Energie-Control Austria
Rudolfsplatz 13a
A-1010 Wien

Per E-Mail: IMA-VO@e-control.at

Betreff: **IMA-VO Begutachtung** Wien, am 12.8.2011

Sehr geehrte Damen und Herren,

„Cyber Security Austria (kurz CSA) - Verein zur Förderung der IT Sicherheit Österreichs strategischer Infrastruktur“ ist eine gemeinnützige, unabhängige, überparteiliche Organisation auf Vereinsbasis, mit dem Ziel:

> Erfassen, Vernetzen, Vermitteln und Publizieren der vorhandenen Kompetenzen von unterschiedlichen Informationssicherheitsbereichen, sowie die Förderung des Sicherheitsbewusstseins in Österreich.

Diese Stellungnahme wird elektronisch an IMA-VO@e-control.at übermittelt.

Zum Entwurf „**Verordnung der Energie-Control Austria, mit der die Anforderungen an intelligente Messgeräte bestimmt werden - Intelligente Messgeräte-AnforderungsVO 2011 (IMA-VO 2011)“** nehmen wir im Anhang Stellung.

Mit freundlichen Grüßen

Paul Karrer
Obmann/Sprecher

CYBER SECURITY AUSTRIA
Verein zur Förderung der IT Sicherheit Österreichs strategischer Infrastruktur

Porzellangasse 36, 1090 Wien

office@cybersecurityaustria.at

Stellungnahme:

Zu „Vorblatt“

Auswirkungen in konsumentenschutzpolitischer sowie sozialer Hinsicht:

„Gemäß einer von der E-Control in Auftrag gegebenen Studie von PricewaterhouseCoopers Österreich vom Juni 2010 übersteigt der Gesamtnutzen bei jedem untersuchten Szenario die Kosten, weshalb eine Einführung aus volkswirtschaftlicher Sicht positiv ist. Endkunden haben dadurch die Möglichkeit, ihren Energieverbrauch regelmäßig und vor allem zeitnah zu kontrollieren, wobei auch der Stromverbrauch generell reduziert werden kann.“

Feststellung: CSA zweifelt diese Aussage an. In der Studie von PricewaterhouseCoopers wurden lediglich die volkswirtschaftlichen Auswirkungen betrachtet und bewertet ohne jegliche Bedrohungsszenarien bzw. Angriffsvektoren zu berücksichtigen. Ohne einen entsprechenden Bedrohungskatalog kann nach Auffassung von CSA keine seriöse Bewertung möglicher Auswirkungen erfolgen. Ganz im Gegenteil, in der derzeitigen Form wird mit der Einführung von intelligenten Stromzählern neues, erhebliches Risiko im Bereich der Informationssicherheit mit Auswirkungen auf die strategische Infrastruktur geschaffen und somit auch der Staat Österreich, seine Bürger und die Volkswirtschaft überproportional gefährdet.

Anmerkung: CSA verweist hierbei auf die beiden Publikationen verfügbar unter http://www.cybersecurityaustria.at

Smart Metering Executive Summary

Smart Metering - Auswirkungen auf die nationale Sicherheit

Empfehlung: CSA empfiehlt noch vor Erlass dieser Verordnung einen entsprechenden Bedrohungskatalog zu erstellen, die dabei identifizierten Risiken gemeinsam mit den Stromversorgungsunternehmen Österreichs zu bewerten und die Ergebnisse dieser Risikoanalyse in eine überarbeitete Verordnung einfließen zu lassen.

CSA ist gerne bereit das im Verein vorhandene Expertenwissen einzubringen.

Zu „Allgemeiner Teil“

„Gemäß der Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG, ABl. 2009, L 211 vom 14.8.2009, S. 55 haben die Mitgliedstaaten zu gewährleisten, dass intelligente Messsysteme eingeführt werden, durch die die aktive Beteiligung der Verbraucher am Stromversorgungsmarkt unterstützt wird.“

Feststellung: Laut RICHTLINIE 2009/72/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG, siehe Seite L211/91

> *„Entsprechende Bewertungen finden bis 3. September 2012 statt.*
> *Anhand dieser Bewertung erstellen die Mitgliedstaaten oder eine von ihnen benannte zuständige Behörde einen Zeitplan mit einem Planungsziel von 10 Jahren für die Einführung der intelligenten Messsysteme.*
> *Wird die Einführung intelligenter Zähler positiv bewertet, so werden mindestens 80 % der Verbraucher bis 2020 mit intelligenten Messsystemen ausgestattet.“*

ist eine Einführung an eine **positive Bewertung** geknüpft.

