DAS IT-SICHERHEITS-GESETZ

Was bedeutet es für Ihr Unternehmen? Ein Leitfaden

KASPERSKY lab

THE POWER OF PROTECTION

www.kaspersky.de

Immer mehr Cyberangriffe in Deutschland

Cyberattacken, Sicherheitslücken, Hackerangriffe: Wer erinnert sich nicht an die Cyberattacke auf den Bundestag im Juni 2015? Oder an den Bug namens „Stagefright", der im Juli 2015 zum Albtraum von Millionen Android-Nutzern wurde? Doch diese Fälle sind nur die Spitze des Eisbergs. Die meisten Sicherheitsschäden werden gar nicht erst publik gemacht.

Die Zahlen sind allerdings besorgniserregend: Deutschen Unternehmen sind in den letzten fünf Jahren Schäden von insgesamt 65,2 Milliarden Euro durch Internetattacken entstanden. Zu diesem Ergebnis kommt eine aktuelle Studie des Center for Economics and Business Research. Das bedeutet eine jährliche Schadenssumme für die deutsche Wirtschaft von rund 13 Milliarden Euro. Besonders stark betroffen ist die herstellende Industrie. Die Folgen: enorme Kosten für die jeweiligen Unternehmen – und ein nicht kalkulierbarer Imageschaden.

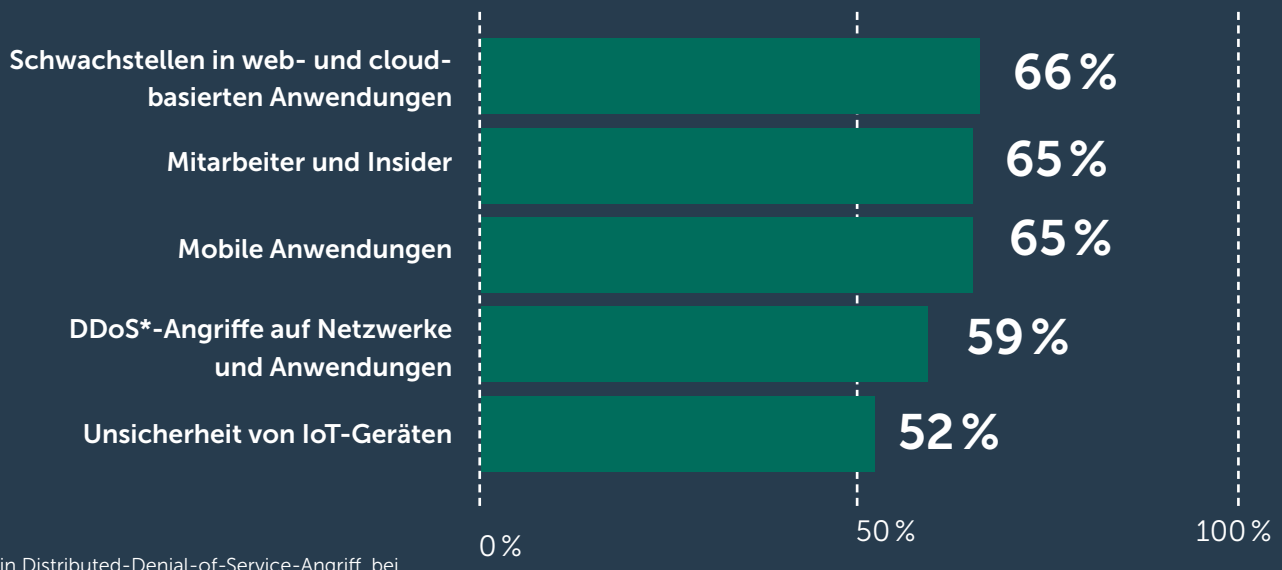
Der Grund für den massiven Anstieg von Hackerangriffen liegt in der Globalisierung der Datenströme, in der starken Vernetzung des Geschäfts, aber auch in der zunehmenden Digitalisierung der Industrie. Kurz: Die Industrie 4.0 birgt viele Chancen, aber auch einige Gefahren. Auch in Zukunft wird es immer mehr Sicherheitsrisiken geben. Das Internet of Things bietet neue Einfallstore für Hacker. Das zeigte unlängst der Hack eines Jeep Cherokee in den USA. Die Schwachstelle war das Entertainmentsystem des Wagens.

