BDI
Bundesverband der
Deutschen Industrie e.V.

Positionspapier

Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz

Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz

Die deutsche Industrie hat ein hohes Eigeninteresse, die Funktionsfähigkeit und Verfügbarkeit ihrer IT-Systeme nachhaltig abzusichern. Sie hat deshalb auf die stetig steigende Cyber-Bedrohungslage mit einer Vielzahl an freiwilligen Maßnahmen reagiert: Das Sicherheitsniveau wird kontinuierlich verbessert und unterliegt regelmäßigen Audits. In einigen Branchen – wie der Telekommunikations- und Versicherungsbranche – bestehen bereits heute verschiedene und umfängliche gesetzliche Melde- und Transparenzverpflichtungen auf nationaler Ebene, denen die Unternehmen nachkommen. Im Rahmen des Umsetzungsplans KRITIS (UP KRITIS) zum Schutz der kritischen Infrastrukturen gibt es in einigen Branchen etablierte und gut funktionierende Meldeprozesse, sowohl gegenüber staatlichen Behörden als auch zwischen Unternehmen. Der Austausch der Wirtschaft untereinander wird bereits heute praktiziert – sowohl bilateral als auch im CERT-Verbund.

Im Koalitionsvertrag für die 18. Legislaturperiode haben sich CDU, CSU und SPD darauf verständigt, *„ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher Sicherheitsvorfälle“* zu schaffen.

Der BDI setzt sich nachdrücklich für eine Stärkung der IT-Sicherheit, den Ausbau des staatlichen IT-Lagebilds sowie für einen verbesserten Informationsaustausches zwischen Industrie und Amtsseite ein. Nach Auffassung der deutschen Industrie wird das IT-Sicherheitsgesetz (ITSiG) keines dieser Ziele erreichen.

Executive Summary

1. Branchenspezifische Mindeststandards im Wege der Selbstorganisation definieren
2. Kritische Infrastrukturen klar definieren
3. Begriff „erhebliche IT-Sicherheitsvorfälle“ präzise bestimmen
4. Unternehmensdaten durch anonymisierte und verschlüsselte Meldungen schützen
5. Flankierung von bestehenden freiwilligen Initiativen
6. Kompatibilität mit EU-Vorgaben/EU-Richtlinie sicherstellen
7. Nutzung international anerkannter Security-Standards
8. Meldung an eine einzige Behörde
9. Dienstleistungsangebot der Amtsseite fördern/ausbauen
10. Umsetzungsfrist verlängern

Argumente gegen den 1. Entwurf des ITSiG

Das Bundesinnenministerium hat bereits am 5. März 2013 einen ersten Entwurf eines ITSiG vorgelegt. Der BDI hat zu dem Referentenentwurf am 5. April 2013 Stellung genommen und ihn in dieser Form mit nachfolgenden Argumenten abgelehnt.

1. Kontraproduktiv

Bereits heute unterliegen Unternehmen im Bereich der kritischen Infrastrukturen gesetzlichen Meldepflichten. Diese Pflicht hat, dies zeigen Beispiele von Verteidigungs- und Telekommunikationsunternehmen, keine Cyberangriffe verhindert. Im Gegenteil: Der Zwang zur Meldung unter „Klarnamen“ hat zu einem öffentlichen Bekanntwerden und damit zu einem erheblichen Reputationsschaden der Unternehmen geführt. Darüber hinaus haben bestehende Meldepflichten keinerlei Aufklärungs- und Erkenntnisbeitrag im Kontext der NSA-Affäre geliefert.

2. Ineffektiv

Bei Bedrohungslagen aus dem Cyberraum ist eine schnelle Weitergabe von Informationen entscheidend. Eine Meldepflicht verlangsamt die Weitergabe von Informationen über Angriffe zwischen Unternehmen und der Amtsseite signifikant. Denn für viele Firmen entsteht ein rechtliches Problem: Sie müssten vor einer Meldung mögliche Konsequenzen für das Unternehmen prüfen. Börsennotierte Unternehmen müssen zudem überlegen, ob eine Meldung über einen umfassenden Hacker-Angriff auch börsenrelevant sein könnte – dann wären sie verpflichtet, ihre Aktionäre zu warnen. Bis diese Fragen geklärt sind, ist es für eine Warnung anderer Unternehmen oft zu spät.

