



Münchner Kreis - Arbeitskreis Security

Protokoll des dritten Arbeitstreffens

Aktionsliste

Themenfeld	Aufgabe	Kümmerner	Deadline
<u>Gesellschaftliche Dimension / Berliner Gespräch</u>	Thema des Berliner Gesprächs ändern in: „Cyber-Security - Neue Services im Spannungsfeld zwischen Regulierungen und Selbstverantwortung“ → Telefonkonferenz ansetzen	Prof. Dr. Udo Helmbrecht/ENISA, Prof. Dr.-Ing. Georg Sigl, Prof. Dr. Heinz Thielmann , Dr.-Ing. Udo Bub	asap
	Berliner Gespräch abwarten und gewonnene Erfahrungen daraus in Planung für Fachkonferenz einfließen lassen		asap
	Team aus ca. 6 Personen sollen Thesen als Briefing für die Referenten formulieren	Koordinator: H. Thielmann	asap
<u>Trendbeurteilung</u>	Unterarbeitsgruppe zum Thema Blockchain: Meeting ansetzen, Thema aufbereiten: Pros & Cons im Überblick. 2-4 Seiter erstellen	Dr. Rolf Reinema , Prof. Dr. Claudia Eckert, Dr. Detlef Houdeau	September
	Workshop organisieren, um Thema des Papiers einzugrenzen, Fokus festlegen; Ressourcen prüfen und Timeline festlegen.	Michael Montag , Kai Dörnemann, Jamie Wilkie, Hartmut Fuchs	September
<u>Architektur</u>	Idee von Neutraler Plattform weiter vorantreiben. Themenabend für Politik & Verbände geplant: Erstellen des Einseiter für das Wirtschaftsministerium.	Ramon Mörl , Kai Dörnemann, Stefan Maierhofer	September
<u>Dokumentenarchiv</u>	Share für Dokumente anlegen	Eckert, Starzer	done
<u>Konferenz</u>	Net.Law.S Konferenz in Nürnberg, 2017	Herr Mörl versendet Infos zur Konferenz	asap

ACHTUNG:

Alle Protokolle, Papiere, Präsentationen werden auf dem MK Server abgelegt: Zugriff für MK Mitglieder über ihre jeweiligen Logins, für nicht-MK Mitglieder ist ein Zugriff über **Login: ak_security, PW: 7xYEHrb5** möglich.

Protokoll des dritten Arbeitstreffens

Datum: 18. Juli 2016, 17:00 – 20:00 Uhr

Ort:

Vodafone Kabel Deutschland
Betastr. 6-8
85774 Unterföhring

Teilnehmer:

Jürgen Arnold
Dr.-Ing. Udo Bub, EIT ICT Labs Germany GmbH
Abdou Naby Diaw, Vodafone GmbH
Dr. Jörg Dörr, Fraunhofer IESE
Prof. Dr. Gabrijela Dreo Rodosek, Universität der Bundeswehr München
Prof. Dr. Claudia Eckert, Fraunhofer AISEC / TU München
Prof. Dr. Udo Helmbrecht, ENISA
Dr. Detlef Houdeau, Infineon Technologies AG
Michael Montag, Nokia
Wolf-Rüdiger Moritz, Infineon Technologies AG
Ramon Mörl, itWatch GmbH
Christoph Raab, AIRBUS Defence und Space
Dr. Rolf Reinema, Siemens AG
Manfred Ruttmar, Atos Solutions and Services GmbH
Prof. Dr. Peter Scholz, Institut für Forensik in der Informatik
Prof. Dr.-Ing. Georg Sigl, Fraunhofer AISEC / TU München
Prof. Dr. Heinz Thielmann, Emphasys GmbH
Jamie Wilkie, Fujitsu Technology Solutions GmbH
Eva Sophie Wiesmüller, Power2Progress
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, Vorstellungsrunde
2. Kurze Vorstellung des Gastgebers Vodafone: Herr Diaw
3. Zusammenfassung des Standes der Diskussion aus den letzten AK Sitzungen: Frau Eckert
4. Stand der Planung des Berliner Gesprächs am 13.10.2016 (Tischvorlage): Herr Thielmann
5. Diskussion der Weiterführung des Schwerpunktthemas: Gesellschaftliche Dimension:
Impuls: Herr Helmbrecht, Herr Sigl
6. Diskussion der Weiterführung des Schwerpunktthemas: Trendentwicklung:
Impuls: Herr Montag