Web- und Cloud-Schwachstellen verursachen die größten Sorgen

- Sicherheit spielt bei der Anwendungsentwicklung keine große Rolle – daraus resultiert ein großes Risikopotenzial.
- **Zwei Drittel (66 %) der Unternehmen in Deutschland sind von Cyberattacken betroffen, die Sicherheitslücken in web- und cloudbasierten Anwendungen ausnutzen.**
- Die Anzahl der **kritischen Schwachstellen in Anwendungen** hat sich gegenüber dem Vorjahr **drastisch erhöht.**
- 2015 wurden bis **Ende September in nur 11 gängigen Anwendungen 847 kritische Schwachstellen identifiziert.***
- Die Informationssicherheit muss sich verändern, um den Anforderungen einer benutzer- und anwendungsorientierten Welt gerecht zu werden – durch die Integration von Anwendungssicherheit in Entwicklungs-, Test- und Einsatzphasen.

* Bundesamt für Sicherheit in der Informationstechnik (BSI). „Die Lage der IT-Sicherheit in Deutschland 2015"

Arten von Cyberattacken, die Unternehmen betreffen; Anteil der Unternehmen, die zumindest durch einen Angriff betroffen sind:



* DDoS ist ein Distributed-Denial-of-Service-Angriff, bei dem mehrere Systeme kompromittiert werden, um einen Denial-of-Service-Angriff auf ein einziges System durchzuführen.

Die Lösung: das IT-Sicherheitsgesetz

Die Lösung: strengere Sicherheitsstandards. Deshalb verabschiedete der Bundestag bereits im Juni 2015 das IT-Sicherheitsgesetz, das einen Monat später in Kraft getreten ist: Es soll die Sicherheit und den Schutz von IT-Systemen und -Diensten stärken. Und die digitale Infrastruktur Deutschlands zu einer der sichersten weltweit machen.

Die neue Rolle des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Als Folge des neuen IT-Sicherheitsgesetzes haben sich auch die Zuständigkeiten des BSI geändert. Nach dem durch das IT-Sicherheitsgesetz überarbeiteten BSI-Gesetz ist das Bundesamt für Sicherheit in der Informationstechnik die Meldestelle für sämtliche Informationen zu Sicherheitslücken und Cyberangriffen.

Das BSI:

- darf Protokolldaten und Angriffsmuster sammeln und auswerten, die in der Kommunikationstechnik des Bundes anfallen
- darf Informationen und Warnungen vor Sicherheitslücken in IT-Produkten und -Diensten an die Öffentlichkeit weitergeben
- darf Sicherheitsstandards für die Bundesverwaltung definieren und entsprechende Produkte für die Stellen des Bundes entwickeln lassen
- ist die zentrale Meldestelle für IT-Sicherheit und Ansprechpartner für Betreiber Kritischer Infrastrukturen (KRITIS)
- darf Bußgelder verhängen
- kann weitere Maßnahmen zum Schutz der IT-Sicherheit vornehmen

Was ist ein Betreiber Kritischer Infrastrukturen?

Betreiber Kritischer Infrastrukturen sind sämtliche Unternehmen aus bestimmten Sektoren, deren Einrichtungen oder Anlagen von hoher Bedeutung für das Funktionieren des Gemeinwesens sind. Ein Ausfall oder eine Störung würde erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit nach sich führen. Doch was sind die Anforderungen an Kritische Infrastrukturen? Das BSI hat dazu eine sogenannte KRITIS-Verordnung erlassen. Sie ist am 3. Mai 2016 in Kraft getreten und definiert, aufgeschlüsselt nach Sektoren, welche Unternehmen vom geänderten BSI-Gesetz betroffen sind. Recherchen haben ergeben, dass es in Deutschland bisher ca. 750 Unternehmen gibt, die unter die jetzige KRITIS-Verordnung fallen.

