Bundesamt
für Sicherheit in der
Informationstechnik

Schutz Kritischer Infrastrukturen

durch IT-Sicherheitsgesetz und UP KRITIS

Inhaltsverzeichnis

1 Die Gefährdungslage im Cyber-Raum

1 Die Gefährdungslage im Cyber-Raum

Mit der voranschreitenden Digitalisierung hat die Informationstechnologie Einzug in unseren Alltag gehalten. Die Verknüpfung von Daten und die Vernetzung von technischen Geräten eröffnen einzigartige Möglichkeiten, Computersysteme zu nutzen. Das Internet der Dinge und die Industrie 4.0 zeigen das enorme Entwicklungspotenzial, das im digitalen Wandel steckt. Dabei darf allerdings nicht vergessen werden, dass all diese Neuerungen auch mit einem immensen Zuwachs an Sicherheitsrisiken einhergehen. Die zunehmende Vernetzung von IT-Komponenten und daraus erwachsende Abhängigkeiten führen zu einer erhöhten Verletzlichkeit der eingesetzten Systeme.

Gleichzeitig steigt das potenzielle Schadensausmaß bei einer Beeinträchtigung des korrekten und verlässlichen Funktionierens der IT-Systeme. Cyberkriminelle entwickeln ihre Angriffsmethoden stetig weiter und gestalten Cyber-Attacken hoch professionell. Die Motivation, die hinter solchen Angriffen steckt, kann von unterschiedlicher Natur sein. Wirtschaftsspionage, Diebstahl und Manipulation werden gezielt als Mittel genutzt, um die angestrebten Ziele zu erreichen. Diese reichen von der Verursachung eines größtmöglichen Schadens bis hin zur Erzielung eines maximalen Profits.

Erfolgreiche Cyber-Attacken können zu Misstrauen der Anwender gegenüber dem korrekten und verlässlichen Funktionieren der Informationstechnologie führen und lassen uns an der Digitalisierung und damit am Fortschritt zweifeln. Damit diesen Zweifeln begegnet werden kann, bedarf es umfassender Investitionen in Cyber-Sicherheit. Durch sie kann Vertrauen in die IT erhalten und wieder aufgebaut werden, damit sich die Chancen und Potenziale der Innovation vollumfänglich entfalten können.

Betreiber von Kritischen Infrastrukturen sind genauso lukrative Angriffsziele wie andere Unternehmen auch, besitzen jedoch ein besonders hohes Schadenspotenzial in Bezug auf die Gesellschaft. Ausfälle oder Beeinträchtigungen bei Kritischen Infrastrukturen können zu nachhaltig wirkenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen. Die Absicherung der IT-Systeme, die von KRITIS-Betreibern eingesetzt werden, ist hoch komplex. Erschwerend kommt hinzu, dass die Systeme der Informationsinfrastruktur zum Teil einen langen Lebenszyklus haben und häufig nicht oder nicht zeitnah mit Sicherheitsupdates versorgt werden können.

Zahlreiche Vorfälle aus den letzten Jahren verdeutlichen, dass die Gefahr aus dem Cyber-Raum Realität ist. Um dieser Bedrohung effektiv entgegenzuwirken, ist eine enge Zusammenarbeit von Wirtschaft und Staat notwendig. Widerstandsfähige IT in Kritischen Infrastrukturen ist der erste Baustein für mehr Sicherheit.

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft und trägt somit dazu bei, dass Kritische Infrastrukturen trotz zunehmender IT-Abhängigkeit und -Vernetzung auch in Zukunft zuverlässig funktionieren.

Ransomware im Krankenhaus

Sachverhalt: Im Februar 2016 brachten Unbekannte ein Schadprogramm in das interne Netz des Lukaskrankenhauses in Neuss ein. Dieses Schadprogramm führte zeitnah zu Störungen in IT-Systemen und behinderte auch die Behandlung von Patienten. Zur Vermeidung möglicher weiterer Schäden, insbesondere der Kompromittierung von Patientendaten, und zur Analyse der Störungen wurde das interne Computer-Netzwerk heruntergefahren.

Ursache: Die Analyse ergab, dass ein Ransomware-Trojaner Ursache der Störung war. Das Schadprogramm hinterließ vereinzelte Hinweise, wie das Krankenhaus die für die Wiederherstellung der Daten notwendigen kryptographischen Schlüssel bekommen könnte. Da das Netzwerk allerdings unmittelbar nach den ersten Auffälligkeiten heruntergefahren worden war, wurde nur ein sehr kleiner Anteil der gesamten Datenmenge verschlüsselt. Das Krankenhaus entschied sich gegen eine Lösegeldzahlung und stellte nach der Überprüfung aller Server und Rechner mit einer neu geschriebenen Anti-Schadsoftware die Daten aus den verfügbaren Backups wieder her. Das BSI hat das Krankenhaus vor Ort bei der Analyse und Bewältigung des Vorfalls unterstützt.

Methode: Das Eindringen von Schadprogrammen in interne Netze ist schon allein deshalb nicht auszuschließen, weil in gängigen Programmen immer wieder Schwachstellen gefunden werden, die durch Angreifer ausgenutzt werden können. Ausnutzbar werden diese Schwachstellen, weil die Durchdringung der Gesellschaft mit IT nahezu in allen größeren Organisationen zu einer Vielzahl komplexer Kommunikationsverbindungen geführt hat - und zwar auch unter Verwendung des Internets mit Rechnern, die unter Kontrolle böswilliger Dritter stehen. Die Schutzmechanismen von Computer-Netzwerken müssen also darauf ausgerichtet sein, dass ein erfolgreicher Angriff auf ein einzelnes internes System nicht sofort Auswirkungen auf das gesamte Netzwerk hat. Im konkreten Fall konnte das Schadprogramm mit wenig Aufwand weitere IT-Systeme schädigen, da die internen Schutzmechanismen dem infizierten System vertrauten.

