Bundesamt
für Sicherheit in der
Informationstechnik

Das IT-Sicherheitsgesetz

Kritische Infrastrukturen schützen

Inhaltsverzeichnis

1 Das IT-Sicherheitsgesetz

1 Das IT-Sicherheitsgesetz

Im Juli 2015 ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in Kraft getreten. Das IT-Sicherheitsgesetz ist ein Artikelgesetz, das neben dem BSI-Gesetz auch das Energiewirtschaftsgesetz, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze ändert und ergänzt. Das IT-Sicherheitsgesetz leistet einen Beitrag dazu, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen.

Bereits 2011 hat die Bundesregierung mit der Cyber-Sicherheitsstrategie für Deutschland den Grundstein für mehr Sicherheit im Cyber-Raum gelegt. Die dort verankerten strategischen Ziele werden mit der 2014 beschlossenen Digitalen Agenda der Bundesregierung weiter verfolgt. Das IT-Sicherheitsgesetz ist ein erstes konkretes Ergebnis der Agenda, zu deren Kernzielen die Verbesserung der Sicherheit und des Schutzes der IT-Systeme und Dienste zählt. Insbesondere im Bereich der Kritischen Infrastrukturen (KRITIS) - wie etwa Strom- und Wasserversorgung, Gesundheitswesen, Finanzwesen oder Telekommunikation - hätte ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland. Regelungen zur Verbesserung der Verfügbarkeit und Sicherheit der IT-Systeme, speziell im Bereich der Kritischen Infrastrukturen, sind somit ein zentraler Teil des IT-Sicherheitsgesetzes. Ziel des Gesetzes ist aber auch die Verbesserung der IT-Sicherheit bei Unternehmen und in der Bundesverwaltung sowie ein besserer Schutz der Bürgerinnen und Bürger im Internet.

Digitalisierung erfordert Schutzmaßnahmen

Die zunehmende IT-Durchdringung und Vernetzung praktisch aller Lebensbereiche eröffnet ökonomische wie gesellschaftliche Potenziale, auf die ein hochentwickeltes und industrialisiertes Land wie Deutschland nicht verzichten kann. Gleichzeitig aber entstehen durch die zunehmende Digitalisierung neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss. Die besondere Gefahr durch gezielte Cyber-Angriffe auf die IT-Infrastruktur betrifft staatliche Stellen ebenso wie Kritische Infrastrukturen und andere Unternehmen, die mit besonders wertvollen Informationen umgehen.

Das IT-Sicherheitsgesetz ist Ausdruck der Schutzverantwortung des Staates gegenüber den Bürgerinnen und Bürgern, der Wirtschaft und seinen eigenen Institutionen und Verwaltungen. Es reflektiert zum einen, dass IT-Sicherheit mit der zunehmenden Digitalisierung des Lebens immer mehr zu einem zentralen Baustein der inneren Sicherheit wird. Es berücksichtigt zum anderen, dass durch zunehmende Mobilität und Vernetzung bestehende Paradigmen in der IT-Sicherheit überholt oder unwirksam geworden sind. Zudem zieht es die Konsequenz aus der Erfahrung, dass ein rein freiwilliger Ansatz bei der Herstellung von IT-Sicherheit nicht immer zum nötigen Engagement in der Wirtschaft geführt und nicht flächendeckend bzw. in allen sicherheitsrelevanten Bereichen gewirkt hat.

Mehr Informationen:
https://www.bsi.bund.de/
IT-Sicherheitsgesetz

2 Zielgruppen und Neuregelungen

2 Zielgruppen und Neuregelungen

Das IT-Sicherheitsgesetz setzt unter anderem dort an, wo sich eine moderne Gesellschaft Ausfälle am wenigsten leisten kann: bei den IT-Systemen der Kritischen Infrastrukturen. Betreiber kritischer Anlagen aus den Bereichen Energie, IT und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen müssen künftig ein Mindestniveau an IT-Sicherheit einhalten und erhebliche IT-Störungen an das BSI melden. Zur Steigerung der Sicherheit im Internet sind darüber hinaus die Anforderungen für Telekommunikations- und Telemedienanbieter erhöht worden.

Das IT-Sicherheitsgesetz hat somit mehrere Adressaten:

1. **Betreiber Kritischer Infrastrukturen**

   - werden – sofern nicht andere Spezialregelungen bestehen – verpflichtet, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern und diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen. Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen.
   - können – sofern nicht andere Spezialregelungen bestehen – die Absicherung ihrer IT-Infrastruktur ausgestalten, solange ihre Maßnahmen dem Stand der Technik entsprechen.
   - können – sofern nicht andere Spezialregelungen bestehen – branchenspezifische Sicherheitsstandards gemäß dem jeweiligen Stand der Technik erarbeiten.
   - müssen dem BSI erhebliche Störungen ihrer IT melden, sofern diese Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können. Diese Meldepflicht betrifft zunächst nur die Betreiber von Kernkraftwerken und Telekommunikationsunternehmen. Für andere KRITIS-Betreiber tritt sie nach Verabschiedung einer Rechtsverordnung in Kraft, die festlegt, welche Unternehmen den Regelungen des Gesetzes unterliegen. Der Entwurf der Rechtsverordnung ist auf der Webseite des Bundesinnenministeriums veröffentlicht worden.