7. Diskussion der Weiterführung des Schwerpunktthemas: Robustheit von IT Sicherheitsarchitekturen:
Impuls: Herr Mörl
 8. Next Steps
 9. Weitere Termine
Abschluss und lockerer Ausklang
-

1.) Begrüßung und Vorstellungsrunde

- Vorstellung der Agenda: Keine Änderungsvorschläge von Seiten der Teilnehmer
- Kurze Vorstellungsrunde der anwesenden Teilnehmer

2.) Kurze Vorstellung des Gastgebers Vodafone: Herr Diaw

Die Präsentation von Herrn Diaw wird auf dem Share den AK Teilnehmern zur Verfügung gestellt.

3.) Zusammenfassung des Standes der Diskussion aus den letzten AK Sitzungen: Frau Eckert

Der AK Security hatte bisher zwei Arbeitstreffen. Im ersten Treffen wurden die Ziele des AK Security diskutiert und festgelegt:

- Handlungsempfehlungen für alle Stakeholder
- Zukunftsorientierte Szenarien
- Bewusstsein schärfen
- Stärken bewusster machen

Des Weiteren wurden die Themenfelder, die im Rahmen des AK Security bearbeitet werden sollen, festgelegt:

- Branchenübergreifende Konzepte, Lösungen, Architekturen
- Technologie Souveränität
- Standards
- Trends, neue Herausforderungen
- Aus- und Weiterbildung
- Awareness, Gesellschaft
- Ordnungsrahmen

Nach der Priorisierung der Themenfelder ergaben sich drei Schwerpunktthemen, die nach dem ersten Treffen in Arbeitsgruppen weiter erarbeitet wurden:

- 1) Gesellschaftliche Diskussion (U. Helmbrecht, G. Sigl)

2) Trendbeurteilung (M. Montag, H. Fuchs)

3) Robustheit von IT-Sicherheitsarchitekturen (R. Mörl, M. Schneider)

In den Arbeitsgruppen wurden Positionspapiere zu den drei Themen erarbeitet, die während des 2. Arbeitstreffens besprochen wurden. Veranstaltung der Berliner Gespräche im Oktober bei EIT ICT Labs Germany GmbH/EIT Digital Germany in Berlin wurde beschlossen.

4.) Stand der Planung des Berliner Gesprächs am 13.10. 2016 (Tischvorlage): Herr Thielmann

Save the Date wurde versandt:

Berliner Gespräch des MÜNCHNER KREIS zum Thema "Cyber-Security - wieviel Regulierung - wieviel Selbstverantwortung?" am 13. Oktober 2016, 16:00 - 22:00 Uhr bei EIT ICT Labs Germany GmbH/EIT Digital Germany in Berlin.

In einem Kreis von max. 100 Teilnehmern (Politik, Wirtschaft, Wissenschaft) sollen in kurzen Keynotes und Impulsvorträgen (Politik, Anbieter, Anwender, F&E) folgende Aspekte behandelt werden:

- Welche Anforderungen stellt dies an die staatliche Regulierung?
- Welche Folgen hat dies für die Wirtschaft?
- Welche Technologien für Lösungen kann die Forschung bieten?

