Deloitte.

# Cyber Security
# Empfehlungen zum IT-Sicherheitsgesetz

„Betreiber solcher kritischer Infrastrukturen werden mit dem Gesetz verpflichtet, Mindeststandards an IT-Sicherheit einzuhalten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik zu melden“

BM Thomas de Maizière
17.12.2014 bei der 1. Lesung zum IT-Sicherheitsgesetz im Deutschen Bundestag

## Hintergrund

Im Verlauf des Jahres 2015 wird in Deutschland erstmalig ein „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ (kurz: IT-Sicherheitsgesetz) durch den Bundestag verabschiedet. Bereits im Koalitionsvertrag hatten sich die beiden Regierungsparteien auf die Einführung einer gesetzlichen Regelung geeinigt. Nun wurde das Gesetz im Dezember im Kabinett gebilligt und ist auf dem Weg ins Parlament. Aufgrund der aktuellen Mehrheitslage ist dort eine breite Zustimmung zu erwarten.

Die Begründung für das Gesetz basiert auf zwei wesentlichen Punkten. Zum einen nimmt die Zahl der Cyberangriffe auf Unternehmen und staatliche Stellen weiterhin dramatisch zu. Egal welche Studien man heranzieht, der Anstieg gegenüber dem Vorjahreswert liegt bei ca. 50 Prozent. Dieser Wert ist bereits sehr hoch, aber dennoch nur die Spitze des Eisbergs. Viele Sicherheitsvorfälle gelangen nicht an die Öffentlichkeit, da sie von den Unternehmen häufig aus Reputationsgründen intern gehalten werden, oder – und das ist fast noch besorgniserregender – sie werden durch die Betroffenen erst gar nicht bemerkt.

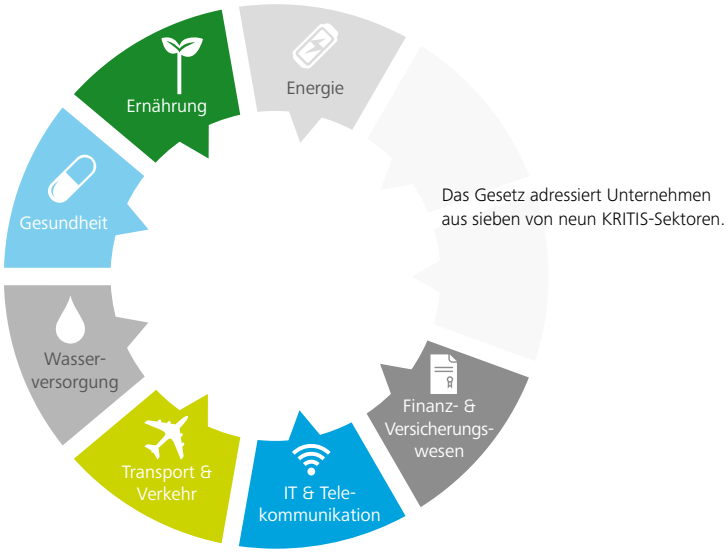
Zum anderen ist in Deutschland das Sicherheitsniveau im Bereich der Informationstechnik in den verschiedenen Sektoren der Wirtschaft sehr unterschiedlich ausgeprägt. Aufgrund der durchaus hohen Vernetzung untereinander und der damit einhergehenden Abhängigkeiten der verschiedenen Branchen sollen auch die im Bereich der Informationssicherheit bisher nicht regulierten Branchen zukünftig branchenspezifische Mindeststandards einhalten.

## Wer ist betroffen?

In erster Linie sind die Unternehmen von den Regelungen des IT-Sicherheitsgesetzes betroffen, die zu den kritischen Infrastrukturen (KRITIS) gezählt werden, also für das Gemeinwohl des Staates und seiner Bürger eine besondere Bedeutung haben.

Im Fokus stehen hierbei insbesondere Telekommunikation und Energie, da auf deren ständige Verfügbarkeit unsere Gesellschaft und die deutsche Wirtschaft kaum verzichten können.