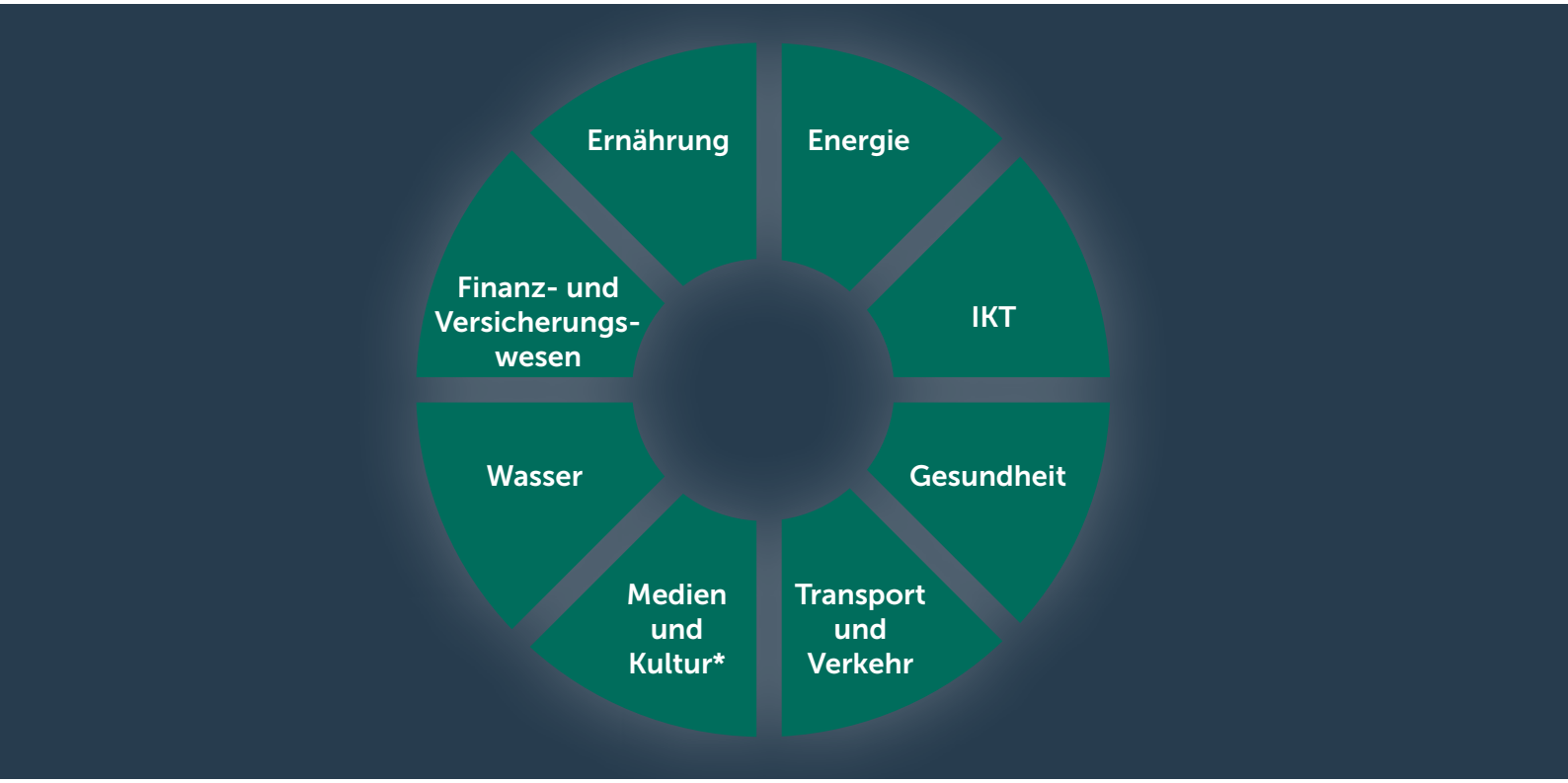
Betreiber Kritischer Infrastrukturen sind Unternehmen aus folgenden Sektoren:

- **ENERGIE**
- **WASSER**
- **ERNÄHRUNG**
- **INFORMATIONSTECHNIK UND TELEKOMMUNIKATION**

- **TRANSPORT UND VERKEHR**
- **GESUNDHEIT**
- **FINANZ- UND VERSICHERUNGSWESEN**

} Zu diesen Sektoren gibt es noch keine Qualifizierungskriterien. Sie werden für Anfang 2017 erwartet.

Nicht jedes Unternehmen qualifiziert sich als Betreiber von KRITIS. Dazu müssen, je nach Sektor, diverse Kriterien erfüllt bzw. Schwellenwerte erreicht werden.



Gehört Ihr Unternehmen auch zu den Kritischen Infrastrukturen?

