IT·Grundschutz
Informationsdienst

Liebe Leserin, lieber Leser,
es ist eine Premiere, für uns und für Sie. Zum ersten Mal erscheint der Infodienst IT-Grundschutz als Teil der <kes>. Wir versprechen uns davon einen breiteren Leserkreis und mehr Fokus auf den IT-Grundschutz, denn allgemeine IT-Sicherheitsthemen sind in der <kes> bereits bestens aufgehoben. Sagen Sie uns was Sie davon halten, am besten per E-Mail an redaktion@grundschutz.info.

ISIS12 – Informationssicherheit für den Mittelstand *Seite 91*
Interview Isabel Münch - Die Zukunft des IT-Grundschutz *Seite 93*
IT-Grundschutz in der Energiewirtschaft *Seite 96*
IT-Grundschutz nach BSI strategisch planen *Seite 98*

ISIS12 – Informationssicherheit für den Mittelstand

Praxisnahes Verfahrensmodell bringt mehr Informationssicherheit

Michael Gruber, IT-Security Consultant, BSP. SECURITY

ISIS12 ist ein praxisnahes Verfahrensmodell um ein Informationssicherheits-Managementsystem (ISMS) mit integriertem IT-Servicemanagement (IT-SM) zu etablieren und zu betreiben. Es wurde speziell für den Mittelstand entwickelt und ist für diese Unternehmen als Einstieg in die Informationssicherheit gedacht, bevor der BSI IT-Grundschutz angegangen werden kann.

Der Geschäftsführer des mittelständischen Unternehmens „Musterfirma Präzisionsmaschinenbau GmbH“ sieht sich immer mehr mit den Themenbereichen IT-Compliance und Wirtschaftsspionage, den stetig ansteigenden Qualitätsanforderungen durch Kunden und mit verbindlichen Lieferterminen von Aufträgen konfrontiert. Dadurch spielen die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit für die strategische Planung eine zentrale Rolle.
Die Musterfirma betreibt bereits seit Jahren erfolgreich ein Qualitätsmanagement-System und ist nach ISO 9000 zertifiziert. Die existierenden Standards für die Bereiche Informationssicherheit und IT-Servicemanagement wie ISO/IEC 27001, BSI Grundschutz, ITIL oder ISO 20000 sind jedoch für den Mittelstand zu komplex, die Kosten für die Einführung und den laufenden Betrieb zu hoch. Unsere „Musterfirma Präzisionsmaschinenbau GmbH“ benötigt ein einfaches und trotzdem skalierbares Verfahren – ein ISMS light. Welche Wege stehen dem Unternehmen für die strategische Ausrichtung der Informationssicherheit zur Verfügung?

ISMS light: ISIS12

Ein solches ISMS light wurde vom Netzwerk für Informationssicherheit im Mittelstand (NIM) speziell für mittelständische Unternehmen (100 - 1000 PC-Arbeitsplätze) entwickelt: Das ISIS12 – Informationssicherheit Managementsystem in 12 Schritten. Die Entwicklung von ISIS12 durch NIM, bestehend aus sieben Unternehmen und zwei Hochschulen, wurde vom Bayerischen Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie gefördert. Das Bayerische IT-Sicherheitscluster hat das Netzwerkmanagement übernommen.
ISIS12 wurde bereits im Rahmen des BSI IT-Grundschutztages in Regensburg im Oktober 2011 vorgestellt. Mittlerweile steht ein fertig entwickeltes Vorgehensmodell bereit. Im „Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand“ wird das Verfahren didaktisch aufbereitet erklärt. Von der Universität Regensburg wurde auch ein begleitendes ISIS12 Software-Tool entwickelt.
ISIS12 ist ein zwölfstufiger Workflow, um ein Informationssicherheitsmanagement-System einfach einzuführen, zugeschnitten speziell für mittelständische Unternehmen. Es handelt sich um eine leicht verständliche Anleitung, die von ausgebildeten ISIS12-Consultants begleitet wird. Durch den integrierten Management-Ansatz werden

Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand

ISMS und IT-SM verknüpft. Das Verfahren kann als mögliche Vorstufe zur ISO/IEC 27001- oder BSI IT-Grundschutz-Zertifizierung verwendet werden.
Dazu wurde ein speziell angepasster ISIS12-Katalog aus dem BSI-Grundschutzkatalog und dem Standard ISO/IEC 27001 (Maßnahmenziele A.5– A.15) und den Konkretisierungen in ISO/IEC 27002 abgeleitet. Um die Anforderungen des Mittelstands besser abzubilden, behandelt ISIS12 nur eine Untermenge der in den genannten Standards vorgefundenen Sicherheitsmaßnahmen. Trotzdem stehen die Breitenwirkung, Umsetzbarkeit und systematische Abdeckung von Gefährdungen durch korrespondierende Sicherheitsmaßnahmen im Mittelpunkt. Der Detailierungsgrad zwischen BSI IT-Grundschutz (extrem hoch) und der ISO/IEC 27001 (minimalistisch und abstrakt), wurde bewusst auf die Zielgruppe der mittelständischen Unternehmen angepasst.

Phasenweises vorgehen

Phase 1: Initialisierungsphase

ISIS12 ist ein klassischer Top-Down-Ansatz. Die Unternehmensleitung trägt die Gesamtverantwortung für die Informationssicherheit und initiiert den dafür notwendigen Prozess. Dazu wird als erster Schritt eine Leitlinie zur Informationssicherheit erstellt und von der Unternehmensleitung als zentrales Strategiepapier unterzeichnet. Darin sind die Informationssicherheitsziele, sowie die daraus abgeleitete Strategie festgehalten. Im zweiten Schritt kommuniziert die Projektleitung auf allen Organisationsebenen, wie wichtig ISIS12 ist. Alle Mitarbeiter werden über den ISIS12-Workflow informiert, auf die Bedeutung der Informationssicherheit für das Unternehmen wird hingewiesen. Die Mitarbeiter werden regelmäßig über Neuerungen wie Ansprechpartner, Änderungen der Leitlinie oder Hinweise auf Verhaltensfehler informiert. Halten die Mitarbeiter Vorgaben der Leitlinie nicht ein, gibt es Sanktionen.

Phase 2: Aufbau- und Ablauforganisation festlegen

Es ist sinnvoll vor der eigentlichen Umsetzung und Entwicklung des Sicherheitskonzeptes, die Aufbau- und Ablauforganisation zu etablieren. Viele Projekte haben gezeigt, dass sich die operative Phase ohne diese Vorarbeiten erheblich verzögert. Daher wird im dritten Schritt ein Informationssicherheitsteam aufgebaut und Zusammensetzung, Aufgaben und Pflichten des Teams festgelegt. Die zentrale Rolle nimmt der Informationssicherheitsbeauftragte (ISB) ein, der auch für die Einführung und Betrieb von ISIS12 verantwortlich ist. Weitere Mitglieder können unter anderem sein: Datenschutzbeauftragter, QM-Beauftragter, IT-Mitarbeiter, Anwender-Vertreter, externer ISIS12-Berater. Die Unternehmensleitung erhält Berichte vom Team.
Schritt vier legt die Struktur der IT-Dokumentation fest. Neben formalen Festlegungen wie etwa Versionierung und verpflichtende Dokumenteninformationen werden verbindliche Rahmendokumente als Basis für das IT-Betriebshandbuch und IT-Notfallhandbuch erarbeitet. Im nächsten Schritt fünf geht es darum, die drei generischen IT-Service-Managementprozesse von ISIS12 einzuführen: Wartung, Änderung und Störungsbeseitigung. Die drei Basisprozesse greifen auf eine einzuführende Configuration Management Data Base (CMDB) zu. Sie enthält die Anforderungen an die IT-Systeme, die im ISIS12 Schritt sechs (MTA und SLA) in Form eines Service-Katalogs definiert werden.