Für die Keynotes (Dauer ca. 15-20 Minuten) haben bereits zugesagt:

- Staatssekretär Klaus Vitt, Bundesministerium des Inneren, CIO des Bundes
- Prof. Udo Helmbrecht, Präsident der ENISA
- Arne Schönbohm, Präsident des BSI

Für die Panel mit den Keynote-Referenten und eingeladenen Impuls-Referenten (Dauer der Impulsvorträge max. ca. 10 Minuten) haben zugesagt:

- Anbietersicht: Dr. Magnus Harlander, genua GmbH
- juristische Sicht: Dr. Alexander Duisberg, Bird & Bird
- F&E-Sicht: Prof. Dr. Claudia Eckert, Fraunhofer-AISEC
- Anwendersicht: Joachim J. Reichelt, CIO-Bosch-Siemens-Hausgeräte
Dr. Jürgen Sturm, CIO-ZF
- Herr Kammer, DIVSI, Hamburg

Plenum soll einbezogen werden: mindestens 2 Stunden offene Diskussion ist geplant.

Aktueller Status: In der endgültigen Planung – Einladungen wurden inzwischen versendet; bereits mehr als 70 Anmeldungen

Herr Wilkie weiß evtl. einen Security CTO, der einen Impuls-Vortrag halten könnte. Noch möglich?
→ Ja, aber wird nicht mehr in Agenda aufgenommen. Aufruf: Wer gute Leute kennt oder sonstige Anregungen etc. hat, soll sich bitte melden.

Bem: Inzwischen konnte zusätzlich Herr Kammer, Geschäftsführer des DIVSI, gewonnen werden, im Panel mitzuwirken und die Ergebnisse der aktuellen DIVSI Internet-Milieu-Studie zu präsentieren.

6. Berliner IT-Sicherheitskonferenz:

Am Folgetag, dem 14. Oktober 2016, findet am gleichen Ort die **6. Berliner IT-Sicherheitskonferenz** zum Thema "**Cyber-Security zwischen Innovation und Schutzbedürfnis**" statt. Format der Konferenz: findet alle zwei Jahre statt (seit 2008). Es soll sichergestellt werden, dass die thematische Kohärenz zwischen den beiden Veranstaltungen gegeben ist.

Anmerkungen:

- Herr Thielmann: Mehrere AKs des MÜNCHNER KREIS, deshalb sollte man darauf achten, dass sich die AKs gegenseitig informieren. Herr Arnold ist z. B. im AK Energie: Dort kommen auch Sicherheitsfragen auf. In die anderen AKs sollen Themen gespiegelt werden, Querverbindungen geschaffen werden – keine Silos bauen. Protokolle sollten ausgetauscht werden

Evtl. Besuch der anderen AKs mit Vorträgen. Ziel: Kein Aktionismus, sondern Themen bearbeiten, die so noch nicht bearbeitet werden, Infos austauschen, Infopapiere ausarbeiten für Politik und Stakeholder aus der Wirtschaft.

- Herr Mörl: Regulierung und Selbstverantwortung: Net.Law.S Konferenz im Februar 2017 in Nürnberg. Herr Mörl sendet Mail mit Infos zur Konferenz an die Teilnehmer.

5.) Diskussion der Weiterführung des Schwerpunktthemas: Gesellschaftliche Dimension:

Impuls: Herr Helmbrecht, Herr Sigl

Die Präsentation von Herrn Sigl wird auf dem Share abgelegt.

- Folie 1: Chancen und Risiken der Digitalisierung und wie sie sich für Individuen, Firmen, Betreiber und Staat darstellen
- Folie 2: Fragen und Ziele

Diskussion bzgl. Berliner Gespräch:

Thema sehr breit – kann oder soll man es eingrenzen/fokussieren?

Keynotes von Vitt und Schönbohm: Fokussiert, nicht zu breit, durch Moderation lenken bzw. vorher mit ihnen abstimmen, in welche Richtung der Vortrag gehen soll. Schönbohm soll in seiner Keynote alle Themen/Stakeholder ansprechen

→ Referenten und Impulsgeber sollen eine Leitlinie erhalten; Basis evtl. die Folien von Herrn Sigl

AP: H.Thielmann

→ Anpassung des Themas des Berliner Gesprächs. Neuer Titel: „**Cyber-Security - Neue Services im Spannungsfeld zwischen Regulierungen und Selbstverantwortung**“.

