NETZ- UND INFORMATIONSSICHERHEIT

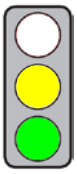
cep**Analyse** Nr. 26/2013

Centrum für Europäische Politik

KERNPUNKTE

Ziel der Richtlinie: Gewährleistung eines Mindeststandards der Netz- und Informationssicherheit in der EU.

Betroffene: Anbieter kritischer Infrastrukturen, Internetfirmen, öffentliche Verwaltung.



Pro: (1) Nationale NIS-Strategien stärken das Risikobewusstsein und die Reaktionsfähigkeit gegenüber Cybergefahren.

(2) Die hoheitliche Vorgabe von Sicherheitsmaßnahmen für Betreiber kritischer Infrastrukturen ist sachgerecht.

Contra: (1) Kleine und mittlere Unternehmen sollten von der Meldepflicht ausgenommen werden.

(2) Es fehlen inhaltliche Mindestkriterien für die Meldungen von Sicherheitsvorfällen.

(3) Die Einrichtung einer zentralen nationalen Behörde für die NIS ist nicht mit dem föderalen Aufbau des deutschen Staates vereinbar.

INHALT

Titel

Vorschlag COM(2013) 48 vom 7. Februar 2013 für eine **Richtlinie** über Maßnahmen zur **Gewährleistung einer hohen** gemeinsamen **Netz- und Informationssicherheit** in der Union

Kurzdarstellung

- **Hintergrund und Ziele**
  - Ziel der Richtlinie ist es, EU-weit eine hohe Netz- und Informationssicherheit (NIS) zu gewährleisten. Insbesondere soll sie verhindern:
    - Netzausfälle und
    - Einbrüche in die Informationstechnologie.
  - Die Richtlinie zwingt Mitgliedstaaten dazu (Art. 1 Abs. 1, Art. 2, Art. 4),
    - nationale Strategien für die Netz- und Informationssicherheit (NIS) auszuarbeiten,
    - mit der EU-Kommission bei der Erkennung von und Reaktion auf „Sicherheitsvorfälle" zusammenzuarbeiten,
    - „Marktteilnehmern" und öffentlichen Verwaltungen technische Anforderungen und Meldepflichten aufzuerlegen.
  - Die Mitgliedstaaten dürfen höhere Sicherheitsanforderungen festlegen (Mindestharmonisierung) (Art. 2).
- **Geltungsbereich**
  - Die Richtlinie gilt für „Netze und Informationssysteme" der Informationstechnologie (IT). Dies sind (Art. 3 Abs. 1)
    - elektronische Kommunikationsnetze – z.B. Telekommunikations-, Mobilfunk und Hörfunknetze,
    - Geräte zur Verarbeitung von Computerdaten – z.B. Computer, Mobiltelefone – und
    - Computerdaten, die gespeichert, verarbeitet, abgerufen oder übertragen werden.
  - Die Richtlinie gilt für „Marktteilnehmer" und öffentliche Verwaltungen.
    - Marktteilnehmer sind (Art. 3 Ziffer 8)
      - Anbieter von „Diensten der Informationsgesellschaft" – z.B. von Suchmaschinen und sozialen Netzen – und
      - Betreiber „kritischer Infrastrukturen", die für die Aufrechterhaltung zentraler wirtschaftlicher Tätigkeiten „unerlässlich" sind – z.B. Banken, Energieversorger, Krankenhäuser, Börsen, Transportunternehmen.
    - Weil sie bereits von anderen Vorschriften erfasst sind, gelten nicht als Marktteilnehmer (Art. 1 Abs. 3):
      - Betreiber öffentlicher Kommunikationsnetze, etwa Mobilfunknetze,
      - Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, etwa Telefondienste,
      - Anbieter von „Vertrauensdiensten", etwa elektronischer Siegel.
- **Zentrale nationale Behörde, nationale NIS-Strategie, Notfallteam**
  - Jeder Mitgliedstaat muss eine zentrale Behörde benennen, die die Anwendung dieser Richtlinie auf nationaler Ebene überwacht (Art. 6 Abs. 1 und Abs. 2).
  - Jeder Mitgliedstaat muss eine nationale NIS-Strategie ausarbeiten und beschließen.
  - Diese Strategie muss u.a. folgende Aspekte umfassen (Art. 5 Abs. 1 und 2):
    - die Definition von Zielen und Prioritäten auf Basis einer aktuellen Analyse der Sicherheitsrisiken und -vorfälle,
    - einen „Steuerungsrahmen" zur Erreichung der Ziele,
    - allgemeine Maßnahmen zur „Abwehrbereitschaft, Reaktion und Wiederherstellung",
    - einen nationalen NIS-Kooperationsplan, der u.a. Kommunikationsabläufe zur Gewährleistung der „Prävention, Erkennung, Reaktion, Reparatur und Wiederherstellung" festlegt.