Phase 3: Entwicklung und Umsetzung des ISMS

Nach den Vorarbeiten in den vorangegangenen Phasen beginnt mit Schritt sechs der operative Teil des ISIS12 Vorgehensmodells. Zunächst werden unternehmenskritische Anwendungen identifiziert und deren Schutzbedarf, bezogen auf die Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit, bewertet. Daraus lassen sich die maximal tolerierbare Ausfallzeit (MTA) und die Service Level Agreements (SLA) ableiten und im Service-Katalog dokumentieren. Danach, im Schritt sieben, analysiert der ISIS12-Anwender die IT-Struktur. Nachdem bereits kritische Anwendungen identifiziert wurden, ermittelt man nun die dafür notwendigen technischen, personellen, organisatorischen und infrastrukturellen Objekte. Wie relevant diese Rahmenbedingungen für die Applikationen sind, muss ebenfalls erfasst werden. Die Objekte erben dann den Schutzbedarf der kritischen Applikationen und die maximal tolerierbare Ausfallzeit.
Im Schritt acht erfolgt die Zuordnung der empfohlenen Sicherheitsmaßnahmen aus dem ISIS12-Katalog zu den vorher ermittelten Objekten. Gegenüber dem BSI-Grundschutzkatalog ist die Auswahl an Maßnahmen reduziert. Dadurch entsteht ein spezifisch angepasster Prüfplan, der im Schritt neun mit den tatsächlich vorhandenen und umgesetzten Maßnahmen verglichen wird. Der aktuelle Umsetzungsgrad wird mit „ja“, „teilweise“, „nein“ oder „nicht notwendig“ bewertet.

© SecuMedia Verlags-GmbH · D-55205 Ingelheim · IT-Grundschutz 2013/2

Fehlende oder noch nicht vollständig umgesetzte Sicherheitsmaßnahmen werden priorisiert und der Geschäftsleitung zusammen mit einer Kostenschätzung als Vorschlag präsentiert. Die Umsetzung nach einer vereinbarten Priorität ist Bestandteil von Schritt elf. Jede Maßnahme bekommt einen Initiator, einen Umsetzer und den Zeitpunkt der Realisierung zugeschrieben. Während die Sicherheitsmaßnahmen eingeführt werden, begleiten Schulungsmaßnahmen die Mitarbeiter.

Alles hat ein Ende, nur die Sicherheit nicht

Im vorläufig abschließenden Schritt zwölf geht es um Kontinuität. Gemäß des Plan-Do-Check-Act-Zyklus muss das Unternehmen untersuchen, ob die ISIS12-Schritte vollständig durchgeführt wurden. Für noch offene Sicherheitsmaßnahmen ist eine Art Revision notwendig, die Termine und den Reifegrad der Maßnahmen kontrolliert. Doch spätestens jetzt gilt: Das ISMS light ist etabliert und wird weiter optimiert.

Mit ISIS12 steht mittelständischen Unternehmen ein speziell zugeschnittenes ISMS zur Verfügung. Mittels einer abschließenden Zertifizierung durch die Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (DQS), kann der Kunde sein Engagement im Bereich Informationssicherheit eindrucksvoll demonstrieren. Das ist ein Wettbewerbsfaktor, der speziell für mittelständische Unternehmen immer wichtiger wird.

Interview Isabel Münch – Die Zukunft des IT-Grundschutz

Dipl.-Math. Isabel Münch ist seit 1994 beim Bundesamt für Sicherheit in der Informationstechnik (BSI), zurzeit als Referatsleiterin für Grundlagen der Informationssicherheit und IT-Grundschutz. Ihre Arbeitsschwerpunkte sind die Weiterentwicklung des IT-Grundschutzes, außerdem vertritt sie das BSI in verschiedenen nationalen und internationalen Gremien mit dem Schwerpunkt Sicherheitsmanagement.

Was ist heute die wichtigste Aufgabe des IT-Grundschutzes?

