

## Münchener Kreis - Arbeitskreis Security

### Protokoll des sechsten Arbeitstreffens

#### Aktionsliste

Themenfeld	Aufgabe	Kümmerner	Deadline
<b><u>Sub-AK: Trust in Data &amp; Sichere Identitäten</u></b>	Aktuellen Entwurf (Draft Version) an Teilnehmer versenden und auf MK-Server ablegen	Hr. Wilkie, Fr. Starzer	
	Kontakt von McKenzie an Prof. Eckert senden	Prof. Dowling	
	Juristen einladen	Prof. Eckert	
	Protection Landscape: erster Entwurf bis zum nächsten Treffen	Dr. Marinos, Hr. Purser und Hr. Mörl	
<b><u>Sub-AK: Blockchain</u></b>	Blockchain-Papier an Fr. Starzer senden	Dr. Reinema	
	Papier auf MK-Server bereitstellen und an Teilnehmer versenden	Fr. Starzer	
	Rückmeldung / Feedback	alle	
	Teilnahme Podiumsdiskussion klären (mit Prof. Krcmar)	Prof. Eckert	
	Abklären, bis wann Input geliefert werden muss	Prof. Dowling	
<b><u>7. Berliner IT-Sicherheitskonferenz</u></b>	Programm an Prof. Dowling senden Versand an MK-Verteiler	Dr. Bub Prof. Dowling	
<b><u>EU-Sicherheitskonferenz</u></b> (1 Tag vor MUC Sicherheitskonferenz)	Münchener Sicherheitsnetzwerk anfragen bzgl. Kooperation zur MCSC	Dr. Houdeau, Prof. Eckert	asap
	Vorbereitung d. Veranstaltung: Themen definieren, Namedropping,...	Dr. Houdeau, Dr. Reinema, Hr. Kranawetter, Hr. Diaw, Hr. Wolfenstetter, Prof. Eckert	zeitnah nach Sommerpause
<b><u>Themenabend für Politik</u></b>	Fragen an Politik an Prof. Thielmann senden	alle	
	Fragen sammeln und clustern	Prof. Thielmann	
		Prof. Thielmann	

	Protokoll Berliner Gespräch 2016: mögliche Themen daraus selektieren für nächste Veranstaltung		
<b>Thema für Fachkonferenz: Threat Intelligence</b>	Infos über CTI-EU Bonding EU Cyber Threat Intelligence an Hr. Kranawetter senden	Dr. Marinos  Hr.Kranawetter erstellt 1- Seiter  Teilnehmer Diskussion: Hr. Kranawetter, Hr. Wilkie, Hr. Montag, Dr. Marinos, Dr. Reinema, Hr. Diaw.	
<b>Thema für Fachkonferenz: Sichere Mobile Identitäten</b>	Unterschiedliche Usecases aus Security- und Privacy-Sicht betrachten.	Dr. Houdeau erstellt 1- Seiter  Teilnehmer Diskussion: Dr. Houdeau, Hr. Kranawetter, Hr. Georgiew, Hr. Diaw, Hr. Wolfenstetter.	

## **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 sechsten Arbeitstreffens**

**Datum:** 24. Juli 2017, 17:00 – 20:00 Uhr

### **Ort:**

Vodafone GmbH  
Betastraße 6-8  
85774 Unterföhring

### **Teilnehmer:**

Jürgen Arnold, Consultant  
Dr. Carsten Bittner, Bertelsmann SE & Co. KGaA  
Dr.-Ing. Udo Bub, EIT ICT Labs Germany GmbH  
Abdou Naby Diaw, Vodafone GmbH

Kai Dörnemann, genua GmbH  
Prof. Dr. Michael Dowling, Universität Regensburg, MÜNCHNER KREIS  
Prof. Dr. Claudia Eckert, Fraunhofer AISEC / TU München  
Wolfgang Fritsche, IABG GmbH  
Emanuel Georgiew, SEMASU GmbH  
Dr. Detlef Houdeau, Infineon Technologies AG  
Michael Kranawetter, Microsoft Deutschland GmbH  
Dr. Louis Marinos, ENISA  
Michael Montag, Nokia  
Ramon Mörl, itWatch GmbH  
Dr. Rolf Reinema, Siemens AG  
Prof. Dr.-Ing. Georg Sigl, Fraunhofer AISEC / TU München  
Prof. Dr. Heinz Thielmann, Emphasys GmbH  
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. Die Unterpunkte zum Agendapunkt 4 wurden in abweichender Reihenfolge zur versendeten Agenda besprochen. Folgende Agenda zeigt die tatsächlich besprochene Reihenfolge der Themen:

