PMeV NETZWERK SICHERE KOMMUNIKATION
KOMPAKT Nr. 3/2019

Kritische Infrastrukturen: Sicherheitsanalyse nach BSI-Grundschutz

Von Stephan Plaspohl *

Mittlerweile existiert eine nahezu unüberschaubare Flut an Informationen, die sich um das Thema kritische Infrastrukturen (KRITIS) ranken. Das übergeordnete Ziel dieses Paragraphen- und Gesetzesdschungels besteht darin, die gemeinsame Verantwortung für Staat und Wirtschaft zur Sicherstellung der Versorgung der Bevölkerung und der Wirtschaft nachhaltiger und umfassender wahrzunehmen. Das IT-Sicherheitsgesetz und die KRITIS-Verordnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verpflichten die Betreiber kritischer Infrastrukturen zur Umsetzung von Sicherheitsmaßnahmen nach dem „Stand der Technik“ und zur Meldung von Sicherheitsvorfällen.

Umsetzung von Sicherheitsmaßnahmen

Hierzu zählen die regelmäßige Überprüfung und der Nachweis der IT-Sicherheit, die Einrichtung einer Kontaktstelle für das BSI zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie die Einführung eines Informations-Managementsystems (ISMS). Für die Energiewirtschaft gelten ergänzend Regelungen im Energiewirtschaftsgesetz (EnWG). Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) lässt den Betreibern bewusst viel Spielraum, wie die Umsetzung des geforderten „Stands der Technik“ realisiert und eine Prüfung vorgenommen werden kann. Dabei können und sollen die Betreiber kritischer Infrastrukturen auf bereits bestehende Sicherheitsmechanismen aufsetzen. Wer allerdings eine auf BSI IT-Grundschutz basierende oder native ISO 27001-Zertifizierung vorlegen und gleichzeitig auch nachweisen kann, dass sowohl der Regelungsbereich als auch Maßnahmen geeignet sind, um die kritischen Dienstleistungen ausreichend zu schützen, der hat die Voraussetzungen zur Erfüllung der Anforderungen des BSIG geschaffen.

Einstieg in ein Sicherheitsmanagement

Die im Oktober 2017 veröffentlichten neuen BSI-Standards 200-1 bis 200-3 machen einen abgestuften Einstieg in ein Sicherheitsmanagement möglich und bieten Hilfestellung bei der Einführung und Aufrechterhaltung eines ISMS. Die Standards der 200er-Reihe lösen dabei die alten Standards 100-1 bis 100-3 ab. Während der BSI-Standard 200-1 allgemeine Anforderungen an ein ISMS definiert, hat der BSI-Standard 200-2 die IT-Grundschutz-Methodik zum Thema. Die Risikoanalyse auf der Basis von IT-Grundschutz wird durch den BSI-Standard 200-3 abgedeckt. Ergänzt werden diese drei Standards durch IT-Grundschutz-Bausteine, die im IT-Grundschutz-Kompendium zusammengefasst sind.

Abhängig davon, welche Ansätze zur Informationssicherheit bereits im Unternehmen verfolgt werden, kann es zweckmäßig sein, zunächst von einer „vollständigen“ IT-Grundschutz-Vorgehensweise („Standard-Absicherung“) abzusehen. Beispielsweise kann sich ein Unternehmen zum Ziel setzen, zunächst möglichst flächendeckend alle Basis-Anforderungen umzusetzen (sog. „Basis-Absicherung“), um schnellstmöglich die größten Risiken zu senken, bevor die tatsächlichen Sicherheitsanforderungen im Detail analysiert werden. Ein weiterer möglicher Ansatz ist, sich zunächst auf den Schutz der wesentlichen Werte des Unternehmens zu konzentrieren (sog. „Kern-Absicherung“). Der BSI-Standard 200-3 beschreibt, wie für bestimmte Zielobjekte festgestellt werden kann, ob und in welcher Hinsicht über den IT-Grundschutz hinaus Handlungsbedarf besteht, um Informationssicherheitsrisiken zu reduzieren. Dabei kann die im IT-Grundschutz-Kompendium enthaltene Liste von elementaren Gefährdungen als Hilfsmittel verwendet werden.

Sicherheitsprozess ins Leben rufen

Die Leitung des Unternehmens muss den Sicherheitsprozess anstoßen, steuern und kontrollieren. Hierfür sind sowohl strategische Leitaussagen zur Informationssicherheit als auch organisatorische Rahmenbedingungen erforderlich.