Der IT-Grundschutz soll auch heute das tun, was er schon immer getan hat: Nämlich möglichst konkrete Empfehlungen zur Informationssicherheit geben, die aus Praxiserfahrungen abgeleitet sind. Die Zwickmühle ist damals wie heute, so konkret wie möglich zu sein und die Vorgaben trotzdem nicht zu eng zu definieren, damit der gesunde Menschenverstand nach wie vor eine wichtige Rolle bei der Informationssicherheit spielen kann. Unsere Empfehlungen sollten an die konkreten Rahmenbedingungen einer Institution angepasst werden, es ist wichtig, dass das draußen in den Institutionen und Unternehmen ankommt. Weil wir konkretere Vorgaben machen als beispielsweise die ISO-Standards 27001 und 27002 ist der IT-Grundschutz umfassender, und darum sind wir auch konstant auf der Suche nach neuen Wegen, wie wir unsere Expertise vermitteln können. Es ist heute wichtiger als je zuvor, den Anwendern ideale Einstiegspunkte in die zur Zeit relevanten Thematiken zu bieten.

Es ist nicht einfach, Zertifizierungsreife zu erlangen. Wie sieht der Trend aus? Gibt es mehr Zertifizierungen?

Ich kann ganz klar sagen, dass die Nachfrage nach Zertifizierungen stark zunimmt. Im Januar 2013 haben wir bereits mehr laufende Zertifizierungsverfahren und Neuanträge als im ganzen Jahr 2012. Hinzu kommen Nachüberprüfungen und Überwachungsaudits. Wir stehen wirklich einem enormen Interesse gegenüber, was den IT-Grundschutz im Allgemeinen und die Zertifizierungen im Besonderen angeht. Ich sehe den Trend hin zum IT-Grundschutz vor allem durch die Forderungen nach entsprechenden Nachweisen von potenziellen Kunden gegenüber ihren Dienstleistern und von Aufsichtsstellen begründet. Ursprünglich war der IT-Grundschutz ja für Bundesbehörden geschaffen worden, aber von Anfang an nutzten auch viele Unternehmen den IT-Grundschutz als günstige, kompetente Sicherheitsanleitung, auch wenn keine Zertifizierung angestrebt wurde. Mittlerweile wird aber zunehmend bei Behörden und Firmen nachgefragt, wie diese ihre Informationssicherheit betreiben, und weil dort ohnehin schon nach IT-Grund-

schutz vorgegangen wird, ist es die logische Folge, eine Zertifizierung nachzuholen und so die korrekte Umsetzung von IT-Grundschutz nachzuweisen. Wir wissen natürlich auch, dass es nicht einfach ist, die Zertifizierungsreife zu erreichen, das dauert seine Zeit. Die gestiegene Nachfrage zeigt jedoch, dass wir nun langsam die Früchte unserer Arbeit der vergangenen Jahre ernten.

Bleiben Unternehmen und Behörden zertifiziert? Die Audits sind ja regelmäßig zu wiederholen, was immer wieder Aufwand nach sich zieht.

Natürlich werden immer wieder Zertifikate obsolet. Firmen verschwinden vom Markt oder der Geschäftsschwerpunkt verlagert sich, so dass sich der regelmäßige Nachweis der Zertifizierung nicht mehr lohnt. Trotzdem steigt die Gesamtzahl der zertifizierten Institutionen jedes Jahr an. Den IT-Grundschutz gibt es schon seit 1994, die Zertifizierung seit 2002. Wir haben in der Anfangszeit viel Überzeugungsarbeit geleistet und der Gedanke musste sich erst in den Köpfen der Anwender festsetzen. Als das BSI mit Common Criteria Zertifizierungen angefangen hat, lief das ganz ähnlich. Am Anfang lief es zäh, bis die Forderungen der Aufsichtsstellen und der Anwender in den Firmen angekommen waren, danach wurde das BSI von der Nachfrage förmlich überrollt. Im Moment sehen wir eine ganz ähnliche Stufe beim IT-Grundschutz erreicht. Vor allem die Bundesbehörden haben die Zertifizierung nach IT-Grundschutz auf ihren ToDo-Listen, wir erwarten hier in der nächsten Zeit enormes Interesse .

Wie viel Aufwand steckt von Ihrer Seite in einer solchen Zertifizierung?

