

Steckbrief: Thema „Trendbeurteilung“

Autoren: Hartmut Fuchs (fuchsCCC), Michael Montag (Nokia)

Datum: 14. April 2016

Vorlage für: Meeting des AK am 19.4. 2016

Der vorliegende Steckbrief ist ein Vorschlag, wie der AK Security zu der öffentlichen Diskussion im Themenfeld Cyber-Security „Trendbeurteilung“ beitragen kann. Er beschreibt die grundlegende Idee, Motivation und Zielstellung sowie einen Vorschlag, wie das Thema „Trendbeurteilung“ angegangen werden könnte. Zudem beinhaltet er eine erste Liste möglicher Themen / Trends, die Gegenstand der Trendbeurteilung sein könnten.

Motivation und Zielsetzung

Die „Trendbeurteilung“ hat das Ziel, eine fortlaufende und fundierte Einschätzung wesentlicher Entwicklungen im Bereich Cyber-Security zu geben und neben den technischen Aspekten auch die damit zusammenhängenden ökonomischen und gesellschaftlichen Aspekte zu beleuchten. Es soll erreicht werden, dass die wichtigen Interessengruppen und Entscheider (in allen Stakeholdergruppen, insbesondere auch außerhalb der Cyber-Security Community) sich der relevanten aktuellen Fragestellungen im Zusammenhang mit Cyber-Security bewusst werden und deren Abhängigkeiten und möglichen Auswirkungen besser verstehen. Dabei sollen auch Bewertungen aus der Sicht der Technologiefolgenabschätzung und Zukunftsforschung (fundiert spekulativ) einbezogen werden. Letztlich soll die Fähigkeit der Interessensgruppen und Entscheider zur Trendbeurteilung gestärkt werden damit sie aktiv und faktenbasiert die Weiterentwicklung aus ihrer jeweiligen Verantwortlichkeit heraus vorantreiben können.

Vorschlag zur Umsetzung

Für die Umsetzung wird der folgende Ansatz verfolgt:

- Der AK Security des Münchner Kreises erstellt und pflegt kontinuierlich einen „**MK Cyber-Security Trend-Report**“, der regelmäßig mit „Trendbewertungen“ zu neuen Themen / Fragestellungen erweitert wird. Der Report besteht neben einem einführenden Teil (Motivation, Ansatz) im Kern aus einer Serie / Kollektion von jeweils in sich geschlossenen einzelnen Opinion-/Positionspapieren (2 bis max 3 Seiten) mit einer aktuellen Einschätzung zu einem Trend / einer Fragestellung, die einzeln veröffentlicht werden. Diese einzelnen Trendbeurteilungspapiere können als Kapitel des so ständig wachsenden Gesamtreports verstanden werden.
- Bezüglich der **Periodizität** für die Veröffentlichung neuer Trendthemen / Kapitel ist zwischen zwei möglichen Varianten zu entscheiden:
 1. festgelegter regelmäßiger Zeitraum (jährlich / halbjährlich / ...) und Veröffentlichung aller in diesem Zeitraum erstellten Beiträge
 2. oder unregelmäßig, d.h. Veröffentlichung jedes Beitrags sobald dieser verfügbar ist.
 - Empfehlung: Variante 2, allerdings sollte die Erstveröffentlichung zumindest bereits drei Trendbeurteilungen enthalten
- **Art der Veröffentlichung:** Die in sich geschlossenen Kapitel sollten einzeln verfügbar gemacht werden. Zusätzlich sollte zu jedem Zeitpunkt auch der aktuelle

Gesamtreport (Einführung plus alle verfügbaren Kapitel) als Download angeboten werden.

- Um den Charakter der regelmäßigen Erweiterung zu betonen könnte auch eine Veröffentlichung in Form eines Blogs sinnvoll sein (alternativ oder zusätzlich).
- Der mit der Veröffentlichung angesprochene Personenkreis / Verteiler ist noch zu definieren (siehe dazu auch „Motivation und Zielsetzung“).
- Anmerkung: zwecks größerer Verbreitung sollten wir darüber nachdenken die Beiträge zumindest zusätzlich auch in Englisch verfügbar zu machen.
- Jedes **einzelne Trendpapier / Kapitel** sollte einer grob vorgegebenen und damit einheitlichen und wiedererkennbaren Struktur folgen, die im Detail noch festzulegen ist, aber z.B. folgende Punkte enthalten sollte:
 - eine Kurzdarstellung, was unter dem Trend sachlich verstanden wird
 - eine Einschätzung der aktuellen Entwicklung zu einem oder mehreren wesentlichen / aktuellen Aspekten in der Sache (Darstellung)
 - eine Bewertung, welchen Impact diese aktuelle Entwicklung hat/haben kann auf a) den Einzelnen/das Individuum, b) die Wirtschaft, c) auf Politik und Gesellschaft
- Ein **Redaktionsteam** betreut den Report organisatorisch, ruft zu Beitragsvorschlägen auf, wählt die nächsten Themen / Beiträge aus und ist verantwortlich für die Qualitätssicherung.
- Für jedes einzelne Trendpapier / Thema werden 1-2 **inhaltlich Verantwortliche** (Themenpaten) bestimmt, die persönlich oder in ihrem Netzwerk / ihrer Organisation für jeweils die Erstellung des entsprechenden Beitrages sorgen.
 - Die jeweiligen Autoren stehen für ihren Beitrag. Damit ist eine Publikation in diesem Report auch attraktiv z.B. für den wissenschaftlichen oder unternehmensbezogenen Nachwuchs.
- Der **AK Sicherheit** bestimmt und verfolgt die thematische Schwerpunktsetzung und passt diese ggf. an

Dieser Ansatz erlaubt es, klein“ zu beginnen, den periodischen Report modular aufzubauen und ihn je nach Leistungsfähigkeit des AK / der Autoren und ggf. Änderung der Sachlage thematisch anzupassen. Zudem erlaubt er thematisch eine große Offenheit gegenüber aktuellen Entwicklungen bzw. einzelnen sachlich vertiefenden Aspekten.