#### **Agenda:**

1. Begrüßung und Vorstellungsrunde
2. Protokoll der letzten Sitzung, Zusammenfassung des Standes der Diskussion
3. Berichte aus den Arbeitsgruppen durch die Teilnehmer der Arbeitsgruppen:
  - 3.1 Trust in Data & Sichere Identitäten
  - 3.2 Blockchain
  - 3.3 Robustheit von IT-Sicherheitsarchitekturen
  - 3.4 Gesellschaftliche Dimension
4. Planungsstand von Veranstaltungen des AK
  - 4.1 Stand der Planung der Berliner Sicherheitskonferenz EIT
  - 4.2 Stand der Planung zu einer EU Sicherheitskonferenz
  - 4.3 Themenabend für die Politik zum Thema Cybersicherheit Ende 2017
    - Handlungsempfehlungen für die neue Regierung?
    - Fortsetzung des Berliner Gesprächs vom Oktober 2016, oder eher Münchner-Dialog
  - 4.4 Vorbereitung einer Fachkonferenz in 2018: Themensammlung, PC
5. Weitere Berichte zu aktuellen Aktivitäten: alle
6. Sonstiges

Abschluss und lockerer Ausklang

---

## 1.) Begrüßung & Vorstellungsrunde

- Vorstellung der Agenda; Dr. Bub wird ergänzend zum Agendapunkt 3.2 *Blockchain* von der EIT Digital Finance Summer School „Blockchains for Economic Security“ berichten.
- Kurze Vorstellungsrunde der anwesenden Teilnehmer

## 2.) Protokoll der letzten Sitzung, Zusammenfassung des Standes der Diskussion

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

Aktueller Stand der Aktionspunkte vom letzten Treffen:

- Teilnehmerliste aussieben: Alle Teilnehmer, die sich nicht rückmelden, wurden angeschrieben mit der Bitte um Recommitment → viele Rückmeldungen, dass weiterhin Interesse bestehen.
- Berliner Gespräch: Keynote-Speaker um Korrektur bzw. Freigabe des Audioprotokolls bitten: Erledigt bzw. Verworfen, da keine Freigabe von Herrn Schönbohm erfolgte.
- Forderungskatalog an Parteien zur Bundestagswahl: Verworfen, da bereits Forderungen von Bitkom und andere Institutionen gestellt wurden.
- Bewerbung Security Hub (Digitale Hub-Initiative von BMWi und Bitkom): Bewerbung wurde abgegeben; München bekommt jedoch keinen Security Hub; geplant sind gemeinsame Aktivitäten mit den beiden bestehenden Münchner Hubs: Mobility & InsurTech Hub.

## 3.) Berichte aus den Arbeitsgruppen durch die Teilnehmer der Arbeitsgruppen:

### 3.1) Trust in Data & Sichere Identitäten (Hr. Wilkie)

Es wurden bisher neun Seiten Bericht verfasst und in den internen Review gegeben; seitdem ruhiger geworden. Erkenntnis aus Gesprächen mit Zielgruppe: Es gibt bereits ein Angebot an Übersichtspapieren; daher besser Handlungsempfehlungen anbieten.

Nächste Schritte: Treffen vor der Sommerpause geplant; prüfen, ob die Ausrichtung richtig ist; Papier guter Anfang, weiterführen und konkrete Empfehlungen formulieren. Überdenken, welcher Impact erzielbar ist. Veranstaltung oder politischen Abend machen? Dort Handlungsempfehlungen vorstellen.

Handlungsempfehlungen für verschiedene Ebenen: auch Politik, bisher eher für Praktiker gedacht. Die richtige Ansprache finden. Agenda passt nach wie vor; nur die Inhalte nochmal an der Zielgruppe ausrichten.

Vorschlag Prof. Eckert: Mehr Trust in Data; bisher Ausrichtung auf Sichere Identitäten; zum Thema Trust in Data gibt es noch nicht viel; Identity-Thema schon gut besetzt; Fokus darauf wäre gut.

Dr. Houdeau stimmt zu: DIN/DKE-Projekt „Sichere digitale Identitäten“ erstellen Roadmap; geförderte Initiative vom Bundeswirtschaftsministerium; über alle Verticals dauert die Aufstellung mehrere Monate; schwer zu erfüllen, da aufwendig → daher mehr auf Trust in Data gehen.

