Änderungen und Anpassungen

Auswirkungen des IT-Sicherheitsgesetzes auf Kritis-Betreiber

Evren Eren

Aufgrund der voranschreitenden Digitalisierung und Vernetzung der Gesellschaft wächst das Schadens- und Angriffspotenzial, das durch Missbrauch oder Ausfall hervorgerufen werden kann. Das von der Bundesregierung im Juli 2015 erlassene IT-Sicherheitsgesetz (IT-SiG) ist eine Reaktion auf diesen Sachverhalt. Die Schwerpunkte sind dabei eine Meldepflicht für sicherheitskritische Vorkommnisse und die Umsetzung eines technisch-organisatorischen Mindeststandards für Betreiber kritischer Infrastrukturen (Kritis). Welche Auswirkungen hat das Gesetz auf Kritis-Betreiber und welche Änderungen bzw. Anpassungen sind vonnöten?

Prof. Dr. Evren Eren ist Professor am Lehrstuhl für IT-Sicherheitsarchitekturen an der Hochschule Bremen

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) ist ein Artikelgesetz, das u.a. das Telemediengesetz und das BSI-Gesetz (BSIG) ergänzt. Mit ihm sollen IT-Systeme und digitale Infrastrukturen sicherer betrieben werden. Das IT-SiG verfolgt den Ansatz, dass alle Gefahren betrachtet werden sollen und keine Differenzierung zwischen Bedrohungen stattfindet. Jeder Vorfall soll registriert und untersucht werden. Neben Bedrohungen nehmen auch Schwachstellen eine wichtige Rolle ein.

Kritische Infrastrukturen

Als kritische Infrastrukturen werden Organisationen und Einrichtungen bezeichnet, die eine wichtige Bedeutung für das staatliche Gemeinwesen haben. Ein Ausfall oder eine Beeinträchtigung würde eine bedeutende Störung der öffentlichen Sicherheit bedeuten oder gar katastrophale Folgen oder nachhaltig wirkende Versorgungsengpässe implizieren. Für solche Einrichtungen oder Organisationen sind Maßnahmen erforderlich, die zur Schadensbewältigung und -begrenzung beitragen. Vor allem sind vorbeugende Maßnahmen zu entwickeln und vorzuhalten, mit deren Unterstützung a priori das Entstehen umfangreicher Störungen unterbunden werden kann. Sofern dies nicht vermieden werden kann, sollen Maßnahmen zumindest die Auswirkungen so weit wie möglich eingrenzen. Zur Einordnung, ob eine Organisation oder Einrichtung eine kritische Infrastruktur ist, werden u.a. messbare Kriterien wie z.B. der Marktanteil und die Zugehörigkeit zu einem Sektor herangezogen (*Bild 1*).

Ziele des IT-SiG

Mit der zunehmenden Beeinflussung aller Bereiche unserer Gesellschaft durch

Der Kritis-Geltungsbereich laut § 2 Abs. 10 des IT-SiG (Quelle: https://tinyurl.com/yy5xmeym)

neue Techniken, Digitalisierung und Vernetzung erhöht sich u.a. das Schadens- und Angriffspotenzial, dass durch Missbrauch oder Ausfall von IT-Systemen initiiert werden kann. Der deutsche Gesetzgeber wirkt mit dem Erlass des IT-Sicherheitsgesetzes dieser Entwicklung entgegen. Inhaltlich sind zwei Maßnahmen vorgesehen, die zur Verbesserung der geänderten Sicherheitslage beitragen sollen. Zum einen ist nach § 8a BSIG die Einführung eines technisch-organisatorischen Mindeststandards für kritische Infrastrukturen vorgesehen. Zum anderen sind Kritis-Betreiber verpflichtet, sicherheitskritische Vorkommnisse gemäß § 8b BSIG beim BSI zu melden. In technischer Hinsicht ist die Umsetzung dieser abstrakten gesetzlichen Anforderungen bisher nicht hinreichend bestimmt.

