Deutscher AnwaltSpiegel
Ausgabe 02 // 27. Januar 2016

Unternehmen sollten jetzt aktiv werden

Neue EU-Richtlinie für Cybersicherheit sieht Meldepflicht für Internetkonzerne bei schweren Hackerangriffen vor – Vergleich mit IT-Sicherheitsgesetz verdeutlicht Reichweite

Von Sebastian Wypior und Kathrin Isabelle Lausen, LL.M.

NIS-Richtlinie

Ende 2015 wurde die vorläufige Endfassung der EU-Richtlinie zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der EU (NIS-Richtlinie) vereinbart. Nach dem geplanten Inkrafttreten im Frühjahr 2016 haben die Mitgliedstaaten 21 Monate Zeit zur Umsetzung. Ziel ist es, die EU-Mitgliedstaaten zur Erhöhung der Cybersicherheit im Bereich kritischer Infrastrukturen zu verpflichten. Die Regelungen der Richtlinie finden nur auf die in Art. 3 Abs. 8 als „Marktteilnehmer" bezeichneten und legaldefinierten Unternehmen bestimmter Sektoren Anwendung. Marktteilnehmer sind Anbieter von „Diensten der Informationsgesellschaft", die die Bereitstellung anderer „Dienste der Informationsgesellschaft" ermöglichen. Hierunter fallen etwa Plattformen des elektronischen Geschäftsverkehrs, soziale Netzwerke, Suchmaschinen und App-Stores. Marktteilnehmer sind auch Betreiber „kritischer Infrastrukturen", die für die Aufrechterhaltung zentraler wirtschaftlicher und gesellschaftlicher Tätigkeiten etwa in den Bereichen Energie, Verkehr, Banken und Gesundheit unerlässlich sind. Eine nicht erschöpfende Aufzählung der Dienstanbieter und Betreiber „kritischer Infrastrukturen" ist im Anhang II der Richtlinie hinterlegt. Soziale Netzwerke wie Facebook oder Twitter fallen jedoch ebenso wenig in den Anwendungsbereich wie kleine digitale Unternehmen mit bis zu 50 Mitarbeitern.

© 123ArtistImages/iStock/Thinkstock/Getty Images

Stromnetze zählen zu den „kritischen Infrastrukturen". Ihre Betreiber sind zur Meldung von Sicherheitsvorfällen, insbesondere auch Hackerangriffen, verpflichtet.

Marktteilnehmer sind zur Meldung von Sicherheitsvorfällen mit erheblichen Auswirkungen auf die Sicherheit der bereitgestellten Kerndienste (etwa Hackerangriffe) verpflichtet. Schwere Angriffe auf Systeme können anonym gemeldet werden, solange kein Systemausfall droht. In diesem Zusammenhang wird den Marktteilnehmern eine Abwägungsbefugnis eingeräumt. Dabei sind das Informationsinteresse der Öffentlichkeit bei Bedrohungen und das Schutzinteresse des betroffenen Marktteilnehmers vor möglichen wirtschaftlichen Schäden gegeneinander abzuwägen. Eine Melde- und Aufklärungspflicht gegenüber Verbrauchern und Nutzern, ▶

insbesondere von Plattformbetreibern, ist jedoch nicht vorgesehen. Auch öffentliche Institutionen sind der Meldepflicht nicht unterworfen. Verstöße gegen die Meldepflicht sollen sanktioniert werden. Entsprechende Regelungen werden auf nationaler Ebene erlassen.

Außerdem ist der Aufbau einer strategischen Kooperationsgruppe vorgesehen. Diese soll den Austausch von Informationen und bewährten Verfahren im Umgang mit IT-Sicherheitsschwachstellen und den Aufbau von Kapazitäten in den Mitgliedstaaten fördern. Daneben sollen die Mitgliedstaaten IT-Notfallteams einrichten, die grenzüberschreitend den Umgang mit Sicherheitsvorfällen koordinieren und damit den Austausch von Informationen verbessern sollen.

IT-Sicherheitsgesetz

Bereits Mitte 2015 hat der deutsche Gesetzgeber das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) verabschiedet. Im Rahmen der nationalen Cyber-Sicherheitsstrategie soll hierdurch eine signifikante Verbesserung der Sicherheit im Internet erreicht werden.

Der Anwendungsbereich des Sicherheitsgesetzes ist auf die in § 2 Abs. 10 BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) legaldefinierten „kritischen Infrastrukturen“ beschränkt. Erfasst sind die Sektoren Energie, Informationstechnik & Telekommunikation, Transport & Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- & Versicherungswesen – jedoch nur, wenn sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Nicht in diesen Anwendungsbereich fallen der öffentliche Sektor und Kleinstunternehmen. Zur Bestimmung des Begriffs „kritische Infrastrukturen“ wurde in § 10 Abs. 1 BSIG eine Verordnungsermächtigung eingefügt. Die Bestimmung der relevanten Sektoren hat daher nach den in der noch zu erlassenden Verordnung festgelegten Maßstäben zu erfolgen.