Nur wer gewisse Schwellenwerte erreicht oder gewisse Dienste anbietet, fällt unter die Kategorie der Betreiber Kritischer Infrastrukturen:

ENERGIE

Strom

Für die Stromversorgung gilt: Ein Betreiber von Stromerzeugungsanlagen, -speicheranlagen, Stromsteuerungs- oder -bündelungsanlagen ist dann betroffen, wenn er einen Jahresschwellenwert (installierte Netto-Nennleistung) von 420 MW erreicht.

Für Stromübertragungsnetze gilt: Ein Betreiber von Übertragungs- und Verteilernetzen ist dann betroffen, wenn die durch den Verbraucher oder Weiterverteiler entnommene Arbeit 3.700 GWh pro Jahr beträgt.

Für Betreiber von Anlagen und Systemen für den Stromhandel (physischer kurzfristiger Spothandel auf dem deutschen Marktgebiet) gilt: ein Handelsvolumen an der Börse von 200 TWh pro Jahr.

Für Betreiber von Messstellen gilt: eine Leistung der angeschlossenen Verbrauchsstelle bzw. eine Einspeisung von 420 MW.

* Der Sektor „Medien und Kultur" wird in dem Zusammenhang zwar häufig erwähnt, ist aber im IT-Sicherheitsgesetz nicht als eigener Sektor Kritischer Infrastrukturen aufgeführt. Die Pflichten des BSI-Gesetzes finden auf Unternehmen dieses Sektors also auch keine Anwendung (es sei denn, sie fallen auch unter einen der anderen Sektoren).

ENERGIE

Gas

Für die Gasversorgung gilt: Ein Betreiber von Gasförderanlagen, Gasspeichern, Gasfernleitungs- und -verteilernetzen ist dann betroffen, wenn die Energie des geförderten Gases (Gasförderung), die entnommene Arbeit (Gasspeicherung) oder die entnommene Jahresarbeit (Gasfernleitung und -verteilung) 5.190 GWh pro Jahr entspricht.

Kraftstoff- und Heizöl

Für Betreiber von Ölförderanlagen und Mineralölfernleitungen gilt: ein Umschlag bzw. eine Förderung oder ein Transport von 4,4 Mio. Tonnen Rohöl pro Jahr.

Für Betreiber von Raffinerien gilt: eine Erzeugung von 420.000 Tonnen Kraftstoff pro Jahr bzw. 620.000 Tonnen Heizöl pro Jahr.

Für Betreiber von Tankstellennetzen gilt: 420.000 Tonnen verteilter Kraftstoff pro Jahr.

Für Betreiber von Öl- und Produktenlager gilt: ein Umschlag von 4,4 Mio. Tonnen Rohölmenge pro Jahr. Oder 420.000 Tonnen umgeschlagener Kraftstoff pro Jahr bzw. 620.000 Tonnen umgeschlagenes Heizöl pro Jahr.

Für Betreiber von Anlagen und Systemen von Aggregatoren zum Vertrieb von Kraftstoff gilt: 420.000 Tonnen verteilter Kraftstoff pro Jahr.

Fernwärme

Für Betreiber von Heizwerken und Heizkraftwerken gilt: Sie sind dann von der KRITIS-Verordnung betroffen, wenn die ausgeleitete Wärmeenergie 2.300 GWh pro Jahr beträgt.

Für Betreiber eines Fernwärmenetzes gilt der Schwellenwert von 250.000 angeschlossenen Haushalten.

WASSER

Abwasser

Für Betreiber von Kanalisationen (Siedlungsentwässerung), Abwasserbehandlung, Gewässereinleitung, Kläranlagen und Leitzentralen (Abwasserbehandlung und Gewässereinleitung) gilt ein Schwellenwert von 500.000 angeschlossenen Einwohnern (Kanalisationen) oder einer entsprechenden Ausbaugröße der Anlage (Kläranlage und Leitzentrale).

Trinkwasser

Für Betreiber von Gewinnungsanlagen, Wasserwerken, Aufbereitungsanlagen, Wasserverteilungssystemen sowie Leitzentralen gilt ein Schwellenwert von 22 Mio. Kubikmeter gewonnene Wassermenge (Gewinnungsanlage), Wasseraufkommen (Wasserwerk), aufbereitetes Trinkwasser (Aufbereitungsanlage), verteilte Wassermenge (Wasserverteilungssystem) bzw. gewonnene, transportierte oder aufbereitete Menge Wasser (Leitzentrale).