Schadenswirkung: Im Krankenhaus gab es keinen Schaden an Leib und Leben, da der Betrieb auch ohne umfassende IT-Unterstützung weitergeführt werden konnte. Aber allein die Kosten für die Analyse des Angriffs und die Wiederherstellung des IT-Betriebs werden von der Geschäftsführung des Lukaskrankenhauses mit einem Betrag in Höhe von ca. 1 Million Euro angegeben.

Technische Fähigkeiten: Angreifer können sich Ransomware am Markt einkaufen und Lösegeldzahlungen anonym über das Internet abwickeln, sodass sie für ihre Angriffe kein ausgeprägtes Fachwissen benötigen. Die Spezialisten hinter solchen Angriffen sind die Programmierer der Schadsoftware, die immer wieder Methoden finden, Schutzmechanismen zu umgehen.

Großflächige Störung von DSL-Internet-Zugängen der Deutschen Telekom AG

Sachverhalt: Am Sonntag, 27. November 2016, um 16:00 Uhr hatten zahlreiche DSL-Kunden der Deutschen Telekom AG Probleme beim Zugang zum Internet sowie zu davon abhängenden Diensten wie Voice-over-IP-Telefonie und IP-TV.

Ursache: Grund für den Ausfall war ein Angriff unter Verwendung des Mirai-Botnetzes, das weltweit versucht, Internet-Router/-Modems mit Schadcode zu infizieren, um sie zum Teil des Botnetzes zu machen. Mittels des Mirai-Botnetzes wurden in der Vergangenheit bereits extrem wirkungsvolle DDoS-Angriffe durchgeführt. Wie wirkungsvoll die Angriffe sind, zeigt der Angriff auf die DNS-Infrastruktur des US-Unternehmens Dyn, wodurch Dienste von großen Internetdiensten wie Netflix, PayPal, Amazon und Twitter in Teilen von Europa und den USA zeitweise nicht verfügbar waren. Auch die DDoS-Attacke auf den unabhängigen Security-Journalisten Brian Krebs verdeutlicht die enorme Schlagkraft des Mirai-Botnetzes.

Eine solche Infektion war zumindest bei Geräten des Herstellers Zyxel nachweisbar erfolgreich. Die von der Deutschen Telekom vertriebenen Speedport-Geräte wurden durch den Angriff hingegen nicht infiziert. Allerdings kam es bei einigen Gerätetypen durch die Angriffsversuche zu Kollateralschäden. Betroffen waren u. a. die Modelle Speedport W921V und Speedport W723. Diese gerieten aufgrund des Angriffs in einen undefinierten Zustand, wodurch in vielen Fällen der Domain-Name-System-Dienst nicht mehr nutzbar war. Dieser hat die Aufgabe, Webaufrufe wie www.bund.de in die zugehörige IP-Adresse (77.82.229.48) zu übersetzen.

Methode: Seit dem 25. November 2016 kam es zu einem Anstieg der Internet-Aktivitäten auf Port 7547. Normalerweise werden darüber mittels des sogenannten TR-069-Protokolls DSL-Internetzugangsgeräte durch die Provider aus der Ferne administriert. Am 7. November 2016 war eine Schwachstelle für das Modem Eir D1000 des Herstellers Zyxel veröffentlicht worden. Die zugehörige Beschreibung enthielt einen Beispielcode, der eine Ausnutzung der Schwachstelle ermöglichte. Der Anstieg der Aktivitäten am 25. November 2016 ließ sich auf den Netzwerkverkehr einer neuen Version von Mirai-Bots zurückführen. Diese Version enthielt Module, die es ermöglichten, nach offenen Ports 7547 zu scannen und dabei zu versuchen, unter Ausnutzung der zuvor gefundenen Schwachstelle den Mirai-Schadcode nachzuladen.

Schadenswirkung: Nach offiziellen Angaben der Deutschen Telekom waren bundesweit ca. 900.000 Internetanschlüsse betroffen. Es liegen keine Erkenntnisse vor, ob es in Deutschland Router von anderen Anbietern gibt, bei denen die Schadsoftware erfolgreich installiert wurde.

Zielgruppe: Auf Basis der Veröffentlichung der Schwachstelle wurde der großflächige Angriff auf die Geräte gestartet. Der Angriff richtete sich allerdings nicht gezielt gegen die Speedport-Router der Deutschen Telekom, sondern gegen Geräte des Herstellers Zyxel, um diese zum Teil des Mirai-Botnetzes zu machen.

Technische Fähigkeiten: Die technischen Fähigkeiten der Angreifer sind als mittelmäßig einzuschätzen, da der veröffentlichte Sourcecode des Mirai-Botznetzes lediglich ergänzt wurde. Allerdings wird deutlich, dass durch die ständige Weiterentwicklung des Botnetzes ein großes Angriffspotenzial auf Internet-Infrastrukturen besteht.

Weitere aktuelle Cybersicherheitsvorfälle finden sich im jährlich erscheinenden Bericht zur Lage der IT-Sicherheit in Deutschland:

https://www.bsi.bund.de/Lagebericht.html

2 Digitalisierung erfordert Schutzmaßnahmen

2 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 Unternehmen, die mit besonders wertvollen Informationen umgehen.

Schon seit 2007 adressiert der Staat den Schutz Kritischer Infrastrukturen durch zwei Initiativen: Mit dem UP BUND wurde die Grundlage für den Schutz der IT der Bundesverwaltung gelegt, mit dem UP KRITIS eine öffentlich-private Partnerschaft zum Schutz insbesondere der IT in den anderen acht, zumeist privatwirtschaftlich betriebenen KRITIS-Sektoren gegründet. 2009 wurde der Schutz der Bundes-IT zudem im BSI-Gesetz verankert. Unreguliert blieben seinerzeit weiterhin die anderen acht KRITIS-Sektoren.

Das 2015 in Kraft getretene Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) ist ein neuerlicher und deutlich weitergehender 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 Gewährleistung von IT-Sicherheit nicht immer zum nötigen Engagement in der Wirtschaft geführt und nicht flächendeckend in allen sicherheitsrelevanten Bereichen gewirkt hat.