Autoren: Ariane Kiesow und Philipp Eckhardt | kiesow@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Telefon 0761 38693-246 | www.cep.eu

- Jeder Mitgliedstaat muss ein IT-Notfallteam („Computer Emergency Response Team", CERT) einrichten. Das CERT steht unter Aufsicht der zuständigen nationalen Behörde und „kann" bei dieser angesiedelt sein (Art. 7 Abs. 1 und 5).
- Das CERT übernimmt u.a. folgende Aufgaben (Art. 7 Abs. 1 i.V.m. Anhang 1):
  - Überwachung und Analyse von sowie Reaktion auf Sicherheitsrisiken und -vorfälle,
  - Herausgabe von Frühwarnungen und Verbreitung von Informationen über Sicherheitsvorfälle an potenziell Betroffene und Beteiligte, etwa Unternehmen und Privatpersonen.
- Das CERT muss über eine „sichere, robuste" Kommunikations- und Informationsinfrastruktur verfügen (Art. 7 Abs. 3).

- **Kooperation zwischen Mitgliedstaaten und EU-Kommission**
  - Die nationalen Behörden und die Kommission arbeiten über ein „Kooperationsnetz" zusammen (Art. 8 Abs. 1).
  - Die nationalen Behörden und die Kommission geben Frühwarnungen zu Sicherheitsrisiken und -vorfällen heraus, sofern diese (Art. 8 Abs. 3 lit. a, Art. 10)
    - sich „rasch" ausbreiten (könnten),
    - die „nationale Reaktionskapazität" übersteigen (könnten),
    - mehrere Mitgliedstaaten betreffen (könnten).
  - Die nationalen Behörden und die Kommission müssen dabei alle für die Beurteilung der Risiken und Vorfälle relevanten Informationen veröffentlichen (Art. 10 Abs. 2). Besteht ein „mutmaßlich" krimineller Hintergrund, muss das Europäische Zentrum zur Bekämpfung der Cyberkriminalität informiert werden (Art. 10 Abs. 4).
  - Liegt eine Frühwarnung vor, sollen sich die Behörden auf eine „koordinierte Reaktion" einigen (Art. 8 Abs. 3 lit. b, Art. 11).
  - Die Kommission regelt die Einzelheiten
    - der Kriterien einer Frühwarnung mit delegierten Rechtsakten (Art. 10 Abs. 1 und 5),
    - der „koordinierten Reaktion" mit Durchführungsrechtsakten (Art. 12 Abs. 2 lit. b).
  - Die Behörden sollen u.a. (Art. 8 Abs. 3 lit. c, g, h)
    - ihre Frühwarnungen und koordinierten Reaktionen „regelmäßig" auf einer Website veröffentlichen,
    - sich gegenseitig beim „Kapazitätsaufbau" der NIS unterstützen,
    - ihre Kapazitäten und Abwehrbereitschaft gegenseitig überprüfen.
  - Jeder Mitgliedstaat und die Kommission können verlangen, dass nationale NIS-Strategien, die NIS-Kooperationspläne und die „Wirksamkeit" der CERTs „gemeinsam erörtert und bewertet" werden (Art. 8 Abs. 3 lit. d und e).
- **Sicherheitsmaßnahmen und Meldepflicht**
  - Die Mitgliedstaaten stellen sicher, dass Marktteilnehmer und öffentlichen Verwaltungen Sicherheitsmaßnahmen ergreifen, die „technisch und organisatorisch geeignet" sind, um Sicherheitsrisiken und -vorfälle zu „managen". Die Maßnahmen müssen unter Berücksichtigung des „Standes der Technik" ein „Maß an Sicherheit" gewährleisten, das dem „bestehenden Risiko angemessen" ist, und die „Kontinuität" der Dienste „gewährleisten" (Art. 14 Abs. 1). Den konkreten Inhalt der Maßnahmen legen die Mitgliedstaaten fest.
  - Die Marktteilnehmer und öffentlichen Verwaltungen müssen Sicherheitsvorfälle, die „erhebliche" Auswirkungen auf die Sicherheit ihrer Kerndienste haben, der zuständigen Behörde melden. Die Kommission legt in delegierten Rechtsakten die für die Meldepflicht geltenden „Formen und Verfahren" fest und „unter welchen Umständen" die Meldepflicht gilt (Art. 14 Abs. 2, 5 und 7).
  - „Kleinstunternehmen" sind von den Sicherheitsanforderungen und Meldepflichten befreit (Art. 14 Abs. 8).
  - Berührt ein Sicherheitsvorfall das öffentliche Interesse, kann die zuständige Behörde (Art. 14 Abs. 4)
    - den Sicherheitsvorfall veröffentlichen oder
    - die öffentliche Verwaltung oder die Marktteilnehmer zur Veröffentlichung verpflichten.
  - Die zuständige Behörde kann
    - Verstöße gegen die Sicherheitsanforderungen und Meldepflichten untersuchen (Art. 15 Abs. 1),
    - von den Marktteilnehmern und den öffentlichen Verwaltungen Informationen über ihre Netz- und Informationssysteme verlangen (Art. 15 Abs. 2 lit. a),
    - bei den Marktteilnehmern und öffentlichen Verwaltungen Sicherheitsüberprüfungen vornehmen (Art. 15 Abs. 2 lit. b),
    - den Marktteilnehmern und öffentlichen Verwaltungen verbindliche Anweisungen erteilen (Art. 15 Abs. 3).
- **Sanktionen**
  Die Mitgliedstaaten müssen „wirksame, angemessene und abschreckende" Sanktionen für Verstöße gegen die Richtlinie festlegen (Art. 17).