- Juristische Rahmenbedingungen,
- Umsetzung: Was heißt das für die Dienstleister? und
- politische Betrachtung interessant.

Die juristischen Themen sollen durch Experten abgedeckt werden. Dazu Juristen (Dr. Alexander Duisberg oder McKenzie) einladen. Prof. Eckert kontaktiert diese direkt; Prof. Dowling schickt Kontakt von McKenzie.

„Rechtssicherer Umgang mit Daten“ ist interessantes Thema; als Topic für Workshop/Diskussion aufgreifen.

Teilnehmer der Arbeitsgruppe: Hr. Dörnemann, Hr. Wilkie, Hr. Arnold, Hr. Montag. Weitere Teilnehmer werden gesucht!

Hr. Wilkie versendet aktuellen Entwurf (Draft Version); wird auf MK-Server abgelegt.

#### Vorschlag: *Threat-Landsscape von ENISA zu Protection-Landscape*

Protection-Landkarte entwerfen: Wo Handlungsbedarf von Politik (Rahmenbedingungen); Was müssen Technologieanbieter anbieten? Orientierung geben.

Als lebendes Dokument; auf andere Papiere verweisen; evtl. nicht nur ENISA, evtl. mit bayerischer Regierung...?

Share zwischen Teilnehmern: Dr. Marinos, Hr. Steve Purser und Hr. Mörl. Offline-Austausch zu dritt; erster Entwurf bis zum nächsten Treffen; dann ausführlicher diskutieren.

### **3.2) Blockchain (Dr. Reinema)**

Vorläufig finale Version des Papiers ist gerade in der Abstimmung. Verfasser: Hr. Schanzenbach und Hr. Aschauer. Hausinterner Blockchain-Vortrag fand statt - kam sehr gut an.

Alle Inputs zum Thema Blockchain möglichst bald sammeln, da am 22./23. November die Mitgliederkonferenz des MÜNCHNER KREIS stattfindet. Dort soll vorgestellt werden, was der AK Security zum Thema Blockchain erarbeitet hat. Handout soll verteilt werden und an

Podiumsdiskussion teilnehmen; Wer ist Referent? Dr. Reinema, Schanzenbach oder Aschauer? → Dr. Reinema stimmt terminlich ab, wer das übernehmen wird.

Ca. 4 Wochen vor MK-Mitgliederkonferenz Input einreichen (Prof. Dowling klärt das genau ab).

Reiseveranstalter TUI wird Blockchain-Technologie einsetzen; Booking.com und andere wollen nachziehen. Wird interessant, wie standhaft die Technologie ist. Dr. Reinema kennt den CEO von TUI (ehemals Vodafone)– evtl. auch für MK-Mitgliederkonferenz anfragen?

Erstelltes Papier an MK-Mitglieder, Verbände und Multiplikatoren streuen. ENISA fragen, ob unter ENISA-Label verteilt werden kann. In Deutsch liegt es vor; evtl. MÜNCHNER KREIS finanziert Übersetzung, da Verbreitung via ENISA ermöglicht werden soll.

Auch Pressekonferenz bzw. Pressegespräch dazu veranstalten; evtl. Executive Summary daraus erstellen – Aufklärungsarbeit für diejenigen, die vor der Entscheidung stehen, das einzusetzen. Blockchain ist mehr als nur Bitcoin!

Dr. Reinema sendet Blockchain-Papier an Fr. Starzer → Versand an die Teilnehmer und auf MK-Server ablegen – Rückmeldungen/Feedback erwünscht!

Prof. Eckert klärt mit Prof. Krcmar die Beteiligung an Podiumsdiskussion ab.

----

### **Bericht: EIT Digital Finance Summer School „Blockchains for Economic Security“ (Dr. Bub)**

Von 23. Juli bis 5. August findet in Budapest die EIT Digital Finance Summer School zum Thema „Blockchains for Economic Security“ statt.

Einführung in die Themen Economic Security Engineering und Financial Cryptography.

Blockchain: Bitcoin und Ethereum (Plattform zum Ausführen von Smart Contracts)

Ökosysteme um Blockchains und die Zusammenarbeit zwischen Blockchains werden diskutiert.

Smart Contracts Plattform vorgestellt, Businesscase angeteasert und zwei Wochen bearbeiten lassen; läuft momentan noch.

