Verband Schweizerischer Elektrizitätsunternehmen
Association des entreprises électriques suisses
Associazione delle aziende elettriche svizzere

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit (BACS)
3003 Bern

Elektronisch an: ncsc@ncsc.admin.ch

15. August 2024

Markus Riner, Direktwahl +41 62 825 25 27, markus.riner@strom.ch

Stellungnahme zur Cybersicherheitsverordnung (CSV)

Sehr geehrte Damen und Herren

Der Verband Schweizerischer Elektrizitätsunternehmen (VSE) dankt Ihnen für die Möglichkeit, sich zur Einführung einer Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe zu äussern. Er nimmt diese Gelegenheit gerne wahr.

Der VSE vertritt als Dachverband die Interessen der schweizerischen Elektrizitätswirtschaft entlang der gesamten Wertschöpfungskette von der Produktion über den Handel bis zur Übertragung und Endverteilung von Strom. Eine sichere Stromversorgung ist für eine funktionierende Gesellschaft und Wirtschaft lebensnotwendig. Die Infrastrukturen der Strombranche gehören daher eindeutig mit zu den wichtigsten kritischen Versorgungsinfrastrukturen. Um diese möglichst effektiv vor den zunehmenden Cyberbedrohungen zu schützen, engagiert sich der VSE stark durch die Erarbeitung von Branchendokumenten und unterstützt die Branchenunternehmen in Belangen der Cybersicherheit. Der VSE hat sich ebenfalls aktiv und konstruktiv in die Grundlagenarbeiten für die Gesetzesrevision des Informationssicherheitsgesetzes ISG eingebracht.

Der VSE hält die Meldepflicht für wichtig und unterstützt die Strategie des Bundes im Bereich Cybersicherheit und deren Steuerung durch die Betroffenen Akteure. In diesem Zusammenhang hält der VSE als unabdingbar, dass die Vertreter der kritischen Infrastrukturen eine aktive Rolle im StA NCS (Art. 4 Zusammensetzung des StA NCS) wahrnehmen können.

Betreffend die technische Analyse von Cybervorfällen und Cyberbedrohungen (Art. 7), plädiert der VSE für eine gemeinsame Präzisierung der Leistungen und der Zusammenarbeit zwischen BACS und privaten CERTs, sowie von der Meldepflicht betroffenen Unternehmen der kritischen Infrastrukturen.

Priorisierungskriterien erst in Krisensituationen festzulegen ist schwierig. Solche Kriterien und Rangfolgen sollten Transparent sein. Daher sollten die Kriterien und die Priorisierung der Beratung und Unterstützung bei Cyberangriffen (Art. 8 Abs. 1) in der Verordnung transparent festgelegt werden. Als Basis dafür kann die Liste der kritischen Infrastrukturen des BABS dienen.

Der Art. 19 Abs. 3 bezieht sich auf «betroffene Einheiten der Organisation oder Behörde». Aus diesem Grund sollen «angegriffene Systeme» ebenfalls in der Meldung enthalten sein (Art. 19 Abs.1).

Anträge:

Die kritischen Infrastrukturen sollen auch in StA NCS vertreten werden.

Art. 4 Zusammensetzung des StA NCS
[1] Der StA NCS setzt sich aus Vertreterinnen und Vertretern der Departemente, der Bundeskanzlei, der Kantone, der Wirtschaft, der kritischen Infrastrukturen, der Gesellschaft und der Hochschulen zusammen.
[2] Der Bundesrat bestimmt alle fünf Jahre die Mitglieder des StA NCS, mit Ausnahme der Vertreterinnen und Vertreter der Kantone; diese werden von der Konferenz der Kantonsregierungen bestimmt.
[3] Er ernennt aus dem Kreis der Vertreterinnen und Vertreter der Wirtschaft, der kritischen Infrastrukturen, der Gesellschaft und der Hochschulen die vorsitzende Person.

Die angegriffenen Systeme gehören zur Meldung.

Art. 19 Inhalt der Meldung
[1] Die Meldung muss folgende Informationen zum Cyberangriff enthalten:
a. Datum und Uhrzeit der Feststellung des Angriffs;
b. Datum und Uhrzeit des Angriffs;
c. Art des Angriffs;
d. Angriffsmethode; ~~und~~
e. Sofern bekannt, Angaben zum Verursacher;
f. Angegriffene Systeme~~.~~; und
g. Ergriffene Gegenmassnahmen.

Wir danken Ihnen für die Berücksichtigung unserer Anliegen und unterstützen das BACS gerne bei der weiteren Festlegung des effizienten Zusammenspiels von Akteuren im Ernstfall eines Cyberangriffs.

Für allfällige Rückfragen oder zur Diskussion stehen wir Ihnen gerne zur Verfügung.

Freundliche Grüsse

Michael Frank
Direktor

Thomas Marti
Leiter Netz, Digitalisierung und Sicherheit