
Bild: Shutterstock / chombosan

Kritische Infrastrukturen (KRITIS)

# Das neue IT-Sicherheitsgesetz und seine Folgen

Was Unternehmen im eigenen Rechenzentrum und in der Cloud jetzt beachten müssen.

Am 25. Juli 2015 ist in Deutschland ein neues IT-Sicherheitsgesetz in Kraft getreten. Nun ist die zweijährige Übergangszeit abgelaufen und es wird ernst – für weit mehr Unternehmen als zunächst abzusehen war. Betroffen sind außer den klassischen Betreibern kritischer Infrastrukturen, den sogenannten KRITIS – etwa Energieversorger –, nämlich auch viele IT- und TK-Anbieter, Banken, Versicherungen, Logistikunternehmen, Lebensmittelhändler oder Verlagshäuser. Sie alle sind nach Ansicht der Bundesregierung für das Land von großer Bedeutung und bedürfen daher eines besonderen Schutzes – und besonderer Auflagen mit teils erheblichen Auswirkungen auf den Betrieb ihrer IT.

Das neue IT-Sicherheitsgesetz soll nichts weniger als die „IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit" machen. Das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme", so der vollständige Name, verpflichtet jeden Betreiber einer kritischen Infrastruktur, seine IT-Systeme „angemessen zu sichern" beziehungsweise auf den jeweiligen „Stand der Technik" zu bringen. Zudem sieht das Gesetz eine Meldepflicht bei schweren Vorkommnissen und „erheblichen IT-Sicherheitsvorfällen" vor. Bei Nichtbefolgen drohen empfindliche Strafen.

**51 Mrd.**
**Euro Schaden entsteht der deutschen Wirtschaft pro Jahr durch digitale Angriffe**

Quelle: Bitkom Research 2015

## Mehr Sicherheit fürs ganze Land

Das erklärte Ziel des neuen IT-Sicherheitsgesetzes ist nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI), das mit ihm deutlich mehr Befugnisse erhalten

hat, vor allem „die Verbesserung der IT-Sicherheit bei Unternehmen und in der Bundesverwaltung sowie ein besserer Schutz der Bürgerinnen und Bürger im Internet“.

So gelten manche Regelungen des Gesetzes auch für Betreiber von kommerziellen Webangeboten, die nach Ansicht der Bundesregierung ebenfalls „höhere Anforderungen an ihre IT-Systeme erfüllen müssen“. Das heißt, sie müssen nun für „technische und organisatorische Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme“ sorgen.

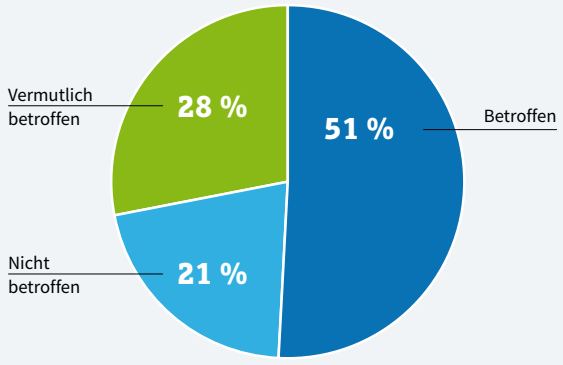
Darüber hinaus sind TK-Anbieter künftig stärker gefordert, da sie verpflichtet werden, „ihre Kunden zu warnen, wenn sie einen Missbrauch eines Kundenanschlusses feststellen“. Das kann zum Beispiel der Fall sein, wenn Kundenrechner als Teil eines Bot-Netzes missbraucht werden und dies dem TK-Anbieter bekannt wird. Aber nicht nur das. Sie sollen den Kunden auch „auf mögliche Wege zur Beseitigung der Störung hinweisen“.

Zusätzlich trat am 30. Juni 2017 das „Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit“ in Kraft. Die sogenannte NIS-Richtlinie der EU definiert „Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der europäischen Union“.

Die Richtlinie soll nicht nur einen einheitlichen Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cybersicherheit darstellen. Sie soll auch eine stärkere Zusammenarbeit der Mitgliedsstaaten gewährleisten. Zudem legt sie Mindestsicherheitsanforderungen und Meldepflichten für die Betreiber kritischer Infrastrukturen sowie für bestimmte Anbieter digitaler Dienste wie Cloud-Services, Suchmaschinen und Online-Marktplätze fest.

