

Münchner Kreis - Arbeitskreis Security

Protokoll des fünften Arbeitstreffens

Aktionsliste

Themenfeld	Aufgabe	Kümmerner	Deadline
<u>AK Security Teilnehmerliste</u>	Alle anschreiben, die sich nicht rückmelden – Bitte um Recommitment und Formulierung der Wunschthemen	Herr Thielmann → MK Office	
<u>Berliner Gespräch</u>	Keynote-Speaker um Korrektur bzw. Freigabe bitten	Frau Starzer	
<u>EU-Sicherheitskonferenz</u> (1 Tag vor MUC Sicherheitskonferenz)	Telko veranstalten und Input sammeln	Herr Houdeau, Herr Pieper, Herr Wolfenstetter, Herr Thielmann, Herr Wilkie; vermutlich auch Udo Helmbrecht	
<u>7. Berliner IT-Sicherheitskonferenz</u>	Beteiligung AK Security	Herr Bub, Herr Wolfenstetter	
<u>Konferenz AK Energie (28.06.)</u>	Anfrage: Beitrag zum Thema „Einbruchssicherheit“ (Intrusion) beitragen?	alle	
<u>SEKOP 2017</u>	Ramon Mörl macht Workshop und sucht noch Unterstützer	Herr Mörl, alle	
<u>Sub-AK: Sichere Identitäten</u>	Einbindung Frau Wiesmüller wg. Ansprache Mittelstand, dann Entwurf zur Review an Herrn Thielmann	Herr Arnold, Herr Wilkie, Frau Wiesmüller	
<u>Sub-AK: Blockchain</u>	- Bitte um weitere Mitwirker, Input - Usecases - Linksammlung zu Blockchain - MK Mitgliederkonferenz: Herrn Krcmar kontaktieren	alle Herr Thielmann Frau Wiesmüller Frau Eckert	
<u>Forderungskatalog an Parteien</u>	- wurde vorab per Mail gesendet mit Bitte um Ergänzung/Feedback - Bitkom-Papier verteilen - Recherche: was Parteien auf Agenda haben	alle Herr Houdeau Herr Pieper	
<u>Bewerbung: Security-Hub</u>	- Bitte um Unterstützung: Koordination: Frau Eckert	alle	

ACHTUNG:

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

Protokoll des fünften Arbeitstreffens

Datum: 01. März 2017, 17:00 – 20:00 Uhr

Ort:

Business Campus
Parking 4
85748 Garching

Teilnehmer:

Jürgen Arnold, Consultant
Prof. Dr. Claudia Eckert, Fraunhofer AISEC / TU München
Wolfgang Fritsche, IABG GmbH
Emanuel Georgiew, EMASU GmbH
Dr. Detlef Houdeau, Infineon Technologies AG
Michael Montag, Nokia
Frank Pieper, netextend GmbH
Prof. Dr.-Ing. Georg Sigl, Fraunhofer AISEC / TU München
Prof. Dr. Heinz Thielmann, Emphasys GmbH
Eva Sophie Wiesmüller, Power2Progress
Jamie Wilkie, Fujitsu Technology Solutions GmbH
Klaus-Dieter Wolfenstetter

Protokoll: Prof. Dr. Claudia Eckert, Susanne Starzer

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

Agenda:

1. Begrüßung und Vorstellungsrunde
2. Protokoll der letzten Sitzung, Zusammenfassung des Standes der Diskussion: Herr Thielmann
3. Berichte aus den AKS:
 - Sichere Identität & Trust in Data: Herr Wilkie
 - Blockchain: Frau Eckert

4. Weitere Berichte zu aktuellen Aktivitäten: alle
 5. Kurzfristige Formate zum Agenda-Setting; zeitnah: was, wie, wo, wer
 6. Planung der Fachkonferenz Security: Herr Thielmann
 7. Formulierung von Forderungen/Todos an die politischen Parteien für den Wahlkampf
- Abschluss und lockerer Ausklang
-