Anmerkung: CSA zweifelt die bisherige positive Bewertung an, insbesondere aufgrund der Erläuterungen zum „Vorblatt“ (siehe oben). Die Berücksichtigung möglicher Gefahren im Bereich der Informationssicherheit ergibt nach Ansicht von CSA eine maßgebliche Veränderung der bisherigen Bewertung.

Darüber hinaus stellt CSA die angenommene Lebensdauer der Smart Meter mit 15 Jahren stark in Frage. Einerseits gibt es Herstelleraussagen, die von der halben Lebensdauer sprechen und auf der anderen Seite muss mit hoher Wahrscheinlichkeit davon ausgegangen werden, dass Schwachstellen entdeckt werden, die durch kostenintensive Maßnahmen behoben werden müssen. Zusätzlich liegen Erkenntnisse vor, dass die derzeitigen Geräte aufgrund des hohen Kostendrucks nur minimale Reserven für Software-Updates aufweisen, was im schlimmsten Fall einen Hardware-Tausch erfordern würde.

Informationen des deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) zufolge, soll in Deutschland die Eichung nur 8 Jahre lang gültig sein!

In diesem Zusammenhang stellen sich CSA die folgenden Fragen:

Welche Dauer der Gültigkeit der Eichung ist für Österreich geplant?

Wodurch und wie soll diese Dauer spezifiziert werden?

Empfehlung: Die Bedrohungen der nationalen Sicherheit aufgrund der Informatisierung zukünftiger intelligenter Messgeräte müssen bei der Bewertung berücksichtigt werden und Einfluss auf das Ergebnis haben.

Zu §1. (Regelungsgegenstand)

Kein Kommentar

Zu §2 (Anwendungsbereich)

Feststellung: Der Begriff des „Lastprofilzählers“ ist in dieser Verordnung nicht definiert und es gibt auch keinerlei Referenz auf sonstige Definitionen.

Anmerkung: Für CSA sind die Kriterien nicht definiert, warum einem Endverbraucher-Haushalt ein „Smart Meter“ und kein „Lastprofilzähler“ installiert wird.

Empfehlung: CSA empfiehlt die Ergänzung der Begriffsbestimmung und die Aufnahme entsprechender Erläuterungen in die Verordnung.

Zu §3 (Anforderungen an intelligente Messgeräte)

§ 3 Abs. 1:

„Die intelligenten Messgeräte haben über eine bidirektionale Kommunikationsanbindung zu verfügen.“

Feststellung: In dieser Anforderung an die Kommunikationsanbindung sind keinerlei Sicherheitsfunktionen festgelegt. Aufgrund der Kritikalität von intelligenten Messgeräten und der übertragenen Informationen ist dies jedoch eine Notwendigkeit.

Anmerkung: Beim bidirektionalen Informationsaustausch ist es aus Sicherheitsgründen notwendig, dass sich beide Kommunikationspartner gegenseitig ausweisen und die Authentizität verifizieren. Aufgrund der unterschiedlichen Kommunikationswege und der sensiblen übertragenen Informationen ist die Verschlüsselung der Übertragung ebenfalls notwendig.

Empfehlung: CSA empfiehlt den folgenden Text:

*„Die intelligenten Messgeräte haben über eine **verschlüsselte und authentisierte** bidirektionale* Kommunikationsanbindung zu verfügen.“

Des Weiteren erscheint CSA die folgende Erläuterung (und Aufnahme in die Verordnung) als notwendig:

„Dabei ist als Kommunikationsanbindung sowohl die Verbindung des intelligenten Messgeräts zum Konzentrator als auch vom Konzentrator zu weiteren Komponenten des Netzbetreibers zu verstehen.“

§ 3 Abs. 2:

„Die intelligenten Messgeräte sind dahingehend auszustatten, dass eine Messung und Speicherung von Zählerständen oder Leistungsmittelwerten in einem Intervall von 15 Minuten möglich ist. Weiters sind die Geräte so auszustatten, dass sie die Speicherung des zum erfassten Zählerstands oder Leistungsmittelwerts gehörenden Zeitstempels und des entsprechenden Datums ermöglichen.“

Feststellung: Ein „einfacher“ Zeitstempel ist nicht ausreichend, da die Uhren der intelligenten Messgeräte untereinander aber auch in Relation zum Konzentrator oder sonstigen Komponenten auseinanderlaufen können und somit einerseits die Echtheit einzelner Messwerte in Frage gestellt werden kann, aber auch Probleme bei der Betriebsführung (Software-Update durch den Stromnetz-Betreiber) auftreten können.