Das Bundesinnenministerium geht nach eigenen Angaben davon aus, dass hierzulande zwischen 500 und 1500 Firmen von der NIS-Richtlinie betroffen sind, die ab Mai 2018 in nationales Recht umzusetzen ist. Das BSI soll künftig als Kontrollinstanz prüfen, ob die neuen Auflagen auch eingehalten werden.

## Digitale Angriffe auf Unternehmen




**Betroffen:** Jedes zweite Unternehmen war binnen zwei Jahren mindestens einmal Opfer eines digitalen Angriffs.

**com! professional** 11/17 Quelle. Bitkom Research 2015

Bild: Bitkom

**„Nur Virenscanner und Merkblätter reichen für gelebte IT-Sicherheit nicht aus.“**

**Bernd Rohleder**
Hauptgeschäftsführer
Bitkom e. V.
**www.bitkom.org**

„Die NIS-Richtlinie schafft einen einheitlichen Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für Cybersicherheit“, kommentierte Arne Schönbohm, amtierender Präsident des BSI, die Umsetzung der Richtlinie in deutsches Recht. „Wie wichtig das ist, haben zuletzt die Cyberangriffe mit Ransomware wie WannaCry oder Petya gezeigt, die im globalen Maßstab Schäden verursacht haben.“

Bedenken hinsichtlich zu stark ausgeweiteter Rechte und Möglichkeiten des Bundesamts versuchte Schönbohm bereits im Vorfeld zu zerstreuen: „Wir werden diese Befugnisse auch in Zukunft in guter und vertrauensvoller Zusammenarbeit mit unseren Partnern in Staat, Wirtschaft und Gesellschaft ausüben und dafür sorgen, dass das IT-Sicherheitsniveau in Deutschland weiter steigt.“ Dies sei eine „notwendige Voraussetzung für eine erfolgreiche Digitalisierung“, so Schönbohm.

## Cyberfeuerwehr

Aber wie kann das BSI Unternehmen beim Schutz vor Cyberangriffen unterstützen? Nach eigenen Angaben hat die Behörde dazu mehrere sogenannte Mobile Incident Response Teams (MIRTs) eingerichtet, die aus etwa 20 Experten bestehen. Diese Teams sollen besonders schwerwiegende Cyberattacken vor Ort untersuchen und bei deren Bewältigung helfen – bislang nur auf Wunsch der betroffenen Unternehmen.

Als Beispiel für diese Art von Einsätzen nennt das BSI etwa einen „Cyberangriff, der wichtige IT-Steuerungen eines Kraftwerks lahmlegt“. Aber auch eine „Attacke auf eine Chemieanlage, bei der von einer großen Gefährdung der Bevölkerung auszugehen ist“, könnte den Einsatz eines MIRT rechtfertigen. Laut Medienberichten sollen die MIRTs auch weitere Mitarbeiter des BSI einbeziehen können, sofern es die Lage erfordert.

Zwar ist die Hoffnung des BSI, dass Unternehmen Vertrauen fassen und die Experten bei einem schwerwiegenden Cyberangriff selbst rufen, letztlich sei aber auch denkbar, dass die MIRTs irgendwann das Recht erhalten, von sich aus tätig zu werden. Vielen Unternehmen, die auch in Notfällen keine externen Zugriffe auf ihre IT haben wollen, dürfte das nicht recht sein. So kennen die BSI-Experten in der Regel nicht die Infrastruktur des betroffenen Unternehmens und haben nur wenig Einblick in interne Abläufe und Prozesse. Mehr als vergleichsweise oberflächliche Hilfen dürften deswegen in vielen Fällen kaum möglich sein. Wie viele Einsätze bereits erfolgten und wo sie stattfanden, das wollte ein Sprecher des BSI „aus Gründen der Vertraulichkeit“ nicht bekannt geben. Mehr als die Aussage, dass „die bestehenden MIRTs anlassbezogen eingesetzt“ werden und dass ▶

sie „derzeit erweitert und ausgebaut“ werden, war nicht zu erfahren.