1.) Begrüßung & Vorstellungsrunde

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

Vorschlag von Herrn Thielmann:

15 – 20 % sind regelmäßig dabei, jedoch gibt es viele auf der Teilnehmerliste, die sich auf die Einladungen hin nicht melden und nicht teilnehmen. Alle anschreiben, die sich nicht rückmelden, mit der Bitte um Recommitment und Formulierung ihrer Wunschthemen → anwesende Teilnehmer stimmen dem Vorschlag zu, Herr Thielmann veranlasst das durch MK-Office.

2.) Protokoll der letzten Sitzung, Zusammenfassung des Standes der Diskussion: Herr Thielmann

Das Protokoll der letzten Sitzung wurde per E-Mail versandt. Des Weiteren ist das Protokoll auf dem MK-Server abgelegt.

Berliner Gespräch:

- Verbesserungspotential: es waren keine politischen Vertreter dabei
- Mitschrift des Sprachprotokolls:
 - insgesamt 80 Seiten, zu viel um das Korrektur zu lesen; Protokoll liegt auf dem MK-Server im Ordner „Berliner Gespräch“
 - Frau Starzer bittet die Keynote-Speaker um Korrektur ihrer Keynote-Mitschriften; dann an alle Teilnehmer und Interessenten des AK Security versenden

EU-Sicherheitskonferenz fehlt:

Am Vortag der Münchner Sicherheitskonferenz fand die „International Munich Cyber Security Conference“ (MCSC) im Bayerischen Hof statt. Veranstalter ist das Sicherheitsnetzwerk München. Die Veranstaltung ist nur für geladene Gäste.

Überlegen, ob man den Sicherheitstag gemeinsam veranstaltet oder der MÜNCHNER KREIS zu einer Konkurrenzveranstaltung einladen soll. Rahmen und Zeitpunkt vor Sicherheitskonferenz ist ideal.

Vorschlag von Herrn Houdeau: Internationale Cybersicherheitsmesse in Lille (FIC); Dauer: 2 Tage; französischer Partner wäre nötig, um auf das gleiche Niveau zu kommen; selbst eine solche Veranstaltung aufzubauen dauert mehrere Jahre.

Next Step: Telko veranstalten und Input sammeln. Folgende Teilnehmer haben Interesse: Herr Houdeau, Herr Pieper, Herr Wolfenstetter, Herr Thielmann, Herr Wilkie; vermutlich auch Udo Helmbrecht

7. Berliner IT-Sicherheitskonferenz (19. – 20.10.2017):

Veranstalter ist das European Institute of Innovation and Technology (EIT); reine IT-Sicherheitskonferenz → mehr Sichtbarkeit für den MK ohne vorne anfangen zu müssen → AK Security beteiligt sich an 7. Berliner IT-Sicherheitskonferenz

AK-Treffen im Februar

Die Leiter der AKs haben sich im Februar getroffen – AK Security war aus terminlichen Gründen nicht vertreten; Protokoll fehlt noch, daher kann darüber nicht berichtet werden.

Konferenz am 28.06.2017 des AK Energie

Beiträge von Seiten des AK Security sind gewünscht; Kurzpräsentationen max. 15 Min und zwei moderierte Fragen; Slot 1: Herr Dörr mit dem Thema Datensouveränität; 2. Slot noch frei. Anfrage, ob AK Security zum Thema „Einbruchssicherheit“ (gemeint ist „Intrusion Detection“) noch einen Beitrag liefern kann.

SEKOP 2017

SEKOP findet von 17. - 19.06.2017 am Tegernsee statt; Peter Köhler (Geschäftsführer von Finaki) hat angefragt, ob wir uns beim Workshop beteiligen möchten; Ramon Mörl macht einen Workshop, er sucht noch Unterstützer.

