Baden-Württemberg
MINISTERIUM FÜR UMWELT, KLIMA UND ENERGIEWIRTSCHAFT
GESCHÄFTSSTELLE DER UMWELTMINISTERKONFERENZ 2014

Ministerium für Umwelt, Klima und Energiewirtschaft Baden-Württemberg
Postfach 103439 • 70029 Stuttgart

An die ständige Konferenz der Innenminister- und Senatoren der Länder

Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen

Haroldstr. 5
40213 Düsseldorf

Stuttgart 17.12.2014
Name Frau Dr. Saken-Braunstein
Durchwahl 0711 126-2555
E-Mail UMK2014@um.bwl.de
Aktenzeichen Z-8804.11/49
(Bitte bei Antwort angeben!)

Stellungnahme lt. Umlaufbeschluss 18/2014 der UMK zum "Abschlussbericht der AG Cybersicherheit und des AK V zur Bestandsaufnahme der Cybersicherheit kritischer Infrastrukturen am Beispiel der Energiewirtschaft"

Bezugnehmend auf Ihr Schreiben vom 24.06.2014 wurden die Umweltressorts der Länder abgefragt mit der Bitte um Prüfung des genannten „Abschlussberichtes der AG Cybersicherheit und des AK V zur Bestandsaufnahme der Cybersicherheit kritischer Infrastrukturen am Beispiel der Energiewirtschaft“ im Hinblick darauf, welche Maßnahmen in der Zuständigkeit der Umweltressorts zu ergreifen sind, um die Cybersicherheit bei Kritis-Unternehmen weiter zu verbessern.
Die Umweltministerkonferenz sendet folgende abschließende Stellungnahme der (Umlaufbeschluss UMK 18/2014) zusammengefasst aus den Einzelstellungnahmen der Umweltressorts der Länder Baden-Württemberg, Sachsen, Bayern, Niedersachsen, Saarland, Sachsen-Anhalt und Schleswig Holstein mit der Bitte, die Aktualisierungen (Präzisierungen des BMUB auf Seite 4, zweiter Absatz, s. Anlage mit gekennzeichneter Änderung) gegenüber der Fassung vom 14.10.2014 zu berücksichtigen.

Grundsätzliches

Die Aussagen des vorliegenden Abschlussberichts werden von der Umweltministerkonferenz geteilt und die vorgeschlagenen Maßnahmen begrüßt. Insbesondere ist die UMK der Meinung, dass die verstärkte Zusammenarbeit

staatlicher und gewerblicher Unternehmen sowie der verschiedenen staatlichen Ebenen im Fokus stehen sollte.
Herausragende Bedeutung kommt dabei vor allem dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu. Dies betrifft einerseits die fortwährende Aktualität und Praxistauglichkeit der vom BSI beschriebenen, in Deutschland für sowohl öffentliche Verwaltung als auch Privatwirtschaft meist maßgeblichen Methodik zur Gewährleistung eines Mindestmaßes an Informationssicherheit; andererseits jedoch auch die Funktion des BSI als direkter Mittler zwischen den einschlägigen Vorschriften des Bundes und der betroffenen Wirtschaft. Neben der Kontrolle entsprechender staatlicher Vorgaben an die Betreiber Kritischer Infrastrukturen sollte aus Sicht der UMK auch die im vorliegenden Abschlussbericht erwähnte Sensibilisierung von Klein- bzw. Kleinstbetrieben vorgenommen werden, da denen die beschriebene Thematik teils noch gar nicht bewusst ist.

Es wird vorgeschlagen die Länder bei der Erarbeitung branchenspezifischer Standards zur Umsetzung sicherheitsbezogener Vorgaben des Bundes einzubeziehen. Betroffene Einrichtungen, auch im nachgeordneten Bereich der Ressorts, müssten die Erarbeitung entsprechender, später aufgrund ihrer Mitgliedschaft in einschlägigen Branchenverbänden mit hoher Wahrscheinlichkeit auch für sie geltenden Regelungen ohnehin zumindest zur Kenntnis nehmen, wenn nicht gar aktiv begleiten.

