Formblatt für die Übermittlung der Stellungnahme zur Konsultation des „IT-Sicherheitskatalog“ gem. § 11 Abs. 1a Energiewirtschaftsgesetz (EnWG)

Hinweise:

1.) Ausschließlich weiter zu bearbeitende Dateien (im Format „.doc“ oder „.rtf“) werden berücksichtigt. Sollten Sie Ihre Anmerkungen zusätzlich als pdf übermitteln wollen, so ist dies auch möglich.
2.) Bitte senden Sie diese Datei per Email an **it-sicherheitskatalog@bnetza.de**.

Abkürzungen:

Lfd. Nr.	Laufende Nr. des Kommentars
S.	Seite des Konsultationsentwurfs
GNr.	Gliederungsnummer des Konsultationsentwurfs

Datum	12.02.2014

Name	**Vorname**	**E-Mail**	**Telefon**
Nord	Friedrich	n/a	n/a
Organisation	**Kürzel (Abkürzung für Unternehmen / Organisation)**	**Straße**	**Ort**
Chaos Computer Club e.V.	CCC	n/a	n/a

Lfd. Nr.	**S.**	**GNr.**	**Kommentar (ggfs. mit Angabe, ob nur auf den Elektrizitäts- oder Gasbereich bezogen)**	**Kürzel[1]**
0	4	A.	Die BNetzA stellt die Bedeutung des Stromnetzes als kritische Infrastruktur in den Vordergrund. Der Schutzbedarf für die ITK-Systeme wurde von der BNetzA als sehr hoch eingeschätzt. Kernforderung des einzuführenden Sicherheitskatalogs ist jedoch lediglich die Einführung eines Informationssicherheits-Managementsystems. Im Hinblick auf die konkret vorgeschlagene Umsetzung halten wir diese Maßnahme jedoch für nicht ausreichend. Die im Dokument konkret vorgeschlagenen Maßnahmen lassen zu, dass die Sicherheit auf sehr niedrigem Niveau verwaltet wird - ohne jedoch die Sicherheit der ITK-Systeme zu erhöhen. In der Einleitung sollen die Netzbetreiber nicht nur zur Einführung eines ISMS verpflichtet werden, sondern zu einem sicheren und verantwortungsvollen Betrieb ihrer ITK-Systeme. Das ISMS ist nur ein Baustein, um dieses Ziel zu erreichen.	CCC-0

