisse durch Prof. Dr. Helmbrecht und Prof. Dr.-Ing. Sigl (vorab verteiltes Papier als Grundlage)

Herausforderung?

- Daten: Was passiert mit den Daten? Wie können/wollen wir das gestalten?
- Krypto-Debatte: Freie vs. regulierte Kryptografie, Exportkontrolle, organisierte Kriminalität
- Terrorismus: Datenschutz als Blockade der Strafverfolger vs. Kunden/Bürger-Schutz, freier Datenaustausch
- Staat schützt Bürger: Durch Regulierung? Bürger vor sich selbst schützen?
- Daten-Owner-Ship, Datenschutzregelungen
- Sektoren-bezogener Umgang mit Daten
- Aufzeigen und Nutzen von (almost) Best Practices, z. B. Banking
- Einbettung in international Entwicklung, keine Insellösung, pragmatische Vorgehensweise, welche Sicherheitsstandards benötigen wir?
- Datenlebenszyklus gestalten, loslösen von jahrzehntelang gelebten Privacy-Paradigmen!
 - Datenschutz bei Erfassung: Status Quo gemäß Datenschutzgesetz (a priori Schutz, Datensparsamkeit, Zweckbindung etc.) versus
 - Benutzungsbezogen: A posteriori, Dienste bezogen, freie Erfassung und Speicherung, Kontrollen und Schutz erst bei deren Nutzung
 - Chancen/Risiken für deutsche Unternehmen herausarbeiten

Ziel/Nicht-Ziel?

- Was ist möglich, wie geht man mit dem technischen Möglichkeiten um?
- Welche Technologien sollen gefördert werden: Was beherrschen wir schon vs. was wäre gewünscht?
- Vorgehen: rote Linie erforderlich, oder alles zulassen, was möglich ist?
- Festlegen von „Leitplanken“, nicht 100%ige Security
- Befähigung zum kompetenten Dialog/Einschätzung: Was bedeutet Datenschutzverordnung, Datensicherheit, Geschäftsmodell (trotz Regelung, durch Regelung,...), nationale Schutzinteressen
- Dilemma: Positionierung zu der Problematik „Totale Überwachung vs. Freiheit“
- Balance zwischen Hemmnis/Schutz und Enabling/Innovationsfähigkeit
- Zielgruppenfokussiert: KMUs, Empfehlungen erarbeiten, Automotive OEMs

Umsetzung?

Themen für Fachkonferenz:

- Anwendungen und technische Möglichkeiten der Datenanalyse
- Individualschutz: Vor Datenmissbrauch schützen, Bewusstsein über Risiken schaffen
- Staatliche Interessen: Kritische Infrastrukturen schützen, Kryptographie vs. Abhörmöglichkeiten zum Zivilschutz

Granularität: - personenbezogen, kritisch: Gesundheit
- businessbezogen: Know-How-Schutz

Berliner Gespräch im September als mögliche Veranstaltung: Thesen diskutieren, Moderierter Dialog, Fachkonferenz des MÜNCHNER KREIS.

NEXT STEPS:

- Aufbereiten und vertiefen der Themen: Grundverordnung, Krypto-Debatte und Lebenszyklus der Daten
- Ziel/Ergebnis: Agenda für Fachkonferenz, Expertenworkshop erarbeiten
- Berliner Gespräch im September: Vorschlag: Krypto-Debatte thematisieren (Regulierung versus frei etc.)
- Kümmerer: Prof. Dr. Udo Helmbrecht/ENISA & Prof. Dr.-Ing. Georg Sigl, Einbindung von Dr.-Ing. Udo Bub (siehe letzten TOP)

3.2 Trendbeurteilung (Kümmerer: Michael Montag & Hartmut Fuchs)

Vorstellen der Ergebnisse durch Michael Montag (vorab verteiltes Papier als Grundlage)

Herausforderung?