Energieversorgung

Die Elektrizitätsversorgung zählt auch aus Sicht der UMK zu den kritischen Infrastrukturen. Es wird begrüßt, dass die Bundesregierung insbesondere zum Schutz kritischer Infrastrukturen wie der Stromversorgung eine Cyber-Sicherheitsstrategie beschlossen hat, mit der unter anderem ein Zentrum zur Abwehr digitaler Angriffe aufgebaut werden soll. Insbesondere Informationswege, die einem direkten Zugriff auf Netzkomponenten im Sinne von Fernsteuerung dienen, sind seitens der Netzbetreiber mit einem höchstmöglichen Sicherheitsgrad gegen das Eindringen Dritter bzw. unbefugte Nutzung abzusichern. Die Anforderungen an den Schutzbedarf sind ähnlich zu bewerten wie das Schutzniveau, welches beispielsweise in der Telekommunikations- oder der Finanzdienstleistungsbranche festgestellt und umgesetzt wurde.
Die Dezentralisierung der Energieversorgung, induziert durch die Energiewende-Gesetzgebung, stellt ein wachsendes Potential von Sicherheitslücken dar, zumal der

Aufwand pro Anlage für Sicherheitsmaßnahmen im Vergleich zu Kraftwerken und Netzen proportional höher ist.
Bei verstärkt vernetzten, intelligenten Stromversorgungssystemen wird die Gefährdung durch Cyberangriffe zunehmen. Es wird begrüßt, dass das Bundesamt für Schutz in der Informationstechnik im Auftrag des BMWI ein Schutzprofil zum Schutz intelligenter Netze (Smart Grids) erarbeitet, das insbesondere den Fremdzugriff über ein sogenanntes Smart Meter (digitaler Energiezähler) und somit auf Kleinstanlagen im Haushaltsbereich verhindern soll. Darüber hinaus gehende Sicherheitsanforderungen sind mit den zuständigen Behörden und den Betreibern bzw. Herstellern abzustimmen. Der im Abschlussbericht vorgeschlagene Aufbau gemeinsamer Computer Emergency Response Teams (CERTs) bzw. die Prüfung der Einbeziehung einschlägiger Unternehmen in existierende CERT-Strukturen wird ebenfalls begrüßt.

Datenschutz

Auch wenn die UMK fachlich nicht direkt zuständig ist, sieht sie es als erforderlich, hinsichtlich der in intelligenten Netzen ermittelten und verarbeiteten personenbezogenen Daten, Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit zu ergreifen. Auszugehen ist zunächst davon, dass es sich bei der Erhebung, Verarbeitung, Nutzung und Übermittlung von Verbrauchsdaten von Strom, Gas, Wasser und Wärmeenergie, die mit intelligenten Messsystemen (Smart Meter) gewonnen und verarbeitet werden, um personenbezogene Daten handelt, die Einblick in die Verbrauchs- und damit Lebensgewohnheiten der Betroffenen geben können. So sind Smart Meter als technische Bausteine der Smart Grid-Technologie schutzbedürftig. Im Auftrag des Bundesministeriums für Wirtschaft und Technologie wurden daher so genannte Schutzprofile (Protection Profiles) entwickelt, in denen eine Vielzahl von Bedrohungsszenarien dargestellt und die daraus resultierenden Sicherheitsanforderungen aufgeführt sind. Intelligente Messsysteme müssen den Nachweis erbringen, dass sie die in den Schutzprofilen definierten Sicherheitsanforderungen erfüllen.

Weitere kritische Infrastrukturen im Bereich der UMK

Weitere kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Das BMI hat bisher nur

die Netze aber nicht die Kraftwerke als kritische Infrastruktur angesehen, da der Ausfall einzelner Kraftwerke kein Problem darstellte. Gemäß des Berichtes wurden Energieversorger bzw. Netzbetreiber wie die EnBW bereits befragt und bewertet. Kernkraftwerke selbst sind vom BMI nicht als kritische Infrastruktur eingestuft. Kernkraftwerke könnten im weiteren Sinne auch als kritische Infrastruktur verstanden werden, da ein Unfall mit Freisetzungen schwerwiegende Folgen für Umwelt- und Gesundheit hätten.

Um den Herausforderungen im Bereich der Cybersicherheit zu begegnen, wurde von Bund und Ländern 2013 eine Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen gegen Störmaßnahmen und sonstigen Einwirkungen Dritter verabschiedet. Diese Richtline enthält konkrete Vorgaben im Bereich der Cybersicherheit, mit denen der erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD) gewährleistet werden soll. Meldungen der Betreiber der Kernkraftwerke, bzw. der kerntechnischen Anlagen über relevante Vorkommnisse im Bereich der IT werden über die in der klassischen Sicherung bereits etablierten Meldewege an die Landesbehörden und weiter an das BMUB berichtet. Das BMUB zieht dann ggf. das BSI hinzu. Umgekehrt haben die Betreiber die Möglichkeit der Teilnahme am Traffic Light Protocol (TLP) des BSI, um so direkt und ohne Zeitverzögerung auch vertrauliche Warnungen zu erhalten.