3. Bürokratisch und teuer

Diese intensiven unternehmensinternen Prüfprozesse vor Weiterleitung von Informationen an die Amtsseite sind für Unternehmen äußerst aufwendig und damit kostspielig. Die hierfür notwendigen Ressourcen fehlen letztlich für Investitionen zum eigentlichen Schutz vor IT-Angriffen. Dies trifft insbesondere auf KMU zu.

4. Fehlende Aussagekraft

Das Bundeskriminalamt (BKA) schätzt, dass täglich ca. 30.000 Cyberangriffe auf Unternehmen in Deutschland stattfinden. Eine Meldepflicht würde dazu führen, dass ein Großteil dieser „Angriffe“, unabhängig von Ausmaß und Qualität, an die Amtsseite gemeldet werden müsste.

5. Überforderung von Behörden

Neben der Qualität der eingegangenen Meldungen ist auch deren Anzahl problematisch. Es ist unrealistisch, dass eine Behörde in der Lage ist, ca. 30.000 Meldungen pro Tag qualifiziert und zeitnah auszuwerten und entsprechende Warnmeldungen zu generieren.

Sicht der deutschen Industrie

Aus Sicht der deutschen Industrie könnte eine Stärkung der IT-Sicherheit, der Ausbau des staatlichen IT-Lagebilds sowie ein verbesserter Informationsaustausch zwischen Industrie und Amtsseite mittel- und langfristig mit nachfolgenden Maßnahmen effizienter und besser erreicht werden.

1. Stärkung der „Allianz für Cybersicherheit“
Die Allianz ermöglicht bereits heute die unbürokratische, anonymisierte und zeitnahe Meldung von qualifizierten Meldungen an die Amtsseite – mit steigendem Erfolg und mittlerweile über 500 beteiligten Unternehmen.

2. Anreize für Investitionen in Forschung
Deutschland muss nicht nur Nachfrager, sondern auch verstärkt Anbieter von Cloud- und IT-Sicherheitsleistungen sein. Zertifizierung, verstärkte Investitionen in Forschung und das Setzen von Standards sind adäquate Mittel, mit denen die Cybersicherheit in Deutschland und der EU langfristig und dauerhaft gestärkt werden kann. Ebenso wie die Stärkung des Gütesiegels „Made in Germany“ bei IT-Technologien.

Erwartungen und konstruktive Vorschläge

Darüber hinaus hat die deutsche Industrie Erwartungen und konstruktive Vorschläge für die Ausgestaltung eines möglichen ITSiG am 31. Januar 2014 im Ausschuss für Sicherheit verabschiedet.

1. Branchenspezifische Mindeststandards im Wege der Selbstorganisation definieren

Der BDI unterstützt das Anliegen, brancheneinheitliche Mindeststandards für IT-Sicherheit zu schaffen. Diese Mindeststandards müssen für jede Branche passgenau sein, um effektiv wirken zu können. Die Mittel und Wege der Zielerreichung müssen für die Unternehmen frei wählbar sein.

BDI-Forderung:
Erarbeitung von branchenspezifischen Standards im Wege der Selbstorganisation der Industrie. Brancheninterne Lösungen sollten stets staatlichen Maßnahmen vorgezogen werden. Es sollten Anreize für die Unternehmen gesetzt werden, um Mindeststandards zunächst selbstverpflichtend zu erfüllen. Ein angemessener Zeitraum wäre drei Jahre.

Nach Ablauf der drei Jahre sollte geprüft werden, ob die Mindestanforderungen von den einzelnen Branchen umgesetzt wurden. Die Unternehmen gesetzlich zu verpflichten, sollte stets der letzte Schritt sein.

2. Kritische Infrastrukturen klar definieren

Aus Sicht der deutschen Industrie muss klar definiert werden, wer der Adressatenkreis des ITSiG ist. Dazu muss definiert werden, was „kritische Infrastrukturen“ im Sinne des Gesetzes sind.

Auf eine mögliche Definition „kritische Infrastrukturen“ (KRITIS) haben sich 2003 die Ressorts auf Bundesebene geeinigt.

Unter diese Definition fallen neun Sektoren: Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur.

Der Großteil der kritischen Infrastruktur „Verwaltung“ ist auf Länderebene organisiert. Die Einbeziehung der Landesverwaltung in den Regelungsbereich des IT-Sicherheitsgesetzes ist daher zwingend notwendig. Gleiches gilt für Körperschaften öffentlichen Rechts in Selbstverwaltung, wie die Deutsche Rentenversicherung und die Bundesagentur für Arbeit. Hier sollten ebenfalls hohe Standards angelegt werden, da hier hochsensible Personendaten in beträchtlichem Umfang verarbeitet werden, der Schutzbedarf aber noch nicht angepasst wurde.