Empfehlung: *CSA empfiehlt den folgenden Text:*

*„Die intelligenten Messgeräte sind dahingehend auszustatten, dass eine Messung und Speicherung von Zählerständen oder Leistungsmittelwerten in einem Intervall von 15 Minuten möglich ist. Weiters sind die Geräte so auszustatten, dass sie die Speicherung des zum erfassten Zählerstands oder Leistungsmittelwerts gehörenden **qualifizierten** Zeitstempels und des entsprechenden Datums ermöglichen.“*

Erläuterung: „qualifiziert“ bezieht sich auf die entsprechende Definition im Signaturgesetz, § 2 Z 12.

§ 3 Abs. 3:

Kein Kommentar

§ 3 Abs. 5:

„Die intelligenten Messgeräte haben die Möglichkeit zu bieten, über eine Kommunikationsschnittstelle mit jedenfalls vier externen Mengenmessgeräten die Kommunikation in beide Richtungen aufzubauen und die Datenübertragungen für diese externen Geräte zu gewährleisten. Davon sind zwei ***Kommunikations-schnittstellen*** *für batteriebetriebene Geräte vorzusehen, um die längstmögliche Batterielebensdauer zu garantieren. Der Zugriff sowie die Spezifikationen dieser Schnittstelle sind bei gemeinsamer Nutzung mit anderen Sparten mit allen Berechtigten ab Einbau zu harmonisieren und diskriminierungsfrei zur Verfügung zu stellen."*

Feststellung: Dieser Absatz ist für CSA unverständlich formuliert. CSA versteht diesen Absatz folgendermaßen: Ein intelligentes Messgerät muss über **EINE** Kommunikationsschnittstelle verfügen an welche maximal VIER externe Mengenmessgeräte angeschlossen werden können. Davon können ZWEI Mengenmessgeräte batteriebetrieben werden. Für CSA stellt sich die Frage nach der Anzahl der benötigten Kommunikationsschnittstellen. Wie viele physische Kommunikationsschnittstellen benötigt ein intelligentes Messgerät? Handelt es sich nicht um EINE physische Schnittstelle an der zwei von vier Geräten über die Leitung mit Strom versorgt werden können.

Anmerkung: CSA empfiehlt die Reduzierung von physischen Schnittstellen auf ein Minimum und eine exakte Spezifizierung dieser.

Hinsichtlich der Verwendung von drahtlosen Schnittstellen (z.B.: Wireless LAN, Mobiltelefonie) verweist CSA auf die Grenzwerte bei drahtloser Kommunikation in Haushalten.

Empfehlung: CSA empfiehlt die folgende Änderung.

„Die intelligenten Messgeräte haben die Möglichkeit zu bieten, über eine Kommunikationsschnittstelle mit jedenfalls vier externen Mengenmessgeräten die Kommunikation in beide Richtungen aufzubauen und die Datenübertragungen für diese externen Geräte zu gewährleisten. ~~*Davon sind zwei Kommunikations-schnittstellen für*~~ ***An dieser Kommunikationsschnittstelle müssen mindestens zwei batteriebetriebene Geräte betrieben werden können*** ~~*vorzusehen*~~*, um* ~~*die*~~ ***eine*** *längstmögliche Batterielebensdauer zu garantieren. Der Zugriff sowie die Spezifikationen dieser Schnittstelle sind bei gemeinsamer Nutzung mit anderen Sparten mit allen Berechtigten ab Einbau zu harmonisieren und diskriminierungsfrei zur Verfügung zu stellen."*

§ 3 Abs. 7:

„Die intelligenten Messgeräte sowie ihre Kommunikation, auch zu externen Geräten gemäß Z 5 und 6, sind nach anerkanntem Stand der Technik abzusichern und zu verschlüsseln, um Unberechtigten den Zugriff nicht zu ermöglichen."

Feststellung 1: CSA findet die Verwendung des Begriffs „ *anerkanntem Stand der Technik"* problematisch. Es stellt sich auch die Frage nach dem Zeitpunkt des Stands der Technik. Gilt der Stand der Technik zum Zeitpunkt der Installation des intelligenten Messgeräts oder auch später während der Lebenszeit des Messgeräts? Insbesondere in der Informationstechnik ist der Stand der Technik sehr dynamisch und einem konstanten Wandel unterzogen.

Empfehlung 1: CSA empfiehlt auf die Verwendung des Begriffs „anerkannter Stand der Technik" zu verzichten.

Feststellung 2: Der Aufbau des Satzes ist missverständlich. Sollen auch die Messgeräte verschlüsselt werden? Vergleiche nachfolgenden Text ohne den Verweis auf die externen Geräte!

Die intelligenten ***Messgeräte*** *sowie ihre Kommunikation sind nach anerkanntem Stand der Technik* ***abzusichern*** *und zu* ***verschlüsseln****, um Unberechtigten den Zugriff nicht zu ermöglichen."*

Anmerkung: CSA empfiehlt außerdem die Kommunikation zu authentisieren und hierzu einen individuellen Schlüssel pro Netzkunden einzusetzen. Der kundenbezogene Schlüssel kann zum Beispiel mittels Bürgerkarte generiert werden.