Wesentliche Änderungen zum Status quo

- Bisher sind lediglich Unternehmen, die öffentlich zugängliche Kommunikationsnetze und -dienste sowie „Vertrauensdienste" bereitstellen, verpflichtet, Sicherheitsstandards einzuhalten und Sicherheitsvorfälle zu melden (Richtlinie 2002/21/EG).

Subsidiaritätsbegründung der Kommission

Ein EU-weit einheitlicher Mindestschutz der NIS ist laut Kommission erforderlich, um eine ausreichende Abwehrbereitschaft zu erzielen und eine vertrauensvolle Zusammenarbeit zu ermöglichen. Angesichts des grenzübergreifenden Charakters von Sicherheitsrisiken und -vorfällen kann der Mindestschutz besser auf EU-Ebene als durch die Mitgliedstaaten erreicht werden.

Politischer Kontext

2009 schlug die Kommission in der Mitteilung über den Schutz kritischer Infrastrukturen [KOM (2009) 149] für diese höhere Sicherheitsstandards vor. Die „Digitale Agenda für Europa" [KOM(2010) 245] von 2010 (s. cep**Analyse**) enthält Vorschläge, die die Sicherheit des digitalen Binnenmarktes verbessern sollen. 2011 stellte die Kommission in der Mitteilung „Ergebnisse und nächste Schritte: der Weg zur globalen Netzsicherheit" [KOM(2011) 163] fest, dass ein nationales Vorgehen zur Bewältigung der Sicherheitsprobleme nicht ausreiche und eine engere zwischenstaatliche Kooperation notwendig sei. Der vorliegende Vorschlag ist die wichtigste Maßnahme der „Cybersicherheitsstrategie", die im Februar 2013 veröffentlicht wurde [JOIN(2013) 1]. Parallel soll das Mandat der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) verlängert und deren Zuständigkeiten erweitert werden [KOM(2010) 521]. Zukünftig kann die ENISA die Kooperation der Mitgliedstaaten untereinander und mit der Kommission stärker koordinieren und unterstützen. Des Weiteren wird sie zukünftig stärker an der Arbeit der CERTs beteiligt und steht fortan in engerer Verbindung mit den nationalen Datenschutzbehörden und Europol.

Stand der Gesetzgebung

07.02.13	Annahme durch Kommission
Offen	Annahme durch Europäisches Parlament und Rat, Veröffentlichung im Amtsblatt, Inkrafttreten

Politische Einflussmöglichkeiten

Generaldirektionen:	GD Connect
Federführender Ausschuss des EP:	Binnenmarkt und Verbraucherschutz (federführend); Berichterstatter Andreas Schwab (EVP-Fraktion, DE)
Federführendes Bundesministerium:	Bundesinnenministerium
Federführender Ausschuss des BT:	Innenausschuss
Entscheidungsmodus im Rat:	Qualifizierte Mehrheit (Annahme durch Mehrheit der Mitgliedstaaten und mit 255 von 345 Stimmen; Deutschland: 29 Stimmen)

Formalien

Kompetenznorm:	Art. 114 AEUV (Binnenmarkt)
Art der Gesetzgebungszuständigkeit:	Geteilte Zuständigkeit (Art. 4 Abs. 2 AEUV)
Verfahrensart:	Art. 294 AEUV (ordentliches Gesetzgebungsverfahren)