BDI-Forderung:
Festlegung des Adressatenkreises auf Grundlage der bestehenden Definition KRITIS. Diese sollte allerdings noch präziser ausdifferenziert werden. Es sollten klar die zu schützenden Infrastrukturelemente, z.B. ein Umspannwerk und nicht das gesamt Netz, identifiziert werden. Einbeziehung der Bundes- und Landesverwaltungen sowie aller Körperschaften des öffentlichen Rechts.

3. Begriff „erhebliche IT-Sicherheitsvorfälle“ präzise bestimmen

Um Rechtssicherheit für die betroffenen Unternehmen zu schaffen, sollte eine eindeutige Definition des Begriffs „erheblicher IT-Sicherheitsvorfall“ gefunden werden. Denn nicht jeder Cyberangriff ist ein „erheblicher IT-Sicherheitsvorfall.“ IT-Sicherheitsvorfälle können vielseitig sein und im Bereich der physikalischen Sicherheit oder im Bereich der IT-Sicherheit auftreten.

Dabei gilt es zwischen verschiedenen Schadensarten und deren Ausmaß zu unterscheiden. Ist die Funktionsfähigkeit des Gesamtunternehmens in erheblicher Art und Weise eingeschränkt? Als solche sind vor allem Angriffe auf Produktiv-, Regel- und Kontrollsysteme anzusehen. Oder handelt es sich um einen gescheiterten Login-Versuch?

BDI-Forderung:
Präzise und praxistaugliche Definition eines „erheblichen IT-Sicherheitsvorfalls“ zwingend erforderlich.

4. Sensible Unternehmensdaten durch anonymisierte und verschlüsselte Meldungen schützen

Der Umgang mit Angriffen auf IT-Strukturen berührt einen hochsensiblen Bereich. Werden entsprechende Vorkommnisse bekannt, drohen irreparable Image- und Vertrauensverluste bei Kunden wie Geschäftspartnern. Unternehmen fürchten Erpressungsversuche und Know-how-Diebstahl.

Es ist deshalb von zentraler Bedeutung für die Unternehmen, dass mit ihren Unternehmensinformationen und Meldungen sensibel auf der Amtsseite umgegangen wird. Die Meldung sollte aus der möglichst genauen Beschreibung des Angriffsvorgehens und der Auswirkung des Angriffs sowie der Benennung von getroffenen Gegenmaßnahmen bestehen. Ziel muss es sein, Information über Angriffsverhalten bereitzustellen, sodass andere Opfer in der Lage sind, geeignete Gegenmaßnahmen zu treffen. Die Nennung des Unternehmens ist dafür nicht notwendig.

BDI-Forderung:
Alle Meldungen sollten standardmäßig anonymisiert und hochsicher verschlüsselt an eine zentrale Meldestelle übermittelt werden können.

Die Analyse, Auswertung und Weitergabe von sensiblen Informationen sollte nur in Absprache mit dem betroffenen Unternehmen und der gebotenen Sorgfalt im Umgang mit kritischen Unternehmensdaten erfolgen.

5. Flankierung von bestehenden freiwilligen Initiativen

Bestehende Initiativen, wie die „Allianz für Cybersicherheit“, die Initiative „IT-Sicherheit in der Wirtschaft“ sind weiter zu stärken.

Im ersten Jahr hat die Allianz einen erfolgreichen Start hingelegt. Inzwischen hat sie mehr als 500 Teilnehmer. Darunter sind viele DAX-Unternehmen, aber auch kleine und mittlere Unternehmen.

Die bereits vorhandene Möglichkeit zur freiwilligen Meldung eines Cyberangriffs bei der Meldestelle der „Allianz für Cybersicherheit“ sollte bei der Ausgestaltung des ITSiG berücksichtigt und mit den vorgesehenen Maßnahmen verzahnt werden.

BDI-Forderung:
Nutzung und Synchronisierung der Meldeprozesse mit bestehenden freiwilligen Initiativen, um Redundanzen zu vermeiden.

6. Kompatibilität mit EU-Vorgaben / EU-Richtlinie sicherstellen

Deutschland verfügt bereits heute bei der IT-Sicherheit über eine sehr gut Infrastruktur und hohe Standards. Zukünftige EU-Regulierungen in diesem Bereich sind deshalb von großer Bedeutung für die nationale IT-Infrastruktur.