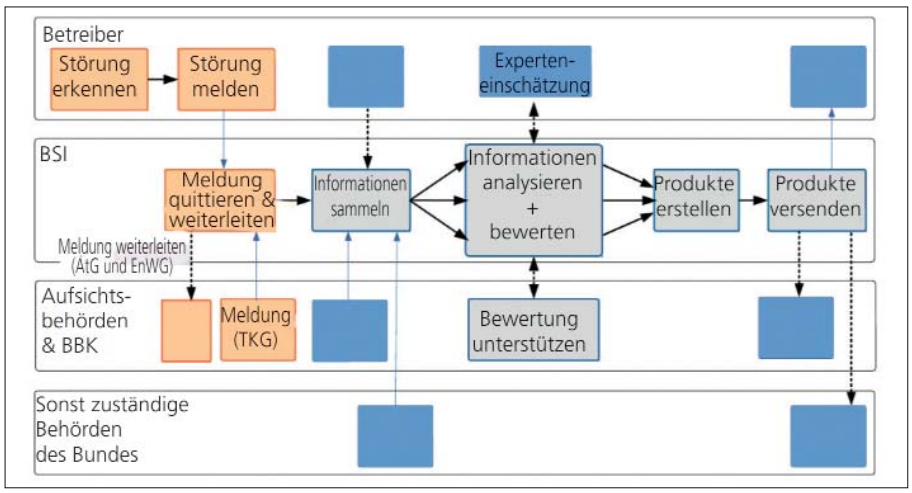
Mit dem IT-SiG wird ein All-Gefahren-Ansatz verfolgt. Es ist somit nicht relevant, weshalb ein IT-System ausfällt, sondern dass es ausgefallen ist. Dazu sind alle Bedrohungen zu betrachten, zu denen nicht nur die klassischen IT-Bedrohungen wie DDoS, APT-Spoofing oder Hacking gehören, sondern auch Naturkatastrophen oder Social Engineering und der dadurch entstehende mögliche Missbrauch. Des Weiteren müssen neben den Bedrohun-

gen auch Schwachstellen (technische und organisatorische oder Fehlverhalten des Menschen) betrachtet werden.

Mindestniveau

Mithilfe des IT-SiG werden Mindeststandards, also ein Mindestsicherheitsniveau, innerhalb des BSI-Gesetzes reguliert. Insbesondere § 8a „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" gibt vor, dass spätestens zwei Jahre nach Inkrafttreten des Gesetzes (gemäß § 10) Kritis-Betreiber verpflichtet sind, adäquate technische und organisatorische Schutzmaßnahmen zu gewährleisten. Dies bezieht sich auf die Schutzziele (Integrität, Vertraulichkeit, Verfügbarkeit und Authentizität) der Informationssicherheit der informationstechnischen Systeme. Der Stand der Technik ist dabei nicht nur zu berücksichtigen, sondern auch einzuhalten. Jedoch führt die Gesetzgebung den Begriff „Stand der Technik" nicht näher aus. Ebenso wird jedem einzelnen die Umsetzung überlassen, auch werden die Vorgaben nicht näher definiert. Allein in der Gesetzesbegründung wird der Begriff konkretisiert und auf internationale, europäische und nationale Normen und Standards verwiesen. Dennoch besteht für jede einzelne Branche gemäß § 8b des BSIG die Möglichkeit, dass die Betreiber spezifische Sicherheitsstandards verfassen und dem BSI vorlegen. Die Vorschläge müssen analog zu den Anforderungen nach § 8a Abs.1 BSIG sein. Einzig zu berücksichtigen bei der Erarbeitung ist der Umsetzungsplan KRITIS (UP KRITIS).

An dieser Stelle wird auf den IT-Grundschutz des BSI referenziert. Dort beschreibt der Maßnahmenkatalog die Abläufe, um IT-Sicherheit auf ein gegebenes Maß zu bringen und optional eine entsprechende Zertifizierung zu erlangen. Mit dem Ziel einer internationalen Vergleichbarkeit können die BSI-Standards der ISO-27000-Normenreihe zugeordnet werden. Dennoch ist nicht eindeutig, wie die technisch-organisatorischen Maßnahmen branchenspezifisch vollzogen werden müssen. Die Sollvorschrift mit der Ausgestaltung des Begriffs „Stand der Technik" resultiert aus dem Umstand, dass



Melde- und Informationsflüsse nach § 8b des BSIG *(Quelle: https://tinyurl.com/yy5xmeym)*

Kritis-Betreiber teilweise Maßnahmen nicht umsetzen können. Denn z.B. müssten zeitnah Sicherheits-Updates durchgeführt werden, damit das System wieder dem „Stand der Technik" entspricht. Es kann jedoch nicht sichergestellt werden, dass die Sicherheits-Updates nicht zu Systemausfällen von IT-Systemen führen und ob sie notwendige Betriebsprozesse stören.

