esatus AG
The CISO Consulting Company

Das IT-Sicherheitsgesetz von 2015: Adressaten, Auswirkungen und Kritik

Betreiber kritischer Infrastrukturen werden durch das IT-Sicherheitsgesetz verpflichtet, die für die Erbringung ihrer Dienstleistung notwendige IT nach dem Stand der Technik abzusichern. Zudem wird eine Meldepflicht von wesentlichen Sicherheitsvorfällen eingeführt, die bei einer Beeinträchtigung oder einem Ausfall einer kritischen Infrastruktur beachtet werden muss. Nach dem IT-Sicherheitsgesetz können aufgrund ordnungswidriger Handlungen Bußgelder verhängt werden. Eine Missachtung des Gesetzes könnte für Betreiber kritischer Infrastrukturen existenzgefährdend werden. In diesem Whitepaper werden neben der Definition wichtiger Kernbegriffe des Gesetzes auch öffentliche Kritiken an diesem diskutiert sowie ein Ausblick auf die nächsten Schritte zur Verabschiedung ausstehender Rechtsverordnungen gegeben.

Einleitung

Aufgrund stetig besser werdender Auswertungsmöglichkeiten für Daten, beispielsweise durch Big Data Analysen, ergeben sich sowohl gegenwärtig, als auch in Zukunft erhebliche Sicherheitsrisiken beim Umgang mit sensiblen Daten. Dies betrifft gleichermaßen Unternehmen und private Nutzer. Um auf die steigenden Risiken zu reagieren, hat der deutsche Staat 1991 das Bundesamt für Sicherheit in der Informationstechnik (BSI) gegründet, um einen sicheren Einsatz von Informations- und Kommunikationstechnik für die Gesellschaft zu gewährleisten. Der vom BSI entwickelte IT-Grundschutz, welcher sich stark an den europäischen ISO 2700X Normen orientiert, war ein erster Schritt, um effektive, technisch wirksame Informationssicherheitsmanagementsysteme (ISMS) in Unternehmen zu implementieren. Der BSI Grundschutz bietet hierfür ein Regelwerk und Empfehlungen für die Einführung eines ISMS.

Der Ausfall von Informationsinfrastrukturen kann zu erheblichen Beeinträchtigungen der technischen, wirtschaftlichen und administrativen Leistungsfähigkeit Deutschlands führen. Um auf die Gefährdungslage von Informationsinfrastrukturen zu reagieren, wurde 2011 durch das Bundesministerium des Innern die Cyber-Sicherheitsstrategie für Deutschland beschlossen.

Darauf aufbauend wurde im Juni 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – das IT-Sicherheitsgesetz – verabschiedet. Dieses ist Teil der Daseinsfürsorge des Staates, um ein Mindestniveau an IT-Sicherheit gesetzlich zu verankern. Beim „neuen" IT-Sicherheitsgesetz handelt es sich um eine Ergänzung des schon vorher bestehenden BSI-Sicherheitsgesetzes, welches Zuständigkeiten, Definitionen und Aufgabenbereiche des BSI definiert. Das IT-Sicherheitsgesetz hat Einfluss auf verschiedene bestehende Gesetze, unter anderem das Telemedien-, Telekommunikations- und das Energiewirtschaftsgesetz.

Die wichtigsten Änderungen des bestehenden BSI-Sicherheitsgesetzes zeigen sich z.B. in der Einführung einer Meldepflicht für IT-Sicherheitsvorfälle bei sogenannten Betreibern kritischer Infrastrukturen. Zudem sind Betreiber kritischer Infrastrukturen dazu aufgefordert, ihre Informationssicherheitsmanagementsysteme regelmäßig auf den Stand der Technik zu prüfen, um die technische Wirksamkeit des ISMS dauerhaft gewährleisten zu können. Überwiegend werden die oben genannten Regelungen in den §§ 8a bis 8d des Sicherheitsgesetzes definiert.

Um das neue IT-Sicherheitsgesetz zu verstehen, müssen also folgende Fragen beantwortet werden:

- Wer ist Betreiber kritischer Infrastruktur?
- Was bedeutet der Begriff 'Stand der Technik'?

- Was bedeutet die Meldepflicht von IT-Sicherheitsvorfällen in der Praxis?
- Was umfasst das Sanktionierungsmodell des Gesetzes?
- Gibt es Kritik an dem Gesetz und wie fällt diese aus?

Die folgenden Seiten geben Antworten auf diese Fragestellungen und definieren, welche Unternehmen von der Gesetzgebung betroffen sind.