3.) Berichte aus den AKS

3.1) Sichere Identität & Trust in Data: Herr Wilkie

Bericht von Herrn Wilkie:

Der Sub-AK „Identity Management und Trust in Data“ arbeitet an einem Papier, das auf ca. 15 Seiten interessierte Leser, insbesondere aus dem deutschen Mittelstand, über die hohe Wichtigkeit von Vertrauen in Datenquellen, Identitäten und Schutz der Datengewinnung und –verarbeitung informieren soll. Diese Themen werden vor dem Hintergrund der entstehenden I40/IoT-Unternehmensverbände als wichtig angesehen.

Die vorgesehene Kapitelstruktur:

- **Kapitel 1:** Einleitung: Knappe Zusammenfassung der Situation, Trends, Gefährdungen und Zweck des Papiers. (1. Draft: Draeger (Fujitsu))
- **Kapitel 2:** Bedeutung von Daten und Vertrauen für Sicherheit und Erfolg in neuen Formen der Zusammenarbeit von Unternehmen. Zukunftsszenario (1. Draft: Montag (Nokia))
- **Kapitel 3:** Technologien (Blockchain, Biometrie, Datennutzungskontrolle, smart contracts, smart markets, Data Analytics, AI, trusted identities). Illustrative Beispiele. (1. Draft: Blöcher (Siemens))
- **Kapitel 4:** Empfehlungen für Maßnahmen

Zu Kapitel 1-3 liegen erste Rohentwürfe vor. Diese sollen nun zunächst noch konsolidiert und aneinander angepasst werden. Als nächster Schritt ist danach eine Feedbackrunde mit Mittelstandsfirmen oder -Verbänden geplant, um das Interesse an den Themen zu verifizieren. Bis zum Sommer (Konferenz des AK Energie im Juni, Herr Arnold) soll das Papier fertiggestellt werden.

Mitglieder des Sub-AKs sind: Jürgen Arnold (Consultant), Uwe Blöcher (Siemens), Kai Dörnemann (Genua), Jörg Dörr (Fraunhofer IESE), Dr. Markus Draeger (Fujitsu), Michael Montag (Nokia), Jamie Wilkie (Fujitsu).

Frage: Wann gibt es was zum Lesen?

Einbindung von Frau Wiesmüller wg. Ansprache für Mittelstand, dann Entwurf an Herrn Thielmann zur Review (gegen Ende Mai; rechtzeitig für AK Energie Event) → danach an AK Security zum Lesen; Termine werden offline abgestimmt.

Frage: Fake News: Wird das aufgegriffen, oder ist es out of scope?

Wird momentan noch nicht beleuchtet; Vorschlag von Herrn Montag: In Richtung Fake Reality gehen; in der Zukunft: Gefährdung durch falsche Messdaten etc.; gaukeln etwas vor, was so nicht ist; Prävention durch Sichere Identitäten.

→ Ergebnisse aus der Sub-AK fließen auch in den Forderungskatalog für die Wahlprogramme der politischen Parteien ein (siehe Agendapunkt 5.)

3.2) Blockchain: Frau Eckert

Thema Blockchain: Alle sprechen darüber, was ist das? Verschiedene Varianten mit unterschiedlichen Eigenschaften und Usecases: was kann man damit machen? Kritisch aus Expertensicht beleuchten; aus Sicht der Security und des Datenschutzes.

Ausrichtung des Papiers: Konkrete Handlungsempfehlungen, Einschätzungen an den Mittelstand.

Wo der Schwerpunkt liegen soll ist noch nicht klar. Vom TeleTrust gibt es ein aktuelles Papier; hier muss noch geprüft werden, ob sich das überschneidet; evtl. anderen Schwerpunkt wählen.

Frage an die Runde: Was ist das Interessanteste für Sie?