AP: H.Thielmann

Fachkonferenz?

Ist es sinnvoll, eine Fachkonferenz zu machen, bei der die Themen etwas breiter aufbereitet werden?
Falls ja: muss zügig ein Gremium identifiziert werden sowie festgelegt werden, welches Format die Konferenz haben soll. Workshop-Charakter? Thesenpapier erstellen?

Aufgrund von langen Vorlaufzeiten: bald mit der Planung starten! Erfahrung von Seiten MÜNCHNER KREIS: Dreivierteljahr Vorlaufzeit nötig, um gute Qualität zu erhalten.

Diskussion: Wo stehen wir? Sind wir schon soweit? Oder sollte man das Berliner Gespräch abwarten?

→ Fachkonferenz wäre gut. Eine Veranstaltung pro Jahr sollte angestrebt werden. Letzte Fachkonferenz war vor ca. 4 Jahren – es wird Zeit, wieder sichtbar zu werden.

Fazit:

- Thema des Berliner Gesprächs ändern in: „**Cyber-Security - Neue Services im Spannungsfeld zwischen Regulierungen und Selbstverantwortung**“
- Berliner Gespräch abwarten und gewonnene Erfahrungen daraus in Planung für Fachkonferenz einfließen lassen
- Team aus ca. 6 Personen sollen Thesen als Briefing für die Referenten formulieren

6.) Diskussion der Weiterführung des Schwerpunktthemas: Trendentwicklung: Herr Montag

Regelmäßige Trendreports sollen erstellt werden. Soll jedoch nicht „yet another Security Trendreport“ sein. Thema für erstes Papier: **Sichere Identitäten & Trust in Data**

- Umfang: 8-10 Seiten
- Trust in Data: Sehr viele Systeme betreiben Datenanalyse, KI Revival → Reaktion von einem System, ohne dass ein Mensch dazwischen steht; Vertrauen in die Daten: manipulationssicher, nachverfolgbar, Qualität?
- Trust in Analytics: Trust in Ergebnis, malicious data. Wie weit kann ich den Analytics vertrauen? Rohdaten von Sensor: sicher? IT-Systeme die Daten kumulieren: sicher? Vertrauenswürdig? → Transformation von Vertrauen ist nötig

Momentan: Entwurf für Outline steht, teilweise schon mit Inhalten gefüllt. Wird im Anhang mit dem Protokoll versendet.

Ziel: Noch in diesem Jahr das erste Papier fertigstellen. Input zu Berliner Gespräch liefern? → wird offen gelassen, ob man es schafft – hängt von Ressourcen ab. Zumindest möchte man verwertbare Zwischenergebnisse beitragen können.

Hinweis: Von Plattform Industrie 4.0 gibt es so ein Papier – Abgrenzung nötig, neuerer Ansatz!
→ Hinweise wichtig von Seiten der Teilnehmer, damit man nichts übersieht! Daher bitte um Feedback bzw. Anregungen von Seiten der Teilnehmer!

→ **Konsens: Thema noch nicht final!**

Vorschlag: Im Rahmen eines Workshops über Themenzuschnitt und Feinheiten diskutieren. Überlegen, ob man eine Art „Weckruf“ senden sollte - welche Themen kommen auf uns zu?

Möglichst bald:

- Kreis der Beitragenden soll erhöht werden, allerdings soll der Kernautorenkreis nicht zu groß sein, um einheitliche Sprache und Stil zu gewährleisten.
- Ein Workshop wird organisiert (Teilnehmer organisieren diesen selbst, nicht von Seiten des MÜNCHNER KREIS), um Thema des Papiers nochmal einzugrenzen/glatt zu ziehen, Fokus festzulegen; Ressourcen prüfen → Timeline festlegen. Thesenpapier vorab an die Teilnehmer des AK Security senden und intern diskutieren. Dann entscheiden, ob zu Berliner Gespräch oder nächstes Jahr veröffentlichen.