## Die KRITIS-Branchen

Bei Inkrafttreten des IT-Sicherheitsgesetzes, war noch nicht endgültig klar, wer neben Energielieferanten, TK-Anbietern und Wasserversorgern noch zu den KRITIS gehört. Mittlerweile hat das Bundesministerium des Inneren (BMI) nachgelegt und eine „Definition Kritische Infrastrukturen“ veröffentlicht (siehe auch die Tabelle auf Seite 21).

Diese Definition stuft neun Sektoren und knapp 30 Branchen als kritische Infrastrukturen ein. Neben Versorgern aus den Bereichen Energie, Gas, Mineralöl und Wasser/Abwasser zählen dazu IT- und TK-Anbieter, Fluglinien, Speditionen, Logistikunternehmen, der Lebensmittelhandel, Behörden, Justizeinrichtungen, Rettungsdienste sowie der Katastrophenschutz, Krankenhäuser, Labore, Banken, Börsen, Versicherungen und andere Finanzdienstleister, aber auch Fernseh- und Radiosender sowie die gedruckte und elektronische Presse und sogar Kulturgüter und sogenannte symbolträchtige Bauwerke. Sie alle sind vom neuen IT-Sicherheitsgesetz betroffen. Wann und in welchem Umfang, wird durch Verordnungen festgelegt.

So ist im Mai 2016 der erste Teil der „BSI-Kritisverordnung“ zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten. Betroffen sind die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung. Im Juni 2017 wurden mit Hilfe einer weiteren Verordnung die Sektoren Finanz- und Versicherungswesen, Gesundheit sowie Transport und Verkehr hinzugefügt.

## Übergangsfristen

Unternehmen aus diesen Branchen haben nach Inkrafttreten der Verordnungen zwei Jahre Zeit, die „für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern“, so das BSI. Diese Sicherheit soll dann zudem alle zwei Jahre überprüft werden. Außerdem müssen die Unternehmen dem BSI „binnen sechs Monaten“ eine „Kontaktstelle für Vorfallsmeldungen“ nennen.

Bild: Airbus

**„Eine sicherheitstechnische Bestandsaufnahme ist unumgänglich, um den digitalen Wandel auf eine solide Basis zu stellen.“**

**Michael Gerhards**
Managing Director Germany bei Airbus Cyber Security
**www.cybersecurity-airbusds.com/de**

Bei nicht fristgerechter Erfüllung der Vorgaben drohen Bußgelder in Höhe von bis zu 100.000 Euro. Betreiber von Webseiten, also fast alle vom IT-Sicherheitsgesetz betroffenen Unternehmen in Deutschland, müssen nun darauf achten, dass auf ihren Webservern keine veralteten und angreifbaren Software-Versionen mehr laufen. Stattdessen sollen sie „regelmäßig und rasch“ Software-Updates und Sicherheits-Patches einspielen, empfiehlt das BSI. Nicht kommerzielle Webseiten von Privatpersonen und Vereinen sind davon nach Angaben des Bundesamts nicht betroffen. Anders sieht es aus, wenn „mit der Webseite dauerhaft Einnahmen generiert werden sollen“. Das sei bereits der Fall, wenn auf der Webseite bezahlte Werbung in Form von Bannern platziert werde.

## Stand der Technik

Wer sich mit den Vorgaben durch das IT-Sicherheitsgesetz befasst, stößt immer wieder auf den „Stand der Technik“, der von den betroffenen Unternehmen einzuhalten sei. Was ist darunter zu verstehen?

Unternehmen müssen wie erwähnt spätestens zwei Jahre nach Inkrafttreten der für sie geltenden Verordnung gegenüber dem BSI nachweisen können, dass sich ihre informationstechnischen Systeme auf dem „Stand der Technik“ befinden. Der Nachweis kann entweder durch Sicherheits-Audits oder andere Überprüfungen erfolgen, die dem BSI inklusive der dabei ermittelten Sicherheitsmängel zu übermitteln sind.

Das Problem dabei ist jedoch, dass der Stand der Technik keine messbare Größe ist, sondern nicht mehr als ein allgemeiner Grundsatz für die Festlegung geeigneter Maßnahmen zur Absicherung eines Unternehmens. Welche das genau sein können, ist aber für viele Branchen noch nicht geklärt. Daher sind die betroffenen Unternehmen verunsichert.