BDI-Forderung:
Die Ausgestaltung der nationalen IT-Sicherheit muss mit bestehenden und zukünftigen EU-Vorgaben zu 100% kompatibel sein. Die Bundesregierung sollte sich aktiv an der Ausgestaltung von europäischen Vorgaben einbringen. Doppelregulierungen sind zu vermeiden.

7. Nutzung international anerkannter Security-Standards

Im Bereich der Audits gibt es bereits viele Vorgaben für Security / Risk / Quality-Management Systeme. Diese Systeme basieren auf freiwilliger Basis und werden regelmäßig erfolgreich auditiert.

BDI-Forderung:
Anerkennung von unternehmensspezifischen Managementsystemen nach international gültigen Standards. Die, noch zu entwickelnden branchenspezifischen Mindeststandards, sollten als Absicherung dienen, für den Fall, dass keine international anerkannten Standards genutzt werden.

8. Meldung an eine einzige Behörde

Es bestehen bereits heute zahlreiche Regelungswerke mit entsprechenden Meldebestimmungen in den einzelnen Branchen. Beispiele hierfür sind das Telekommunikationsgesetz (TKG) oder das Energiewirtschaftsgesetz (EnWG).

Im Rahmen dieser bestehenden Gesetze melden Unternehmen bereits heute Cybersicherheitsvorfälle an unterschiedliche Behörden, wie u.a. die Bundesnetzagentur, das Bundesamt für Sicherheit in der Informationstechnik sowie das Bundeskriminalamt.

Auf Grundlage des ITSiG müssten die Unternehmen zusätzlich an das BSI melden. Dies würde zu unnötiger Bürokratie und Doppelarbeit führen, denn jede Behörde hat unterschiedliche Anforderungen und Regularien an eine Meldung.

BDI-Forderung:
Meldung eines Sicherheitsvorfalls an eine zentrale Behörde, um den organisatorischen und verwaltungstechnischen Aufwand möglichst gering zu halten.

Möglich wäre auch eine „Portallösung“. Diese hätte den Vorteil, dass verschiedene betroffene Behörden auf die Meldung über ein Portal zugreifen könnten. Damit wäre zugleich die multiple Meldepflicht für Unternehmen mit einem Single Point of Contact (SPOC) erfüllt. Eine starke Authentifizierung und eine geeignete Transportverschlüsselung sind zwingend erforderlich.

9. Dienstleistungsangebot der Amtsseite fördern/ ausbauen

Die bestehenden Dienstleistungsangebote der Amtsseite für Unternehmen sollten weiter ausgebaut werden. Ein gutes Beispiel ist die „Allianz für Cybersicherheit“, die Unternehmen aktuelle Informationen im Bereich IT-Sicherheit zur Verfügung stellt. Ziel ist es, eine Win-Win-Situation für alle Beteiligten zu erreichen.

BDI-Forderung:
Dienstleistungsangebote der Amtsseite für Unternehmen weiter ausbauen.

10. Umsetzungsfrist verlängern

Die Umsetzung der vorgesehenen Anforderungen an Unternehmen durch das IT-Sicherheitsgesetz macht eine lange Vorlaufzeit nötig. Bei der Fülle an zusätzlichen Verpflichtungen und notwendigen Aktivitäten erscheint die geplante Umsetzungsfrist von zwei Jahren als zu knapp bemessen. Allein die Standardisierungsprozesse innerhalb der Branchen, die vielfach auch in internationale Standardisierungsgremien eingebracht bzw. mit international gültigen Standards abgeglichen werden müssen, benötigen eine längere Vorlaufzeit.

BDI-Forderung:
Verlängerung der Umsetzungsfrist auf mindestens drei Jahre.

Impressum

Herausgeber
Bundesverband der Deutschen Industrie e. V. (BDI)
Breite Str. 29
10178 Berlin
Telefon: +49 30 2028-0
www.bdi.eu

Redaktion
Matthias Wachter, Abteilungsleiter der Abteilung Sicherheit und Rohstoffe
Deborah Klein, Referentin der Abteilung Sicherheit und Rohstoffe

Bildnachweis
Cover: strixcode / Fotolia.com
Seite 3: Daniel Fleck / Fotolia.com
Seite 6: marrakeshh / Fotolia.com

Stand
Februar 2014
BDI-Dokumentennummer: 0639