Redaktion: Helmut Reimer

Report

Cyber-Sicherheit: Eckpunkte zu möglichen gesetzlichen Regelungen

Die Gewährleistung von Cyber-Sicherheit gehört zu den zentralen Herausforderungen unserer Zeit. Übereinstimmend werden größere IT-Ausfälle als reale Gefahr und globale Bedrohung angesehen.

Bundesinnenminister Dr. Friedrich hat daher die Initiative ergriffen und Eckpunkte zu möglichen gesetzlichen Regelungsinhalten zu Verbesserung der IT-Sicherheit vorgestellt. Die Eckpunkte befinden sich derzeit in der Abstimmung zwischen den Ministerien.

Zentrale Regelungsinhalte zur Verbesserung der IT-Sicherheit

- Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Betreiber kritischer Infrastrukturen: Die Betreiber der wichtigsten kritischen Infrastrukturen sollen IT-Sicherheitsmaßnahmen nach dem Stand der Technik ergreifen und ihre Einhaltung sicherstellen. Branchen können brancheninterne Standards entwickeln, die das Bundesamt für die Sicherheit in der Informationstechnik (BSI) als Konkretisierung der gesetzlichen Verpflichtung anerkennt.
- Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle für Betreiber kritischer Infrastrukturen: Die Betreiber der wichtigsten kritischen Infrastrukturen sollen dem BSI unverzüglich IT-Sicherheitsvorfälle mit Auswirkungen auf die Versorgungssicherheit oder die öffentliche Sicherheit über hierfür etablierte Wege melden. Nur so ist zu gewährleisten, dass das Bundesamt ein valides nationales Lagebild erstellen und die Betreiber bei Bewältigung des Vorfalls unterstützten kann.
- Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Telekommunikationsanbieter: Die Anbieter sollen IT-Sicherheit nach dem Stand der Technik nicht nur wie bisher zum Vertraulichkeitsschutz und zum Schutz personenbezogener Daten, sondern auch zum Schutz vor unerlaubten Eingriffen in die Infrastruktur gewährleisten, um die Widerstandsfähigkeit der Netze insgesamt zu verbessern und damit die Verfügbarkeit zu sichern.
- Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle für Telekommunikationsanbieter: Die Anbieter sollen IT-Sicherheitsvorfälle, die zu einer Störung der Verfügbarkeit oder zu einem unerlaubte Zugriff auf Systeme der Nutzer führen können, unverzüglich melden. Über die bestehende Meldeverpflichtung im Falle der Verletzung des Schutzes personenbezogener Daten hinaus, wird so gewährleistet, dass die für das Rückgrat der Informationsgesellschaft verantwortlichen Anbieter zu einem validen und vollständigen Lagebild beitragen.
- Verpflichtung der Telekommunikationsanbieter zur Information der Nutzer über Schadprogramme und zur Bereitstellung technischer Hilfsmittel für ihre Erkennung und Beseitigung: Die vorgeschriebene Information soll die Nutzer in die Lage versetzen, selbst Maßnahmen gegen Schadsoftware zu ergreifen. Außerdem sollen die Anbieter den Nutzern einfach bedienbare Sicherheitswerkzeuge bereitstellen, die vorbeugend genutzt werden können und auch zur Beseitigung von Störungen, die vom infizierten System des betroffenen Nutzers ausgehen.
- Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Telemediendiensteanbieter: Um Verbreitung von Schadprogrammen über Telemedien zu reduzieren, sollen die Anbieter, die Telemediendienste geschäftsmäßig und gegen Entgelt anbieten, verpflichtet werden, anerkannte Schutzmaßnahmen zur Verbesserung der IT-Sicherheit in einem zumutbaren Umfang umzusetzen.
- Jährliche Berichtspflicht des BSI: Durch den vorgesehenen Jahresbericht und dessen Veröffentlichung soll die weitere Sensibilisierung der Bevölkerung für das Thema „IT-Sicherheit" erreicht werden, welche in Anbetracht der Tatsache, dass eine Vielzahl von erfolgreichen IT-Angriffen bei Einsatz von Standardwerkzeugen zu verhindern gewesen wären, von besonderer Bedeutung ist.
- Aufgabe und Befugnis des BSI zur Untersuchung von Hard- und Softwarekomponenten zur Förderung der IT-Sicherheit des Bundes und der Kritischen Infrastrukturen und Befugnis zur Veröffentlichung der hierbei erzielten Ergebnisse: Um die Aufgabe, die IT-Sicherheit zu fördern, möglichst effizient erfüllen zu können, ist das BSI auf solche Untersuchungserkenntnisse angewiesen. Um bestehende Rechtsunsicherheiten zu beseitigen, wird klargestellt, dass BSI relevante Komponenten am Markt erwerben und untersuchen darf.

ENISA: Bericht über Internet-Sicherheitsmaßnahmen für Smart Grids

Die EU Internet-Sicherheits-Agentur ENISA hat sich mit den Herausforderungen der grundlegenden Absicherung von Smart Grids in Europa befasst. Dieser neue Bericht hilft den Anbietern von Smart Grids dabei, ihre Internetsicherheit und die Stabilität ihrer Infrastrukturen mit einer Reihe von minimalen Sicherheitsmaßnahmen zu verbessern.

Im Gegensatz zum streng regulierten Weg, der von der USA vorgegeben wird, ist es die europäische Herangehensweise, ein bestimmtes Maß an 'Freiheit' zuzulassen, bei dem diese Leitlinien in Anbetracht des breit gefächerten Marktes auf die Bedürfnisse verschiedener Akteure zugeschnitten und kombiniert werden können. Die Agentur schlägt daher eine Skalierbarkeit auf circa 40 Sicherheitsmaßnahmen vor, die in drei Stufen der Differenziertheit und zehn Bereiche eingeteilt sind:

1. Sicherheitssteuerung und Risikomanagement
2. Management dritter Parteien
3. Sicherstellen eines Prozesses im Lebenszyklus der Bestandteile/Systeme und Betriebsprozesse von Smart Grids
4. Sicherheit, Bewusstsein und Training von Personal
5. Reaktion auf Vorfälle und Teilen von Informationen
6. Prüfung und Haftbarkeit
7. Kontinuität von Tätigkeiten