Das BSI verweist auf die Arbeitskreise im UP KRITIS (Umsetzungsplan KRITIS, mehr dazu im Abschnitt „Ratgeber“), die sogenannte B3S verfassen können. Die Abkürzung B3S steht für „branchenspezifische Sicherheitsstandards“. Eine gesetzliche Pflicht zu ihrer Erarbeitung besteht jedoch nicht. Für die Unternehmen bedeutet dies, dass sie eine Vielzahl allgemeiner und branchenspezifischer Normen einzuhalten haben und dies auch dokumentieren müssen.

Der Bundesverband IT-Sicherheit e. V. (Teletrust) hat einen eigenen Arbeitskreis zum „Stand der Technik“ gegründet, der Handlungsempfehlungen und Orientierungen für Unternehmen verfassen soll. Vom BSI fordert der Verband mehr Transparenz bei seinen Kriterien. Unternehmen benötigten ein „solides Handwerkszeug“, da es sich bei „Stand der Technik“ nur um einen „unbestimmten Rechtsbegriff“ handele.

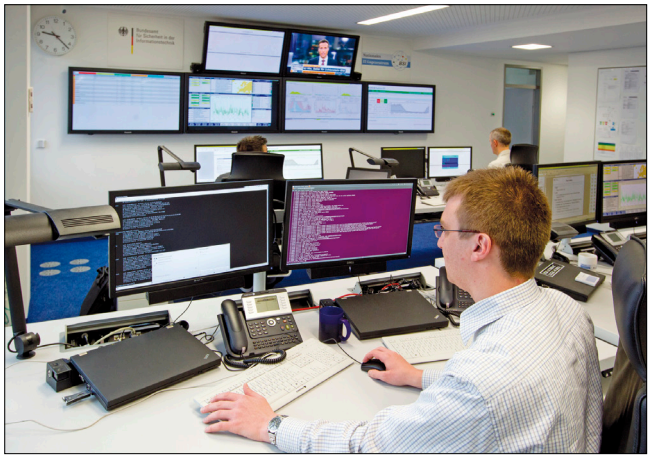


Bild: BSI

**Ansprechpartner für Notfälle:** Das vom BSI betriebene nationale IT-Lagezentrum steht rund um die Uhr zur Verfügung.

## Pro und Contra

Angesichts der komplexen Materie ist es nicht verwunderlich, dass die Meinungen über das Sicherheitsgesetz auseinandergehen. Kritisch äußert sich zum Beispiel Felix Freiling von der Friedrich-Alexander-Universität Erlangen-Nürnberg. Dem TV-Sender 3Sat sagte er, dass das „IT-Sicherheitsgesetz im Wesentlichen ein Gesetz für den Staat" sei. Dieser erhalte dadurch einen besseren Überblick über das, was in kritischen Infrastrukturen passiert, und wisse so schneller und früher Bescheid über die Bedrohungen. Schutz davor, dass etwa Hacker das Stromnetz lahmlegen, bietet das IT-Sicherheitsgesetz nach Ansicht von Freiling jedoch nicht.

Ähnlich sieht es Linus Neumann vom Chaos Computer Club (CCC). In einer Stellungnahme zum IT-Sicherheitsgesetz äußerte sich der CCC-Sprecher so: „Nicht eine einzige der im Gesetzesentwurf vorgeschlagenen Maßnahmen ist zielführend, um die IT-Sicherheit tatsächlich zu erhöhen." Der nun „vorgesehene enorme Bürokratieaufwand" sei nicht nur „zeitaufwendig und in der Sache nutzlos". Das IT-Sicherheitsgesetz halte sogar von wirklich sinnvollen Maßnahmen ab.

Der frühere BSI-Präsident Michael Hange mag dem nicht zustimmen. „Ich bin davon überzeugt, dass sich die Herausforderungen der IT-Sicherheit auch in Zukunft nur kooperativ lösen lassen." Cybersicherheit entstehe durch das Zusammenwirken aller Akteure.

Hange ist außerdem der Meinung, dass „ein rein freiwilliger Ansatz nicht immer zum nötigen Engagement in der Wirtschaft führt und nicht flächendeckend beziehungsweise in allen sicherheitsrelevanten Bereichen wirkt". Die gesetzlichen Vorgaben sollten deswegen „das IT-Sicherheitsniveau der Betreiber kritischer Infrastrukturen und damit die Netzsicherheit erhöhen".