#### Usecases:

IoT Anwendungsfälle für Track und Tracing;

Ausstellen von Micropayment Zertifikaten/Tokens: z.B. Taxidienste; Geschäftsideen: Gutscheine ausstellen; PayPal, Kreditkartenfirmen o. ä. umgehen. Zugangssysteme: Mietwagen vermieten und auf Basis eines Bezahlzertifikates Zugang zu Auto erhalten.

Was wird durch Blockchain einfacher, als konventionell?

----

### **3.3) Robustheit von IT-Sicherheitsarchitekturen (Hr. Mörl)**

Kein Update dazu.

### 3.4) Gesellschaftliche Dimension (Prof. Sigl)

Kein Update dazu. Arbeit nach Berliner Gespräch eingestellt – momentan on hold.

## 4.) Planungsstand von Veranstaltungen des AK

### 4.1 Stand der Planung der Berliner Sicherheitskonferenz EIT (Dr. Bub und Hr. Wolfenstetter)

Die Berliner Sicherheitskonferenz der EIT ICT Labs findet am 19. Oktober in Berlin statt. Thema „New Directions“ - neue Entwicklungen, neue Paradigmen?

Anfrage von Seiten EIT ICT Labs: Kooperation mit MÜNCHNER KREIS? Inhaltliche Impulse von Seiten des MK gewünscht.

Dr. Reinema ist als Speaker von Seiten AK Security dabei. Speaker Slots bereits ausgebucht. Wer noch Interesse hat, bitte trotzdem melden; noch nicht alle fest zugesagt.

Ist es möglich, mit MK-Logo zu werben? MK ist diesbezüglich vorsichtiger geworden; Welcher Mehrwert für MK? EIT ICT Labs allerdings keine Firma, sondern Bildungsinstitut; Bewerben via MK-Verteiler gewünscht; [Kleiner Verteiler (120 Firmen und 130 Akademiker) oder großer Verteiler (4.000 Personen)?]. Laut Prof. Dowling geht das in Ordnung.

Nächstes Jahr: Gemeinsame Konferenz planen!

→ Dr. Bub schickt Programm an Prof. Dowling. Prof. Dowling übernimmt den Versand an MK-Verteiler.

### 4.2 Stand der Planung zu einer EU-Sicherheitskonferenz (Dr. Houdeau)

#### EU-Sicherheitskonferenz – Beispiel 1:

EU-Cybersecurity Conference (14. – 15. September) in Tallinn, Estonia. Dauer: 2 Tage

Ablauf:

- Day 1: Organization from Estonia Presidency;  
Focus: NIS-Implementation in the MS; **non-public event**
- Day 2: Organization from ENISA cyber security policy of the EC;  
Focus: Cybersecurity Policy; **public event**

→ Einzelne Sektoren bekommen einzelne Veranstaltungen. Security ist Querschnittsthema

#### EU-Sicherheitskonferenz – Beispiel 2:

10th International Cybersecurity Forum (FIC 2018) in Lille, Frankreich. Europas größte Cybersicherheitskonferenz mit mehr als 5.000 Teilnehmern; Vorträge und parallel Sessions; Ausstellung ist nur Beiwerk (bei Messe „it-sa“ ist es genau umgekehrt); stark französische Sicht.

→ das Format zu kopieren dauert mehrere Jahre! Nicht sinnvoll.

Wenn sowas aufsetzen, eng an EU-Verordnungen orientieren; aktuelle regulative EU-Maßnahmen aufgreifen, z. B. E-Call.

#### International Munich Cyber Security Conference“ (MCSC)

Am Vortag der Münchner Sicherheitskonferenz findet die „International Munich Cyber Security Conference“ (MCSC) statt. Veranstalter ist das Sicherheitsnetzwerk München. Die Veranstaltung ist nur für geladene Gäste. Bei Münchner Sicherheitsnetzwerk fragen, ob man die MCSC ausweiten sollte – Kooperation möglich?

Sinnvoll, solche Veranstaltung aufzusetzen und in Tradition zu bringen; Regulatorische Schwerpunkte setzen.

Folgende Teilnehmer haben Interesse, an der Vorbereitung mitzuwirken: Dr. Reinema, Dr. Houdeau, Hr. Kranawetter, Hr. Diaw, Hr. Wolfenstetter, Prof. Eckert.

