**Schriftlicher Bericht für die Sitzung der IMK am 23./24.05.2013 in Hannover**

**TOP Bericht von der länderoffenen Arbeitsgruppe Cybersicherheit**

## 1. Nationaler Cyber-SR

Am 19.03.2013 fand die letzte Tagung des nationalen Cyber-SR statt. Neben dem Bericht des BSI zur Gefährdungslage standen vor allem nationale und internationale Regelungen und Aktivitäten zur Ausgestaltung der IT-Sicherheit im Mittelpunkt.

Das BMI berichtete in diesem Zusammenhang zum Sachstand seines Referentenentwurfes für ein IT-Sicherheitsgesetz und kündigt an, nach Auswertung aller Stellungnahmen und Änderungswünschen einen überarbeiteten Gesetzesentwurf zu versenden. Im Übrigen sei eine Verbandsanhörung beabsichtigt.

Ein weiterer TOP befasste sich mit der EU-Cybersicherheitsstrategie. Das BMI bewertet den Ansatz der EU-KOM als der deutschen Cybersicherheitsstrategie sehr ähnlich.
Dem Schutz der Kritischen Infrastruktur werde im Richtlinienentwurf der EU-KOM besondere Bedeutung beigemessen. Der Entwurf enthalte weitgehendere Anforderungen an die Wirtschaft als im Referentenentwurf des BMI und sähe zudem Sanktionsmöglichkeiten vor.

## 2. Länderoffenen Arbeitsgruppe Cybersicherheit (LänderAG Cybersicherheit)

Am 10.04.2013 fand das Treffen der Staatssekretäre/Staatsräte am Flughafen Frankfurt statt. Nach einer Präsentation der IT-Sicherheitsstrategie des Gastgebers Fraport AG[1] und einem wissenschaftlichen Fachbeitrag zum Thema „elektronische Identitäten“[2] wurden die Ergebnisse und Planungen der Unterarbeitsgruppen vorgestellt, die durch ein Treffen der Arbeitsebene im Februar 2013 in Wiesbaden vorbereitet waren.

Die thematischen Schwerpunkte des Treffens waren:

a) Mobile Endgeräte im Cyberraum – UAG MEC,

b) KRITIS und Cybersicherheit – UAG KRITIS,

c) ein Fortschrittsbericht zum CERT-Aufbau in den Ländern.

### Zu a) UAG MEC

Herr Staatssekretär Pschierer (BY) gab einen Zwischenbericht von der UAG, an der unter Federführung BY die Länder BW, HE, HH, MV, NW, RP, ST und TH mitwirken.

[1] Der CIO der Fraport AG, Herr Dr. Krieg, referierte zur IT-Sicherheitsstrategie des Unternehmens und präsentierte nach dem Treffen den Sicherheitsleitstand des Flughafens.
[2] Herr Dr. Kreutzer, Geschäftsführer CASED (Center for Advanced Security Research in Darmstadt) trug einen Folienvortrag von Prof. Dr. Waidner, Leiter Fraunhofer Instituts für Sichere Informationstechnologie, Darmstadt vor.

Ziel ist die Ausarbeitung und Abstimmung eines Leitfadens für den Einsatz mobiler Endgeräte in KMU und Behörden.

Die Arbeiten werden wissenschaftlich begleitet (Fr. Prof. Eckert, Fraunhofer AISEC, München) und sollen die Gefahrenquellen bei der Nutzung mobiler Endgeräte beschreiben und daraus Gegenmaßnahmen ableiten.

Ein Ergebnis soll bis Juli 2013 vorliegen.

**Zu b) UAG KRITIS**

HE berichtete zur UAG KRITIS, an der unter Federführung HE die Länder BW, BY, NI, NW, RP und TH mitwirken sowie BSI und BBK.

Grundlage ist der Beschluss der Konferenz der Innenminister und -senatoren der Länder auf ihrer 195. Sitzung am 31. Mai / 1. Juni 2012, mit dem eine Bund-Länder offene Arbeitsgruppe zur Bündelung sowie zum Austausch der Informationen und zur konzeptionellen Einbindung der Länder im Bereich Cyber-Sicherheit unter Federführung Hessens eingerichtet wurde (TOP 40). Die Arbeitsgruppe wurde gebeten, insbesondere die möglichen Auswirkungen von Cyber-Attacken auf die Funktionsfähigkeit kritischer Infrastrukturen zu untersuchen.