Aus Sicht des BSI ermöglicht die Meldepflicht zudem bessere Lagebilder. Ohne Druck scheint sich dieses Ziel aber nicht erreichen zu lassen. So wies etwa Holger Junker, Leiter des BSI-Referats „Cybersicherheit in kritischen IT-Systemen, Anwendungen und Architekturen" darauf hin, dass man nach Erfahrung der Behörde mit einer freiwilligen Meldepflicht nicht weit komme.

> **„Bei uns gibt es sehr viel zu holen."**
>
> **Holger Junker**
> Referatsleiter Cybersicherheit beim BSI
> **www.bsi.de**

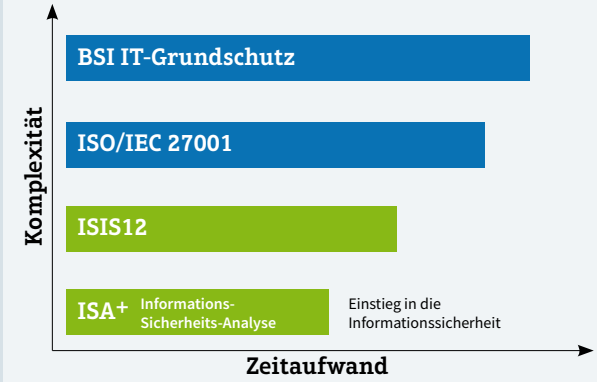
## Ratgeber

Hilfen und Orientierung bietet Unternehmen der UP KRITIS, eine Kooperation aus staatlichen Stellen und KRITIS-Betreibern. Nach Angaben des BSI sind mehrere Hundert Organisationen im UP KRITIS aktiv. Sie nutzen die öffentlich-private Kooperation unter anderem, um sich über aktuelle Vorkommnisse zu informieren, um gemeinsame Positionen zu erarbeiten und um Notfall- und Krisenübungen durchzuführen. Damit unterstützt der UP KRITIS die teilnehmenden Unternehmen dabei, die Vorgaben des neuen IT-Sicherheitsgesetzes zu erfüllen. So können sich ihre Mitarbeiter etwa an Arbeitskreisen beteiligen und Einfluss auf verschiedene Aspekte nehmen, die dann wiederum das Tagesgeschäft im Unternehmen und anderen Firmen aus der jeweiligen Branche oder sogar darüber hinaus beeinflussen können.

Aktuellstes Ergebnis dieser Bemühungen sind die „Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken", die Ende Juli dieses Jahres veröffentlicht wurden. Sie können ohne Registrierung von jedem Unternehmen kostenlos heruntergeladen werden.

Der sechzehnseitige Ratgeber wurde vom UP-KRITIS-Arbeitskreis „Medizinische Versorgung" verfasst. Er enthält zahlreiche konkrete Empfehlungen für die Nutzung so- ▶

### Regelwerke für IT-Sicherheit




**Hohe Anforderungen:** Komplexität und Zeitaufwand sind beim IT-Grundschutz des BSI am größten.

**com! professional** 11/17 Quelle: Bayerischer IT-Sicherheitscluster

### Kritische Infrastrukturen*

| Sektor | Betroffene Branchen |
|---|---|
| **Energie** | Elektrizität, Gas, Mineralöl |
| **Informationstechnik und Telekommunikation** | Informationstechnik, Telekommunikation |
| **Transport und Verkehr** | Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik |
| **Gesundheit** | Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore |
| **Wasser** | Öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung |
| **Ernährung** | Ernährungswirtschaft, Lebensmittelhandel |
| **Finanz- und Versicherungswesen** | Banken, Börse, Versicherungen, Finanzdienstleister |
| **Staat und Verwaltung** | Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/Rettungswesen einschließlich Katastrophenschutz |
| **Medien und Kultur** | Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke |

*Das Bundesinnenministerium hat neun Sektoren und knapp 30 Branchen definiert, die es als „kritisch" für die Sicherheitslage einschätzt und die deswegen vom neuen IT-Sicherheitsgesetz betroffen sind