Adressatenkreis des IT- Sicherheitsgesetzes

Das IT-Sicherheitsgesetz richtet sich an zwei verschiedene Adressatenkreise:

1. Betreiber von Telemedien

Betreiber von Telemedien werden dazu verpflichtet, technische und organisatorische Maßnahmen nach dem Stand der Technik zu ergreifen, um unerlaubten Zugriff auf die technische Einrichtung zu verhindern. Die Telemedien sollen damit gegen Angriffe von außen geschützt werden.

2. Betreiber kritischer Infrastruktur

Unternehmen, deren Dienstleistungen eine hohe Bedeutung für das Funktionieren des Gemeinwesens und die Sicherung der Grundbedürfnisse der Bevölkerung oder der öffentlichen Sicherheit haben, werden unter dem Begriff 'Betreiber kritischer Infrastruktur' zusammengefasst. Die durch das IT-Sicherheitsgesetz betroffenen Branchen sind Energie, Informationstechnik, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen.

Welche Unternehmen kritische Infrastrukturen betreiben, bestimmt eine Rechtsverordnung, die das Bundesministerium des Inneren erlässt. Rechtsverordnungen werden genutzt, um zusätzlich zum eigentlichen Gesetzestext Anpassungen und Spezifikationen vorzunehmen. Die erste Rechtsverordnung zur Definition kritischer Infrastrukturen trat am 03.05.2016 in Kraft und definiert Maßgaben zu den Branchen Energie, Informations- und Telekommunikationstechnik sowie Wasser und Ernährung. Welche Unternehmen dieser Branchen als kritische Infrastruktur eingestuft werden, bestimmen Schwellwerte, die in der Rechtsverordnung definiert sind. Ein Regelschwellwert schreibt eine Versorgung von 500.000 Personen vor, für jede Anlagenkategorie gibt es jedoch einen spezifischen Schwellwert. Unabhängig von den Schwellwerten sind Betreiber von Kernkraftwerken und Telekommunikationsunternehmen direkt von dem IT-Sicherheitsgesetz betroffen.

Auswirkungen für Betreiber kritischer Infrastrukturen

Betreiber kritischer Infrastrukturen werden durch das IT-Sicherheitsgesetz dazu verpflichtet, die für die Erbringung ihrer Dienstleistung notwendige IT nach dem Stand der Technik abzusichern. Diese Maßnahmen müssen mindestens alle zwei Jahre gegenüber dem BSI nachgewiesen werden. Werden im Laufe der Überprüfung Sicherheitsmängel entdeckt, darf das BSI in Einvernehmen mit der zuständigen Aufsichtsbehörde in solchen Fällen die Beseitigung des Mangels anordnen.

Der 'Stand der Technik' ist ein gängiger juristischer Begriff, der dazu dient, konkrete technische Anforderungen im Gesetzestext zu vermeiden. Eine Konkretisierung des Begriffs von Seiten des Gesetzgebers wird nicht erfolgen. Die vom BSI geförderten KRITIS Gruppierung kann jedoch in sogenannten Branchenarbeitskreisen (BAK) branchenspezifische Sicherheitsstandards erarbeiten. Diese können durch das BSI anerkannt werden und bieten den Betreibern kritischer Infrastrukturen laut BSI die Möglichkeit, Rechtssicherheit bzgl. des Begriffs 'Stand der Technik' zu erlangen. Die KRITIS Gruppierung setzt sich aus Unternehmen zusammen, die als Betreiber kritischer Infrastrukturen klassifiziert werden. Diese branchenspezifischen Rechtsverordnungen werden mindestens alle zwei Jahre vom BSI auf Aktualität und Zweckmäßigkeit geprüft.
Zwei Jahre nach Inkrafttreten der Rechtsverordnung 'Stand der Technik' ist dieser durch die Unternehmen

Anerkennungsprozess für Branchenspezifische Sicherheitsstandards.
Quelle: Bundesamt für Sicherheit in der Informationstechnik.

nachzuweisen. Für Betreiber von Kernkraftwerken und Telekommunikationsunternehmen gilt diese zweijährige Übergangsfrist nicht.

Betreiber kritischer Infrastrukturen müssen also dort Absicherungsmaßnamen ergreifen, wo Informationstechnik Einfluss auf die Erbringung der Dienstleistung hat. Dies gilt auch dann, wenn ein externer Dienstleister den Betrieb der IT übernimmt.