2. Für **Betreiber von Webangeboten** gelten erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme.

3. **Telekommunikationsunternehmen**

- sind ab sofort verpflichtet, ihre Kunden zu warnen, wenn sie bemerken, dass der Anschluss des Kunden für IT-Angriffe missbraucht wird. Gleichzeitig sollen die Provider ihre Kunden auf mögliche Wege zur Beseitigung der Störung hinweisen.

- müssen IT-Sicherheitsmaßnahmen nach dem Stand der Technik nicht nur zum Schutz personenbezogener Daten, sondern auch zum Schutz vor unerlaubten Eingriffen in die Infrastruktur einsetzen und erhalten.

- müssen erhebliche IT-Sicherheitsvorfälle ab sofort melden. Die bereits bestehende Meldepflicht gegenüber der Bundesnetzagentur wurde mit dem IT-Sicherheitsgesetz erweitert.

4. Das **Bundesamt für Sicherheit in der Informationstechnik**

- erhält erweiterte Befugnisse zur Untersuchung der Sicherheit von IT-Produkten und erweiterte Kompetenzen im Bereich der IT-Sicherheit der Bundesverwaltung.

- hat sämtliche für die Abwehr von Gefahren für die IT-Sicherheit Kritischer Infrastrukturen relevanten Informationen zu sammeln, zu bewerten und an die Betreiber sowie die zuständigen (Aufsichts-)Behörden weiterzuleiten.

- wird zur Stärkung der IT-Sicherheit der Bundesverwaltung verpflichtet, Mindeststandards für die IT der Bundesverwaltung zu erarbeiten.

- informiert in einem jährlichen Lagebericht die Öffentlichkeit über aktuelle Gefahren für die Sicherheit in der Informationstechnik und trägt so zu einer höheren Sensibilisierung für das Thema IT-Sicherheit bei.

Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen

Nach Verabschiedung des IT-Sicherheitsgesetzes wurde vielerorts die Frage gestellt, welche Unternehmen konkret zu den Betreibern einer Kritischen Infrastruktur im Sinne des IT-Sicherheitsgesetzes gehören. Diese Frage wird durch eine Rechtsverordnung geklärt, deren Entwurf das Bundesministerium des Innern (BMI) im Februar 2016 veröffentlicht hat. Durch die Verordnung sollen Betreiber Kritischer Infrastrukturen in die Lage versetzt werden, anhand messbarer und nachvollziehbarer Kriterien zu prüfen, ob sie unter den Regelungsbereich des IT-Sicherheitsgesetzes fallen. So wird etwa der Versorgungsgrad anhand von Schwellenwerten für jede Anlagenkategorie im jeweiligen KRITIS-Sektor bestimmt. Der Regelschwellenwert beträgt dabei 500.000 versorgte Personen.

Für die Betreiber von Kernkraftwerken und Telekommunikationsunternehmen ergibt sich die Betroffenheit bereits direkt aus dem Gesetz. Die Verordnung bestimmt nun zunächst Kritische Infrastrukturen in den Sektoren Energie, Informationstechnik und (andere) Telekommunikation, Wasser sowie Ernährung. Bis Ende 2016 sollen per Änderungsverordnung auch die Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen geregelt werden.

Sobald die Verordnung in Kraft getreten ist, haben betroffene Unternehmen zwei Jahre Zeit, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern und – sofern nicht andere Spezialregelungen bestehen – diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen.

Binnen sechs Monaten müssen sie zudem dem BSI eine Kontaktstelle für Vorfallsmeldungen benennen. Diese Kontaktstelle muss rund um die Uhr erreichbar sein.

Sektoren Kritischer Infrastrukturen in Deutschland

3 Neue Aufgaben für das BSI

3 Neue Aufgaben für das BSI

Als nationale IT- und Cyber-Sicherheitsbehörde verfolgt das BSI das Ziel, die IT-Sicherheit in Deutschland durch Maßnahmen und Angebote zu wahren und zu fördern, die einerseits auf Prävention ausgerichtet sind, andererseits aber auch helfen, aktuelle Bedrohungen und Angriffe wirksam abzuwehren. Durch das IT-Sicherheitsgesetz wird die Rolle des BSI als zentrale Stelle für die Belange der IT-Sicherheit vor allem gegenüber der Wirtschaft gestärkt. Mit der Übertragung von mehr Verantwortung und Kompetenzen durch Erweiterung der bisherigen operativen Aufgaben wächst aber auch die Verpflichtung des BSI, dieser Verantwortung gerecht zu werden.