Die periodisch publik gemachten Ergänzungen erhöhen zudem die öffentliche Aufmerksamkeit.

Trends / Inhalte

Der Vorschlag für die Wahl der folgenden Trends erfolgt vor dem Hintergrund der Entwicklung zu Industrie 4.0 / Digitalisierung auf der Basis des IoT. Für den Beginn werden folgende Themen vorgeschlagen:

- Authentifizierung und Identität (Kommunikation zwischen Organisationen / Menschen, Mensch-Maschine / Maschine, M2M) : Entwicklung, Sicherheitsbezogene Risiken / Herausforderungen
- Robotik – autonom und vernetzt : Entwicklung, Sicherheitsbezogene Risiken / Herausforderungen
- Sicherheitsstandards für unternehmensübergreifende Wertschöpfungsketten

Die endgültige Festlegung der initialen Themen / Kapitel unterliegt natürlich dem AK Security und ist wesentlich auch abhängig davon für welche Themen sich „Freiwillige“ finden.

Eine Liste weiterer möglicher Trend-Themen findet sich in der Anlage.

Nächste Schritte

Die nächsten Schritte sind:

- Diskussion und Entscheidung im AK über den Ansatz (s.o. 2.)
- Falls dem Grunde nach akzeptiert: Entscheidung über die ersten Trend-Themen (s.o. 3 und Anhang)
- Für die Umsetzung (falls noch relevant)
 - Benennung eines Redaktionsteams (Freiwillig: Herr Fuchs)
 - Benennung von 1-2 Themenpaten für jeden gewählten Trend
 - Danach: Etablieren des Redaktionsteams und des Arbeitszusammenhangs mit den Themenpaten / Autoren und Beginn der Arbeit; u.a. auf der Basis eines „Best practice“ Beispiels für ein Kapitel
 - Bericht in den folgenden Meetings des AK über den Fortschritt

Anhang: Liste von möglichen Trend-Themen

Anmerkung: Diese Liste ist weder komplett noch systematisch erstellt worden. Einige Themen sind allgemeine Trends, die zunächst einmal nicht originär aus dem Bereich Security kommen. Bei deren Behandlung geht es dann natürlich darum herauszuarbeiten, warum sie auch aus der Sicht der Security relevant sind. Außerdem ist es evtl. sinnvoll bestimmte Themen zusammenzufassen.

Vorschlag für den initialen Report

- Authentifizierung und Identität (Kommunikation zwischen Organisationen / Menschen, Mensch-Maschine / Maschine, M2M) : Entwicklung, Sicherheitsbezogene Risiken / Herausforderungen
- Robotik – autonom und vernetzt : Entwicklung, Sicherheitsbezogene Risiken / Herausforderungen
- Sicherheitsstandards für unternehmensübergreifende Wertschöpfungsketten

Weitere Kandidaten

Technologie / Elementare technische Entwicklungen

- Next Generation Networks (network architectures / 5G / internet und internet-Protokoll(e))
- Kryptografie
 - z.B. Quanten-Computing
 - physical layer security
- Supply-Chain Security und nationale Souveränität
 - Integritätsschutz
 - Zertifizierungsmodelle

Umsetzung der Digitalisierung in der Praxis

- Implementierung von Industrie 4.0 - international / europaweit / national: Entwicklungslinien in den großen Industrie-Gruppen
- Entwicklung der Dienstleistungsspektren der IT Industrie
 - Infrastrukturen (die unteren Layer des ISO Schichtenmodells)
 - Plattformen (Cloud, TK Unternehmen, Business-Modell-Plattformen wie zB salesforce, Soziale Netzwerke....)
- IoT and Cyber physical systems/networks
 - How merging the cyber and physical space creates dependencies between security and safety.
- Sharing Economy (security as an enabler)

Risiken, Bedrohungen (evtl Themen für den AK-Schwerpunkt 3: Awareness/gesellschaftliche Diskussion ?)

- Megatrends in der Cyber Kriminalität / Dark Net
 - z.B. Future of Ransomware
- Megatrends in der Nutzung der ICT durch die Bevölkerung
 - Privacy-Risiken, Privacy Engineering, zukünftige Einstellung der Bevölkerung zu Privacy oder warum ist Snapshot so erfolgreich ?
- Security Co-operation: security related information sharing and collaboration
 - z.B. common and shared threat intelligence

Risiko-Management (evtl Themen für den AK-Schwerpunkt 3: Awareness/gesellschaftliche Diskussion ?)

- Resilienz der Unternehmen / Organisationen / Körperschaften
- (Re-)Aktionsfähigkeit der Strafverfolgung und Justiz
- Tempo und Qualität der regulatorischen und gesetzlichen Entwicklungen (international / europaweit / national)
- Tempo und Qualität des gesellschaftlich-politischen Diskurses über Cyber Risiken und Security
- Einfluss des wachsenden Cyber-Security Versicherungsmarktes
 - Standardisierung und stärkere Verbreitung von Sicherheitszertifizierungen
 - Risiko-Outsourcing