Der Schutz Kritischer Infrastrukturen

Das neue IT-Sicherheitsgesetz der Bundesregierung stellt hohe Anforderungen an Unternehmen, die kritische Infastrukturen betreiben. Wie die Betreiber diesen begegnen können, erläutert Jennifer Lüken, Beraterin Informationssicherheit bei Security Spezialist ConSecur.

Mit zunehmender Vernetzung werden kritische Infrastrukturen wie Energieversorgung anfälliger für Angriffe und IT-Ausfälle. Damit die Unternehmen Vorsorge treffen und ihre IT schützen, hat die Bundesregierung das IT-Sicherheitsgesetz verabschiedet.

Im §1 Abs. 2 ist definiert: „Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."

Eine Bestimmung der Kritischen Infrastrukturen und ihrer Betreiber erfolgt mittels einer Verordnung zum IT-Sicherheitsgesetz. Für die Sektoren Energie, Ernährung, Wasser sowie Informations- und Kommunikationstechnik existiert bereits eine solche Verordnung. Die Identifizierung der Kritischer Infrastrukturen und Betreiber der übrigen Sektoren soll bis Anfang 2017 mittels Änderungsverordnung erfolgen.

Das fordert das IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz beinhaltet zwei wesentliche Pflichten für die Betreiber Kritischer Infrastrukturen. Die erste ist, ein Mindestniveau an IT-Sicherheit einzuhalten. Innerhalb von zwei Jahren nach Inkrafttreten der Verordnung sollen die Betreiber nach § 8a Abs. 1 Satz 1 des IT-Sicherheitsgesetzes „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse [...] treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Infrastruktur maßgeblich sind".

Die zweite ist die Meldepflicht. Betreiber Kritischer Infrastrukturen haben nach § 8b Abs. 4 Satz 1 des IT-Sicherheitsgesetzes „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder geführt haben [...] unverzüglich an das Bundesamt [für Sicherheit in der Informationstechnik] zu melden".

Die Auswirkungen für Unternehmen

Ein Mindestniveau an Informationssicherheit umzusetzen und aufrecht zu erhalten, bedeutet ein Information Security Management Systems (ISMS) einzuführen und zu betreiben.

Es gibt diverse IT-Sicherheitsstandards, die Unternehmen unterstützen können diese Anforderung des IT-Sicherheitsgesetzes umzusetzen. Die bekanntesten Standards sind der „IT-Grundschutz" des BSI und die „ISO/IEC 27001". Ferner lässt das IT-Sicherheitsgesetz den Betreibern die Freiheit, über ihre Branchenverbände eigene, sektorspezifische Standards auszuarbeiten und dem BSI zur Genehmigung vorzulegen. Die Entscheidung, welcher Standard zum Einsatz kommt, liegt bei den Betreibern.

ConSecur Incident Management Spezialisten.

Die Empfehlung zur Umsetzung eines ISMS, lässt sich aus den Vorgaben des IT-Sicherheitsgesetzes ablesen. So ist zum Beispiel in § 8a Abs. 1 Satz 2 gefordert, dass für die Sicherheit der Kritischen Infrastruktur der „Stand der Technik" eingehalten werden muss. Dies bedarf einer ständigen Überarbeitung, Überwachung und Verbesserung der IT-Sicherheitstechnik. In § 8a Absatz 3 schreibt das IT-Sicherheitsgesetz vor, dass Unternehmen die Einhaltung der Anforderungen mindestens alle zwei Jahre nachweisen müssen. Darauf zielt auch ein ISMS ab. Darüber hinaus basiert ein ISMS auf einem Risikomanagement. Das Betreiben eines Risikomanagements wird im IT-Sicherheitsgesetz durch das Wort „angemessen" in § 8a Abs. 1 Satz 1 gefordert. „Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht" (§8a Abs. 1 Satz 3). Die Verhältnismäßigkeit stellt ein Risikomanagement fest.

Ergebnisse des Risikomanagements können etwa das Umsetzen von Network Access Control (NAC) Lösungen sein, die das Netzwerk vor Eindringlingen schützen.

Aus der in § 8a Abs. 1 Satz 1 geforderten „Vermeidung von Störungen der Verfügbarkeit" ergibt sich eine weitere Anforderung: das Betreiben eines Business Continuity Managements. Notfallpläne helfen während eines Krisenfalls die kritischen Infrastrukturen schnellstmöglich wieder aufzubauen.

Eine weitere Forderung innerhalb des IT-Sicherheitsgesetzes ist das Betreiben eines Incident Managements. Dies ergibt sich aus der Meldepflicht.

Zu meldende Sicherheitsstörfälle zuverlässig erkennen

Unternehmen können Störungen nur melden, wenn sie Vorfälle, die zu solchen Störungen führen, erkennen, bewerten und behandeln. Um dem Gesetz Genüge zu tun, müssen sie Vorfälle dann an das Bundesamt melden.

Hierzu müssen die Betreiber zunächst Vorfälle erkennen und die Ursachen ermitteln, um sie im Anschluss zu bewerten und zu melden. Als Werkzeug hierzu eignet sich ein Security Information und Eventmanagement (SIEM). Ein SIEM kann helfen, das Ausmaß der Störungen zu reduzieren, indem ein Vorfall schnellstmöglich erkannt wird und durch entsprechende Maßnahmen die Auswirkungen minimiert werden.

Daher ist ein SIEM besonders für Kritische Infrastrukturen unabdinglich. Es sorgt dafür, dass Störungen der Kritischen Infrastrukturen beseitigt werden und dass der definierte Betriebszustand einer Infrastruktur schnellstmöglich wiederhergestellt wird.

Unterstützung bei der Umsetzung

Die Einführung und der Betrieb eines ISM-Systems oder eines SIEM-Systems stellt erhebliche technische und organisatorische Anforderungen an das Management aber auch die IT-Organisation der betroffenen Unternehmen. Als hersteller-unabhängiges Consultinghaus unterstützt ConSecur bei sämtlichen Prozessschritten: Von der Interpretation des IT-Sicherheitsgesetzes über die Analysen im Rahmen des Risiko Managements bis zur Umsetzung der erforderlichen Maßnahmen.

ConSecur Cyber Defense Center.

www.consecur.de