- Übernahme der Verantwortung durch die Unternehmensleitung
- Bereitstellung von finanziellen und personellen Ressourcen
- Konzeption und Planung des Sicherheitsprozesses
- Festlegung für eine Vorgehensweise

Leitlinie zur Informationssicherheit

Die Leitlinie zur Informationssicherheit beschreibt, welche Sicherheitsziele und welches Sicherheitsniveau das jeweilige Unternehmen anstrebt, was die Motivation hierfür ist und mit welchen Maßnahmen und mit welchen Strukturen dies erreicht werden soll. Jeder Mitarbeiter sollte die Inhalte der Sicherheitsleitlinie kennen und nachvollziehen können.

Organisation des Sicherheitsprozesses

Für das Informationssicherheitsmanagement muss eine für Größe und Art der Institution geeignete Organisationsstruktur aufgebaut werden.

Erstellung einer Sicherheitskonzeption

Nachdem ein Informationssicherheitsprozess initiiert worden ist und die Sicherheitsleitlinie und Informationssicherheitsorganisation definiert wurden, ist für das Unternehmen die Sicherheitskonzeption zu erstellen. Als Grundlage finden sich in den Bausteinen des IT-Grundschutz-Kompendiums für typische Komponenten von Geschäftsprozessen, Anwendungen, IT-Systeme und weitere Objekte entsprechende Sicherheitsanforderungen nach dem Stand der Technik. Diese sind thematisch in Bausteine strukturiert; sie setzen modular aufeinander auf.

Abhängig davon, ob eine Basis-, Standard- oder Kern-Absicherung angestrebt wird, unterscheiden sich die einzelnen Aktivitäten zur Erstellung einer Sicherheitskonzeption etwas. Bei Anwendung des IT-Grundschutzes wird ein Soll-Ist-Vergleich zwischen den Sicherheitsanforderungen aus den relevanten Bausteinen des IT-Grundschutz-Kompendiums und den im Unternehmen bereits umgesetzten Maßnahmen durchgeführt. Dabei festgestellte fehlende oder nur unzureichend erfüllte Anforderungen zeigen die Sicherheitsdefizite auf, die es durch die Umsetzung von Maßnahmen zu beseitigen gilt. Bei einem signifikant höheren Schutzbedarf ist unter Beachtung von Kosten- und Wirksamkeitsaspekten zusätzlich eine Risikoanalyse durchzuführen.

Umsetzung der Sicherheitskonzeption

Ein ausreichendes Sicherheitsniveau ist nur zu erreichen, wenn bestehende Defizite ermittelt, der aktuelle Status in einem Sicherheitskonzept festgehalten, erforderliche Maßnahmen identifiziert und diese Maßnahmen insbesondere auch konsequent umgesetzt werden.