Die Arbeitsgruppe ist am 2. August 2012 erstmals zusammengetreten. An dieser und den weiteren Besprechungen haben neben den IT-Fachleuten auch Vertreter aus dem Bereich Bevölkerungsschutz / Katastrophenschutz bzw. Krisenmanagement des Bundes und der Länder teilgenommen.
Um die richtigen Anforderungen an eine nationale Cyber-Sicherheitsstrategie in Bezug auf den Schutz der Funktionsfähigkeit von Kritischen Infrastrukturen entwickeln zu können, sollen - gemeinsam mit den KRITIS-Betreibern und den Fachressorts - für die jeweiligen Sektoren eine Bestandserhebung erstellt und ggfs. Handlungsempfehlungen formuliert werden. Der Aufbau paralleler KRITIS-Strukturen unter dem Gesichtspunkt der Cyber-Sicherheit soll dabei vermieden und die im Bund und in den Ländern eingerichteten Koordinierungsstellen Kritische Infrastrukturen als wichtige Ansprechpartner einbezogen werden.
Die Arbeitsgruppe bearbeitet zunächst den Sektor Energie (Stromversorgung) und prüft dabei auch, ob hierauf aufbauend ein Referenzmodell für die übrigen KRITIS-Sektoren (Transport / Verkehr; IKT; Finanzen und Versicherungen; Gesundheit; Wasser; Medien und Kultur; Ernährung sowie Staat und Verwaltung) entwickelt werden kann.

Ziel ist zunächst die Erstellung einer exemplarischen Bestandserhebung für den Bereich der Stromversorgung. Hierzu wurde ein Gesprächsleitfaden sowie ein Fragenkatalog erstellt, mit dem eine Bestandserhebung bei den KRITIS-Betreibern dieses Sektors erfolgen kann. (Anlage 1)

Der Konferenz der Innenminister und –senatoren der Länder soll zur Herbstsitzung 2013 über die gewonnenen Ergebnisse berichtet und ggfs. Handlungsempfehlungen vorgelegt werden. Die Bewertung der so gewonnenen Erkenntnisse und die Ermittlung ggfs. erforderlicher Umsetzungsschritte obliegen dann den fachlich zuständigen Ressorts im Rahmen der bewährten Zuständigkeiten bzw. den jeweiligen Betreibern.

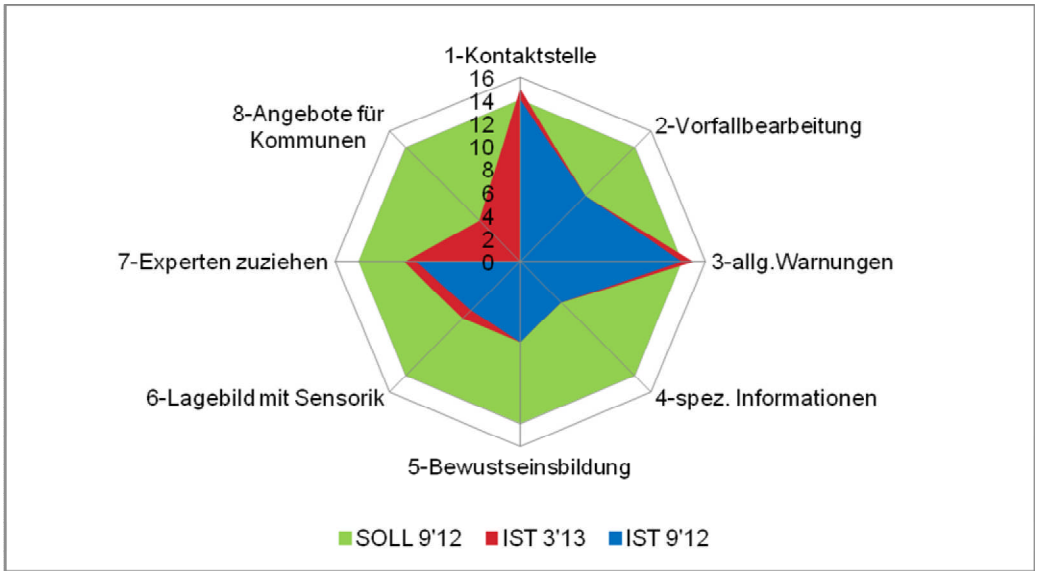
**Zu c) CERT-Aufbau in den Ländern**

Zum Status des CERT-Aufbaus in den Ländern fasste HE die Ergebnisse einer erneuten Länderabfrage mit Stand März 2013 zusammen; eine erste Bestandsaufnahme vom September 2012 war der Länder AG Cybersicherheit und dem nationalen Cyber-SR im Oktober 2012 vorgestellt worden.