[1] in jeder Zeile ein Kürzel für Ihr Unternehmen eintragen

Lfd. Nr.	S.	GNr.	Kommentar (ggfs. mit Angabe, ob nur auf den Elektrizitäts- oder Gasbereich bezogen)	Kürzel[1]
			Die Risikoabschätzung darf in keinem Fall in den Händen der betroffenen Unternehmen liegen (vgl. Nr. 1). Diese Einschätzung darf nur von unabhängigen Institutionen vorgenommen werden und muss sich am volkswirtschaftlichen Schaden eines Stromausfalles orientieren. Wir fordern daher, in Ergänzung zur o.a. Pflicht zur Einführung eines ISMS, die Einrichtung einer Stelle zur Bewertung und Überwachung der Risiken im Stromnetz. Diese Stelle soll darüber hinaus nicht nur die Schutzbedarfsermittlung innerhalb eines einzelnen Unternehmens, sondern auch für die unternehmensübergreifenden Schnittstellen übernehmen. Weiterhin soll diese Stelle in der Lage sein, die Verwendung von Altsystemen zu untersagen (vgl. Nr. 1).	
1	14	E.4	Die Sicherheitseinschätzung von Maßnahmen darf nicht durch wirtschaftliche Überlegung des Betreibers selbst gelenkt sein. Stattdessen muss sich die Sicherheitseinschätzung an den volkswirtschaftlichen Folgeschäden eines Stromausfalls orientieren. Die grundsätzliche Herangehensweise, die Schutzbedarfsermittlung durch das betroffene Unternehmen selbst vornehmen zu lassen, sehen wir sehr kritisch. Es ist nicht vermeidbar, dass es durch dieses Verfahren zu Interessenskonflikten kommt. Daher fordern wir die Einführung einer unabhängigen Stelle, die einerseits das konkrete ISMS nach ISO 27001 mit den betroffenen Unternehmen umsetzt, andererseits aber auch die dabei eingesetzten Technologien auditiert und anhand hoher Sicherheitsanforderungen zulässt. Die Verwendung von nicht zugelassenen Geräten soll auch entsprechende Haftungsfolgen für die Unternehmen bedeuten. So wird gleichzeitig ein entsprechender Druck auf die Hersteller der Prozesssteuerungssysteme aufgebaut, um entsprechende Sicherheitsmechanismen auch in diese Systeme zu integrieren. Es gibt in den Energieversorgungsnetzen viele Bereiche, in denen der Schutzbedarf nicht von einem einzelnen Betreiber isoliert bewertet werden kann. In unserem Verbundnetz ist eine Vielzahl von Netzbetreibern miteinander verbundenen. Gerade die Schnittstellen der Netzbetreiber haben einen sehr hohen Schutzbedarf, sind allerdings im Konsultationsentwurf nicht berücksichtigt. Gerade hier gibt es aber Kommunikation zur Netzsteuerung, an welche sehr hohe Forderungen in Bezug auf Verfügbarkeit und Vetraulichkeit zu stellen sind (z.B. verpflichtender Einsatz kryptographischer Verfahren).	CCC-1
2	5	B	Hier wird ein angemessener Schutz vermutet, wenn der Netzbetreiber die Forderungen des Sicherheitskatalogs einhält. Leider kann er diese Forderungen durchaus mit komplett veralteten und damit risikobehafteten Infrastrukturen einsetzen. Es wird zwar beschrieben, daß er sich am Stand der Technik orientieren muß. Die Formulierung ist aber insofern ungenau, daß unklar ist, ob er sich am Stand der Technik der von ihm eingesetzten Systeme (diese vielleicht komplett veraltet, s.o.) oder am Stand der Technik der ITK insgesamt und der damit verbundenen Bedrohungslage für seine eingesetzten Systeme orientieren muß. Somit könnte der Betreiber gemäß der derzeitigen Formulierung weiterhin	CCC-2