- Fokussierte Auswahl der Themen: Was ist/wird relevant für wen? Cybersecurity muss im Fokus stehen, Themen nicht zu breit aufbereiten, es gibt schon viele Trendstudien
- Konkrete Beispiele bewerten und mögliche Auswirkungen aufzeigen (z. B. Autonomes Fahren: Security Impact auf Safety)
- Szenarien durchspielen: Was wäre wenn? IT als Auslöser, Haftungsprobleme
Beispiele: Ransomware-Angriffe, Klinikum Neuss Vorfall
- Szenarien-orientierte Analyse? Reaktions-Optionen (Föderalismus-Debatte als Beispiel)
- Was kann der **AK-Security an Mehrwerten schaffen in der Trend-Debatte**
 - Raum der Optionen, der möglichen Spiel- und Gestaltungsräume ausloten
 - Kurzfristige Reaktion auf aktuelle Themen? Stellungnahmen?
Die Diskussion hat ergeben, dass dies nicht durch den AK zu leisten sein wird
 - Qualifizierte, bewertende Analyse bestehender Reports, fokussiert auf zentrale, durchgehende Trends, nachhaltige Themen identifizieren und kompetent begleiten (Fokus auf Security!)
 - Abgrenzung gegenüber existierende Studien – Mehrwert entsteht erst durch technologie-bezogene Bewertung, Nachhaltigkeit: gesellschaftliche Auswirkungen.
Diskussion: diese Bewertungen erfordern erheblichen Zeit- und Ressourcen-Einsatz, könnten aber mehrwertig sein

Ziel/Nicht-Ziel?

- Erstellen von Trend-Reports zu umrissenen Themen, Trends: Optionen, Entscheidungsspielräume

Diskussion: keine ‚yet another Trend‘-Vorgehensweise, sondern Sicherheit als Fokus und bewertend, einordnend

- Regelmäßige Updates, homogene Struktur, modulare Struktur

Diskussion: ressourcenkritisch, wie sieht das Qualitätsmanagement aus

- Blog des MÜNCHNER KREIS zur Trendbeurteilung

Diskussion: ressourcenkritisch!

- Breite Erreichbarkeit: Online verfügbar
- Methoden der Technologie-Folgeabschätzung

Diskussion: besser stärker fokussieren auf Sicherheitsthemen

Start: Mögliche Themen als Diskussionsgrundlage

- autonome, collaborative Robotik (Automobile, Home)
- Identität, M2M Objekt-IDs, Unfälschbarkeit
- Sicherheitsstandards: Rolle der Cyber-Security Versicherer
- Zertifizierungen

Umsetzung?

- Editorial Board etablieren
- Trendteam: Regelmäßige Telefonkonferenzen/Treffen
 - Kriterien für Themenauswahl?
 - Nachhaltigkeit/Disruptions-Pontential
 - Handlungsoptionen sind vorhanden
 - „Agenda Setting“ Ziel: Bewusstsein schaffen bei den Interessengruppen und Entscheidern über die relevanten aktuellen Fragenstellungen und deren möglichen Auswirkungen
 - Zielgruppe pro „Modul“ festlegen

NEXT STEPS:

- Trendteam bestehend aus Michael Montag, Kai Dörnemann, Jamie Wilkie, Hartmut Fuchs
- Kümmerer/Ansprechpartner: Hartmut Fuchs
- Analyse existierender Reports, Prüfen der vorgeschlagenen Themen, Plan für weitere Vorgehensweise

3.3 Robustheit von IT-Sicherheitsarchitekturen (Kümmerer: Ramon Mörl & Michael Schneider)

Vorstellen der Ergebnisse durch Ramon Mörl.

Herausforderung?

- Robustheit von IT-Security-Infrastrukturen: Die Fähigkeit, Veränderung der Umwelt standzuhalten (hier: Angriffen standzuhalten)
- Identifikation von schwächsten Gliedern: Robustheit der Handlungskette? Organisatorische Einbettung und benötigtes Know-How? Haftung und Rechtssicherheit?
- Metrik für die Bewertung der Robustheit fehlen
- (Anonymisierte) Bereitstellung von u. a. Robustheitsevaluationen auf neutrale Plattform: Qualität?
- Sichere Identität

Ziel/Nicht-Ziel?