Anmerkungen:

- Herr Thielmann: Wen können wir einladen von der Anwenderseite? Kommt zu kurz! Aufruf an Teilnehmer, bitte Rückmeldungen geben! >> Rückmeldungen an Thielmann; bisher nichts erhalten
- Gemeinsame Sitzung mit CSSA/CSSC, DAX 30, nicht extra Termin o.ä.; VOICE oder CSSA Thema adressieren (Herr Reinema); Ergebnisse aus dem Treffen mit CSSC etc. als Input verwenden >> Thema für Herrn Reinema

Themenvorschläge:

- Trusted Data/Machine Learning; Wie funktioniert das eigentlich? Nächste Hackingwelle! Falsche Daten einspeisen durch Analytics.
- Trusted Label: Security-Plakette wird es bald geben; neue europäische Vorschläge zu Trusted Label. Neues Modell erstellen: Worauf muss Bürger achten, worauf Unternehmen? Welche Arten von Kennzeichnungen bräuchte man? Nicht klassische Identität, sondern neuen Raum aufspannen, dann ist das Thema interessant. Nicht durch Zertifizierung – auch andere Wege möglich? z. B. neue Arten des Insurance Labeling.
- Impact der Wechselwirkungen: Aus Cyberspace KRITIS angreifen! Sensoren manipulieren etc. ist möglich – aktuelle Cases vorhanden, die man beleuchten kann.

Papier für uns intern erstellen?

→ Nicht zur Selbsterhaltung – Ziel ist schon eine Veröffentlichung. Aber vorab im Rahmen des AK Security prüfen, Abstimmung ist sinnvoll, als Basis für Diskussionen verwenden.

Interessantes Thema: „Weckruf: Blockchain“ – Charakteristik der Technologie deutlich machen und seriös beleuchten: wo macht Blockchain Sinn, wo keinen Sinn? Das Aufbereiten dieses Themas wird als guter Anspruch des MÜNCHNER KREIS gesehen.

→ **Beschluss:** Unterarbeitsgruppe wird gebildet zum Thema Blockchain

- Organisation übernimmt Herr Reinema
- Interessenten bitte melden
- Bisher gemeldet haben sich: Frau Eckert (am Fraunhofer AISEC ist ein Blockchain-Lab geplant), Herr Houdeau weiß jemanden von NIST.
- Weiteres Vorgehen: Meeting ansetzen, Thema aufbereiten: Pros und Cons im Überblick. Thema sollte relativ schnell aufgegriffen werden → 2-4 Seiter erstellen. Bezug zu TRUST herstellen: TRUST als Klammer.

7.) Diskussion der Weiterführung des Schwerpunktthemas: Robustheit von IT

Sicherheitsarchitekturen: Herr Mörl

Die Präsentation von Herrn Mörl wird auf dem Share abgelegt.

Es wurde ein Fragenkatalog erstellt und durchgeführt: Open Space und mehrere Einzelinterviews: Welche Fragestellungen erscheinen den Leuten wichtig? Sicherheit messen, Ausrichtung an Schutzziele, ... (siehe Präsentation). Kann man KPIs auf IT-Sicherheit ableiten?

Handlungskette Audit, Pen-Test, Grundschutz, ISO 27001, ISIS 12 bis zum etablierten Schutz fortsetzen.

Funktion ohne Schutz ist wertlos: Vertrauensketten nur so stark, wie ihr schwächstes Glied.

- Durchgehende Sicherheitsbetrachtung: Einzelne Sicherheitslösungen bieten keine gesamtheitliche Sicherheit. Man braucht durchgehende Vertrauensketten und transparente Lieferketten.
- Thema Knowhow problematisch. Metrik wäre gut, so dass der Konsument ohne eigenes Knowhow verlässlich entscheiden kann → vertrauenswürdige Handlungsketten sinnvoll
- Verfügbarkeit: Messgrößen/Benchmarks, wie kann man Indikatoren für Funktionalität bzw. sicheres Handeln schaffen. Wenn ich beim Pen-Test gehackt worden bin, an wen wende ich mich?

