Vorgehensweise zur Modellierung der unternehmensindividuellen Informationsverarbeitung

KRITIS-relevante Prozesse und Komponenten bestimmen

Das IT-Sicherheitsgesetz verpflichtet Betreiber kritischer Infrastrukturen dazu, angemessene Maßnahmen zum Schutz ihrer IT umzusetzen – allerdings nur für solche Systeme, Komponente oder Prozesse, die für den Betrieb der kritischen Infrastruktur entscheidend sind. Vor allen anderen Maßnahmen, wie zum Beispiel der Einführung eines Informationssicherheitsmanagementsystems, sollten Unternehmen also sehr sorgfältig ermitteln, welche Prozesse und Komponenten das überhaupt sind.

Von Dr.-Ing. Michael Gehrke, TTS Trusted Technologies and Solutions GmbH

Mit dem „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ oder kurz „IT-Sicherheitsgesetz“ (ITSiG) wurden, zum Beispiel im BSI-Gesetz (BSIG), neue Anforderungen an die IT-Sicherheit für Unternehmen der kritischen Infrastrukturen festgeschrieben. Danach müssen betroffene Unternehmen angemessene Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse umsetzen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind und die Umsetzung alle zwei Jahre nachweisen. Weiterhin ist eine Kontaktstelle zu benennen und sind Störungen der IT-Sicherheit an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden.

Wie kann nun aber ein Unternehmen der kritischen Infrastruktur bestimmen, welche seiner informationstechnischen Systeme, Komponenten oder Prozesse von den gesetzlichen Anforderungen betroffen sind? Und warum ist eine solche Abgrenzung überhaupt wichtig? Warum kann man nicht einfach sämtliche informationstechnischen Systeme, Komponenten oder Prozesse angemessen absichern?

Zunächst zur letzten Frage: Selbstverständlich kann ein Unternehmen, sofern es dies wirtschaftlich darstellen kann, sämtliche informationstechnischen Systeme, Komponenten oder Prozesse auf den geforderten Stand der Technik bezüglich der IT-Sicherheit bringen. Jedoch sind die Pflichten zum Nachweis der Umsetzung gemäß BSIG zur anlassbezogenen Meldung von IT-Sicherheitsvorfällen auf die-

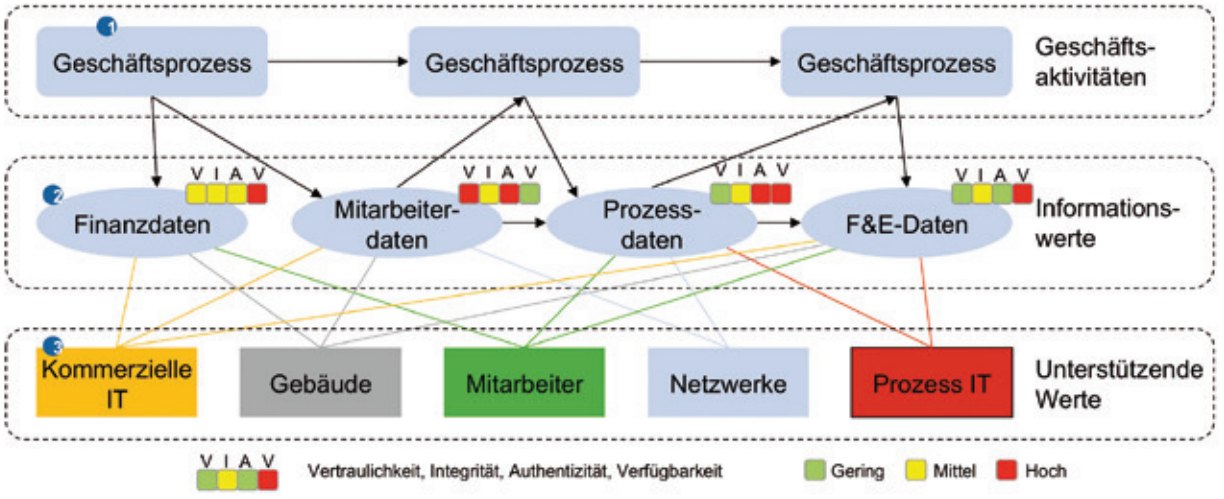

Abbildung 1: Modellierung der Informationsverarbeitung

© DATAKONTEXT GmbH · 50226 Frechen · <kes> Special „Kritische Infrastrukturen“ · Mai 2016

jenigen IT-Systeme, -Komponenten oder -Prozesse beschränkt, die für die Funktionsfähigkeit der kritischen Infrastrukturen maßgeblich sind. Damit ist klar, dass die Bestimmung des „Anwendungsbereichs der kritischen Infrastruktur IT“ frühzeitig und sorgfältig durchzuführen ist.