Eine bedeutende Änderung wurde durch die Einführung von Meldepflichten für IT-Sicherheitsvorfälle vorgenommen. Betreiber kritischer Infrastrukturen sind hiernach verpflichtet, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT-Systemen, Komponenten und Prozessen über eine Kontaktstelle an das BSI zu melden. Allerdings müssen die Störungen erheblich sein und zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der kritischen Infrastrukturen führen oder geführt haben. Nicht der Meldepflicht unterworfen hat der Gesetzgeber öffentliche Telekommunikationsnetze und Erbringer öffentlich zugänglicher Telekommunikationsdienste, Betreiber von Energieversorgungsnetzen und Energieanlagen, Inhaber atomrechtlicher Genehmigungen sowie Betreiber kritischer Infrastrukturen mit vergleichbaren Vorgaben. Für diese gelten die spezialgesetzlichen Regelungen des Telekommunikationsgesetzes (TGK), des Telemediengesetzes (TMG) oder des Atomgesetzes (AtomG).

Betreiber kritischer Infrastrukturen haben zur Aufrechterhaltung der Funktionsfähigkeit angemessene organisatorische und technische Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme, Komponenten oder Prozesse zu treffen. Die konkreten Maßnahmen orientieren sich an branchenspezifischen Sicherheitsstandards. Spätestens zwei Jahre nach Inkrafttreten der oben genannten Verordnung sollen Betreiber kritischer Infrastrukturen die erforderlichen Maßnahmen umgesetzt haben.

Verstöße gegen die Meldepflicht können mit Bußgeldern von bis zu 50.000 Euro, andere Verstöße sogar mit Bußgeldern von bis zu 100.000 Euro geahndet werden.

Vergleich NIS-Richtlinie mit IT-Sicherheitsgesetz

Ein Vergleich beider Regelungswerke verdeutlicht, dass das Sicherheitsgesetz deutlich hinter der vorläufigen Endfassung der NIS-Richtlinie zurückbleibt. Der Aufbau einer strategischen Kooperationsgruppe, die Einrichtung eines IT-Notfallteams sowie Regelungen für die Kooperation zwischen den Mitgliedstaaten sind nicht vorgesehen. Lediglich das BSI soll als internationaler Ansprechpartner fungieren. Außerdem hat die NIS-Richtlinie einen weitergehenden Anwendungsbereich, da sie insbesondere digitale Diensteanbieter erfasst.

Fazit und Handlungsempfehlung

Nichts Genaues weiß man nicht! – so lässt sich der momentane Zustand wohl am besten beschreiben. Fest steht nur, dass der deutsche Gesetzgeber nach Inkrafttreten der NIS-Richtlinie Umsetzungsarbeit zu leisten hat, denn diese ist breiter aufgesetzt als das IT-Sicherheitsgesetz. Dennoch sind Unternehmen der im IT-Sicherheitsgesetz genannten Branchen gut beraten, schon jetzt zu prüfen, ob sie zu einer kritischen Infrastruktur zählen könnten. Denn sobald die Verordnung erlassen ist und feststeht, dass ein Unternehmen dem Anwendungsbereich des IT-Sicherheitsgesetzes unterfällt, sind insbesondere die geforderten organisatorischen und ▶

technischen Maßnahmen zur Vermeidung von Bußgeldern zügig umzusetzen.

Rein vorsorglich sollten Unternehmen in diesem Zusammenhang prüfen, ob sie als Marktteilnehmer dem weiten Anwendungsbereich der Richtlinie unterfallen, zumal der Prüfungsaufwand aufgrund der im Anhang der Richtlinie beigefügten (leider nicht erschöpfenden) Aufzählung gering sein dürfte. Die Frage, wann ein schwerer, die Meldepflicht auslösender Angriff vorliegt, kann hingegen nicht im Vorhinein beantwortet werden. Dies ist stets eine Frage des Einzelfalls. ◀

Hinweis der Redaktion:
Zum IT-Sicherheitsgesetz siehe die Beiträge von Dr. Flemming Moos (Deutscher AnwaltSpiegel 18/2014: HIER) sowie Dr. Alin Seegel (Deutscher AnwaltSpiegel 19/2015: HIER). (tw)

Sebastian Wypior,
Rechtsanwalt, Buse Heberer Fromm, Düsseldorf

wypior@buse.de
www.buse.de

Kathrin Isabelle Lausen, LL.M.,
Rechtsanwältin, Buse Heberer Fromm, Düsseldorf

lausen@buse.de
www.buse.de