3 Das IT-SiG ist Pflicht

3 Das IT-SiG ist Pflicht

Das IT-Sicherheitsgesetz ist ein Artikelgesetz, das neben dem BSI-Gesetz auch das Energiewirtschaftsgesetz, das Atomgesetz, das Telemediengesetz, das Telekommunikationsgesetz und weitere Gesetze ändert. Das IT-Sicherheitsgesetz leistet einen Beitrag dazu, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen.

Die Bundesregierung hat mit der Cyber-Sicherheitsstrategie von 2016 den Fokus auf mehr Sicherheit im Cyber-Raum gelegt. Ein Kernziel ist die Verbesserung der Sicherheit durch den Schutz von IT-Systemen und Diensten. 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.

Gesetzesentwurf zur NIS-Richtlinie:

Die NIS-Richtlinie ist ein wichtiger Schritt für mehr Cyber-Sicherheit in Europa. Die Bundesregierung hat nun die Grundlage dafür geschaffen, die europäischen Vorgaben rechtzeitig und zeitnah auch in nationales Recht umzusetzen. Dabei war die Ausgangsposition hierfür denkbar gut: In Deutschland existiert seit Juli 2015 mit dem IT-Sicherheitsgesetz bereits ein einheitlicher Rechtsrahmen für die Zusammenarbeit von Staat und Unternehmen für mehr Cyber-Sicherheit bei den Kritischen Infrastrukturen. Es schreibt KRITIS-Betreibern vor, IT-Sicherheit nach dem „Stand der Technik“ umzusetzen und erhebliche IT-Sicherheitsvorfälle an das BSI zu melden. Der Gesetzesentwurf zur Umsetzung der NIS-Richtlinie erweitert nun die Aufsichts- und Durchsetzungsbefugnisse des BSI gegenüber KRITIS-Betreibern. Gleichzeitig wird die Zusammenarbeit zwischen den Bundesländern und dem BSI gestärkt. Das BSI hat so die Möglichkeit, Länder in Zukunft noch umfassender zu unterstützen und ihnen seine technische Expertise zur Verfügung zu stellen.

Trotz stärkerer Befugnisse wird sich das BSI dafür einsetzen, dass der im IT-Sicherheitsgesetz verankerte, mit dem UP KRITIS seit 10 Jahren gelebte kooperative Ansatz auch bei der Umsetzung der NIS-Richtlinie weiterverfolgt wird, da die Herausforderungen nur von Staat und Wirtschaft gemeinsam angenommen werden können. Damit wird das BSI seiner Vorreiterrolle in Europa auf dem Gebiet der Cyber-Sicherheit gerecht. Gleichzeitig ergänzt der Gesetzesentwurf das IT-Sicherheitsgesetz sinnvoll. Denn künftig sollen auch Anbieter von digitalen Diensten Mindestanforderungen und Meldepflichten unterliegen. Davon betroffen sind sowohl Online-Marktplätze und -Suchmaschinen als auch Anbieter von Cloud-Computing-Diensten. Das Bundesinnenministerium geht davon aus, dass hierzulande zwischen 500 und 1.500 Unternehmen von der Neuregelung betroffen sind. Das BSI wird künftig als Kontrollinstanz prüfen, ob sie die neuen Auflagen einhalten.

4 Zielgruppen und Neuregelungen

4 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 Sektoren 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. Für Betreiber von Kritischen Infrastrukturen gibt es im wesentlichen fünf Neuerungen. Wann und wie diese auf welche Betreiber zutreffen, zeigt die Abbildung 1.

Tabelle zum IT-Sicherheitsgesetz

	Pflicht zur Umsetzung IT-Sicherheit nach Stand der Technik	Pflicht zur Überprüfung der Absicherung (z. B. durch Audit)	Unverzügliche Versorgung mit relevanten Informationen durch BSI	Meldepflicht von IT-Sicherheitsvorfällen	Möglichkeit der Beratung und Unterstützung durch das BSI
KRITIS-Betreiber gemäß BSI-Kritis-Verordnung (bis auf die nachfolgend aufgelisteten Sonderfälle)	Ja. Konkretisierung in Branchen möglich. Spätestens 2 Jahre nach Inkrafttreten der Verordnung.	Ja. Überprüfung und Nachweis alle 2 Jahre, erstmalig 2 Jahre nach Inkrafttreten der Verordnung.	Ja.	Ja. Spätestens ½ Jahr nach Inkrafttreten der Verordnung.	Ja.
Öffentliche Telekommunikationsnetze gemäß BSI-Kritis-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altregelung)	BNetzA überprüft Umsetzung alle 2 Jahre.	Ja.	Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung).	Ja.
Öffentliche Telekommunikationsnetze (sonstige Betreiber)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §109 TKG. (Altregelung)	BNetzA überprüft Umsetzung alle 2 Jahre.	Nein.	Ja, sofort. Meldepflicht an die BNetzA (Erweiterung einer Altregelung).	Nein.
Energieversorgungsnetze gemäß BSI-Kritis-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung).	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG.	Ja.	Ja. Mit Inkrafttreten der Verordnung.	Ja.
Energieversorgungsnetze (sonstige Betreiber)	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG (Erweiterung einer Altregelung).	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1a) EnWG.	Nein.	Nein.	Nein.
Energieanlagen gemäß BSI-Kritis-Verordnung	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG.	Ja. Konkretisierung durch IT-Sicherheitskatalog nach §11 (1b) EnWG.	Ja.	Ja. Mit Inkrafttreten der Verordnung.	Ja.
Genehmigungsinhaber nach §§ 6, 7 oder 9 Atomgesetz (z. B. Kernkraftwerke, atomare Lager)	Ja. (Keine Änderung zum bestehenden Atomgesetz.)	Ja. (Keine Änderung zum bestehenden Atomgesetz.)	Ja.	Ja (seit 25.07.2015).	Nein. Es sei denn, sie sind KRITIS-Betreiber (z. B. Betreiber von Energieanlagen).

Tabelle 1: Neuregelungen für KRITIS-Betreiber gemäß IT-Sicherheitsgesetz.

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. Werden Sicherheitsmängel aufgedeckt, kann das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung verlangen.

» können – sofern nicht andere Spezialregelungen bestehen – die Absicherung ihrer IT-Infrastruktur selbst ausgestalten, solange ihre Maßnahmen dem Stand der Technik entsprechen.