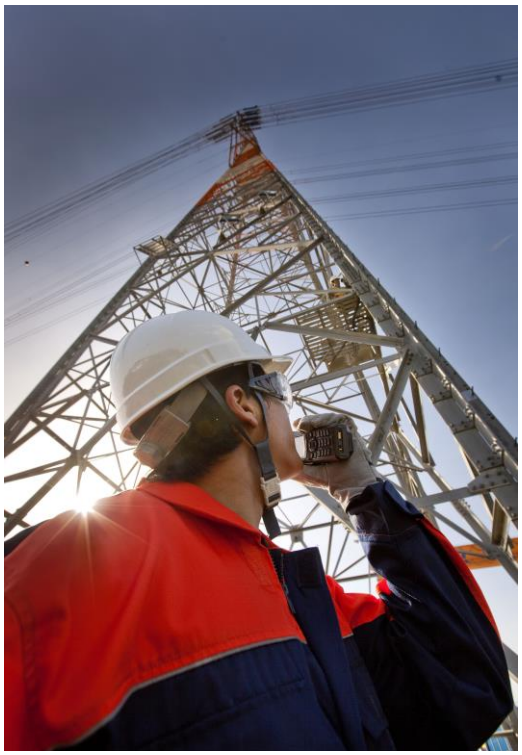
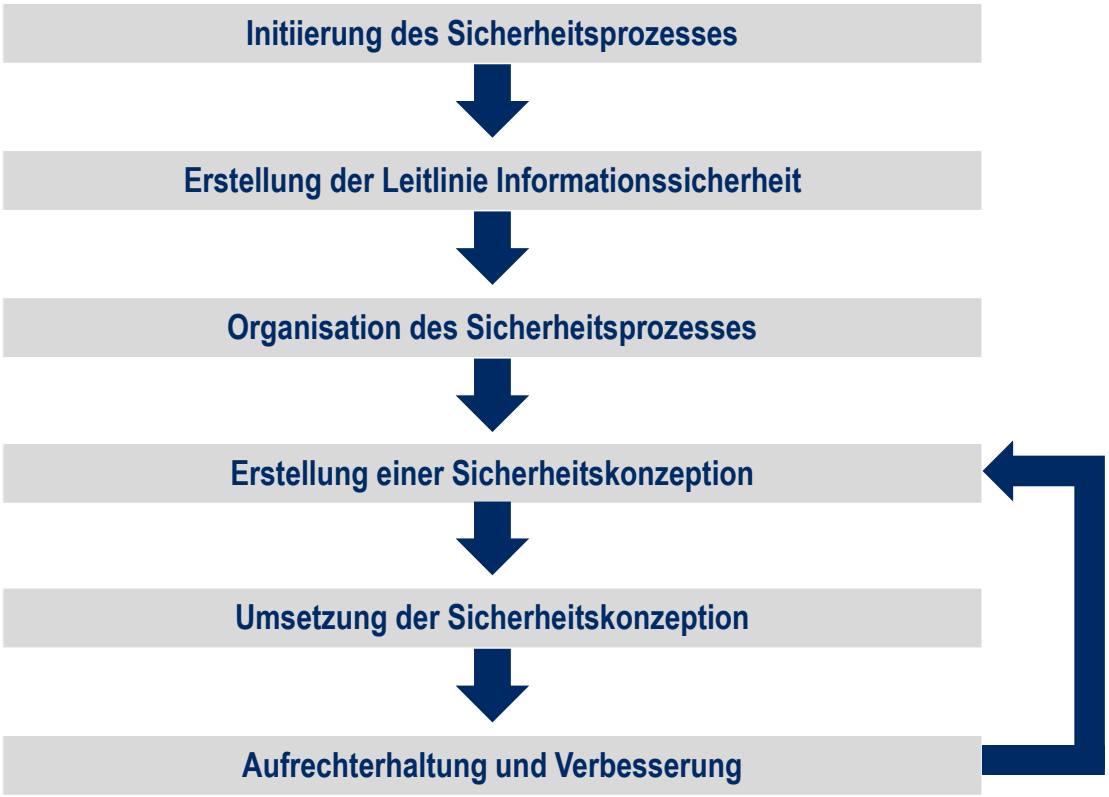


Bild: Airbus Defence and Space

Aufrechterhaltung und Verbesserung

- Beseitigung von Fehlern
- Aktualisierung / Fortentwicklung des ISMS
- Erweiterung der gewählten Vorgehensweisen
- Kontinuierliche Verbesserung von Sicherheitsmaßnahmen



Grafik: DOK Systeme – in Anlehnung an BSI-Standard 200-2

Zertifizierung

Um die erfolgreiche Umsetzung von IT-Grundschutz eines Unternehmens nach außen transparent machen zu können, kann sich das Unternehmen nach ISO/IEC 27001 zertifizieren lassen. Grundlage für die Vergabe eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz ist die Durchführung eines Audits durch einen externen, beim BSI zertifizierten Auditor. Das Ergebnis des Audits ist ein Auditbericht, der der Zertifizierungsstelle vorgelegt wird, die über die Vergabe des ISO 27001-Zertifikats auf der Basis von IT-Grundschutz entscheidet. Über ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz wird zunächst nachgewiesen, dass IT-Grundschutz im betrachteten Informationsverbund erfolgreich umgesetzt worden ist. Darüber hinaus zeigt ein solches Zertifikat auch, dass in dem jeweiligen Unternehmen

- Informationssicherheit ein anerkannter Wert ist,
- ein funktionierendes ISMS vorhanden ist und
- zu einem bestimmten Zeitpunkt ein definiertes Sicherheitsniveau erreicht wurde.

Fazit

Ein Vorgehen nach IT-Grundschutz stellt eine langjährig erprobte und effiziente Möglichkeit zum Aufbau und zur Aufrechterhaltung eines angemessenen Schutzes aller Informationen eines Unternehmens dar; nicht zuletzt auch für Betreiber kritischer Infrastrukturen. Mit den seit Oktober 2017 veröffentlichten novellierten BSI-Standards 200-1 bis 200-3 stehen hierfür probate Anleitungen und Hilfsmittel zur Verfügung. Die erfolgreiche Implementierung und Aufrechterhaltung eines ISMS kann durch ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz unabhängig nachgewiesen werden.

* Der Autor:
Stephan Plaspohl ist Senior Consultant der DOK SYSTEME GmbH, einem Mitgliedsunternehmen des PMeV
info@doksysteme.de