Schichtwechsel !
Multidimensional mit neuen Intel®-Prozessoren
©ANDREY KISELEV – stock.adobe.com SCHACHTZEICHEN 2010 ©Stefan Ziese
TARGOX
SecurityAllianz
ERLEBEN SIE DEN VIERMALIGEN
BESTEN HERSTELLER DES JAHRES
MIT SEINER SECURITY ALLIANZ
AUF DER ITSA 2017 !
Halle 10.1, Standnummer 416
CRN
2016
Bester
Hersteller
15
14
13
Intel Inside®. Neue Möglichkeiten Outside.
Mehrfach ausgezeichnete Serversysteme
Intel, das Intel Logo, Xeon, und Xeon Inside sind Marken der Intel Corporation in den USA und anderen Ländern.


intel XEON PLATINUM inside™

© interemotion.com

# Wechseln Sie jetzt zur neuesten Generation TAROX Server mit Intel® Xeon® Platin-Prozessor

- Maximale Performance für Ihre Applikation mit hoch skalierbarer Architektur
- Flexible interne Datenspeicherkonfigurationen
- Integrierte Sicherheitsfunktionen zum Schutz der Hardware
- Neuste Generation der Netzwerkkomponenten für einen effizienteren Datentransfer
- Optimiertes Energie- und Temperaturmanagement
- Verbessertes Ressourcenmanagement

Diesen Artikel finden Sie unter **www.tarox.de**



TAROX

IT-Technologie made im Ruhrgebiet

TAROX Aktiengesellschaft | Stellenbachstr. 49–51 | 44536 Lünen | Telefon: +49 (0)231/98 98 0-300 | vertrieb@tarox.de

wohl in eigenen Rechenzentren als auch in Cloud-Infrastrukturen, deren „Umsetzung für Kliniken mit einem überschaubaren Aufwand möglich“ sein soll. Dem Arbeitskreis war es dabei wichtig, deutlich zu machen, dass es sich bei den besonderen Anforderungen an die IT-Sicherheit um kein reines IT-Thema handelt. Die Absicherung der Dienstleistungen erfordere „Konzepte und Verfahrensrichtlinien, die über die jeweiligen IT-Abteilungen hinausreichen“. Insbesondere müsse die Verantwortlichkeit dafür in der Nähe der Geschäftsführung angesiedelt werden, etwa indem eine Stabsstelle mit einem Beauftragten für Informationssicherheit geschaffen werde.

Neben dem UP KRITIS arbeiten auch viele Unternehmen und spezialisierte Dienstleister an ganzheitlichen Sicherheitsstrategien, die auf wiederkehrenden beziehungsweise anlassbezogenen Risikoanalysen basieren. Ein Beispiel ist Airbus Cyber Security. Nach Aussage von Michael Gerhards, Managing Director Germany bei Airbus Cyber Security, ist das Ziel dabei, jeweils die fünf Top-Risiken für ein Unternehmen in direkter Zusammenarbeit mit seinen IT- und Produktionsteams zu identifizieren und dann geeignete Gegenmaßnahmen zu empfehlen.

Zu den konkreten Maßnahmen kann unter anderem der Aufbau von sicheren Remote-Zugängen für Wartung und Analyse gehören, eine Absicherung des Produktionsverbunds und eine Überwachung von mit Schwachstellen behafteten Altsystemen durch passive Security-Sensoren sowie eine Sicherung von Endpoints, Datenbanken, Servern, USB-Sticks und CDs. Airbus Cyber Security will die Unternehmen zudem mit einem Wissenstransfer und dem Aufbau einer kontinuierlichen Risikoanalyse unterstützen.

„Vor dem Hintergrund von Industrie 4.0 und IoT (Internet of Things) ist eine sicherheitstechnische Bestandsaufnahme unumgänglich, um den digitalen Wandel auf eine solide Basis zu stellen“, so Gerhards. Die Absicherung ihrer Produktionsanlagen sei „gerade für Hochtechnologieunternehmen eine komplexe Herausforderung mit zuweilen hohem Kostenaufwand“. Gerhards empfiehlt deswegen, unbedingt erst ein Security-Assessment durchführen zu lassen. „Dieses dient als sinnvoller Einstiegspunkt und ist der Grundstein für alle weiteren Handlungsempfehlungen sowie den Aufbau einer langfristigen Sicherheitsstrategie.“


Bild: BSI

**Mehr Macht:** Das BSI hat mit Inkrafttreten des neuen IT-Sicherheitsgesetzes etliche neue Aufgaben und Befugnisse erhalten.