» können – sofern nicht andere Spezialregelungen bestehen – sich branchenintern zusammenfinden und 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.

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

3. Telekommunikationsunternehmen

» sind 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 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.

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

5 Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen im Sinne des BSIG

5 Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen im Sinne des BSIG

Regelmäßig wird 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 (BSI-KritisV), deren erster Teil im Mai 2016 veröffentlicht wurde. Durch die Verordnung werden Betreiber Kritischer Infrastrukturen in die Lage versetzt, anhand messbarer und nachvollziehbarer Kriterien zu prüfen, ob ihre Anlagen unter den Regelungsbereich des BSI-Gesetzes 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.

Der Schwellenwert von 500.000 versorgten Menschen wurde deswegen gewählt, weil ein Ausfall oder eine Beeinträchtigung der Versorgung von 500.000 oder mehr Menschen mit einer (lebens-) wichtigen Dienstleistung (z. B. der Strom- oder Wasserversorgung) zu einer Versorgungskrise in der Bundesrepublik Deutschland führen könnte, die nicht ohne Weiteres gelöst werden kann. Ausfälle oder Beeinträchtigungen von Anlagen in dieser Größenordnung sind daher für Deutschland besonders „kritisch“ und sollen daher möglichst verhindert werden.

Beispiel: Der Durchschnittsverbrauch an Strom pro Person pro Jahr liegt in Deutschland bei 7.375kWh (einschließlich des auf die Bevölkerung umgerechneten Verbrauchs von Unternehmen). Ein Kraftwerk, das 420 MW oder mehr Netto-Nennleistung erzeugt, kann somit also rein rechnerisch 500.000 Personen versorgen und fällt damit unter die BSI-Kritisverordnung im Bereich Stromversorgung.

Die Verordnung bestimmt zunächst Kritische Infrastrukturen im Sinne des BSIG in den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung (sogenannter Korb 1; dargestellt durch große gelbe Punkte in Abbildung 2). Mit der Veröffentlichung des zweiten Teils der Verordnung im Frühjahr 2017 werden per Änderungsverordnung auch die Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen (sogenannter Korb 2; dargestellt durch große rote Punkte in Abbildung 2), geregelt.

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 alle zwei Jahre nachzuweisen.

Binnen sechs Monaten, nach Inkrafttreten der Rechtsverordnung, müssen sie zudem dem BSI eine Kontaktstelle für Meldungen von IT-Störungen benennen. Diese Kontaktstelle muss rund um die Uhr erreichbar sein.

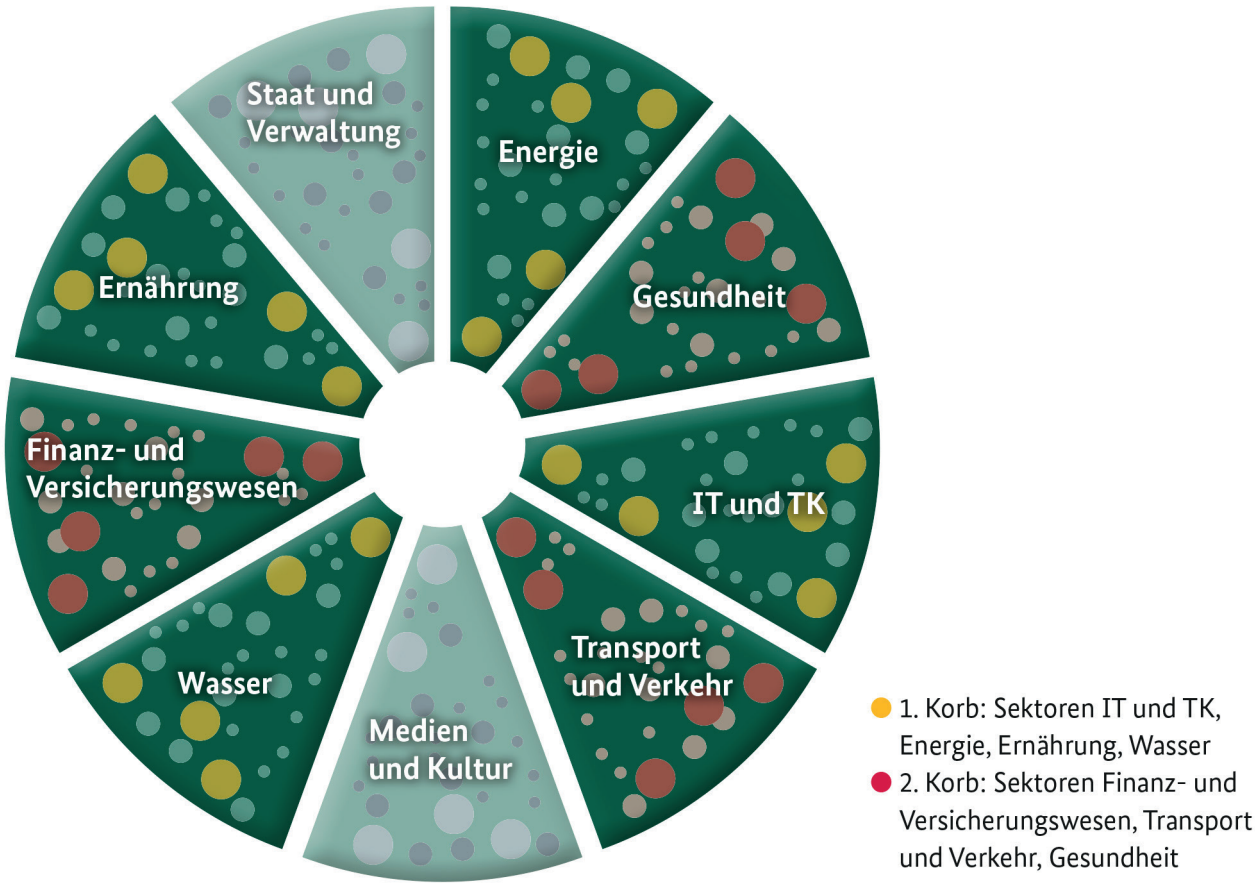

Abbildung 2: Kritische Infrastrukturen im Sinne des BSIG sind die besonders wichtigen Infrastrukturen aus sieben der neun Sektoren, sie stellen eine Teilmenge aller Kritischen Infrastrukturen dar und sind in der Abbildung durch große farbige Punkte dargestellt.