**KRITIS-Sektoren**
(entsprechend der nationalen Strategie zum Schutz kritischer Infrastrukturen)



## Was sind die Ziele des Gesetzes?

Cyberangriffe lassen sich nicht verhindern und werden auch weiterhin – und sogar noch zunehmen – stattfinden. Besonders Unternehmen der kritischen Infrastrukturen müssen daher sicherstellen, dass Angriffe keine oder möglichst geringe Auswirkungen auf die wichtigsten Geschäftsprozesse haben. Wesentliches Ziel des Gesetzes ist daher, die Widerstandsfähigkeit von Staat, Unternehmen und Bürgern gegen Cyberattacken deutlich auszubauen.


## Was bedeutet das konkret?

### Effektive Sicherheitsorganisation

Im Rahmen der Prävention müssen KRITIS-Unternehmen im Zwei-Jahres-Rhythmus ihre Sicherheitsmaßnahmen prüfen lassen (Audits/Zertifizierungen) und so deren Wirksamkeit gegenüber den Aufsichtsbehörden wie der Bundesnetzagentur oder dem Bundesamt für Finanzaufsicht (BaFin) sowie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen. Insbesondere etablierte Standards für Informationssicherheit wie die ISO/IEC 27000-Familie oder der BSI-Grundschutz können dabei von Unternehmen angewandt werden. Branchen sind allerdings auch berechtigt, eigene Mindestsicherheitsstandards zu definieren. Sie müssen sich diese allerdings durch das BSI genehmigen lassen. Durch den Einsatz eines Informationssicherheitsmanagementsystems nach der ISO 27001 (ISMS) werden Unternehmen zum Beispiel angehalten, die Verantwortlichkeit für Informationssicherheit im Unternehmen festzulegen und Notfallpläne für IT-Krisen zu entwickeln.

### Meldepflichten

Im Hinblick auf eine verbesserte Reaktionsfähigkeit müssen wesentliche Vorfälle, die zu einem Ausfall geführt haben oder hätten führen können, im Unternehmen erkannt und an die Behörden weitergemeldet werden.

### Schutz von Kunden

Neben den Regelungen zum Schutz kritischer Infrastrukturen werden auch die Anbieter von kommerziellen Telemediendiensten und öffentlichen Telekommunikationsservices verpflichtet, mehr zur Absicherung der eigenen Systeme zu tun sowie zur Aufklärung der Nutzer beizutragen.

## Wie geht es weiter?

Das Gesetz wurde Mitte Dezember 2014 im Kabinett verabschiedet und wird in diesem Jahr im Parlament beraten. Auch wenn eine Zustimmung des Bundesrates für das Gesetz nicht erforderlich ist, haben die Länder im Rahmen der Kommentierung ihre breite Unterstützung und Zustimmung für das Gesetz signalisiert. Mit einer Verabschiedung des Gesetzes im Parlament ist im Frühjahr 2015 zu rechnen.

Im Gesetz erfolgt noch keine detaillierte Bestimmung, welche Unternehmen den KRITIS-Sektoren zuzurechnen sind. In einer zusätzlichen Rechtsverordnung, die durch das Bundesinnenministerium voraussichtlich im Sommer 2015 verabschiedet wird, werden Schwellenwerte festgelegt, ab wann ein Unternehmen zu den KRITIS-Branchen gezählt wird. Wesentliche Voraussetzung für die Einstufung als KRITIS-Unternehmen werden die Größe des Unternehmens sowie die potenzielle Auswirkungen eines Ausfalls von Leistungen des Unternehmens auf das Gemeinwohl (z.B. Anzahl der betroffenen Bürger) sein.

Nach der Verabschiedung der Verordnung haben die betroffenen Unternehmen zwei Jahre Zeit, die geforderten Sicherheitsmaßnahmen einzuführen und deren Wirksamkeit durch ein Audit oder zum Beispiel eine geeignete Zertifizierung nachzuweisen.

## Was sind unsere Empfehlungen?

Das vorliegende Gesetz ist in vielen Punkten nicht bis ins Detail ausformuliert und wirft derzeit bei vielen unserer Mandanten Fragen darüber auf, ob und wie weit sie vom Gesetz betroffen sind und wie das Gesetz konkret umgesetzt wird. Wir empfehlen allen Unternehmen, die im weitesten Sinne zu den KRITIS-Branchen zu rechnen sind oder aber eng mit KRITIS-Unternehmen zusammenarbeiten, möglichst umgehend die vom Gesetz aufgeworfenen Risiken zu analysieren. Das empfiehlt sich auch für Unternehmen, die heute nicht unmittelbar unter die Regelungen des IT-Sicherheitsgesetzes fallen.

