EU-weite Mindeststandards für sichere IT Produkte

Dr. Thomas Stubbings

ViS!T Tagung, Bern

29.6.2016

Problemstellung

- Fehlende einheitliche Standards und Zertifizierungen
- Fragmentierung: unterschiedliche nationale Gesetzgebungen und Regulatorien
- Fehlende Transparenz
- Hersteller unter Kostendruck
- Sicherheit als Kostenfaktor für Kunden
- Unklares Restrisiko

Zielsetzung

- Schaffung einer gemeinsamen Basis: unternehmensübergeifend, national und international (EU-weit)
- Schaffung eines Kriterienkataloges für IT Produkte (Baseline Security)
  - Unternehmen könnten darauf vertrauen, dass IT Produkte die sie einsetzen gewissen Mindeststandards genügen und ersparen sich daher eigene teure Tests
  - Anbieter von IT Produkten können sich anhand klarer Vorgaben orientieren und Produkte entwickeln, die der Markt wünscht in einer Qualität, die er erwartet.
    - Kriterium in Vergabeverfahren
- Überprüfbarkeit / Messbarkeit der Kriterien!
- Berücksichtigung spezieller Bedürfnisse des Datenschutzes im europäischen Raum: "EU data protected"
- Förderung europäischer Technologien im IT Bereich, Stichwort "digitale Souveränität“

Umfang

- Folgende IT-Produktklassen werden in scope gesehen:
  - Internet, Basisinfrastruktur
  - Endgeräte (aus Business-Sicht) inkl. Betriebssysteme
  - Backend-Systeme (HW/SW)
  - Webservices inkl. Cloud-Services
  - Sicherheitssysteme (Firewall, AV, Berechtigungssysteme, etc.)

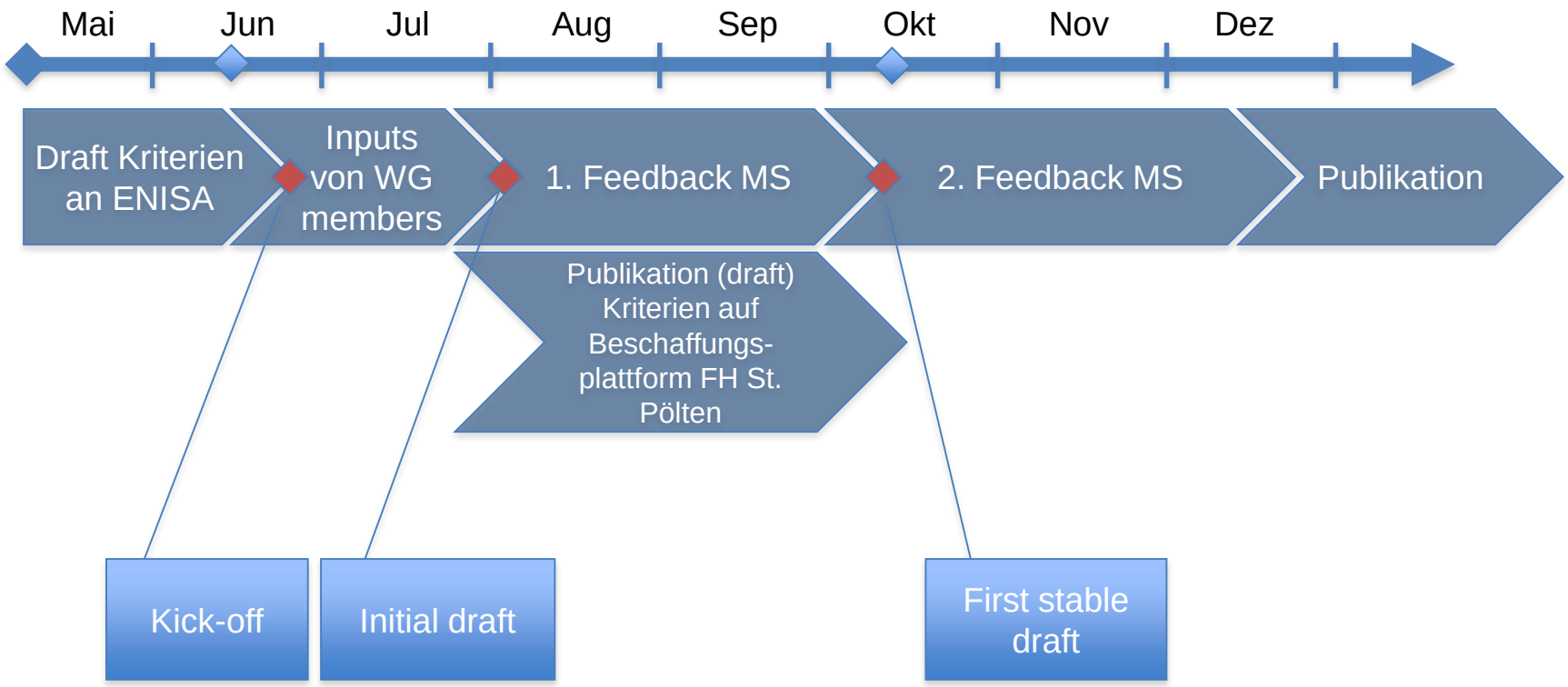
Bisherige Ergebnisse

- **Analyse bestehender Ansätze**
- **Identifikation möglicher Kooperationspartner**
- **Initiierung einer Arbeitsgruppe auf europäischer Ebene**
  - „Common baseline security requirements for the procurement of secure ICT products and services“
  - Lead: ENISA
  - Derzeit 8 Länder zugesagt (A, D, FIN, CZ, ES, FR, NL, SWE)
- **Erstellung einer Draft Kriterienliste**

Kriterien

- Stand der Technik
  - Sichere Grundkonfiguration
  - Sichere Protokolle
  - Verschlüsselung
  - Authentifizierung & Authorisierung
  - Plausibilitäts und Integritätsprüfung
  - Protokollierung
  - Websicherheit
- Sicherheitszertifizierung
- Integritätsverifikation
- Source Code Authentizität
- Spyware/Malware-Freiheit
- Patch Management
- Mindestlebenszyklus
- Sichere Softwareentwicklung
- Tests
- Dokumentation
- Datenschutz
- Rechtsstand

Zeitplan


Mai
Jun
Jul
Aug
Sep
Okt
Nov
Dez
Draft Kriterien an ENISA
Inputs von WG members
1. Feedback MS
2. Feedback MS
Publikation
Publikation (draft) Kriterien auf Beschaffungs-plattform FH St. Pölten
Kick-off
Initial draft
First stable draft

Zu klären

- Umsetzung der Baseline Security als Standard / Zertifizierbarkeit
- Geltungsbereich / Verbindlichkeit

Fragen?

Kontakt

Dr. Thomas Stubbings
thomas.stubbings@rbinternational.com
thomas.stubbings@tsmc.at

+43 664 8888 2582