Weiteres Vorgehen: Zeitnah nach der Sommerpause Themen definieren; Namedropping, wer soll angesprochen werden.

#### **4.3 Themenabend für die Politik zum Thema Cybersicherheit (Ende 2017):**

- Handlungsempfehlungen für die neue Regierung?
- Fortsetzung des Berliner Gesprächs vom Oktober 2016, oder eher Münchner-Dialog

Alle Arbeitskreise des MÜNCHNER KREIS sollen Fragenkatalog an Politik erstellen. Diese sollen gebündelt ausgehändigt werden. Dient als Basis für Diskussion. AK Security: Fragenkatalog erstellen und Kaminabend organisieren.

→ Fragen an Politik überlegen. Prof. Thielmann ruft via Mail zum Zusenden der Fragen auf, sammelt und clustert diese.

**Politischer Kaminabend:** Nutzen, um Themen zu erklären und Personen aufzuschlagen. Neue Regierung soll Themen aufgreifen.

Veranstaltung noch in diesem Jahr? Bundestagswahl im Herbst; bis Posten neu besetzt werden dauert es bis Oktober/November. **Konsens: Nicht mehr in diesem Jahr!** Besser Januar/Februar 2018. Jetzt planen und nach der Wahl einladen.

Vorgehen: Erst Inhalte, dann Format festlegen und Veranstaltung planen. Die Inhalte sind prinzipiell bereits da - siehe Handlungsempfehlungen.



Prof. Thielmann erklärt sich bereit, das Protokoll Berliner Gespräch 2016 durchzusehen und mögliche Themen daraus für nächste Veranstaltung zu selektieren.

#### **4.4 Vorbereitung einer Fachkonferenz in 2018: Themensammlung, PC**

Prof. Dowling: Im Rahmen des MK sind in diesem Jahr bisher zwei Fachkonferenzen geplant (AK Energie und AK Infrastruktur). Von Seiten des MK-Vorstands besteht keine Erwartung – eine Fachkonferenz des AK Security ist nicht zwingend erforderlich. Für das Jahr 2018 gibt es noch keine festen Termine – Thema Quanten-Computing ist geplant.

##### Besteht Interesse an Fachkonferenz? Mögliche Themen?

- **Threat Intelligence:** Informationen über Bedrohungen sammeln und austauschen. Bisher geschieht das in Silos getrennt voneinander. Evtl. wäre eine Konferenz um sich auszutauschen und zu diskutieren sinnvoll (im Sinne der Shared Economy – geteiltes Gemeinschaftsgut).

Dr. Marinos: Am 30. Oktober wird es in Rom ein Event zu dem Thema geben: CTI-EU Bonding EU Cyber Threat Intelligence; von ENISA zusammen mit u. A. der European Defence Agency. Dr. Marinos schickt Infos an Hr. Kranawetter. Auch DCSO bietet Threat Intelligence Feed an.

Hr. Kranawetter erstellt 1-Seiter, dann Diskussion via Telefonkonferenz. Teilnehmer Diskussion: Hr. Kranawetter, Hr. Wilkie, Hr. Montag, Dr. Marinos, Dr. Reinema, Hr. Diaw.

- **Sichere Mobile Identitäten:** Smartphone als Identitätsmedium z. B. im Gesundheitswesen (Versichertenkarte liegt Zuhause, Smartphone zur Identifikation benutzen) → Geräte werden sich verändern. Unterschiedliche Usecases aus Security- und Privacy-Sicht betrachten. Aktuell Trends im Bereich Sichere Mobile Identitäten für den Bürger.

Dr. Houdeau erstellt 1-Seiter, dann Diskussion via Telefonkonferenz. Teilnehmer Diskussion: Dr. Houdeau, Hr. Kranawetter, Hr. Georgiew, Hr. Diaw, Hr. Wolfenstetter.

#### **5.) Weitere Berichte zu aktuellen Aktivitäten: alle**

Keine Berichte.

#### **6.) Sonstiges**

Prof. Thielmann war stellvertretender Sprecher des AK Security. Er wurde gebeten, einen neuen Arbeitskreis zu begleiten und er möchte aus diesem Grund seine Sprecherschaft niederlegen. Dieser Posten soll wieder neu besetzt werden: Michael Kranawetter ist neuer stellvertretender Sprecher des AK Security.

## **Weitere Termine**

7. Arbeitstreffen des AK Security: Ort und Datum noch nicht bekannt; Terminfindung via Doodle-Abfrage.