Lfd. Nr.	S.	GNr.	Kommentar (ggfs. mit Angabe, ob nur auf den Elektrizitäts- oder Gasbereich bezogen)	Kürzel[1]
			veraltete riskobehaftete und anfällige Technik einsetzen und eine Nachrüstung umgehen, da der (veraltete) Stand der Technik dies nicht zulasse. Das ist unzureichend! Betreiber müssen sich am jeweils aktuellen Stand der Technik orientieren und damit zu einem ggfs. notwendigen Austausch veralteter Technik verpflichtet sein.	
3	6	C	Für die Angemessenheit von Maßnahmen werden hier auch wirtschaftliche Gesichtspunkte mit in die Überlegung einbezogen. Das sehen wir insofern kritisch, als dass unklar ist, wer über die wirtschaftliche Tragbarkeit entscheidet. Bei einer Entscheidung durch das betroffene Unternehmen selbst sehen wir die Möglichkeit von Interessenskonflikten im Hinblick auf die Kosten von Sicherheitsmaßnahmen. Die Entscheidung muss daher durch eine externe Stelle und nicht von den betroffenen Unternehmen selbst getroffen werden. Auch darf nicht nur wirtschaftliche Bedeutung für das individuellen Unternehmens die Entscheidung beeinflussen, sondern ein es muss der gesamte volkswirtschaftliche Schaden bei einem eintretenden Ausfall berücksichtigt werden.	CCC-3
4	18	F.VI	Die in diesem Abschnitt referenzierten Abschnitte 10.11 und 11.3.1 erlauben es Unternehmen, unsichere Altsysteme u.a. ohne angemessenen Passwortschutz einzusetzen. Dies ist selbst innerhalb geschlossener Anlagen abzulehnen. Der physische Zugriffsschutz darf nicht die einzige Hürde für die Bedienung solcher Anlagen sein. Stattdessen muss diese dem allgemeinen Sicherheitsstandards nicht mehr entsprechende Technik ersetzt werden. Nach einer Übergangsfrist soll eine Verwendung dieser Altsysteme nicht mehr zulässig sein. Ebenso muss jegliche Kommunikation - unabhängig davon, ob sie auf einem Betriebsgelände oder außerhalb stattfindet - verschlüsselt sein. Die dazu eingesetzten Verschlüsselungsverfahren müssen sich jederzeit austauschen lassen, damit eventuell in Zukunft bekanntgewordenen Schwächen in den Verfahren durch den Umstieg auf neue Verfahren behoben werden können.	CCC-4
5	18	F.V	Die hier referenzierte SPEC 27009 Abschn. 9.2.3 "Sicherheit der Verkabelung" spricht nur von physischer Sicherheit der Kommunikationsverbindungen. Wie schon unter Nr. 4 erläutert müssen alle Kommunikationsvorgänge grundsätzlich verschlüsselt werden. Die alleinige physische Sicherung von Kabeln etc. ist nicht ausreichend, um eine sichere Kommunikation herzustellen.	CCC-5
6	8	D.	Die in diesem Abschnitt getroffene Unterscheidung zwischen direkter und indirekter Beeinflussung des Netzbetriebs halten wir für nicht ausreichend, um das geforderte hohe Sicherheitsniveau zu erreichen. Sobald eine Kommunikation über Zustandsdaten des Stromnetzes stattfindet ist es möglich, durch die Einbringung von falschen Messdaten Einfluss auf die Netzsteuerung zu nehmen. Dabei ist ein einzelner, isolierter und gefälschter Messwert nicht maßgeblich. Vielmehr kann ein Angriff auf die Netzsteuerung durch die gezielte Einspeisung von Falschinformation für eine große Menge von z.B. Smart Metern erfolgen. Dementsprechend müssen auch alle Systeme, die nur mittelbar einen Einfluss auf die Netzsteuerung nehmen können, in das Sicherheitskonzept mit einbezogen werden.	CCC-6

Lfd. Nr.	S.	GNr.	Kommentar (ggfs. mit Angabe, ob nur auf den Elektrizitäts- oder Gasbereich bezogen)	Kürzel[1]
7	9	D.	Im letzten Abschnitt wird der Netzbetreiber verpflichtet, bei der Erbringung von Leistungen durch Dritte, diese vertraglich zur Einhaltung der im Sicherheitskatalog genannten Forderungen zu verpflichten. Die Einhaltung der durch die unabhängige Stelle (vgl. Nr. 1) genehmigten vertraglichen Rechten und Pflichten für die Zusammenarbeit muss ebenfalls durch diese Stelle überprüft werden.	CCC-7
8	15	F.V	Der Sicherheitskatalog sieht einen IT-Sicherheitsbeauftragten als Ansprechpartner für die BNetzA vor. Dieser soll der BNetzA auf Anfrage Auskunft über Sicherheitsvorfälle geben. Wir halten diese Herangehensweise für nicht geeignet, eine breite Diskussion über die notwendigen Sicherheitsmaßnahmen zu fördern. Grundlage für jede konstruktive Auseinandersetzung ist ein öffentliches, für jeden einsehbares Verzeichnis der Sicherheitsvorfälle. Daher müssen alle Vorfälle der BNetzA gemeldet werden, die dann ihrerseits die Vorfälle der Öffentlichkeit zur Verfügung stellt. Die Teilnahme an Kommunikationsstrukturen für Lageberichte und Warnmeldungen im Bereich kritischer Infrastrukturen (z.B. UPKRITIS) darf nicht optional ("soll"), sondern muss verpflichtend sein.	CCC-8