ERNÄHRUNG

Speisen

Für Betreiber von Anlagen zur Speisenproduktion, -bearbeitung und -verarbeitung sowie von Anlagen zu Lagerung, Distribution, Verkauf bzw. Bestellung von Speisen gilt ein Schwellenwert von 434.500 Tonnen Speisen pro Jahr. Darunter fallen z. B. Cash-und-Carry-Märkte, Supermärkte, Großschlachtereien, Tierställe, um nur einige zu nennen.

Getränke

Für Betreiber von Anlagen zur Getränkeproduktion, -bearbeitung und -verarbeitung sowie von Anlagen zu Lagerung, Distribution, Verkauf bzw. Bestellung von Getränken gilt ein Schwellenwert von 350 Mio. Liter Getränke pro Jahr.

INFORMATIONSTECHNIK UND TELEKOMMUNIKATION

Sprach- und Datenübertragung

Betreiber Kritischer Infrastrukturen sind all diejenigen, die ortsgebundene Zugangsnetze oder Übertragungsnetze bereitstellen (das gilt z. B. für öffentliche Telefondienste, Datenübermittlungsdienste bzw. Internetzugangsdienste, wie etwa Backbone- und Core-Netze) und gleichzeitig einen kritischen Schwellenwert von 100.000 Teilnehmeranschlüssen erreichen.

Betreiber von IXP für öffentlich zugängliche Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste fallen dann unter die KRITIS-Verordnung, wenn die Anzahl angeschlossener autonomer Systeme 300 im Jahresdurchschnitt erreicht.

Betreiber von DNS-Resolvern, die zur Nutzung öffentlich zugänglicher Dienste angeboten werden, sind dann von der KRITIS-Verordnung betroffen, wenn die Anzahl der abfragenden IP-Adressen im Jahresdurchschnitt 2,5 Mio. pro Tag erreicht. DNS-Server zur Nutzung öffentlich zugänglicher Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste sind dann betroffen, wenn die Anzahl der Domains, für die der Server autoritativ ist oder die aus der Zone delegiert werden, 250.000 beträgt.

Datenspeicherung und -verarbeitung

Rechenzentren sind von der KRITIS-Verordnung betroffen, wenn die vertraglich vereinbarte Leistung am 30. Juni eines Kalenderjahrs 5 MW beträgt.

Serverfarmen dagegen, wenn die Anzahl der laufenden Instanzen im Jahresdurchschnitt 25.000 beträgt.

Content-Delivery-Netzwerke sind betroffen, wenn das ausgelieferte Datenvolumen 75.000 TByte pro Jahr beträgt.

Anlagen zur Erbringung von Vertrauensdiensten (Trusted Third Party), wenn die Anzahl der ausgegebenen qualifizierten Zertifikate 500.000 beträgt oder die Anzahl der Zertifikate zur Authentifizierung öffentlich zugänglicher Server (z. B. TLS/SSL-Zertifikate) 10.000 beträgt.

TELEMEDIENDIENSTE

Einen Sonderfall stellen Anbieter von Telemedien dar. Das sind z. B. **Anbieter von mobilen Applikationen oder Webangeboten:** etwa Onlineshops, Websites von Freiberuflern oder werbefinanzierte Angebote.
Auch sie müssen dafür sorgen, dass die von ihnen genutzten IT-Systeme sicher sind. Und zwar unabhängig von Größe, Umsatz oder Datenverkehr. Es gilt also hier kein Schwellenwert.

Zu den grundlegenden Maßnahmen bei Betreibern von Webseiten und mobilen Apps gehört die Anwendung eines anerkannten Verschlüsselungsverfahrens.

Was müssen Sie tun?

Ihren Betrieb anmelden

Für Betreiber von KRITIS sieht das BSI eine Registrierung beim BSI vor. Das BSI teilt dem registrierten Unternehmen im Gegenzug sämtliche es betreffenden Informationen zu Gefahren für die IT-Sicherheit mit (Warnungen und Lageinformationen).

Eine Kontaktstelle benennen

KRITIS-Betreiber müssen eine Kontaktperson in ihrem Unternehmen nennen. Diese wird dann als Ansprechpartner für das BSI fungieren. Zusätzlich können KRITIS-Betreiber desselben Sektors eine übergeordnete zentrale Kontaktstelle benennen, die den Kontakt zum BSI halten wird.