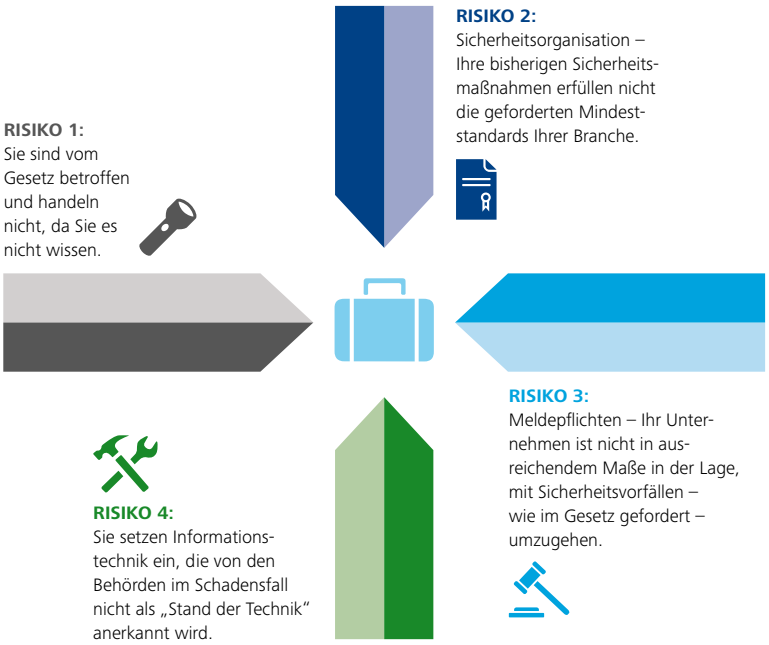
## Das Management von Unternehmen sollte Antworten auf die folgenden Risiken und Fragestellungen haben

**Risiko 1: Sie sind vom Gesetz betroffen und handeln nicht, da Sie es nicht wissen.**
Fällt Ihr Unternehmen unmittelbar oder ggf. mittelbar unter die Regelungen des Gesetzes? Welche weiteren Gesetze und Regelungen werden für Sie mit der Gesetzesänderung unter Umständen relevant?

**Risiko 2: Sicherheitsorganisation – Ihre bisherigen Sicherheitsmaßnahmen erfüllen nicht die geforderten Mindeststandards Ihrer Branche.**
Welche Sicherheitsstandards sind für Ihr Unternehmen maßgeblich? In welchem Umfang erfüllt Ihr Unternehmen heute diese Standards? Welche Maßnahmen haben Sie für die Zukunft vorgesehen?

**Risiko 3: Meldepflichten – Ihr Unternehmen ist nicht in ausreichendem Maße in der Lage, mit Sicherheitsvorfällen – wie im Gesetz gefordert – umzugehen.**
Ist Ihr Unternehmen in der Lage, aktuelle Sicherheitsvorfälle rechtzeitig zu erkennen, externe Warnmeldungen angemessen zu berücksichtigen und eigene Vorfälle rechtzeitig intern und extern weiterzugeben?

**Risiko 4: Sie setzen Informationstechnik ein, die von den Behörden im Schadensfall nicht als „Stand der Technik" anerkannt wird.**
Setzen Sie Sicherheitsmaßnahmen und -technologien ein, die dem sogenannten „Stand der Technik" entsprechen? Haben Sie das Thema Informationssicherheit in Ihrer Roadmap für die Weiterentwicklung Ihrer IT-Landschaft berücksichtigt? Kennen Sie die Auswirkungen auf bestehende vertragliche Verpflichtungen oder Versicherungen?



**Risiko 1: Sie sind vom Gesetz betroffen und handeln nicht, da Sie es nicht wissen.**

*Hintergrund*

Für viele Unternehmen wird das Gesetz unmittelbar relevant sein, da sie zu einer der bekannten KRITIS-Branchen gehören. Ob das einzelne Unternehmen dann den Regelungen des Gesetzes aber auch tatsächlich folgen muss, hängt insbesondere von der konkreten Ausgestaltung der Rechtsverordnung zum Gesetz ab. Ein Unternehmen ist dann betroffen, wenn die in der Verordnung festgelegten Schwellenwerte erreicht werden.