These: Wenn man es schafft, Tests/Analysen/Untersuchungen auf neutraler Plattform verfügbar zu machen und mit einer verständlichen Form einer Metrik zu hinterlegen, dann kann man Synergien nutzen. Allerdings: keiner will Haftung übernehmen. Haftungsproblem und Personalisierungsproblem muss man lösen

Vorschlag: Themenabend des MÜNCHNER KREIS Cybersecurity mit konkreten Handlungsempfehlungen. Welche weiteren Themen gäbe es in dem Feld Robuste Sicherheitsarchitekturen für den AK?

- Plattform Industrie 4.0 – Referenzarchitektur RAMI vorgestellt; Messgrößen definieren
- Konkretes Problem beschreiben, evtl. Tipps geben für Stakeholder, wie Lösung aussehen könnte. Handlungsempfehlungen für Daily Business/was täglich passiert.

Anmerkung: Was soll aus diesem AK für den MÜNCHNER KREIS relevant sein? Welche

Handlungsempfehlungen können daraus entstehen? Wir können keine Produktbewertung machen, keine Tests bewerten!

→ **MÜNCHNER KREIS soll Thema adressieren und Stakeholder anregen, die Plattform zu schaffen und Testergebnisse zu sammeln.**

Weiteres Vorgehen:

- Themenabend? Für Politik und Verbände: Wege von Threat-Landscape zu Protection Landscape. Digitalbonus von Wirtschaftsministerium ab Herbst → über Bayerischen Wirtschaftsministerium versuchen zu platzieren, z. B. Einseiter erstellen.
- Team besteht aus: Herr Mörl, GENUA (Herrn Dörnemann), Herr Maierhofer (Palo Alto) – weitere Interessenten? Wunsch von Herrn Mörl: Integrator und Berater mit dazu nehmen, da bisher zu Hersteller-orientiert.
- Idee Neutrale Plattform weiter vorantreiben, Ergebnisse zusammenzutragen. Was machen wir damit? Was kann man daraus schöpfen? Was kann man heranziehen, um das zu bewerten? Evtl. beginnt man mit dem was man hat und schaut dann weiter in welche Richtung es gehen kann.

→ Thema muss noch ausgefeilt werden. Interesse von Seiten der Teilnehmer ist da

>> AP: Ramon Mörl

8.) Next Steps

Next Steps in den Themen:

- 1.) Berliner Gespräch:
Fokus des Gesprächs wurde etwas verändert: Neue Services! Daher entsprechende Anpassungen nötig → Telefonkonferenz ansetzen. Ein Team aus ca. 6 Personen soll Thesen formulieren als Briefing für die Referenten. >> AP: H.Thielmann
Längerfristig: Ergebnisse aus Berliner Gespräch für Fachkonferenz nutzen, Erfahrungen einspeisen
- 2.) Workshop zum Themenbereich ID & Trust in Data (Herr Montag und Herr Wilkie). Es wird zur Beteiligung aufgerufen. Herr Reinema wird das Thema Blockchain vorantreiben (Meeting ansetzen, Thema aufbereiten: Pros und Cons im Überblick)
- 3.) Idee von Neutraler Plattform weiter vorantreiben. Themenabend für Politik und Verbände geplant: Erstellen des Einseiter für das Wirtschaftsministerium. Frau Eckert versendet den Einseiter an die Teilnehmer des AK Security und sammelt das Feedback, erst dann Versand des Einseiters an Frau Ausfelder.

Es gibt keine weiteren Anliegen von Seiten der Teilnehmer.

9.) Weitere Termine

4. Arbeitstreffen des AK Security am **13. Oktober 2016 in Berlin**. Das Treffen wird ein paar Stunden vor Beginn des Berliner Gesprächs angesetzt. Nähere Informationen werden den Teilnehmern per Mail mitgeteilt. Herr Bub ist dankenswerterweise Ausrichter des 4. Treffens.