

München 07.03.2016

Steckbrief: AK IT-Security des Münchner Kreises

Thema: Blueprint für robuste IT-Sicherheitsarchitekturen

Herausforderung:

Die Investitions-Entscheidung eines Unternehmens für den richtigen adäquaten Schutz einer bestehenden IT-Umgebung ist sehr komplex. Entscheidungsfaktoren über die Robustheit einer Soll-Gesamtarchitektur setzen sich aus Faktoren der erreichbaren technischen Sicherheit, der notwendigen organisatorischen Einbettung inkl. des dafür benötigten Know-hows, der Vertrauenswürdigkeit der Logistikkette der zu beschaffenden Lösungen und der Haftung und Rechtssicherheit, die aus diesen Logistikketten resultiert, zusammen. Bereits vorhandene Informationen zur Robustheit vergleichbarer Installationen sind entweder nicht öffentlich oder nicht vertrauenswürdig, so dass Entscheider und die Risikomanagement-Organisation allein gelassen werden. Hier soll geholfen werden.

Ziel:

1. Beschreibung eines Verfahrens, wie neutrale Organisationen ohne rechtlich problematische Situationen, wie z.B. unerlaubte Markteingriffe, befürchten zu müssen, einen konkreten Blueprint für robuste IT-Sicherheitsarchitekturen veröffentlichen können und
2. der exemplarische Aufbau einer Meta-Struktur zu einem solchen Blueprint.

Nicht-Ziel:

Erstellung und Pflege einer IT-Sicherheitsarchitektur

Vorgehensweise:

Identifikation und Interview der Stakeholder (BSI, LfV, BfV, Allianz für Cybersicherheit, BMWi, VOICE, BDI, VDMA, Städtetag, ...) mit der Interessenslage, die IT-Sicherheit (der KMU) zu verbessern. Interview über die Möglichkeiten, die diese im Markt sehen / haben und der aus ihrer Sicht nötigen Maßnahmen. Auswertung der Ergebnisse – evtl. Schärfen der Ergebnisse in einer Podiumsdiskussion der wesentlichen Stakeholder (z.B. BSI, BMI, VOICE, Münchner Kreis). Erstellung eines Handlungsvorschlages für die identifizierten wesentlichen Stakeholder.