Grundlage der Erörterung zum CERT-Status war eine in der LänderAG Cybersicherheit verabschiedete „Handreichung zum Aufbau von CERTs“. Die Ausarbeitung beschreibt, wie in Kooperation mit Länder-CERTs insbesondere kleinere und mittlere Kommunen von den CERT-Strukturen und –Prozessen der Länder unterstützt und in diese integriert werden können. (Anlage 2)

Die Auswertungen der Länderumfrage zeigt:

1. Alle Länder erbringen bereits Basisdienste in allen wesentlichen CERT-Handlungsfeldern, wenn auch in unterschiedlicher Intensität.
2. Zwischen September 2012 und März 2013 haben sich die Ausbaupläne in den Ländern konkretisiert.
3. Vorhandene Strukturen und Prozesse wurden gefestigt und ausgebaut; vereinzelt wurden – auch in Nachfolge der LÜKEX2011 – Übungen für das IT-Krisenmanagement durchgeführt.
4. Zur Integration der Kommunen in die Warn- und Alarmierungsdienste einzelner Länder sind erste Maßnahmen geplant bzw. befinden sich in der Umsetzung.
5. Die Nutzung von Erkennungs- und Abwehrtechnologien (Detektions- und Präventionssysteme) wird neben organisatorischen und prozessualen Maßnahmen in Angriff genommen bzw. ausgebaut.




*Zusammenfassung der Länderabfrage zu den Fähigkeiten der Länder-CERTs*[3]

[3] Die CERT-Fähigkeiten sind unter folgenden Leistungskategorien zusammengefasst: **Kontaktstelle:** das Landes-CERT betreibt eine Kontaktstelle die Informationen und Warnungen zu Sicherheitsschwachstellen und Meldungen über schwerwiegende IT-Sicherheitsvorfälle entgegen nimmt und bearbeitet; **Vorfallbearbeitung:** das Landes-CERT unterstützt aktiv die Bearbeitung schwerwiegender Sicherheitsvorfälle bei seinen Nutzern; **allg. Warnungen:** das Landes-CERT informiert und warnt seine Nutzer vor aktuellen Bedrohungen; **spez. Informationen:** das Landes-CERT bietet seinen

Die LänderAG Cybersicherheit hält eine Beschleunigung und Verstärkung des CERT-Ausbaus angesichts der wachsenden Bedrohung für erforderlich und unterstützt ausrücklich die entsprechenden Vorhaben des IT-Planungsrates.

Die Teilnehmer waren sich einig, die Aufträge und Arbeiten in der LänderAG Cybersicherheit künftig eng mit der im März 2013 durch den IT-Planungsrat eingerichteten Kooperationsgruppe Informationssicherheit abzustimmen. In jedem Fall soll Doppelarbeit vermieden werden.[4]

**Beschlussvorschlag:**

1. Die IMK nimmt den schriftlichen Bericht des Vertreters des Landes Hessen zu den Ergebnissen und Planungen der länderoffenen Arbeitsgruppe „Cybersicherheit“ zur Kenntnis und bittet diese, zur Herbstsitzung 2013 erneut zu berichten.

2. Die IMK bittet den Vorsitzenden, zwischen der länderoffenen AG Cybersicherheit und der Kooperationsgruppe Informationssicherheit des IT-Planungsrates eine Abstimmung der Themen herbeizuführen, um Synergien zu erzielen und Doppelarbeit zu vermeiden.

---

Nutzern individuell zugeschnittene Informationen; **Bewusstseinsbildung:** das Landes-CERT unterstützt die Ausbildung und die Aufrechterhaltung des erforderlichen Sicherheitsbewusstseins durch Veröffentlichungen und Veranstaltungen; **Lagebild mit Sensorik:** für das Lagebild zur IT-Sicherheit werden neben Informationen Dritter auch Auswertungen aus Mess-systemen und Protokolldateien genutzt; **Experten hinzuziehen**: das Landes-CERT kann bei Bedarf auf Experten außerhalb des CERTs in erprobten Strukturen zugreifen; **Angebote für Kommunen:** (neu abgefragt in 3'13) das Landes-CERT bietet Teile seiner Leistungen für die Kommunen des Landes an.

[4] Ein erste Abstimmung von Themen und der weiteren Zusammenarbeit zwischen der Kooperationsgruppe Informationssicherheit des IT-Planungsrates und der LänderAG Cybersicherheit fand am 24.04.13 mit Teilnehmern aus dem BMI (ITD) sowie BY und HE statt.