Hochwasserschutz- und Abwasserentsorgungsanlagen

Eine durch einen Cyberangriff ausgelöste Gefährdungslage bei Abwasserentsorgungs- oder Hochwasserschutzanlagen und den zugehörigen Steuerungseinrichtungen ist zwar grundsätzlich denkbar, wird aber als eher gering eingeschätzt. Sie werden bei der Aufzählung kritischer Infrastrukturen (KRITIS) auch nicht explizit genannt. Auch hier laufen die meisten Regelungs- und Steuerungssysteme netzunabhängig.

In Baden-Württemberg bspw. werden im Bereich der Abwasserentsorgung IT-gestützte Verfahren zur Steuerung komplexer Anlagen angewendet, zum einen zur direkten Anlagensteuerung einer Kläranlage als auch im Rahmen der Fernüberwachung bzw. –steuerung von Kläranlagen und von Netzsystemen (z.B. Regenbecken, Pumpwerke). Die Strukturen sind bei etwa 1.000 Kläranlagen im Land dezentral angelegt, sodass sich Störungen eher lokal auswirken dürften.

In den landeseigenen Hochwasserschutzanlagen und den zugehörigen Steuerungssystemen sind die steuerungsrelevanten Systeme der Hochwasserrückhaltebecken sowie der Regelungsbauwerke an Gewässern I. Ordnung (GIO) vom Internet getrennt und somit nicht betroffen. Die im Hochwasserfall auf den Betriebshöfen dezentral genutzten Bürokommunikationssysteme sind an die Sicherheitsrichtlinien des Hauses angebunden. Gleiches gilt für die Kulturwehre Breisach und Kehl (incl. Nebenanlagen):

- Die Steuerungsrechner besitzen keinen Internetzugang.
- Alle zurzeit als sicherheitsrelevanter Regelprozess eingestuften Funktionen werden mittels Signal überwacht und bei Störung umgehend als Alarm abgesetzt.
- Alle regel- und alarmrelevanten Funktionen sind benutzerbezogen und passwortgeschützt.

Die beauftragten Firmen haben nur einen Zugriff durch gesicherte Leitungen (VPN Zugänge; Passwort geschützt). Der Zugang über ISDN (KWK) erfolgt im call-back Verfahren (Modem ruft zurück) bei zusätzlichem Passwortschutz.

Das Flutinformations- und Warnsystem (FLIWAS) wurde in der Version 1.1 im Jahr 2011 unter Sicherheitsaspekten geprüft mit dem Ergebnis, dass FLIWAS in der Version 1.1 diverse Standard-Schwachstellen aufwies. Die daraus abgeleiteten Empfehlungen und Hinweise wurden bei der Weiterentwicklung von FLIWAS berücksichtigt und größtenteils bereits umgesetzt. Die Cybersicherheit der aktuellen Programmversion 2.5 wird als gut bis sehr gut eingeschätzt.

Die Hochwasservorhersagezentrale (HVZ) unterliegt als Bestandteil der LUBW der dortigen Leitlinie für Informationssicherheit. Das Datenschutz- und Datensicherheitskonzept der LUBW wird derzeit aktualisiert. Die Cybersicherheit der HVZ wird von den Experten als gut eingeschätzt.

Wasserversorgung

Die UMK begrüßt, dass die Wasserversorgungswirtschaft vom BMI bereits mit einbezogen wurde und Gespräche laufen. Der DVGW (Deutscher Verein des Gas- und Wasserfaches) wird zusammen mit dem DWA ein technisches Regelwerk hierzu erarbeiten. Die erste Projektgruppensitzung ist für Herbst 2014 geplant.
Der autonome Betrieb der erforderlichen IT-Systeme ist ein konkreter Beitrag zur Gewährleistung der Cybersicherheit. Dieser sollte z. B. auch bei der Talsperrensteuerung beibehalten werden.

Abschließend lässt sich sagen, dass es eine Herausforderung bei der Erfüllung der genannten Aufgaben sein wird, die begrenzten bzw. knapper werdenden Ressourcen unter anderem in den jeweiligen Landesverwaltungen in Einklang mit den steigenden Anforderungen an die Gewährleistung eines übergreifenden Mindestmaßes an Informationssicherheit zu bringen. Die letztjährige Diskussion des Referentenentwurfes eines ,,Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSiG)" des Bundes thematisierte in diesem Zusammenhang bereits einen signifikanten Personalmehrbedarf auf Seiten des BSI. Entsprechendes würde ebenfalls auf die Länder zutreffen.