Eine Vielzahl von Unternehmen wird aber auch indirekt betroffen sein, da sie eine sehr enge Zusammenarbeit mit KRITIS-Unternehmen pflegen. Es ist davon auszugehen, dass KRITIS-Unternehmen zukünftig durch vertragliche Vereinbarungen eigene gesetzliche Verpflichtungen an Lieferanten und Partner weiterreichen werden.

**Das können Sie tun**

1. Klären Sie, ob Ihr Unternehmen aufgrund seiner Geschäftstätigkeit definitiv zu einer der KRITIS-Branchen gehört und die Schwellenwerte der Verordnung erreicht werden.
2. Analysieren Sie Ihre Geschäftsprozess- und IT-Landschaft: Welche Ihrer Prozesse und IT-Systeme sind kritisch unter den Gesichtspunkten des IT-Sicherheitsgesetzes? Welche davon sollten Teil eines ISMS werden (Anwendungsbereich/Scope)?
3. Ermitteln Sie die Auswirkungen auf Ihre Geschäftstätigkeit und die Ihrer externen Partner (Kunden, Lieferanten, verbundene Unternehmen), wenn als kritisch eingestufte Prozesse und Systeme ausfallen.

**Risiko 2: Sicherheitsorganisation – Ihre bisherigen Sicherheitsmaßnahmen erfüllen nicht die geforderten Mindeststandards Ihrer Branche.**

*Hintergrund*

Das Gesetz lässt unterschiedliche Mindestsicherheitsstandards für verschiedene Branchen zu. Diese sollen beispielsweise von den jeweiligen Branchenverbänden erarbeitet und vorgeschlagen sowie nachfolgend von den jeweiligen Aufsichtsbehörden sowie dem BSI freigegeben werden. Sie stellen die Untergrenze der zu erfüllenden Maßnahmen dar und werden im Zwei-Jahres-Rhythmus durch Audits überprüft.

**Das können Sie tun**

1. Klären Sie, welche Mindestsicherheitsstandards für Ihre Branche maßgeblich sind.
2. Analysieren Sie, inwieweit Sie die Mindeststandards heute erfüllen und an welchen Stellen Sie aktiv werden müssen (Feststellung des Reifegrads Ihrer Sicherheitsorganisation durch Gap-Analyse).
3. Stellen Sie sicher, dass kritische Prozesse und IT-Strukturen ausreichend im Risikomanagement des Unternehmens eingebunden sind. Hierbei hilft beispielsweise die Einführung eines ISMS.

**Risiko 3: Meldepflichten – Ihr Unternehmen ist nicht in ausreichendem Maße in der Lage, mit Sicherheitsvorfällen – wie im Gesetz gefordert – umzugehen.**

*Hintergrund*

Es liegt in der Natur der Sache, dass bei Sicherheitsvorfällen schnell reagiert werden muss. Besonders der schnelle und umfassende Austausch und die Verarbeitung von Informationen zu den Hintergründen und dem Ablauf der Vorfälle sind einer der Schlüsselfaktoren zur erfolgreichen Abwehr von Cyberangriffen im eigenen Unternehmen und bei den angeschlossenen Geschäftspartnern. Praktisch alle DAX-30-Unternehmen besitzen sogenannte CERTs (Computer Emergency Response Teams) bzw. haben ein SOC (Security Operation Center) aufgebaut oder sind in der konkreten Planung. CERTs sind in aller Regel über verschiedene Netzwerke miteinander verbunden und tauschen regelmäßig Sicherheitsvorfälle und sonstige Lageinformationen aus. Dies erfolgt allerdings bislang von einzelnen Unternehmen auf freiwilliger Basis. Im Gesetz ist zukünftig die verpflichtende Meldung von schwerwiegenden Vorfällen vorgesehen. Unternehmen sollten also in der Lage sein, die eigene aktuelle Sicherheitslage möglichst genau zu erfassen, Angriffe auf die eigenen Systeme festzustellen und umgehend zu reagieren sowie relevante Vorfälle an Partner, Branchenvertreter und ggf. Behörden weiterzugeben.

