smartspacelab.eu
the Scientific Technology Enterprise

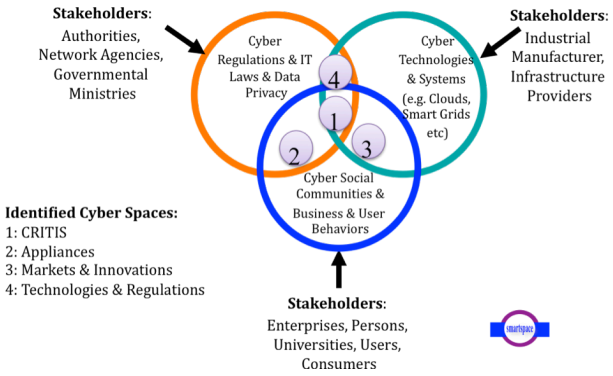
*BEST Position Statemenet No. 02, 12.12.2014*
*R2GS Germany c/o*
*ssl.eu GmbH, Berner Str. 21B,*
*12205 Berlin: demeer@smartspacelab.de*

# *IT Energy & Sicherheit → Teilhaber-Modell, zur Definition von Rollen und Verantwortung in Unternehmen und Organisationen, um Vertrauen der Kunden in Dienstleistungen zu erzielen*

Im nebenan abgebildeten Teilhabermodell der Digitalen Gesellschaft (im Cyber-Raum) gibt es die 3 Maßnahme-Kategorien: *‚I. Regulierung & Gesetzgebung', ‚II. Infrastruktur-Betreiber & Hersteller' und ‚III. Anwender & Verbraucher'.*

Jeder Teilhaber spielt eine oder mehrere dieser Rollen. Zwischen Teilhabern eines Cyber-Raums besteht reger Informationsaustausch, um die Zuverlässigkeit, Sicherheit und vertrauensvolle Kooperation zu gewährleisten.

Der gemeinsam verwaltete und organisierte Cyber-Raum besteht aus den physikalischen/organisatorischen Komponenten: *1.Kritische Infrastruktur - Plattform, 2.Applikationen, 3.Marktgeschehen, 4.Technologie Deployment.*




Kriterien und Maßnahmen werden von folgenden KRITIS/DIGIS-Teilhabern (*stakeholders*) beansprucht, bzw. ausgeführt:

I. Kategorie Regulierer, Gesetzgeber, Ämter, Normung:

1. Normung und Standardisierungsstellen, Zertifizierung, Auditing
2. IT-rechtliche Regulierungs-Einrichtungen und Gesetzgebung
3. Autorisierte Stellen für die Vergabe von Digitalen Rechten und kryptographischen Schlüsseln für verschiedene Zwecke, Verwaltung von Identitäten etc.

II. Kategorie Hersteller, Technologen, Infrastrukturbetreiber:

4. Z.B. Energie-Netzwerk-Infrastruktur-Betreiber (überregionale HGÜ / regionale Wechselspannung-NW etc.)
5. Energie-Lieferanten (volatil, permanent verfügbar) → Energie-Stabilität := grüne + braune + schwarze Energie-Erzeugung + *Smart Community* Verbraucher-Profile
6. *Cloud Computing* (virtuelle) Dienstleister
7. Operative Leitstellen (SOC, SIRT etc.) in Unternehmen und Organisationen (Security/Zuverlässigkeits-Management)
8. Hersteller f elektro- und meßtechnische Infrastrukturkomponenten (Sensoren, Aktoren, IoT, ...)
9. Kommunikationsnetzwerk Betreiber (Funk, Kabel, Internetz, ...)
10. Eigentümer / shareholder kritischer Infrastrukturen (Kommunikation, Wasser, Elektrizität, Transport, etc.)

III. Kategorie Anwender, Verbraucher, Kunden:

11. Energie-Verbraucher (Haushalt, Industrie, Smart City, Cloud Computing RZ) → *Energie-Effizienz := ‚weiße Energie'*
12. *Cloud Computing* (virtuelle) Kunden
13. Nicht legale Dritte mit u.U. gestohlenen Rechten (unauthorized third parties UTP)
14. Legale Dritte mit Recht auf ‚*lawful interception'* (authorized third parties ATP).

Kriterien, Maßnahmen und ISI-Indikatoren zur (Gegen-) Steuerung der Infrastruktur zur Vermeidung von unerwünschtem (Fehl-) Verhalten, werden in der Tabelle ‚Maßnahmenkatalog' [Position Statement Nr.4], unter Angabe der ISI-Klassen (*V/P/I Spezifikationen*) und der *Kritikalität* (vgl. ISI-Klasse *IMPact*), spezifiziert. Das ursächliche Ereignisses, worauf eine Maßnahme einwirken soll, wird mittels eines Klassifikationswertes, des sog. *Information Security Indicator (ISI-Wertes)*[1] ermittelt. Das *ISI*-Klassifikationsschema, stammt von der *ETSI* [2] und hat 5 hierarchische Klassifikationselemente: *‚super classes → classes → families → components → valued parameters'*. Für den *IT S&E*-Maßnahmenkatalog beschränken wir uns auf die Bezeichnungen des *‚super classes → class*es' –Schemas, d.h. der SIEM- Ereignisklassen: ***V****ULnerabilities* – ***P****REvention* – ***I****NCidents (V/P/I) und IMPact.*

[1] ETSI ISG ISI Reference Table [isiQRC v.1.1.1:2013-04-23];
[2] ETSI - ISG ISI – European Telecommunication Standardisation Institute - Information Security Indicators Industrial Specification Group;