Dies gilt zum einen für die in das IT-Sicherheitsgesetz aufgenommene Befugnis, IT-Produkte und Software auf Sicherheitslücken zu untersuchen. Das gilt zum anderen für den Umgang mit den Meldungen, die die KRITIS-Betreiber bei erheblichen IT-Sicherheitsvorfällen an das BSI machen müssen. Das BSI bewertet und analysiert die eingehenden Meldungen und setzt sie mit weiteren Meldungen und Erkenntnissen aus anderen Quellen in Beziehung. Daraus entsteht ein Lagebild, auf dessen Basis beispielsweise kurzfristige Warn- und Alarmierungsmeldungen sowie Handlungsempfehlungen für Betroffene erstellt werden können. Diese tragen dazu bei, dass sich KRITIS-Betreiber, aber auch andere Unternehmen und Behörden, frühzeitig auf Angriffe oder Ausfälle vorbereiten bzw. entsprechende Gegenmaßnahmen treffen können. Die Meldungen der KRITIS-

Zentrale Meldestelle für IT-Sicherheitsvorfälle im IT-Lagezentrum im BSI.

Betreiber sind daher eine wichtige Voraussetzung für die nationale Handlungsfähigkeit und Grundlage für bundesweit abgestimmte Reaktionen. Die Betreiber erhalten somit Informationen und Know-how und können von der Auswertung der Meldungen aller Betreiber sowie vieler anderer Quellen durch das BSI profitieren.

Die Meldestruktur im BSI ist schon heute aufgebaut und einsatzbereit. Hier kann auf Erfahrungen zurückgegriffen werden, die im Rahmen der bereits seit langem geltenden Meldepflicht für IT-Sicherheitsvorfälle in der Bundesverwaltung gewonnen wurden.

4 Gemeinsam für mehr IT-Sicherheit

4 Gemeinsam für mehr IT-Sicherheit

Die Herausforderungen der Digitalisierung lassen sich nicht von einzelnen Akteuren im Alleingang lösen. Daher ist die Zusammenarbeit zwischen Staat, Wirtschaft, Wissenschaft und Gesellschaft ein unverzichtbarer Bestandteil einer nachhaltigen Cyber-Sicherheitsstrategie. Durch das IT-Sicherheitsgesetz werden somit bestehende Kooperationsinstrumente nicht überflüssig, schon allein aufgrund der Anzahl an Unternehmen: Von den gesetzlichen Regelungen für Kritische Infrastrukturen werden nur etwa 2.000 der rund 3,5 Millionen Unternehmen in Deutschland betroffen sein.

Der UP KRITIS

UP KRITIS

Der UP KRITIS ist eine öffentlich-private Partnerschaft zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Er adressiert acht der neun Sektoren Kritischer Infrastrukturen. Den Sektor Staat und Verwaltung adressiert auf Bundesebene der UP BUND. Die notwendigen Regelungen für Länder und Kommunen treffen die Länder.

Das zentrale Ziel des UP KRITIS ist es, die Versorgung mit Dienstleistungen Kritischer Infrastrukturen in Deutschland auch im Zeitalter der Digitalisierung möglichst uneingeschränkt aufrechtzuerhalten. Die Erfahrungen mit dem UP KRITIS haben gezeigt, wie Staat und Wirtschaft in enger Partnerschaft gemeinsam an der kontinuierlichen Verbesserung des Schutzes der Kritischen Infrastrukturen arbeiten können. Zwischen den Beteiligten hat sich ein Netzwerk des Vertrauens gebildet, in dem ein transparenter Know-how-Transfer stattfindet. Dadurch lernen alle Beteiligten voneinander und kommen zu besseren Lösungen. Mit der Anmeldung zum UP KRITIS kann zeitgleich auch durch einfaches Ankreuzen die Aufnahme in die Allianz für Cyber-Sicherheit beantragt werden.

Mehr Informationen:
http://www.upkritis.de

Die Allianz für Cyber-Sicherheit

Allianz für Cyber-Sicherheit

Die „Allianz für Cyber-Sicherheit“ ist eine Initiative des Bundesamts für Sicherheit in der Informationstechnik, die 2012 in Zusammenarbeit mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) gegründet wurde.

Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz für Cyber-Sicherheit das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyber-Angriffen zu stärken, die IT-Sicherheitskompetenz in deutschen Organisationen auszubauen, Informationen und Handlungsempfehlungen bereitzustellen und eine bessere und einheitliche Lagebeurteilung voranzutreiben.

Der Allianz gehören inzwischen mehr als 1.500 Institutionen an, davon knapp 100 Partner-Unternehmen und mehr als 40 Multiplikatoren.

Mehr Informationen:
https://www.allianz-fuer-cybersicherheit.de

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de
Telefon: +49 (0) 22899 9582-0
Telefax: +49 (0) 22899 9582-5400

Stand
Februar 2016

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Fotolia

Artikelnummer
BSI-ITSIG16/602

www.bsi.bund.de