BEWERTUNG

Ökonomische Folgenabschätzung

Moderne Volkswirtschaften sind von funktionierenden Netzen und Systemen der Informationstechnologie (IT) abhängig. Gelingt es Angreifern, die IT-Netze oder -Informationssysteme insbesondere von Betreibern „kritischer Infrastrukturen" wie Strom-, Gas- oder Wasserversorgern zu kompromittieren, kann ein immenser volkswirtschaftlicher Schaden entstehen. **Die Pflicht der Mitgliedstaaten zur Ausarbeitung nationaler NIS-Strategien stärkt deren Risikobewusstsein und Reaktionsfähigkeit gegenüber Cybergefahren** und ist daher sachgerecht. Allerdings bleiben die Vorgaben der Richtlinie recht abstrakt, so dass abzuwarten ist, wie detailliert die nationalen NIS-Strategien tatsächlich ausfallen.

Die hoheitliche Vorgabe von Sicherheitsmaßnahmen greift erheblich in die unternehmerische Freiheit ein und kann mit erheblichen Kosten verbunden sein. **Sie ist im vorliegenden Fall jedoch berechtigt**. Zwar haben die der Richtlinie unterliegenden Unternehmen („Marktteilnehmer") ein Eigeninteresse daran, mit Investitionen in die IT-Sicherheit ihre Netze und Informationssysteme gegen Ausfälle zu schützen, da solche Ereignisse mit Einnahme- oder Reputationsverlusten verbunden sind. Anders als Ausfälle sind Einbrüche in Netze und Informationssysteme für die Öffentlichkeit jedoch nicht oder nicht sofort erkennbar. Kunden können somit zwar einen Missbrauch – etwa die unerlaubte Nutzung persönlicher Daten für kriminelle Handlungen – im Nachhinein feststellen, die Quelle – etwa die gehackte Website – können sie aber kaum identifizieren. Direkte Folge dieser Informationsasymmetrie ist, dass die Unternehmen nicht damit rechnen müssen, für Schäden zu haften, die aufgrund einer mangelhaften IT-Sicherheit verursacht wurden. Das Ergebnis sind unzureichende Investitionen in die IT-Sicherheit. Da das Haftungsprinzip aufgrund dieser fehlenden direkten Zurechenbarkeit des Schadens nicht ausreichend funktioniert, ist die hoheitliche Vorgabe von Sicherheitsmaßnahmen für die Unternehmen vertretbar.

Für die Betreiber „kritischer Infrastrukturen" sollten diese Anforderungen zu den Zulassungsvoraussetzungen gehören, wenn die Betreiber keine angemessene Versicherung vorweisen können: Ausfälle sind hier zwar direkt beobachtbar und zurechenbar, ihre Folgeschäden sind aber in der Regel so hoch, dass eine Entschädigung – etwa für einen mehrtägigen Stromausfall in einer Großstadt – die finanzielle Kapazität des Betreibers übersteigen kann.

Es wäre sinnvoll, die Sicherheitsmaßnahmen EU-weit einheitlich festzulegen, statt sie den Mitgliedstaaten zu überlassen. Sonst drohen Wettbewerbsverzerrungen, etwa weil Unternehmen über den Online-Versandhandel im Wettbewerb mit Unternehmen in anderen Mitgliedstaaten stehen oder weil die Folgen von Sicherheitsvorfällen – etwa bei Finanzinstituten – nicht auf einzelne Mitgliedstaaten begrenzt sind. Auch bilden unterschiedliche nationale Sicherheitsniveaus keinen Standortvorteil: Die technischen Details der Sicherheitsmaßnahmen sind für den Laien nicht verständlich.

Eine große Anzahl an Meldungen von Sicherheitsvorfällen führt dazu, dass Sicherheitslücken – etwa bei Softwareherstellern – rasch und zuverlässig identifiziert werden können. Da davon alle Marktteilnehmer und öffentliche Verwaltungen profitieren, weisen Meldungen Eigenschaften eines öffentlichen Gutes auf. Gleichzeitig hat jedes Unternehmen einen rationalen Anreiz, Vorfälle selbst nicht zu melden, etwa um Rufschädigung zu vermeiden oder um Meldekosten zu sparen**. Eine Meldepflicht über Sicherheitsvorfälle ist** daher **sachgerecht.** Die Kommission sollte jedoch nicht nur die „Formen und Verfahren" und die „Umstände" der Meldung, sondern auch Mindestkriterien für den Inhalt der Meldung vorgeben. Dies könnte sicherstellen, dass die Meldungen einen Rückschluss auf Sicherheitslücken der kompromittierten Systeme erlauben. Denn nur aus einer qualitativ hochwertigen Datenbasis können valide Handlungsempfehlungen abgeleitet werden.