Meldewesen

Das IT-SiG hat zwei Kernforderungen: Als erstes sind Kritis-Betreiber verpflichtet, ein Mindestsicherheitsniveau für ihre IT-Infrastruktur einzuhalten. Zweitens müssen sie ein Meldewesen, das für erhebliche Störungen der IT-Systeme zuständig ist, installieren und unterhalten. Das Meldewesen nach § 8b „Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen" wird durch das IT-SiG reguliert. Das BSI ist als zentrale Meldestelle für Kritis-Betreiber in Bezug auf Angelegenheiten, die die Sicherheit in der IT betreffen, vorgegeben. Kritis-Betreiber haben beim BSI eine Kontaktstelle anzugeben, die der zuständige Empfangspunkt gegenüber dem BSI ist. Dabei muss der Betreiber über die Kontaktstelle jederzeit erreichbar sein. Des Weiteren sind weitreichende Störungen der Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität der Prozesse, Komponenten oder IT-Systeme, die zur Störung oder zum Ausfall führen können oder in der Vergangenheit geführt haben, umgehend (innerhalb 1 h, in Anlehnung an „MaSi"; Mindestanforderungen an die Sicherheit von Internetzahlungen) ans BSI zu melden. Die Meldung muss folgende Angaben enthalten:

- Störung;
- technische Rahmenbedingungen;
- vermutete oder tatsächliche Ursache;
- Art der betroffenen Einrichtung oder Anlage;
- Branche.

Hat die Störung zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der kritischen Infrastruktur geführt, ist der Betreibende zu nennen. Für Betreiber aus dem gleichen Sektor wird die Möglichkeit eingeräumt, einen Single Point of Contact (SPoC) einzurichten, der eine gemeinsame übergeordnete Ansprechstelle und dem BSI gegenüber die einzige Kontaktstelle ist. Der Informationsaustausch zwischen BSI und den Kontaktstellen erfolgt ausschließlich über die gemeinsame Ansprechstelle.

Bild 2 zeigt einen möglichen Informations- und Meldefluss. Erkennt der Betreiber eine Störung, ist diese an das BSI über die Kontaktstelle zu melden. Das BSI quittiert die Meldung, leitet diese an die Aufsichtsbehörde weiter und sammelt von den verschiedenen Institutionen (Behörden des Bundes, Betreiber und Aufsichtsbehörde) Informationen über den Vorfall. Diese Informationen werden analysiert und bewertet. Dabei wird das BSI von Experten des Betreibers und von der Aufsichtsbehörde unterstützt. Nach Abschluss der Analyse und Bewertung

wird ein Protokoll erstellt und an die mitwirkenden Institutionen versendet.

Auswirkungen

Für Kritis-Betreiber bedeutet das IT-SiG, dass ein Meldewesen eingeführt wurde. Jeder Betreiber ist dazu verpflichtet, dem BSI gegenüber eine Kontaktstelle zu nennen. Des Weiteren müssen betroffene Unternehmen oder Organisationen ihre IT-Systemabsicherung auf den „Stand der Technik" bringen. Sofern nicht anders verordnet, muss die IT-Systemabsicherung nach „Stand der Technik" alle zwei Jahre geprüft werden. Kommen Betreiber dieser Pflicht nicht nach, ist mit Bußgeldern zu rechnen. Die Nachweise bzw. Überprüfung liegt erstmal bei den Betreibern selbst in Form von durchgeführten Audits, Prüfungen oder Zertifizierungen. Dadurch wird jedem einzelnen Betreiber Eigenverantwortung eingeräumt. Die verpflichtende Regelung verlangt, dass Vorgänge vertrauensbildend und transparent gehandhabt werden. Dabei sind die Betreiber nicht außen vorgelassen, sondern dazu angehalten, sich bei der Rechtsgestaltung entscheidend einzubringen. Genauso haben Kritis-Betreiber eine offene Handhabung, wie sie den Umgang mit den Meldungen an das BSI ausgestalten bzw. wie die Betreiber damit umgehen.

Handlungsempfehlungen

Die Handlungsempfehlungen stützen sich auf Ergebnisse der durchgeführten Audits. Im Fokus stehen besonders Betreiber, die bisher kein festgelegtes Sicherheitskonzept erstellt haben, aber durch das IT-SiG nun als Kritis-Betreiber erfasst werden. IT-Sicherheitsvorfälle zu dokumentieren, ist nicht nur hinsichtlich der Umsetzung der IT-SiG-Anforderungen von Bedeutung, sondern auch dann, wenn es zu Vermögensschäden durch Betriebsausfälle kommt. Hier ist die Dokumentation wichtig für die zivilrechtliche Haftung. Deshalb stellt die Norm ISO 27001 umfangreiche Dokumentationsanforderungen an die Geschäftsprozesse. Wichtig ist dies in Bezug auf Handlungsanweisungen für Notsituationen, so dass klare personelle Rollen zugeordnet werden können und Maßnahmen gegen vorsätzliche Angriffe oder Naturkatastrophen festgehalten sind. Die Dokumentation ist möglichst dem gesamten Personal zugänglich zu machen. Für einen Notbetrieb und kurze Reaktionszeiten sollte eine aktuelle Liste mit Verantwortlichen vorhanden sein. Die IT-Sicherheit betreffend sind Schutzziele wie Integrität, Vertraulichkeit, Verfügbarkeit und Authentizität zu wahren und diesbezüglich Maßnahmen zu ergreifen. Zum Beispiel können zur Wahrung der Integrität Signaturen für den Versand von E-Mails genutzt werden. Es reicht nicht aus, sich allein auf den beauftragten IT-Dienstleister zu verlassen (sofern vorhanden). Sondern der Prozess sollte intern durch Qualitätsprüfung der erbrachten Leistungen des Dienstleisters überprüft werden.