- Vorgehensweise, um zu einer neutralen Plattform zu kommen: Anregung/Empfehlung zum Etablieren einer Plattform:
Diskussion: Was soll sie sein, welchen Mehrwert soll sie bieten?
 - Was genau? Eigenschaften?
 - Benchmarks?
 - Abgrenzung zu Common Criteria (CC)
- Rolle des MÜNCHNER KREIS hierzu:
 - Bewertung von Produkten?
Diskussion: nein! Keine MK Aufgabe
 - Regulierungsnotwendigkeit aufzeigen?
 - Handreichung zur Bewertung für KMUs? Empfehlungen in Richtung Investitionssicherheit?
Diskussion: schwierig, wer soll das leisten
- Handlungsempfehlungen: Wege zu einer pragmatischen, risikobasierten Entwicklung von Sicherheitsarchitekturen

Problem: Viele wenig erfolgreicher, wenig nachhaltiger Vorarbeiten durch zum Teil große Stakeholder-Gruppen u.a. Capability Maturity Model

Diskussion: was genau kann der MK in diesem Themenumfeld leisten!

Nicht-Ziel: Konkrete robuste Infrastruktur-Blueprints

Umsetzung? / NEXT STEPS:

Erstellen einer Studie:

- Team: Dr. Kim Nguyen, Kai Dörnemann, Stefan Maierhofer, Ramon Mörl, (Dr.-Ing. Udo Bub)
- Kümmerner: Ramon Mörl
- Start: Fragenkataloge für Stakeholder entwickeln, Draft bis Juni erstellen
- Ggf Thema für eine Podiumsdiskussion, Kamingsgespräch
- Was wollen Anwender an Sicherheit (messbar)

4. Konferenz im September in Berlin

- Angebot von Dr.-Ing. Bub (EIT ICT Labs): Gemeinsame Veranstaltung im September in Berlin

- 22. September: Innovationskonferenz; Berliner Gespräch am Abend zuvor: 21. September
- Zeitrahmen: Beginn um 18 Uhr, Ausklang ca. 21 Uhr, Open End
- Zielgruppe: Politik
- Format: Vorträge, Diskussionen
- Ca. 80 geladene Gäste
- Location wird kostenfrei zur Verfügung gestellt, Catering zahlt MÜNCHNER KREIS
- Themensetzung im Juni, Terminankündigung soll bereits im Mai versendet werden

Inhalte:

- Krypto-Debatte: Freie vs. regulierte Kryptografie, Exportkontrolle, organisierte Kriminalität
- Trend-Thema auch denkbar? Bitte prüfen und Feedback geben
- Kümmerer: Dr.-Ing. Udo Bub, Prof. Dr.-Ing Georg Sigl, Prof. Dr. Udo Helmbrecht, Klaus-Dieter Wolfenstetter

5. Weitere Schritte

- Nächstes Arbeitstreffen des AK Security ist für Mitte Juni/Juli angesetzt
- Terminvorschläge kommen von Prof. Dr. Claudia Eckert (via Doodle-Umfrage)
- Ort für das nächste Arbeitstreffen:
Angebot von Vodafone, dort das nächste Treffen zu veranstalten (München oder Düsseldorf).
Von Seiten der anwesenden Teilnehmer ist München als Veranstaltungsort weiterhin gewünscht. Alternativ: Leibniz-Rechenzentrum stellt dem AK Security einen Meetingraum kostenfrei zur Verfügung.
- **Aufruf an alle Interessenten:** Wer sich noch an Themen beteiligen möchte, kann dies sehr gerne tun. Bitte bei Prof. Dr. Claudia Eckert melden (E-Mail: claudia.eckert@aisec.fraunhofer.de) oder direkt bei den jeweiligen Kümmerern der Themen melden.