Die zur Meldung notwendige Analyse eines Sicherheitsvorfalls ist in der Regel sehr aufwendig und kostenintensiv, da die zugrundeliegenden Sicherheitslücken nur mit Fachwissen gefunden und ausgewertet werden können. Kleine und mittlere Unternehmen verfügen regelmäßig nicht über die geeigneten personellen und technischen Kapazitäten, um aussagekräftige Meldungen abzusetzen und Rückfragen zu bearbeiten. **Es wäre** daher **sinnvoll, nicht nur**, wie von der Kommission vorgesehen, **Kleinstunternehmen, sondern alle kleinen und mittleren Unternehmen von der Meldepflicht auszunehmen.**

Verfehlt ist, dass die Richtlinie nicht für die Soft- und Hardwarehersteller gelten soll. Denn gerade diese Marktteilnehmer könnten ihre Systeme auf Grundlage der durch die Meldepflicht erhobenen Sicherheitslücken schließen und ihren Kunden Sicherheitsupdates zur Verfügung stellen. Dadurch könnte die Kommission die Erhöhung der Netz- und Informationssicherheit schneller und effizienter erreichen.

Juristische Bewertung

Kompetenz

Die Richtlinie wird zu Recht auf Art. 114 AEUV (Binnenmarkt) gestützt.

Subsidiarität

Unproblematisch.

Verhältnismäßigkeit

Unproblematisch. Die Kommission wählt die Rechtsform der Richtlinie und strebt nur eine Mindestharmonisierung an.

Vereinbarkeit mit EU-Recht

Unproblematisch.

Vereinbarkeit mit deutschem Recht

Die Vorgaben der Richtlinie finden sich zum Teil bereits im deutschen Recht, insbesondere im Telekommunikationsgesetz (TKG), oder sind auch in Deutschland geplant. Im März 2013 legte das Bundesinnenministerium den Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vor. Danach sollen „Betreiber kritischer Infrastrukturen" in den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen verpflichtet werden, die maßgeblichen „informationstechnischen Systeme, Komponenten oder Prozesse" nach dem jeweiligen Stand der Technik zu schützen. Ferner sollen sie erhebliche Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden müssen. [BSI-Gesetz (Referentenentwurf)]

Das Fernmeldegeheimnis und personenbezogene Daten müssen bereits nach dem jeweiligen Stand der Technik geschützt werden (§ 109 Abs. 1 TKG). Künftig soll auch die Telekommunikationsinfrastruktur nach dem jeweiligen Stand der Technik geschützt werden [§ 109 Abs. 2 S. 5 TKG (Referentenentwurf)]. Die Bundesnetzagentur und der Bundesdatenschutzbeauftragte müssen bereits informiert werden, wenn der Schutz personenbezogener Daten verletzt wurde (§ 109a Abs. 1 TKG). Künftig soll die Bundesnetzagentur auch über Beeinträchtigungen von Diensten und Netzen informiert werden müssen, die die Verfügbarkeit von Diensten stören oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme führen können [§ 109a Abs. 4 TKG (Referentenentwurf)].

Die Einrichtung einer zentralen nationalen Behörde für die NIS verstößt gegen den im Grundgesetz (GG) festgelegten föderalen Aufbau des deutschen Staates (Art. 83 f. GG). Art. 91c GG erlaubt ausnahmsweise ein Zusammenwirken von Bund und Ländern nur bei der Planung, der Errichtung und dem Betrieb ihrer informationstechnischen Systeme.

Zusammenfassung der Bewertung

Die Pflicht der Mitgliedstaaten zur Ausarbeitung nationaler NIS-Strategien stärkt deren Risikobewusstsein und Reaktionsfähigkeit gegenüber Cybergefahren. Die hoheitliche Vorgabe von Sicherheitsmaßnahmen greift in die unternehmerische Freiheit ein und kann mit erheblichen Kosten verbunden sein. Sie ist im vorliegenden Fall jedoch berechtigt. Sicherheitsmaßnahmen sollten EU-weit einheitlich festgelegt werden. Eine Meldepflicht über Sicherheitsvorfälle ist sachgerecht, kleine und mittlere Unternehmen sollten davon jedoch ausgenommen werden. Die Einrichtung einer zentralen nationalen Behörde für die NIS verstößt gegen den im Grundgesetz (GG) festgelegten föderalen Aufbau des deutschen Staates.