Bei der Meldepflicht sind relevante Vorfälle zu dokumentieren. Dadurch lassen sich Vergleiche mit früheren Vorfällen anstellen und gegebenenfalls Angriffsmuster herausarbeiten.

Als Letztes seien bauliche Maßnahmen genannt. Beispielsweise spielt das Thema Brandschutz eine wesentliche Rolle bei der IT-Sicherheit, so dass z.B. Serverräume extra berücksichtigt werden. Weiter wären Zugriffskontrollen zu nennen, die bauliche Maßnahmen implizieren. Dadurch hat nur autorisiertes Personal Zutritt zu bestimmten Bereichen. Abschließend wird empfohlen, Systeme mit einem Monitoring zu versehen, damit Ausfälle oder Störungen an einem zentralen Punkt abrufbar sind und ggf. Benachrichtigungen an die verantwortlichen Personen versendet werden können.

Fazit

Seit Mitte 2015 sind Betreiber besonders gefährdeter Infrastrukturen verpflichtet, ihre IT-Systeme und -Prozesse nach dem „Stand der Technik" zu schützen. Die BSI-Kritisverordnung (BSI-KritisV) legt fest, wer davon betroffen ist. Das IT-SiG erweitert bestehende Gesetze wie das BSIG oder TKG. Dabei haben Kritis-Betreiber ein gewisses Maß an Gestaltungsfreiraum und dürfen bzw. sollen es mitgestalten. Dies ist auch insoweit sinnvoll, da branchenübergreifend nicht dieselben Bedingungen vorliegen. Einzig bleibt die mehr oder weniger nicht klar ausgeführte Definition des Begriffs „Stand der Technik". Die Verantwortung bleibt somit beim Betreiber. Die daraus resultierende Konsequenz ist, dass im Falle eines Vorfalls die Beweislast beim Betreiber liegt. Dieser ist dann in der Pflicht nachzuweisen, dass die Technik tatsächlich dem „Stand der Technik" entsprach. Ohne klare Definition wird dies schwierig sein.

Die mit dem Gesetz verordneten Schnittstellen zwischen Betreibern und BSI bedeuten für die Betreiber einen zusätzlichen Verwaltungsaufwand. Die daraus resultierende Verantwortlichkeit schafft eine klare Richtlinie und vor allem Transparenz (Welche Meldung kommt von welchem Betreiber?) sowie der Verantwortlichkeit, nicht nur dem BSI gegenüber, sondern auch innerhalb des Unternehmens. Die Möglichkeit einer zentralen Stelle innerhalb eines Sektors erscheint sinnvoll, da dort Kompetenz gebündelt werden kann. Außerdem hat dann nicht jeder einzelne Betreiber diesen Verwaltungsmehraufwand. Den aktuell geltenden Meldepflichten nach § 8b BSIG wird oft nicht vollumfänglich nachgekommen, aus Furcht vor Imageschäden oder aber auch aus Gründen der uneindeutigen Definition eines Vorfalls. Eine Webseite mit Erläuterungen zur Meldepflicht mit pragmatischen Beispielen findet sich unter **https://tinyurl.com/y5lgtmzz**.

Gefährdungen kann man nur hinreichend begegnen, wenn das Gesetz weiterentwickelt und angepasst wird. Es wird erwartet, dass weitere Sektoren dazukommen, auch sollen die Schwellenwerte gesenkt werden. Voraussichtlich rückt der Mittelstand stärker in den Fokus. Auch die BSI-KritisV wird wohl angepasst werden. Sektoren, die z.B. von der Bundesnetzagentur und der BaFin betreut werden, müssen oft eigene Kritis-Anforderungen, die i.d.R. konkreter als die allgemeinen Anforderungen gemäß BSIG sind, erfüllen. Wie es in Zukunft weitergeht, ist abhängig davon, wie sich die Betreiber einbringen und das IT-SiG mitgestalten. *(bk)*