Anwendungsbereich und Vorgehensweise

Wie aber kann der Anwendungsbereich sinnvoll festgelegt werden? Eine erste grobe Orientierungshilfe liefert die Rechtsverordnung nach BSIG §10, die voraussichtlich für den Korb 1, also für die Sektoren Energie, Informations- und Kommunikationstechnik, Wasser und Ernährung Anfang Mai in Kraft tritt. Darin werden zunächst qualitativ die relevanten kritischen Dienstleistungen und die zugehörigen Anlagen bestimmt und Schwellenwerte definiert, die festlegen, ab wann eine kritische Infrastruktur vorliegt [2]. Beispielsweise sind „kritische“ Dienstleistungen im Sektor IKT „Sprach- und Datenverarbeitung“ sowie „Datenspeicherung und -verarbeitung“ – als Anlagen werden genannt „öffentliche Telefonnetze“, „Rechenzentren“ oder „DNS-Server“. Für ein öffentliches Telefonnetz liegt dabei der Schwellenwert bei 100 000 Teilnehmern, alles darüber gehört zur kritischen Infrastruktur.

Mit der Anwendung der Kriterien gemäß BSI-KritisV kann ein Unternehmen also zunächst bestimmen, ob es überhaupt zu den Betreibern der kritischen Infrastruktur gehört. Im nächsten Schritt muss eine Modellbildung der unternehmensindividuellen Informationsverarbeitung erarbeitet werden. Dafür hat sich folgende Vorgehensweise bewährt:

- Bestimmung der relevanten Geschäftsaktivitäten
- Bestimmung, Zuordnung und Bewertung der Informationswerte
- Bestimmung und Zuordnung der unterstützenden Werte

Geschäftsaktivitäten bestimmen

Zunächst werden diejenigen Geschäftsaktivitäten identifiziert, die für die Funktionsfähigkeit der kritischen Infrastrukturen notwendig sind (vgl. Abbildung 1, obere Ebene). In Abbildung 1 sind diese als „Geschäftsprozesse“ bezeichnet, aber die Geschäftsaktivitäten lassen sich ebenso gut anhand eines aktuellen Organisationshandbuchs identifizieren. Sollten Unternehmen relevante Aktivitäten im Rahmen eines Prozess-Outsourcings an Dienstleister vergeben haben, so sind auch diese hier mit einzuschließen, da abzusehen ist, dass Betreiber kritischer Infrastrukturen auch für ausgelagerte Dienstleistungen verantwortlich bleiben.

Informationswerte bestimmen, zuordnen und bewerten

Anschließend muss man je relevanter Geschäftsaktivität die Informationswerte bestimmen (vgl. Abbildung 1, mittlere Ebene), die zur Durchführung der Geschäftsaktivität erforderlich sind beziehungsweise die diese Geschäftsaktivität erzeugt. Die Informationswerte sind dann hinsichtlich ihrer potenziellen Schadensauswirkung bei Nichteinhaltung der Sicherheitsziele Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit zu bestimmen. Dabei wird die Frage beantwortet: „Welche geschäftlichen Konsequenzen hat es, wenn die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit eines Informationswertes verletzt wird?“

Damit diese Frage annähernd objektiv beantwortet werden kann, sind vorbereitend Bewertungskriterien festzulegen. Zunächst sollten dabei die möglichen Schadenskategorien definiert werden, beispielsweise „finanzielle Schäden“, „Schäden an Leib und Leben“ oder „Verstoß gegen Gesetze/Verträge“ [3]. Für den Bereich der kritischen Infrastrukturen sollte man besonderes Gewicht auf jene Schadenskategorien legen, die „negative Auswirkungen auf die Gesellschaft“ haben.

Da solche Auswirkungen nun gering oder auch erheblich sein können, müssen noch Schadensauswirkungsstufen und entsprechende Beschreibungen gefunden werden. Für die Stufen kann man die Vorgaben aus dem Sektor Energie zur Hilfe heranziehen. Im IT-Sicherheitskatalog für Energienetzbetreiber nach EnWG § 11 (1a), wurden als Abstufungen „mäßig“, „hoch“ und „kritisch“ festgelegt. In der Unternehmenspraxis werden häufig auch mehr als drei Schadensauswirkungsstufen verwendet, diese sind dann gegebenenfalls auf regulatorische Vorgaben abzubilden. Nun sind für diese Schadensauswirkungsstufen entsprechende Definitionen festzulegen, wie Tabelle 1 beispielhaft zeigt.

Die Bewertungskriterien sollten auch mit dem Unternehmensrisikomanagement abgestimmt werden, damit im weiteren Verlauf erkannte Risiken in das allgemeine Risikomanagement überführt werden können. Anhand der Bewertungskriterien sind dann mit den Vertretern der Geschäftsaktivitäten die Schadensauswirkungspotenziale der Informationswerte zu bestimmen. Entscheidend für diesen Schritt des Verfahrens ist es, die Analyse hier nicht zu detailliert durchzuführen. Als Faustregel gilt: Zwischen 10 und 20 Geschäftsaktivitäten und 5 bis 10 Informationswerte je Geschäftsaktivität sind noch sinnvoll.