Wir versuchen schon vor der Zertifizierung offene Fragen mit Institution und Auditor zu klären. Dabei geht es oft um Grundsätzliches wie die Unabhängigkeit des Auditors oder die Abgrenzung des Informationsverbunds, für den ein Zertifikat angestrebt wird. Die eingereichten Unterlagen durchzusehen und weitere Fragen zu klären, kann zwischen zwei und vier Wochen in Anspruch nehmen, je nachdem wie umfangreich die Umgebung bei der Institution ist. Uns als BSI sind feste Zeiten vorgegeben, wie lange eine solche Prüfung maximal dauern darf.

Was hat sich in den Zertifizierungen über die Jahre geändert? Laufen die noch nach dem gleichen Muster ab?

Wir haben den Zertifizierungsprozess im Lauf der Jahre verschlankt. Und natürlich passen wir uns auch den veränderten Marktanforderungen an. Zurzeit ist die zunehmende Virtualisierung etwas, worüber wir uns sehr viele Gedanken machen. Zusammengefasst geht es darum, wie die starke Nutzung von virtualisierten Systemen mit dem IT-Grundschutz abgebildet und zertifiziert werden kann. Etwas weiter gefasst hängt das natürlich auch mit der Thematik Cloud Computing zusammen. Wir versuchen, das entsprechend mit einzubauen. Auf Seiten der zertifizierten Institutionen sehen wir über die Jahre kleinere Änderungen. Meist ist das Informationssicherheitsmanagement in den Institutionen heute schon reifer, mittlerweile ist es auch üblich, externe Berater im Vorfeld einzubinden und nicht mehr alles allein zu machen. In der Regel ist es inzwischen auch so, dass man frühzeitig Kontakt mit Auditoren oder dem BSI aufnimmt und zu besprechen, ob die Institution schon reif für eine Zertifizierung ist und wo Nachholbedarf besteht. Das ist wichtig, um nicht in die falsche Richtung zu arbeiten. Natürlich haben auch die Auditoren mittlerweile mehr Erfahrung mit dem Prozess. Wir stehen im engen Kontakt mit den Auditoren und versuchen Erfahrungen in beiden Richtungen auszutauschen und schnell in das Prüfschema einfließen zu lassen. Darum gibt es auch mittlerweile im Jahresverlauf zahlreiche Veranstaltungen für den Informationsaustausch.

Ist die Zertifizierung mittlerweile ein Wirtschaftlichkeitsfaktor?

Häufig wirkt sich das indirekt aus. Mittlerweile lassen sich etwa die Hälfte der Institutionen zertifizieren, weil sie durch Kunden oder ein Gesetz dazu aufgefordert werden. Es gibt eine ganze Reihe von Gesetzen und Richtlinien, in denen ISO 27001, IT-Grundschutz oder zumindest dessen Vorgehensweise explizit gefordert werden. Wir erleben es inzwischen beispielsweise häufig, dass Behörden bei der Suche nach einem Dienstleister eine IT-Grundschutz Zertifizierung verlangen. Darum sind zurzeit sehr viele Anbieter von Rechenzentrumsdienstleistungen unter den Antragstellern. Einen direkten finanziellen Vorteil gibt es nicht, beispielsweise niedrigere Versicherungsprämien wenn ein Zertifizierung vorliegt. Das war mal in der Diskussion, wurde aber letztendlich nicht umgesetzt. Der betriebswirtschaftliche Aufwand wäre für die Versicherungen zu hoch gewesen.

Würde es der Verbreitung und dem Image des IT-Grundschutzes helfen, wenn es zusätzliche Berufe im Umfeld des IT-Grundschutzes als anerkannte IT-Berufe geben würde?

Wir hören immer wieder, dass es – neben den Auditoren – Interesse an Ausbildungen im Bereich des IT-Grundschutzes gibt. Etwas wie ein IT-Grundschutz-Experte wird häufig nachgefragt. Auch intern diskutieren wir, dies beispielsweise als Ausbildung aufzusetzen und anzubieten. Bisher haben wir jedoch noch kein Ergebnis.