6 UP KRITIS ist Kür

6 UP KRITIS ist Kür

Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Er adressiert acht der neun Sektoren Kritischer Infrastrukturen. Teilnehmer des UP KRITIS können neben den Betreibern nach IT-SiG auch andere KRITIS-Betreiber aus den acht Sektoren werden. Der Sektor „Staat und Verwaltung“ wird durch den UP BUND und Initiativen auf Landes- und kommunaler Ebene abgedeckt.

In Branchen- (BAK) und Themenarbeitskreisen (TAK) arbeiten KRITIS-Betreiber, Behörden und Verbände seit 2007 gemeinsam am Schutz der Kritischen Infrastrukturen. Derzeit gibt es im UP KRITIS die in Abbildung 3 dargestellten Arbeitskreise.

Abbildung 3: Branchen- und Themenarbeitskreise (BAK und TAK) im UP KRITIS, Stand März 2017.

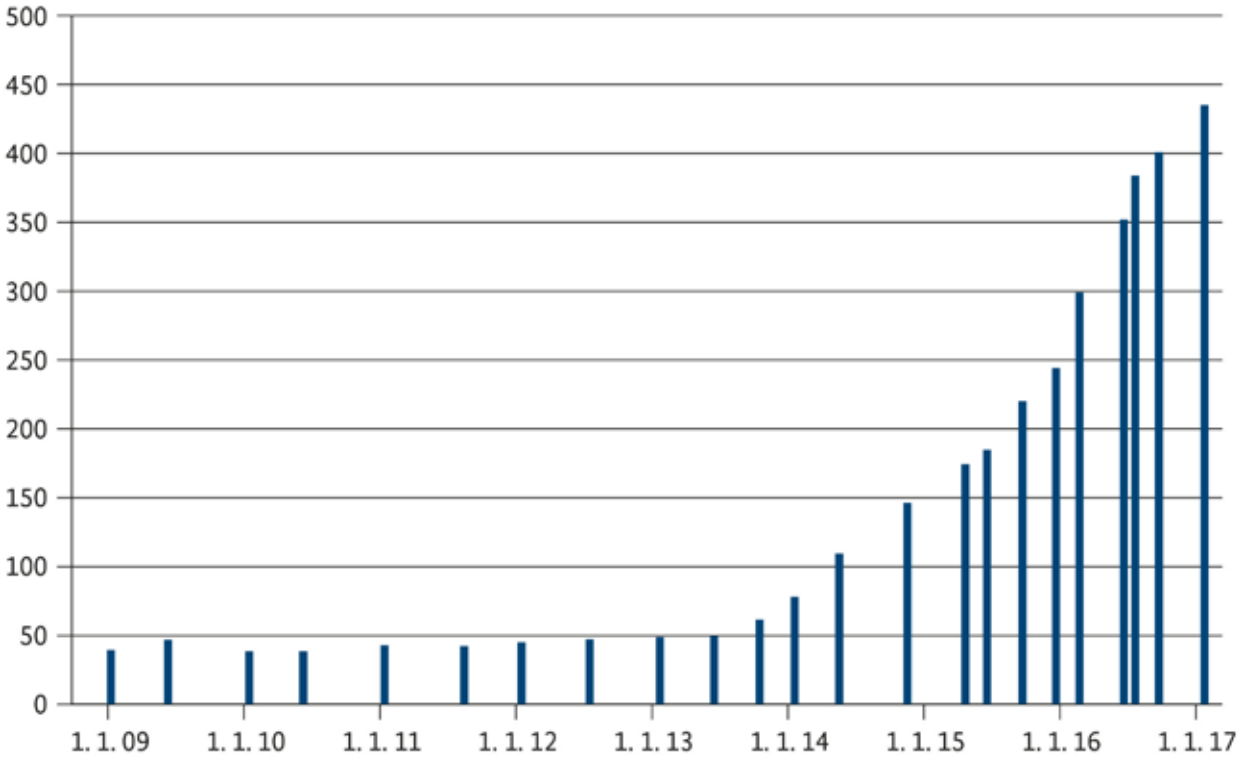

Abbildung 4: Entwicklung der Teilnehmerzahl im UP KRITIS.

Dieser kooperative Ansatz des UP KRITIS zum Schutz Kritischer Infrastrukturen wird mit dem IT-Sicherheitsgesetz weitergeführt, wie die Entwicklung der Teilnehmerzahl des UP KRITIS zeigt (siehe Abbildung 4). So war der UP KRITIS neben Vertretern des BMI, des BSI und des BBK (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe), den zuständigen Aufsichtsbehörden und Fachressorts auf Bundesebene auch maßgeblich an der Erstellung der Rechtsverordnung im Rahmen des IT-Sicherheitsgesetzes beteiligt.

Das zentrale Ziel des UP KRITIS ist es, die Versorgung mit Dienstleistungen Kritischer Infrastrukturen in Deutschland auch im Zeitalter der Digitalisierung möglichst uneingeschränkt aufrechtzuerhalten. Der Leitgedanke des UP KRITIS ist, durch gemeinsame Verantwortung von Wirtschaft und Staat, Kritische Infrastrukturen zu schützen und die Versorgung der Bevölkerung sicherzustellen. Der Schwerpunkt der Arbeit liegt hierbei auf der IT in den kritischen Prozessen. Die Zusammenarbeit im UP KRITIS findet auf verschiedenen Ebenen statt. Auf der strategisch-konzeptionellen Ebene werden Analysen durchgeführt sowie Empfehlungen und Vorgaben erarbeitet (z. B. Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen sowie branchenspezifische Sicherheitsstandards zur Erfüllung der Anforderungen nach § 8a BSIG). Auf der operativ-technischen Ebene findet ein regelmäßiger Austausch über Vorfälle statt und es wird ein gemeinsames Lagebild erstellt. Darüber hinaus wurden Strukturen für die koordinierte Krisenreaktion und -bewältigung geschaffen, diese werden regelmäßig beübt. Persönliche Kontakte, eine schnelle und zuverlässige Kommunikation sowie der Austausch von vertrauensvollen Informationen schaffen den weiteren Rahmen für die vertrauensvolle Zusammenarbeit.