ACHTUNG: Wenn Sie von der KRITIS-Verordnung betroffen sind, müssen Sie bis zum 3. November 2016 eine Kontaktstelle einrichten und sie dem BSI melden! Unter: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Was_tun/Kontaktstelle/kontakt.html

Sicherheitsstandards festlegen

Betroffene Unternehmen müssen dafür sorgen, dass die Systeme, Komponenten und Prozesse ihrer Kritischen Infrastruktur organisatorisch und technisch gegen Störungen gesichert sind. Dabei soll der Stand der Technik eingehalten werden. Die Definition dieser Sicherheitsstandards kann von KRITIS-Betreibern selbst bzw. von ihren Branchenverbänden für ihre Branche vorgeschlagen werden. Das BSI prüft diese auf Antrag und entscheidet, ob diese branchenspezifischen Sicherheitsstandards (B3S) den gesetzlichen Anforderungen genügen.

Sicherheitsstandards einführen

Sollte Ihre IT die erforderlichen Sicherheitsstandards nicht erfüllen, müssen Sie diese einführen und Ihr IT-System entsprechend aufrüsten.

ACHTUNG: Die Umsetzung geeigneter Mindestmaßnahmen muss spätestens zwei Jahre nach Inkrafttreten der KRITIS-Verordnung erfolgt und nachgewiesen sein. Das heißt spätestens im Mai 2018.

Störungen melden

Jeder KRITIS-Betreiber muss erhebliche Störungen umgehend über die eingerichtete Kontaktstelle an das BSI melden. Das gilt für Störungen, die zu einem Ausfall der Kritischen Infrastruktur geführt haben oder führen können. Dazu zählen: Störungen von Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit seiner IT-Systeme, Komponenten und Prozesse.

In diesem Fall müssen Sie:

- die Störung und die technischen Rahmenbedingungen beschreiben
- die Ursachen nennen
- die Branche nennen
- die von der Störung betroffene Technik und die Art der betroffenen Einrichtung oder Anlage benennen

Ein Musterbeispiel einer solchen Meldung finden Sie unter **http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Musterformular_Meldeformular.pdf?__blob=publicationFile**

Audits durchführen

Alle zwei Jahre muss ein Betreiber von KRITIS nachweisen, dass die von ihm getroffenen Maßnahmen zum Schutz der Kritischen Infrastruktur den gesetzlichen Anforderungen entsprechen. Das heißt, er muss interne Audits oder Prüfungen durchführen oder sich von einer externen unabhängigen Stelle zertifizieren oder prüfen lassen. Die durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen und die evtl. dabei festgestellten Sicherheitsmängel muss er dem BSI melden. Das BSI wird Kontrollen durchführen und kann die Vorlage der vollständigen Ergebnisse sowie die Beseitigung von Sicherheitsmängeln vom Betreiber der KRITIS verlangen.

Wer führt Audits durch?

Unabhängige Stellen wie der TÜV-Süd oder TÜV Rheinland beraten Betreiber von KRITIS bei der Erfassung und Bewertung von Sicherheitsrisiken. Außerdem zertifiziert die Prüfstelle Ihr Unternehmen nach ISO 27001. Das kann einen Teil der erforderlichen Sicherheitsmaßnahmen abdecken. Wie Sicherheitsaudits, Prüfungen und Zertifizierungen im Detail vonstattengehen, muss das BSI allerdings noch festlegen. Ebenso muss das BSI noch entscheiden, welche Anforderungen die Nachweise erfüllen müssen. Ebenso ist bisher offen, welche Kriterien die Stelle erfüllen muss, die diese Audits durchführen wird.

Bevor Sie einen Audit von einer externen Stelle durchführen lassen, können Sie schon im Vorfeld anhand eines **Selbst-Checks** feststellen, ob Ihre Infrastruktur Schwachstellen aufweist. Dazu hat das Kompetenzzentrum Kritische Infrastrukturen (KKI GmbH) einen Leitfaden mit Fragenkatalog erstellt:
http://www.kki-verein.de/Downloads/Fachtagungen/KKI_Handlungsempfehlung_IT-Sicherheit.pdf

ACHTUNG: Interne Sicherheitsaudits müssen mindestens alle zwei Jahre durchgeführt und nachgewiesen werden. Das erste Mal spätestens zwei Jahre nach Inkrafttreten der KRITIS-Verordnung, das heißt im Mai 2018.

Welche Kosten kommen auf Sie zu?