Hilfreich kann zudem die Einführung eines Informations-Sicherheitsmanagement-Systems (ISMS) sein, wie es etwa der Bayerische IT-Sicherheitscluster mit ISIS12 beschreibt. Darin sind zwölf Schritte definiert, die ein Unternehmen einhalten muss, um ein ISMS zu implementieren, das die gesetzlichen Vorgaben erfüllt – und damit sehr viel weniger als das Grundschutz-Regelwerk des BSI. ISIS12 soll viel besser auf die Bedürfnisse mittelständischer Firmen zugeschnitten sein, die in der Regel nicht über so umfangreiche Ressourcen verfügen wie Großunternehmen oder Bundesbehörden.

## Exemplarische Prüffragen

IT-Abteilungen, die ihr Unternehmen an die Vorgaben des neuen IT-Sicherheitsgesetzes anpassen wollen, sollten sich eine Reihe von Prüffragen stellen, die der Arbeitskreis Medizinische Versorgung im UP KRITIS exemplarisch formuliert hat. Eine Auswahl:

1. Ist ein unterbrechungsfreier Server-Betrieb gewährleistet?
2. Gibt es eine Datensicherung der Server und wird sie regelmäßig überprüft?
3. Ist ein Langzeitarchiv im Unternehmen etabliert?
4. Ist der Personenkreis der Administratoren eingegrenzt?
5. Sind die Datenzugriffsmöglichkeiten auf das erforderliche Mindestmaß beschränkt?
6. Sind die Regeln der Firewall klar definiert und grenzen sie den Netzwerkverkehr auf den jeweiligen Anwendungsfall ein?
7. Werden VLANs im Netzwerk genutzt? Sind sie klar definiert?
8. Wie sind die Netzwerke vor unbefugter Nutzung geschützt?
9. Sind die nach außen angebotenen Daten, Dienste und Programmfunktionen auf das erforderliche Mindestmaß beschränkt?
10. Erfolgt der Datenaustausch nur über vertrauenswürdige Kanäle?
11. Werden Störungen an die verantwortlichen Personen automatisiert gemeldet?
12. Ist ein Malware-Schutz zugelassen und aktiviert?
13. Existiert für die Anwendungen und Systeme jeweils ein Rechte- und Rollenkonzept?
14. Sind die Administratorenteams redundant ausgelegt?
15. Werden ausgeschiedene Mitarbeiter zeitnah gesperrt?

Diese und weitere Prüffragen finden sich in den „Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken“ unter www.kritis.bund.de/SubSites/Kritis/DE/Aktuelles/Meldungen/170816_Handlungsempfehlung_Kliniken.html.

Als Ansprechpartner beim BSI dient auch das nationale IT-Lagezentrum, das vom Bundesamt betrieben wird. Mit den strategischen Zielen „Prävention, Reaktion und Nachhaltigkeit“ hat es folgende Aufgaben:

- Erkennen, Erfassen und Bewerten von Vorfällen
- Informieren, Alarmieren und Warnen
- Reagieren bei IT-Sicherheitsvorfällen.

Das IT-Lagezentrum steht KRITIS-Unternehmen, Bundesbehörden und Partnern nach Angaben des BSI rund um die Uhr mit mindestens einer Fachkraft zur Verfügung.

## Fazit und Ausblick

„Nur Virenscanner und Merkblätter reichen für eine gelebte IT-Sicherheit nicht aus“, sagte Bernhard Rohleder, Hauptgeschäftsführer des Digitalverbands Bitkom, bei der Vorstellung des „Praxisleitfadens IT-Sicherheitskatalog“, den der Verband zusammen mit dem Verband kommunaler Unternehmen (VKU) veröffentlicht hat. IT-Sicherheit müsse tief in den Managementprozessen von Unternehmen verankert werden, so Rohleder weiter.

Auch beim BSI gab es immer wieder Stimmen, die auf die zunehmenden Gefahren für die IT-Sicherheit hingewiesen haben. So warnte etwa BSI-Referatsleiter Holger Junker bereits 2015 auf der Hannover Messe, dass „viele Branchen in Deutschland im Fokus der Angreifer stehen“. Junker sah daher in erster Linie einen „Handlungsbedarf aufseiten der Hersteller, der Integratoren, Maschinenbauer und letztlich auch der Betreiber“.