Abbildung 5: Sektoren Kritischer Infrastrukturen in Deutschland

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. Die Beteiligten haben ein Netzwerk des Vertrauens aufgebaut, in dem ein transparenter Know-how-Transfer stattfindet. Dadurch lernen alle Beteiligten voneinander und kommen zu besseren Lösungen.

Mehr Informationen zum UP KRITIS finden sich unter: http://www.upkritis.de

7 Neue Aufgaben für das BSI

7 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. 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 zu untersuchen. Hier wird das BSI in erster Linie Produkte untersuchen, die für die Sicherheit von Kritischen Infrastrukturen besonders relevant sind.

Das gilt zum anderen für den Umgang mit den Meldungen, die die KRITIS-Betreiber bei erheblichen IT-Störungen an das BSI abgeben. Das BSI bewertet und analysiert die eingehenden Meldungen und setzt sie mit weiteren Informationen 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 sowie entsprechende Abwehrmaßnahmen treffen können. Die Meldungen der KRITIS-Betreiber sind daher eine wichtige Voraussetzung für die nationale Handlungsfähigkeit und Grundlage für bundesweit abgestimmte Reaktionen. Die Betreiber erhalten dadurch Informationen und Know-how und können von der Auswertung der Meldungen aller Betreiber sowie vieler anderer Quellen durch das BSI profitieren.

Beim Aufbau des Meldewesens für Betreiber Kritischer Infrastrukturen nach BSIG konnte auf Erfahrungen zurückgegriffen werden, die mit der Bundesverwaltung gewonnen wurden, in der es bereits seit langem eine Meldepflicht für IT-Sicherheitsvorfälle gibt.

8 Prävention

8 Prävention

Im Zuge der Änderungen des BSIG hat das BSI gemäß § 8b Absatz 2 die verantwortungsvolle Aufgabe, wichtige Informationen, die für die Abwehr von Gefahren für die Informationstechnik relevant sind, zu sammeln und auszuwerten. Darunter fallen z. B. Informationen zu Sicherheitslücken, Schadprogrammen, versuchten Angriffen und dabei verwendeten Methodiken. Aus diesen gesammelten Informationen und den Meldungen von Betroffenen erstellt das BSI sanitarisierte und zielgruppenorientierte Warn- oder Informationsmeldungen. Wie diese Informations- und Meldeflüsse bis zur Erstellung eines BSI-Produktes aussehen, zeigt Abbildung 6. Zusätzlich wird ein Gesamtlagebild für alle meldepflichtigen Betreiber und weitere Dritte erstellt. Dieses Lagebild über die Sicherheit in der Informationstechnik wird kontinuierlich aktualisiert. In enger Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe werden potenzielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen analysiert.

Gemäß § 8a BSIG haben KRITIS-Betreiber die Pflicht, angemessene organisatorische und technische Vorkehrungen zu treffen, um die informationstechnischen Systeme, Komponenten oder Prozesse, die für die von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, gemäß dem Stand der Technik abzusichern und dies spätestens alle zwei Jahre gegenüber dem BSI nachzuweisen. Zur Definition und Konkretisierung des „Stands der Technik“ können von den Branchen sogenannte branchenspezifische Sicherheitsstandards (B3S) erarbeitet werden. Dies wird in verschiedenen Branchenarbeitskreisen (BAK) des UP KRITIS bereits getan. Das BSI unterstützt die Branchen bei der Erstellung dieser Standards und prüft auf Antrag deren Eignung.

Die Absicherung der informationstechnischen Systeme, Komponenten oder Prozesse gemäß Stand der Technik ist eine wichtige präventive Maßnahme zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Kritischen Infrastrukturen.