- Offenlegen der Probleme aus der Sicherheitssicht
- Welche neuen Business-Cases lassen sich damit realisieren?
- Chancen und Risiken gegenüberstellen?
- Perspektive des Mittelstands
- Gibt es Standardtechniken, die der Blockchain eigentlich überlegen sind? (z. B. PKI)
- Verantwortlichkeiten: fehlende IT-Gesetzgebung! Viele schrecken zurück; fehlende Kenntnis wie man das für sich anwendet;
- Gibt es gut funktionierende Usecases für den Government-Bereich? Auch Behörden und Kommunen Hilfestellung bieten

Mehr Mitwirkende wünschenswert: Bisher schreiben nur Siemens und AISEC an dem Papier. Frau Wiesmüller macht mit als Bindeglied zu den technischen Mitwirkern. Bitte an alle AK Teilnehmer: Mitwirken! Input bitte an Frau Eckert senden.

Herr Thielmann liefert Usecases. Frau Wiesmüller hat Linksammlung zum Thema Blockchain, sie stellt diese gerne zur Verfügung.

Helmut Krcmar organisiert momentan eine MK-Mitgliederkonferenz (Halbtagesveranstaltung) im November zu dem Thema Blockchain. Ergebnisse des Papiers sollen dort präsentiert werden. Frau Eckert kontaktiert Herrn Krcmar diesbezüglich.

4.) Weitere Berichte zu aktuellen Aktivitäten: alle

Keine

5.) Kurzfristige Formate zum Agenda-Setting; zeitnah: was, wie, wo, wer

Forderungskatalog für die Wahlprogramme der politischen Parteien

(wurde bereits vorab mit Bitte um Ergänzung/Feedback per Mail versandt)

Verbände wie Bitkom, VDE etc. versenden üblicherweise vor dem Wahlkampf einen Anforderungskatalog an die Parteien. MÜNCHNER KREIS möchte Forderungen aus den MK-Arbeitskreisen für die Ziele und Umsetzung der Digitalisierung an die politischen Parteien senden. Das Ziel: Sichtbarkeit für den MÜNCHNER KREIS erzeugen, Alleinstellung des MK erarbeiten.

- max. 3 Seiten
- Vorspann: Wer ist der MÜNCHNER KREIS? Gefolgt von einer Überleitung zur Digitalisierung/Security

- Füllen mit Statements von jedem Arbeitskreis; Umfang je Arbeitskreis: ½ - ¾ Seite
- Deadlines:
 - bis 12. März: Ergänzungen durch die AK Security Teilnehmer erbeten
 - 12. – 15. März: Finalisierung der Vorlage für den Vorstand durch Herrn Thielmann und Herrn Dowling
 - 15. März: Forderungskatalog/Papier in der MK-Vorstandsitzung besprechen
 - Bis spätestens Ende März Versand an die Parteien
(Adressaten: alle Fraktionsvorsitzenden und die Schreiber der Wahlprogramme)

Kein „me too“-Papier, keine Wiederholungen; allerdings ist ein Abgleich mit anderen Papieren schwierig, denn viele Verbände haben Forderungen und die Zeit drängt.

Was wären Themen, die wir in dem Papier unterbringen möchten? Handreichung an Politik

MK fordert: Gesamtheitliches Digitalisierungsministerium für Deutschland

In der EU und in anderen Ländern wird das schon umgesetzt, Deutschland hängt hinterher;

Fokus nicht nur auf Sicherheit, aber klar machen: ohne Security geht nichts!

Was erwarten wir von so einem Ministerium? Welche Leitplanken erhoffen wir uns?

Verschiedene Sektoren haben versch. Erfahrungen; zusammentragen welche Erfahrungen gemacht wurden → Synergien nutzen, Lernen von den anderen (Best Practices)

Was gibt es bereits und kann man nutzen? Aber: Einen deutschen Weg finden – nicht nur kopieren von anderen Ländern.