Zusätzlich zu den Absicherungsmaßnahmen müssen erhebliche Störungen informationstechnischer Systeme, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der betriebenen kritischen Infrastrukturen führen können oder geführt haben, an das BSI gemeldet werden. Eine Störung im Sinne des Gesetzes liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Beispiele hierfür sind Schadprogramme und Sicherheitslücken, aber auch unerwartete technische Defekte mit IT-Bezug, wie der Ausfall der Serverkühlung. Eine Störung ist dann erheblich, wenn sie nicht mit Hilfe dem Stand der Technik entsprechender Maßnahmen abgewehrt werden kann.

Sanktionierung

Um die gesetzlichen Regelungen durchzusetzen, wurde in § 14 des IT-Sicherheitsgesetzes eine Bußgeldvorschrift beschlossen, die fahrlässige sowie vorsätzliche, ordnungswidrige Handlungen mit einer Geldbuße bestraft.

Gemäß § 14 wird als ordnungswidriges Handeln aufgeführt, wenn

- eine organisatorische oder technische Sicherheitsvorkehrung nicht, nicht rechtzeitig, nicht vollständig oder nicht richtig getroffen wird,
- eine Anordnung über die Beseitigung vorhandener Sicherheitsmängel missachtet wird oder die Übermittlung von Zertifizierungs- oder Prüfungsergebnissen nicht erfolgt,
- die Kontaktstelle nicht oder nicht rechtzeitig benannt wird oder
- der Meldepflicht nicht, nicht rechtzeitig, nicht vollständig oder nicht richtig nachgekommen wird.

Nach § 14 Absatz 2 können diese Ordnungswidrigkeiten mit einer Geldstrafe von bis zu 50.000 Euro sanktioniert werden. Für den Fall, dass eine Anordnung zur Beseitigung von Sicherheitsmängeln missachtet wird, droht sogar eine Geldstrafe von bis zu 100.000 Euro. Bußgelder wegen ordnungswidrigen Handelns können erst nach Inkrafttreten der jeweiligen Rechtsverordnungen ausgesprochen werden.

Kritik

Das IT-Sicherheitsgesetz wird seit seiner Vorstellung immer wieder scharf kritisiert. Die vorgebrachte Kritik kann in folgende Kernbereiche zusammengefasst werden, die anschließend diskutiert werden:

- Grundsätzlicher Zweifel am Nutzen des IT-Sicherheitsgesetz und der eigenen Betroffenheit durch das Gesetz
- Unbestimmte Rechtsbegriffe im Gesetzestext
- Die Meldepflicht und die dadurch entstehenden Bürokratiekosten sowie die Gefahr von Reputationsverlusten
- Ermöglichung der Vorratsdatenspeicherung von Bestands- und Verkehrsdaten durch die Änderung des Telekommunikationsgesetzes

Grundsätzlicher Zweifel am Nutzen des IT-Sicherheitsgesetz und der eigenen Betroffenheit durch das Gesetz

Immer wieder kam Kritik an dem grundsätzlichen Nutzen des IT-Sicherheitsgesetzes auf, vor allem Verbände aus der Logistikbranche haben sich hier besonders hervorgetan. Das vorgebrachte Hauptargument ist hierbei, dass genügend große Redundanzen innerhalb der Branche vorhanden seien, um einzelne Ausfälle zu kompensieren. Beweggrund für diese Argumentation scheint die Vermeidung von Investitionen in die IT-Sicherheit und Kosten für Zertifizierungsprozesse zu sein. Die Argumentation könnte anfechtbar werden, wenn man die Investitionskosten mit den Kosten durch Sicherheitsvorfälle vergleicht, da alleine durch Schadprogramme jährlich Kosten in Milliardenhöhe entstehen.

Unbestimmte Rechtsbegriffe im Gesetzestext

Weitere Kritik richtet sich gegen unbestimmte (nicht definierte) Rechtsbegriffe in den Gesetzestexten und die Unklarheit darüber, wer von dem Gesetz durch die Verabschiedung weiterer Rechtsverordnungen betroffen sein wird.

Die (teilweise) unbestimmten Rechtsbegriffe sind die folgenden:

- Kritische Infrastruktur
- Stand der Technik
- Vermeidung von Störung
- Erhebliche Störung

Die Definition von kritischen Infrastrukturen nahm mit der ersten verabschiedeten Rechtsverordnung am 03.05.2016 Gestalt an. Zu den Branchen Transport, Verkehr, Gesundheit sowie Finanz- und Versicherungswesen liegt jedoch noch keine Rechtsverordnung vor.