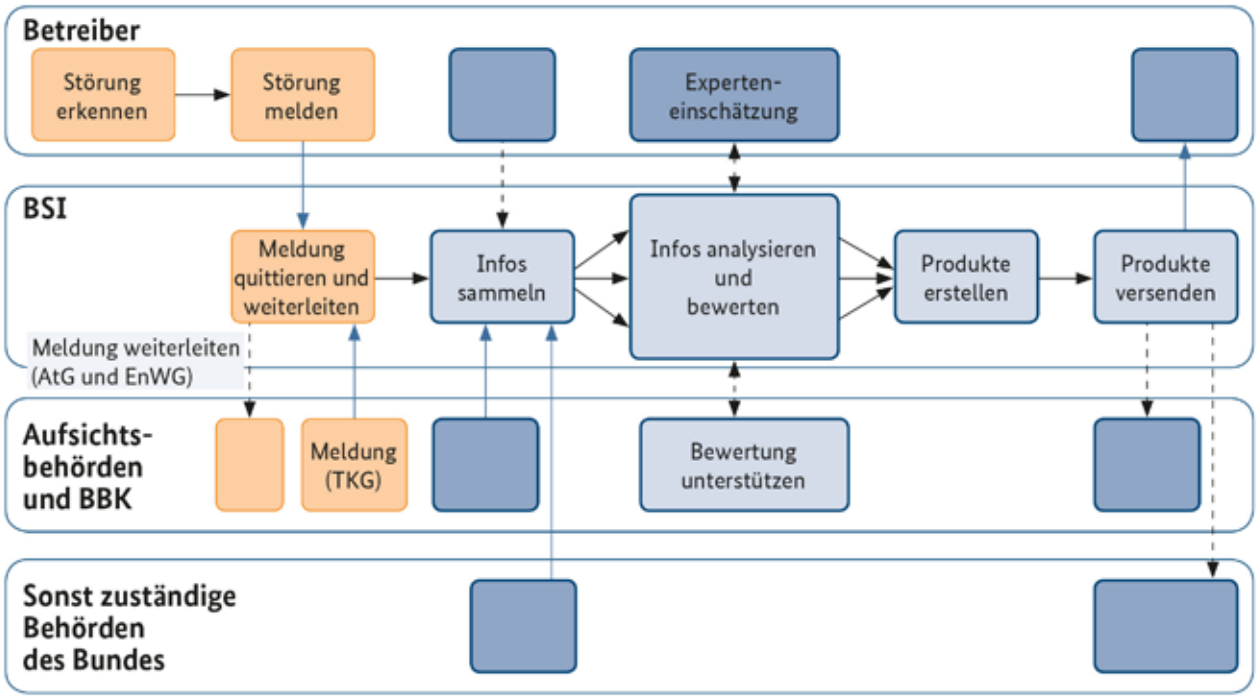

Abbildung 6: Informations- und Meldeflüsse im Rahmen von § 8b BSIG

Das BSI-Lagezentrum

Das IT-Lagezentrum des BSI (siehe Abbildung 7) hat den Auftrag, jederzeit ein umfassendes und verlässliches Bild der aktuellen Sicherheitslage in Deutschland bereitzustellen. Weiterhin soll es auf der staatlichen und wirtschaftlichen Ebene den Handlungsbedarf sowie mögliche Handlungsoptionen bei sicherheitsrelevanten Vorfällen zügig und kompetent einschätzen. Um diese Aufgaben zu erfüllen, ist das BSI-Lagezentrum für Betreiber Kritischer Infrastrukturen sowie Bundesbehörden täglich 24 Stunden erreichbar. Für die Analyse der aktuellen Lage werden täglich mehr als 80 offene und vertrauliche Quellen ausgewertet. Zusätzlich werden die Regierungsnetze mit technischen Sensoren zur Frühwarnung und Erreichbarkeitsüberwachung beobachtet. Die daraus abgeleiteten Informationen und Bewertungen fließen in die Lageprodukte des BSI ein.

Abbildung 7: Das BSI-Lagezentrum

9 Detektion

9 Detektion

Auf Grundlage des § 8b Absatz 4 BSIG haben die Betreiber von Kritischen Infrastrukturen erhebliche Störungen, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastruktur führen können oder geführt haben, unverzüglich über die benannte Kontaktstelle an das BSI zu melden. Voraussetzung für eine schnelle Meldung ist die erfolgreiche Detektion einer IT-Störung. Erfahrungen zeigen, dass IT-Angriffe häufig nicht oder erst spät erkannt werden. Daher fordert das IT-SIG durch den § 8a BSIG auch den Aufbau von geeigneten Detektionsmechanismen. Denn ohne Detektion keine Reaktion und keine Meldung. Und ohne Meldung keine Warnung Dritter. Ob eine Meldung an das BSI erforderlich ist, ergibt sich aus den Meldekriterien des BSI (siehe Abbildung 8).

Häufig wird in diesem Zusammenhang die Frage gestellt, anhand welcher Kriterien entschieden wird, wann eine IT-Störung gewöhnlich bzw. außergewöhnlich ist. Eine Antwort auf diese Frage liefert Abbildung 9.

Meldungen an das BSI müssen über eine Kontaktstelle erfolgen, die vorher beim BSI registriert werden muss. Als Kontaktstelle ist ein Funktionspostfach zu verstehen, das dazu geeignet ist, die jederzeitige Erreichbarkeit an 24 Stunden sieben Tage die Woche zu gewährleisten. Zu den erforderlichen Inhalten der Meldung gehören z. B. Angaben zu der Störung und den technischen Rahmenbedingungen, die vermutete oder die tatsächliche Ursache sowie Informationen über die Art der betroffenen Anlage. Die namentliche Nennung des Betreibers ist nur erforderlich, falls die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung geführt hat. Betreiber, die dem gleichen Sektor angehören, haben die Möglichkeit, eine gemeinsame übergeordnete Ansprechstelle (GÜAS) zu benennen. Ist eine GÜAS benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen der Betreiber und dem BSI in der Regel über diese gemeinsame Ansprechstelle.

Das BSI bewertet und analysiert die eingehenden Meldungen und setzt sie mit weiteren Erkenntnissen aus anderen Quellen in Beziehung. Anschließend erstellt das BSI ein Lagebild, auf dessen Grundlage es ggf. kurzfristige Warn- und Alarmierungsmeldungen sowie Handlungsempfehlungen erstellt und versendet. Dadurch hilft

Abbildung 8: Meldekriterien nach § 8b BSIG

das BSI Betreibern und auch anderen Unternehmen oder Behörden, sich frühzeitig auf Ausfälle oder Angriffe vorzubereiten und notwendige Abwehrmaßnahmen rechtzeitig zu implementieren. Durch die Auswertungen der Meldungen, den daraus gewonnenen Informationen und den Know-how-Aufbau profitieren alle Beteiligten.

Betreiber von Kritischen Infrastrukturen und sonstige Organisationen, die nicht unter die BSI-Kritisverordnung fallen, haben die Möglichkeit, außergewöhnliche Störungen freiwillig über die Meldestelle der Allianz für Cyber-Sicherheit zu melden (siehe: https://www.allianz-fuer-cybersicherheit.de).