Bild: BSI

**„Ein rein freiwilliger Ansatz führt nicht immer zum nötigen Engagement in der Wirtschaft.“**

**Michael Hange**
Ehemaliger Präsident des BSI
**www.bsi.de**

Der BSI-Mitarbeiter verwies in seinem Statement auch auf ein „besonderes Interesse des Staates und auch der Gesellschaft als Ganzes, ein erhöhtes Sicherheitsniveau zu haben“. Unternehmen in Deutschland sähen sich einer besonderen Gefahr ausgesetzt: „Bei uns gibt es sehr viel zu holen.“ Überlegungen wie diese haben letztlich zum neuen IT-Sicherheitsgesetz geführt.

Das Problem für die betroffenen Unternehmen: Ihnen bleibt keine Zeit mehr. Die zwei Jahre Schonfrist zwischen Inkrafttreten und Wirksamwerden des neuen IT-Sicherheitsgesetzes sind in den meisten Fällen bereits abgelaufen. Nun wird sich zeigen, wie schnell und konsequent das BSI die neuen Regelungen durchsetzt. Die Umsetzung von Regelwerken wie ISO 27001 oder ISIS12 dauert aber allein schon bereits mehrere Monate, wenn nicht gar Jahre. Und damit wäre noch längst nicht allen Vorschriften des Sicherheitsgesetzes Genüge getan.

Eine Gefahr besteht allerdings schon jetzt für jedes Unternehmen, das eine öffentliche Webseite betreibt: Marktbeobachter befürchten nämlich, dass Mitbewerber die Regelungen dazu nutzen könnten, missliebige Konkurrenten kostenpflichtig abzumahnen, wenn diese ihre Seiten nicht auf dem aktuellen Stand halten. Und auf diese Weise können schnell zusätzliche Kosten von mehreren Zehntausend Euro entstehen.

In ihrem eigenen Interesse sollten Unternehmen daher die vom IT-Sicherheitsgesetz geforderten Anpassungen ihrer IT ohne weiteren Verzug umsetzen – und zwar nicht nur bei ihren Internetangeboten, sondern auch in ihrem eigenen Rechenzentrum sowie bei allen von ihnen genutzten Cloud-Diensten. ■

Andreas Th. Fischer/js
js@com-professional.de

### Handlungsempfehlungen

Der Arbeitskreis Medizinische Versorgung im UP KRITIS ist eines der ersten Gremien, das konkrete Empfehlungen auf Basis des neuen IT-Sicherheitsgesetzes veröffentlicht hat. Sie lassen sich relativ leicht auf andere Branchen anwenden.

- Einführung einer geeigneten Organisationsstruktur, um den besonderen Anforderungen der IT-Sicherheit begegnen zu können. Insbesondere sollte die Verantwortlichkeit in Geschäftsführungsnähe angesiedelt werden.
- Identifikation der kritischen Prozesse im Unternehmen. Bei Krankenhäusern sind es zum Beispiel die Prozesse zur Versorgung der Patienten.
- Identifikation der diese kritischen Prozesse unterstützenden IT-Infrastruktur, IT-Verfahren sowie Schnittstellen zu unterstützenden Prozessen.
- Einführung eines Information Security Management Systems (ISMS) nach dem Stand der Technik. Diese Anforderung ist für Betreiber von kritischen Infrastrukturen verpflichtend.
- Einbinden des IT-Risikomanagements für die identifizierten kritischen Prozesse in das Risikomanagement für das gesamte Unternehmen. Auf ihrer Grundlage sollte zudem eine Priorisierung vorgenommen werden, um geeignete technische und organisatorische Maßnahmen zu identifizieren.
- Einführung von Business Continuity Management, um die kritischen Prozesse zu unterstützen.
- Etablierung eines Meldeverfahrens, um über relevante Vorkommnisse an das BSI berichten zu können. Diese Anforderung ist ebenfalls für Betreiber von kritischen Infrastrukturen verpflichtend.

Zum Nachlesen empfehlen sich die Normen der ISO-27000-Familie, ISO 20000-1, 22301, 27005 und 31000 sowie IEC 80001 und der Link www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html.