Die Meldepflicht und die dadurch entstehenden Bürokratiekosten sowie die Gefahr von Reputationsverlusten

Die meiste Kritik am IT-Sicherheitsgesetz richtet sich gegen die Meldepflicht. Zum einen ist nicht genau definiert, was meldepflichtig ist, zum anderen fürchten die Unternehmen Vertrauens- und Reputationsschäden, die durch die Meldepflicht entstehen können, sollten Details zu Sicherheitsvorfällen an die Öffentlichkeit gelangen. Um dem entgegenzuwirken, sind der Weitergabe von Informationen durch das BSI enge Grenzen gesetzt. Beispielsweise ist die Nennung des Firmennamens nur erforderlich, wenn eine tatsächliche Beeinträchtigung der Leistungsfähigkeit der kritischen Infrastruktur vorliegt. Die Unternehmen führen an, dass eine Weitergabe an das BSI durch die fehlende Anonymisierung/Pseudonymisierung wegen unternehmensinternen Prüfungen und Freigaben erheblich verlangsamt wird und somit dem Sinn der Meldepflicht entgegensteht. Aus diesem Grund soll mit den Betreibern kritischer Infrastrukturen ein Prozess erarbeitet werden, der eine stufenweise Meldung von Vorfällen an das BSI vorsieht. Jede Stufe enthält dabei mehr Informationen zu einem Vorfall, als die vorherige.

Ermöglichung der Vorratsdatenspeicherung von Bestands- und Verkehrsdaten durch die Änderung des Telekommunikationsgesetzes

Der letzte Kritikpunkt kommt von Datenschützern, die in der Änderung von § 100 des Telekommunikationsgesetzes eine Möglichkeit zur Vorratsdatenspeicherung sehen, da Bestands- und Verkehrsdaten der Teilnehmer und Nutzer erhoben und genutzt werden dürfen, um Störungen oder unerlaubte Zugriffe erkennen zu können. Die Mehrheit der Bundesländer im Bundesrat hat sich deswegen für eine Streichung der Änderung ausgesprochen. Der Paragraph ist jedoch im verabschiedeten Gesetz unverändert vorhanden.

Ausblick

Wie dargelegt, ist es für die Umsetzung des IT-Sicherheitsgesetzes erforderlich, weitere Rechtsverordnungen zur Definition kritischer Infrastrukturen zu verabschieden bzw. die bestehende Rechtsverordnung um die fehlenden Branchen zu ergänzen. Zudem sind die Rechtsbegriffe 'Vermeidung von Störungen' und 'Erhebliche Störungen' im Kontext des IT-Sicherheitsgesetzes zu spezifizieren.

Da die ersten Prüfungen zum Stand der Technik zwei Jahre nach Verabschiedung der entsprechenden Rechtsverordnung anstehen, steht diese Thematik bei Unternehmen aktuell im Fokus. In der KRITIS wurden bereits verschiedene Branchenarbeitskreise gegründet, um branchenspezifische Sicherheitsstandards auszuarbeiten.

Da am 03.05.2016 die entsprechende Rechtsverordnung verabschiedet wurde, ist es für Unternehmen der Branchen Energie, Informationstechnik, Ernährung und Wasser zwingend notwendig geworden, eine Meldestelle einzurichten. So können Unternehmen der genannten Branchen jetzt feststellen, ob sie Betreiber kritischer Infrastruktur sind.

Die **esatus** AG ist ein mittelständisches IT-Beratungsunternehmen. Als „The CISO Consulting Company" ist die esatus AG der qualifizierte, erfahrene und flexible Ansprechpartner für Projekte rund um das Thema Informationssicherheit. Für Kunden werden optimale und individuell gestaltete Lösungen für Herausforderungen in den Bereichen Identity & Access Governance, IT Security, sowie Governance, Risk und Compliance angeboten. Zudem bietet die **esatus** AG eine umfassende Beratung zur Thematik des IT-Sicherheitsgesetzes an, beispielsweise zur Einrichtung einer Meldestruktur. Die Zufriedenheit von Kunden ist der Leitfaden, nachdem sich das gesamte Handeln de Unternehmens richtet.

Herausgeber **esatus** AG

Grafik Seite 3 © Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/ITSiG/Neuregelungen_KRITIS/B3S/b3s_node.hmtl

Weitere Informationen zum Thema „Das IT-Sicherheitsgesetz" bei der **esatus** AG finden Sie unter: esatus.com

Stand der Informationen im vorliegenden Whitepaper: Juni 2017