Die Kosten liegen immer beim Betreiber von KRITIS, das heißt bei Ihnen, falls Sie die Kriterien erfüllen.

Kosten fallen an, wenn:

- eine interne Meldestelle eingerichtet wird
- technische und organisatorische Maßnahmen zum Schutz der Kritischen Infrastruktur getroffen werden müssen
- regelmäßige Sicherheitsaudits, Prüfungen oder Zertifizierungen durchgeführt werden
- eine Störung beseitigt werden muss

Quellen:

http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/Kritis/neue_Sektoreneinteilung.pdf
https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/BSI_Kritis_VO.pdf?__blob=publicationFile&v=3
http://www.tuev-sued.de/anlagen-bau-industrietechnik/technikfelder/risikomanagement/kritische-infrastrukturen

Was, wenn Sie sich nicht an die Verordnung halten?

Bei Verstößen drohen Bußgelder, und zwar in erster Linie in den folgenden Fällen:

- falls KRITIS-Betreiber nicht umgehend ordnungsgemäß melden, wenn eine erhebliche Störung ihrer Kritischen Infrastruktur auftritt
- falls KRITIS-Betreiber die Sicherheit ihrer IT-Systeme nicht rechtzeitig auf den Stand der Technik bringen und auf diesem Stand halten
- falls KRITIS-Betreiber die erforderliche Kontaktstelle nicht oder nicht rechtzeitig benennen.
- falls Anbieter von Telemediendiensten diese nicht durch zumutbare Sicherheitsmaßnahmen gegen unerlaubte Zugriffe und Angriffe schützen

Betreiber von KRITIS können außerdem dazu verpflichtet sein, Kunden Schadenersatz zu zahlen, falls diese durch nachlässige Sicherheitsstandards geschädigt wurden.

Die Höhe der Bußgelder variiert: **bis zu 50.000 Euro** bei Anbietern von Telemediendiensten (Websites oder mobilen Apps) und **bis zu 100.000** für die Betreiber von KRITIS.

Und was macht der Rest Europas? Die NIS-Richtlinie

Nicht nur in Deutschland ist man sich des Problems Cybersicherheit bewusst. Im August 2016 ist eine EU-Richtlinie in Kraft getreten, die gemeinsame Sicherheitsstandards festlegt: die NIS-Richtlinie (Netz- und Informationssicherheit in der Union). Die EU verpflichtet damit die Mitgliedstaaten, Betreiber kritischer Dienste festzustellen. Und binnen 21 Monaten – also bis Mai 2018 – die Richtlinie in nationales Recht umzusetzen.

Außerdem regelt die NIS-Richtlinie die Zusammenarbeit der Mitgliedstaaten auf dem Gebiet der Cyber-Security. Experten gehen derzeit davon aus, dass die NIS-Richtlinie kaum Auswirkungen auf die in Deutschland geltenden Gesetze zur IT-Sicherheit haben wird, da diese den Großteil der Anforderungen der NIS-Richtlinie ohnehin bereits erfüllen.

Hinweis zur Nutzung dieses Ratgebers:

Dieser Ratgeber enthält eine allgemeine und verkürzte Darstellung wesentlicher gesetzlicher Änderungen durch das IT-Sicherheitsgesetz und die KRITIS-Verordnung, insbesondere zur Qualifizierung als KRITIS-Betreiber. Der Leser soll damit in die Lage versetzt werden, die rechtlichen Hintergründe und Anforderungen besser zu verstehen.

Die Darstellung ist deswegen stark vereinfacht und auf bestimmte, häufig adressierte Aspekte beschränkt. Der Ratgeber stellt also nicht alle Rechtsfragen vollständig oder abschließend dar und ersetzt keineswegs eine einzelfallbezogene Prüfung individueller Rechtsverhältnisse.

Der Leitfaden wurde von der Anwaltskanzlei SKW Schwarz Rechtsanwälte erstellt. SKW Schwarz ist eine unabhängige deutsche Anwaltskanzlei. Sie berät Unternehmen auf allen wesentlichen Gebieten des nationalen und internationalen Wirtschaftsrechts. Ein besonderer Beratungsschwerpunkt ist der Bereich IT und Digital Business. Verfasser sind Stefan C. Schicker, LL.M. – s.schicker@skwschwarz.de und Dr. Daniel Meßmer – d.messmer@skwschwarz.de.

KASPERSKY lab