Welche Themen konkret:

- **Stärkung der (europäischen) Sicherheitswirtschaft/-industrie 4.0:**
MK sollte definieren: Was sind die Backbones/Kerntechnologien, die am Wichtigsten sind und beherrscht werden müssen? Sicherheitschips, Hardware, Cloud, Sichere Software-Entwicklung, Analyse-Kompetenz, sichere digitale Identität, ...etc. Deutsche Lösungen oft zu kompliziert, trotzdem darauf pochen und schützen;
Politik soll sicheren Rahmen schaffen, damit wir uns in einem sicheren Raum bewegen können (als Bürger, als Unternehmer, etc.) → Rahmenbedingungen definieren (z. B. Verschlüsselung verpflichtend via Gesetz); wer in Deutschland etwas anbieten möchte muss definierte Rahmenbedingungen erfüllen; High-end Sicherheitslösungen aus Deutschland – Qualitätsstandard; Wie definieren wir sicheren Raum? Wie stark sind gewisse Dinge verpflichtend?
 - **Infrastrukturelle Maßnahmen und Regularien:**
verpflichtend für alle (wie z. B. Haftpflicht-Versicherung); sinnvolle Forderung?
 - **Verbraucherschutz in der digitalen Welt:**

Digitale Lösungen werden oft nicht genutzt (z. B. im Bereich Mobile Payment ist Deutschland hinten dran) aber immer mehr am Markt, Gütesiegel/Label für die digitale Welt schaffen; als Opt-out, nicht als Opt-in: wenn Bürger nicht will, kann er es abschalten; Mit welchen Mechanismen bringe ich Menschen dazu, Technik zu nutzen und zu unterstützen? → Mehrwert muss da sein

- **Forderung nach agilen Zulassungsvoraussetzungen:**

Rechtssystem steht im Weg, wenn man schnell innovative Produkte in den Markt bringen möchte; schnelllebige Zeit, daher sollte man das Rechtssystem ändern: Ausnahmen finden; wie in den USA; - vielleicht etwas abgeschwächt wie zum Thema Design-Thinking: für die Zulassung neuer Produkte eine schnelle Lösung finden, die gilt und parallel verfeinern; man erlaubt mal chaotischen schnellen Weg und wenn es gut geht, dann auf die normale Spur bringen; Innovationshemmnis: wo kann Politik was machen, damit man schneller innovative Ideen umsetzen kann? Time-to-Market verkürzen; bei ersten Prototypen schon die Zulassungsprozesse bedenken;

- **Safe Harbour Prinzip:**

Könnte man hart kontrollieren, will man aber nicht zu eng sehen; als Wettbewerbsschutz → hierzu gibt es wohl kein Konsens; zahnloser Papiertiger → besser Kontrolle einführen, um Security zu schützen / Blickwinkel: nationale Interessen ja, industrielle Interessen eher nein (nicht genau hinschauen)

- **Bildung, Ausbildung und Weiterbildung in der IT-Sicherheit:**

In allen Ebenen; Life-long-Learning; Politik soll unterstützend wirken: Förderung von Weiterbildungsaktivitäten durch das Forschungsministerium; auch Schüler schon aufklären und erziehen, denn sie sind die Experten von morgen

- **Möglichkeiten und Grenzen im digitalen Zeitalter / Kommunikation im digitalen Zeitalter:**

Streitfähig bleiben im Zeitalter der Digitalisierung, kritischer Umgang damit; Digitale Meinungsfreiheit: wie kann man die Kommunikation gestalten, damit sie offen bleibt, aber auch die bestrafen, die das missbrauchen?

- **Sicherheits-CISO/Sicherheitschef für Deutschland?**

- **Ein Thema für den CISO wäre der Digitalbonus**

Momentan: Fördermittel nur für Bayern, wenn mein Standort nicht in Bayern ist, habe ich Pech gehabt. Vereinheitlichung hinbekommen deutschlandweit – Bund soll Förderung zahlen, wenn man sich für eine Länderförderung beworben hat, obwohl man nicht in dem Land seinen Standort hat.