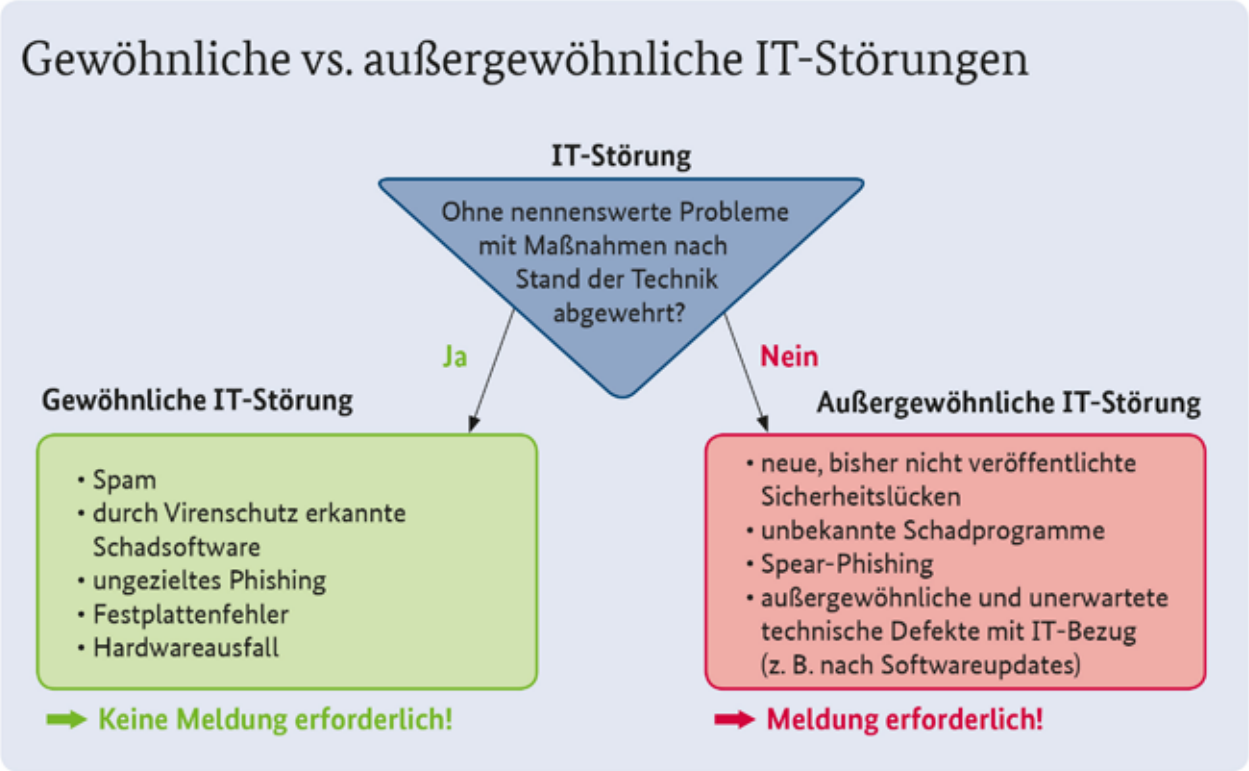

Abbildung 9: Meldekriterien nach § 8b BSIG

Die 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.

Allianz für Cyber-Sicherheit

Der Allianz gehören inzwischen mehr als 2.000 Institutionen an, davon knapp 100 Partner-Unternehmen und mehr als 40 Multiplikatoren. Auch für Betreiber Kritischer Infrastrukturen sind die Informations- und Schulungsangebote von großer Relevanz.

Mehr Informationen zur Allianz für Cyber-Sicherheit: https://www.allianz-fuer-cybersicherheit.de

10 Reaktion

10 Reaktion

Das BSI kann gemäß § 3 Absatz 3 BSIG Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen. Das Lagezentrum ist sowohl organisatorisch als auch technisch darauf vorbereitet, bei einer Krise zum nationalen IT-Krisenreaktionszentrum zu werden.

Das IT-Krisenreaktionszentrum

Das Nationale IT-Krisenreaktionszentrum des BSI soll schnell und wirksam die Behebung von Störungen in Informationsinfrastrukturen sicherstellen. Hierfür werden IT-Sicherheitsvorfälle analysiert, bewertet und an die relevanten Stellen weitergegeben. Das Krisenreaktionszentrum koordiniert die Zusammenarbeit mit den lokalen und brancheninternen Krisenmanagementorganisationen. Um diese Aufgabe erfüllen zu können, hat das BSI eine dynamische Krisenorganisation aufgebaut, die in mehreren Stufen erweitert werden kann. Beispielsweise können im Fall einer Alarmierung weitere Experten hinzugezogen werden. Für diesen Aufwuchs der Instititon und der Stabsarbeit wurden neue standardisierte Verfahren eingeführt.

Der Bereitschaftsdienst, der rund um die Uhr erreichbar ist, alarmiert die Stabsorganisation und beruft sie, der Lage entsprechend, ein. Die notwendigen Räumlichkeiten, die technische Infrastruktur, zu der unter anderem eine Notstromversorgung sowie Telefon- und Videokonferenzmöglichkeiten gehören, sind vorhanden. Zur kontinuierlichen Verbesserung der Arbeit der Stabsorganisationen tragen regelmäßige Übungen bei.

Im Zuge der Umsetzung der NIS-Richtlinie soll die Reaktionsfähigkeit des BSI noch weiter gestärkt werden. Zukünftig sollen sogenannte Mobile Incident Response Teams (MIRT) auch Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Bewältigung von IT-Vorfällen aktiv vor Ort unterstützen.

11 Gemeinsam für mehr IT-Sicherheit

11 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 bereits bestehende Kooperationsinstrumente nicht überflüssig, schon allein aufgrund der Anzahl an Unternehmen in Deutschland, die nicht unter das Gesetz fallen: Von den gesetzlichen Regelungen für Kritische Infrastrukturen werden nur etwa 2.000 Anlagen der rund 3,5 Millionen Unternehmen in Deutschland betroffen sein.

Alle Unternehmen sind daher herzlich eingeladen, mit dem BSI zu kooperieren, um gemeinsam mehr IT- und Cyber-Sicherheit zu erreichen.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

Ihre Ansprechpartner beim BSI

Organisatorische Fragen rund um das IT-Sicherheitsgesetz
KRITIS-Büro
E-Mail: kritis-buero@bsi.bund.de
Telefon 8.00–16.00 Uhr:
+49 (0) 22899 9582-6166
Fax: +49 (0) 22899 109582-6166

Fragen zum UP KRITIS
UP KRITIS-Geschäftsstelle
E-Mail: upkritis@bsi.bund.de
Telefon: 8.00–16.00 Uhr:
+49 (0) 22899 9582-5089
Fax: +49 (0) 22899 109582-5088

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
März 2017

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
60386 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Bilder und Grafiken: BSI
Schaubild S. 21: fotolia

Artikelnummer
BSI-KRITIS 17/200

www.bsi.bund.de