**Das können Sie tun**

1. Prüfen Sie, ob „Security as Service"-Lösungen für Ihr Unternehmen infrage kommen, falls der Aufbau eigener personeller Ressourcen und Strukturen unwirtschaftlich scheint.
2. Etablieren Sie eine Organisation (im Sinne eines CERT oder SOC), um Sicherheitsvorfälle festzustellen, zu dokumentieren und strukturiert abzuarbeiten. Erwägen Sie die Beschaffung eines Security-Information-&-Event-Mangement-(SIEM-)Systems.
3. Seien Sie grundsätzlich bereit, Informationen mit anderen zu teilen. Schaffen Sie auf der anderen Seite Voraussetzungen dafür, jederzeit Warnmeldungen von anderen entgegennehmen und verarbeiten zu können. Benennen Sie hierfür verantwortliche Ansprechpartner im Unternehmen.
4. Klären Sie für Ihre Organisation, welche Vorfälle unter die gesetzliche Meldepflicht fallen. Informieren Sie Ihre Mitarbeiter darüber und legen Sie entsprechende Verantwortlichkeiten, Meldewege und Abläufe fest.

**Risiko 4: Sie setzen Informationstechnik ein, die von den Behörden im Schadensfall nicht als „Stand der Technik" anerkannt wird.**

*Hintergrund*

Das IT-Sicherheitsgesetz fordert Unternehmen auf, zur Sicherung vor Cyberbedrohungen auf Systeme und Maßnahmen zurückzugreifen, die dem Stand der Technik entsprechen. Im Gesetz ist der Stand der Technik nicht genauer definiert, da dieser von Branche zu Branche variieren kann und sich darüber hinaus auch im Zeitverlauf regelmäßig weiterentwickelt. Neben der Vermeidung von Compliance-Risiken empfiehlt es sich ohnehin, die eingesetzte Informationstechnologie regelmäßig auf den Prüfstand zu stellen und das entsprechende Investitionsprogramm an aktuelle Anforderungen anzupassen, insbesondere auch aus dem Blickwinkel der Sicherheit.

**Das können Sie tun**

1. Prüfen Sie, ob die bei Ihnen eingesetzten Systeme aktuell empfohlene Sicherheitsfunktionen berücksichtigen.
2. Prüfen Sie regelmäßig, wie die Struktur der eigenen IT und IT-Sicherheit im Branchenvergleich zu sehen ist, ggf. durch einen Benchmark.
3. Nehmen Sie explizit Sicherheitsanforderungen in die Zielsetzungen Ihrer IT-Strategie auf und setzen Sie die Strategie konsequent um.
4. Berücksichtigen Sie Sicherheitsmaßnahmen mit der notwendigen Priorität in der IT-Investitionsplanung, im Projektportfolio und in der Roadmap für IT-Maßnahmen.

## Wie kann Deloitte helfen?

Das anstehende IT-Sicherheitsgesetz fordert von einer großen Anzahl von Unternehmen, ihr Cybersicherheitsniveau deutlich zu erhöhen und dies auch regelmäßig verlässlich nachzuweisen.

Deloitte unterstützt Unternehmen und Organisationen dabei, einen hohen Sicherheitsstandard zu erreichen. Unsere Dienstleistungen decken den gesamten Lebenszyklus einer Cybersicherheitsorganisation ab – von der Feststellung des Reifegrades und der Widerstandsfähigkeit über Bedrohungsanalysen und der Gestaltung von operativen Sicherheitsprozessen bis zum Vorfalls-Management.

Als Kunde profitieren Sie vom Branchen-Know-how unserer Berater – sei es bei der Entwicklung der Cyber-Strategie, dem Schwachstellen-Management oder bei der Aufarbeitung eines schwerwiegenden Cyberangriffs.

Beim Ethical Hacking und Penetration Testing setzen wir Szenarien-Techniken ein und zeigen mögliche Schwachstellen in Sicherheitssystemen auf. Wir stellen die Reaktionsprozesse Ihrer Organisation im Fall eines Cyber-Angriffs auf die Probe und helfen Ihnen, E-Spionage abzuwehren.

# Ihre Ansprechpartner


**Für mehr Informationen**

**Peter Wirnsperger**
Partner
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

**Peter Kestner**
Partner
Tel: +49 (0)89 29036 8064
pkestner@deloitte.de

**Dr. Andreas Knäbchen**
Partner
Tel: +49 (0)152 0900 7600
aknaebchen@deloitte.de


**Für weitere Informationen besuchen Sie unsere Webseite auf www.deloitte.com/de/cyber**




Stand 03/2015