→ Zwei Forderungen:

1.) Politik soll Rahmenbedingungen setzen, um Infrastruktur sicherer zu machen

2) mehr Bildung

Und das nachhaltig!

ToDo:

- Frau Eckert fordert das Bitkom-Papier an.
- Herr Pieper: Recherche, was die Parteien aktuell zum Thema Digitalisierung sagen/schreiben; was ist auf deren Agenda?

6.) Planung der MK Fachkonferenz Security: Herr Thielmann

AK Security plant keine große eigene Fachkonferenz in diesem Jahr. Herbst 2017 ist ein schlechter Zeitpunkt, da Bundestagswahl → erst im Frühjahr 2018 wieder

MK Mitgliederkonferenz zum Thema Blockchain = Fachkonferenz light

Vorschlag: Einen Tag vor der Münchner Sicherheitskonferenz Veranstaltung für Special Guests veranstalten und zusätzlich eine Veranstaltung für breiteres Publikum. Ort: Innenstadt meiden, Arabella-Park o. ä.; Internationaler Flair: EU-Pendant zu RSA Conference; bewusst mit anderen Ländern zusammenarbeiten → Telko ansetzen, Beirat aufstellen, der das weitertreibt

Kleines Format für dieses Jahr? Welches Thema?

Berliner Gespräch reloaded? Politisch oder nicht? Nachmittag- oder Abendveranstaltung zu einem Thema? Kamingespräch? Thema definieren, das Gehör finden muss.

Fachkonferenz „The Digital Transformation of Manufacturing Industries“: Hier zeigte sich: kleine Firmen sind nicht präsent: sehen Chancen nicht, fürchten hohe Kosten, Angst vor den Unsicherheiten, fehlendes Vertrauen in IT.

Was kann man als MK dagegen machen? Wie kriegt man KMUs dazu, mutiger zu sein?

- Keine Business-Angels, sondern Sicherheits-Angels für KMUs finanziert vom Bund; „Rent an Expert“ – evtl. auch nicht mehr aktive Manager aus der Industrie einbinden (sie kennen Prozesse und Vorgehensweisen); aber gibt es genügend Experten?
- KMUs mit Politiker zusammenbringen; 1-2 Thought Leader identifizieren: welche Erfahrungen haben sie gemacht? Wie sind sie bestimmte Themen angegangen? Best Practices – jedoch ggf. schwer jemanden zu finden, der Best Practice preisgibt.

Bewerbung: Security-Hub

Digitale Hub-Initiative (BMW und Bitkom): Bewerbung für den Security-Hub; wird von bayerischer Landesregierung gefördert: kein Geld, sondern ein Label. Frau Eckert schreibt Proposal (ist bis 15.03. einzureichen) – falls jemand mitmachen möchte, gerne melden!

Ziel: bessere Sicherheitslösungen, Werbung machen, Strahlkraft auf EU-Raum (nicht nur auf Münchner Firmen fokussieren)

Momentan im Proposal: „School of Security“ mit verschiedenen Standbeinen (universitär: Master-Studiengang; erweitertes Ausbildungsangebot, Kooperationsmöglichkeiten, miteinander lernen wie man Systeme aufsetzt und deren Sicherheit beurteilt, Mitarbeiter von Firmen weiterbilden. So entstehen Kreativräume, bis hin zu Prototypen, Spin-offs, etc.

7.) Formulierung von Forderungen/Todos an die politischen Parteien für den Wahlkampf

Bereits im Agendapunkt 5.) diskutiert.

Es gibt keine weiteren Anliegen von Seiten der Teilnehmer.

Weitere Termine

6. Arbeitstreffen des AK Security: Ort und Datum noch nicht bekannt; Terminfindung via Doodle-Abfrage; ca. Mitte/Ende Juni (nicht Pfingsten & Fronleichnam; nicht am 28.06. wg. AK Energie)