Empfehlung 2: CSA empfiehlt die folgende Änderung (ohne Berücksichtigung der Empfehlung 1):

„Die intelligenten Messgeräte sind nach dem Stand der Technik abzusichern, um auch im stromlosen Zustand den Zugriff durch Unberechtigte zu verhindern.

Die Kommunikation, auch zu externen Geräten gemäß Z 5 und 6, ist nach dem Stand der Technik mit einem individuellen kundenbezogenen Schlüssel zu authentisieren und zu verschlüsseln."

§ 3 Abs. 8:

„Die intelligenten Messgeräte sind dahingehend auszustatten, dass die Möglichkeit besteht, die Anlage des Netzkunden von der Ferne abzusperren oder für eine Wiedereinschaltung durch den Kunden freizugeben sowie deren maximalen Bezug an elektrischer Leistung zu begrenzen.“

Feststellung: CSA sieht in der Möglichkeit einer Fernabschaltung ein erhebliches Risiko für die strategische Bedeutung der Stromversorgung als Querschnittsinfrastruktur für den Staat Österreich und seine Bürger. Gerade die Beispiele der letzten Zeit (vgl. Stuxnet, GIS) verdeutlichen diese Problematik und zeigen die generelle Verwundbarkeit von Informationssystemen auf.

Die Übernahme unzähliger intelligenter Messgeräte im Falle einer gefundenen Verwundbarkeit eröffnet den Angreifern die Möglichkeit ungewollte Stromschwankungen zu erzeugen und somit das gesamte Stromnetz und die Versorgung zu gefährden.

Durch die Möglichkeit der Fernabschaltung liefert sich Österreich der Gefahr möglicher Erpressungsversuche durch Cyber-Kriminelle oder Angriff durch Hacker aus!

Empfehlung: CSA empfiehlt folgenden Text:

„Die intelligenten Messgeräte können dahingehend ausgestattet sein, dass die Möglichkeit besteht, die Anlage des Netzkunden von der Ferne für eine Wiedereinschaltung durch den Kunden freizugeben sowie deren maximalen Bezug an elektrischer Leistung zu begrenzen. ***Eine Fernabschaltung darf technisch nicht möglich sein.****“*

Anmerkung*: Lässt sich eine Fernabschaltung technisch nicht verhindern, so ist durch den Stromnetzanbieter ein entsprechendes Sicherheitskonzept zu entwickeln. Ein entsprechender Absatz ist in die Verordnung einzufügen.*

§ 3 Abs. 9:

„Die intelligenten Messgeräte sind mit einer internen Uhr sowie einer Kalenderfunktion auszustatten.“

Anmerkung*: Siehe § 3 Abs. 2. qualifizierte Zeit und Datum.*

Empfehlung: CSA empfiehlt folgenden Text:

Die intelligenten Messgeräte sind mit einer internen Uhr sowie einer Kalenderfunktion auszustatten, ***die eine qualifizierte Zeit und Datum liefern****.“*

§ 3 Abs. 12

„Die intelligenten Messgeräte haben den maß- und eichgesetzlichen und datenschutzrechlichen Bestimmungen sowie dem anerkannten Stand der Technik zu entsprechen.

Anmerkung: Vergleich Erläuterungen zum Stand der Technik unter *§ 3 Abs. 7.*

Feststellung: Diese Verordnung enthält keinerlei Anforderungen und/oder Verweise auf solche. In den Erläuterungen zur Verordnung wird das Ergebnis des Mandates M/441 der EU an die CEN/CENELC/ETSI verwiesen. Das Ergebnis dieses Mandats enthält jedoch noch keinerlei verbindliche technische Standards für intelligente Messgeräte sondern definiert nur weitere Schritte und Projekte.

Die EU-Richtlinie 2004/22 enthält alle Anforderungen an die maß- und eichgesetzlichen Eigenschaften der intelligenten Messgeräte.

Das deutsche BSI erstellt gegenwärtig (Fertigstellung bis Herbst 2011) ein „Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen“. In Deutschland müssen alle zukünftigen intelligenten Messsysteme gemäß diesem Schutzprofils durch das BSI zertifiziert werden, bevor diese ab voraussichtlich 2013 ausgerollt werden

Empfehlung: Die CSA schlägt somit folgenden Text:

„Die intelligenten Messgeräte haben den maß- und eichgesetzlichen und datenschutzrechlichen Bestimmungen sowie ***der EU-Richtlinie 2004/22 und dem BSI Schutzprofil*** **für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen** *zu entsprechen* ***und im Einklang mit den Ergebnissen des Mandats M/441 zu stehen.****“*