Unterstützende Werte bestimmen und zuordnen

Schließlich werden alle diejenigen unterstützenden Werte identifiziert, die zur Verarbeitung jedes Informationswertes erforder-

Schadenskategorie	Schutzbedarf „mäßig“	Schutzbedarf „hoch“	Schutzbedarf „kritisch“
Negative Auswirkungen auf die Gesellschaft	Keine Auswirkungen auf die Gesellschaft, keine Gefährdung der öffentlichen Sicherheit	Auswirkungen auf die Gesellschaft sind möglich oder wahrnehmbar oder eine Gefährdung der öffentlichen Sicherheit kann in geringem Umfang erfolgen	Auswirkungen auf die Gesellschaft können erheblich sein oder eine erhebliche Gefährdung der öffentlichen Sicherheit ist möglich
Schäden an Leib und Leben	Keine Schäden an Leib und Leben zu erwarten	Leichte bis schwere Schäden an Leib und Leben	Lebensbedrohliche Schäden an Leib und Leben
Weitere	…	…	…

Tabelle 1: Beispiel Schadensauswirkungsstufen für „Negative Auswirkungen auf die Gesellschaft“

lich sind, und diesem zugeordnet. Es sollten nicht nur die informationstechnischen Systeme und Komponenten identifiziert werden, sondern auch weitere unterstützende Werte, wie Gebäude oder Mitarbeiter, da mit diesen ebenfalls Risiken und Sicherheitsmaßnahmen für die Informationswerte verbunden sein können. Wie bei der Modellierung eines Informationsverbundes nach BSI-Standard 100-2 [3], sollten auch hier gleichartige unterstützende Werte gruppiert werden, um die Komplexität des Ansatzes zu reduzieren.

Das Schadensauswirkungspotenzial der Informationswerte wird dann als Schutzbedarf auf die unterstützenden Werte weitergegeben beziehungsweise vererbt. Dabei sind einige Sonderfälle zu beachten, wie beispielsweise, dass nicht jeder unterstützende Wert jede Schadensauswirkung erben muss. Werden Gehaltslisten zu Informationszwecken auf einen Dateiserver exportiert, so muss dieser nicht zwangsläufig den Schutzbedarf für Verfügbarkeit erben, wohl aber das zentrale SAP HR-System, welches für die Gehaltsabrechnung genutzt wird.

Ergebnis

Im Ergebnis liegt eine Modellierung der prozessualen, informationellen wie systemtechnischen Landschaft eines Unternehmens vor, wo jedem unterstützenden Wert ein entsprechender Schutzbedarf zugewiesen ist. Im letzten Schritt werden nun diejenigen Werte in den Anwendungsbereich genommen, deren Schutzbedarf mindestens „hoch“ ist und dies auf die Schadenskategorie „Negative Auswirkungen auf die Gesellschaft“ zurückzuführen ist. Der Anwendungsbereich ist dann noch um eine organisatorische Abgrenzung zu vervollständigen, in dem die für die identifizierten Werte relevanten Organisationsteile übernommen werden.

Zum Zweck der Nachvollziehbarkeit sollten diese Analysen in die Dokumentenlenkung des Unternehmens übernommen werden, denn eventuell ist gegenüber einem Auditor und dem BSI nachzuweisen, warum bestimmte informationstechnische Prozesse, Systeme oder Komponenten sich nicht im Anwendungsbereich befinden.

Fazit

Die vorgestellte Vorgehensweise ist bereits in vielen Projekten mit Unternehmen der kritischen Infrastrukturen angewendet worden und zeichnet sich dadurch aus, dass sie zu nachvollziehbaren Ergebnissen über die Ebenen der Geschäftsprozesse, Informationsbestände und informationsverarbeitenden Systeme kommt. Die Definition des Anwendungsbereichs ist somit der Ausgangspunkt für alle weiteren Aktivitäten zur Umsetzung von Sicherheitsmaßnahmen nach dem Stand der Technik und dem wohl zwangsläufig erforderlichen Managementsystem für Informationssicherheit (ISO 27001) und Geschäftskontinuität (ISO 22301). ■

Literatur

[1] Referentenentwurf BSI-Kritisverordnung (BSI-KritisV), Stand: 13.1.2016, www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/kritis-vo.html, abgerufen am 03.04.2016

[2] Die Umsetzung des IT-Sicherheitsgesetzes, Ingrid Dubois, <kes> Nr. 1 2016

[3] BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 2.0, 2008, www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard02/ITGStandard02_node.html, abgerufen am 03.04.2016