In der Vergangenheit gab es immer wieder eine Zusammenarbeit mit

© SecuMedia Verlags-GmbH · D-55205 Ingelheim · IT-Grundschutz 2013/2

großen Herstellern, die Berührungspunkte bei ihren Produkten mit dem IT-Grundschutz gesucht und publiziert haben. Ist das auch für die Zukunft geplant?

Das war und ist sehr wünschenswert. Wir sind in dieser Hinsicht sehr offen für die Zusammenarbeit mit Herstellern, Anwendern und Dienstleistern. Eine ganze Reihe von Firmen hat uns bislang auf diesem Weg unterstützt. Darunter sind beispielsweise Novell, SAP, Apple und Microsoft, um nur einige zu nennen. Immer wieder lassen uns auch Dienstleister und Berater an Erfahrungen aus ihrer täglichen Praxis teilhaben. Gelegentlich stellen uns auch Anwender einen kompletten Baustein zu einem Spezialgebiet zur Verfügung. Auch das ist etwas, was wir gern weiter ausbauen würden. Mehrere Universitäten arbeiten zurzeit auch gemeinsam daran, eine dedizierte Plattform aufzubauen, mit der sich neue Bausteine einfacher im Team planen, schreiben und abstimmen lassen.

Wie sieht die Roadmap für dieses Jahr aus, was ist an festen Terminen beim Grundschutz geplant?

Zur Zeit stellen wir die 13. Ergänzungslieferung zusammen und bereiten sie zur Veröffentlichung vor. Das ist mit viel Aufwand verbunden, daher kann ich leider noch keinen Veröffentlichungstermin nennen. Fest steht nur, welche Bausteine für die nächste Ergänzungslieferung vorgesehen sind: Mac OS X, Exchange/Outlook, Notes, OpenLDAP, Windows 2008, Windows 7, Web-Applikationen, Protokollierung und allgemeines Gebäude. Ebenfalls ganz wichtig ist in diesem Jahr das Thema Cloud Computing. Wir bereiten Cloud-spezifische Bausteine vor und werden auch den Standard 100-2 entsprechend anpassen, damit man in Zukunft Informationsverbünde, die mit Cloud-Computing arbeiten, optimal modellieren kann. Sobald die Entwürfe stabil sind, werden wir die Diskussion mit den Anwendern suchen und führen.

Informationstechnologie reicht immer weiter in die normale Lebenswelt hinein. Smartphones, Tablets und Smart-TV bringen IT in jedes Wohnzimmer. Wird das auch ein Feld für den IT-Grundschutz sein?

Der IT-Grundschutz richtet sich in erster Linie an die IT-Sicherheitsbeauftragten und damit an institutionelle Anwender. Endverbraucher sind eine andere Zielgruppe, die wir auch in Zukunft nicht mit dem IT-Grundschutz adressieren werden. Für die Endanwender bietet das BSI ein umfassendes Informationsangebot im Web, beispielsweise unter www.bsi-fuer-buerger.de oder www.buerger-cert.de. Zum Beispiel gibt es im IT-Grundschutz nur eine recht allgemeine Maßnahme zu Sozialen Netzwerken , während das BSI unter www.bsi-fuer-buerger.de ganz dedizierte Konfigurationsempfehlungen zu Facebook oder Twitter bereithält. Natürlich bin ich aber auch der Meinung, dass der Bereich Smart-TV, Tablet und Co unbedingt durch adäquate Informationssicherheitsmaßnahmen geschützt werden muss, da kommen sicherlich noch große Herausforderungen auf die Nutzer und auf die Hersteller zu.

Wie steht der IT-Grundschutz zu mobilen Endgeräten und Bring-Your-Own-Device? Diese Geräte sind ja durchaus im institutionellen Einsatz.

Hier habe ich gute Nachrichten. Wir haben kürzlich das Überblickspapier „Consumerization und BYOD“ veröffentlicht. Darin handeln wir das Thema kurz, aber umfassend ab. Denn natürlich nutzen Behörden und Unternehmen zunehmend Smartphones und Tablets, die eigentlich als Consumer-Geräte konzipiert waren. Das hat Vorteile, wenn es um Akzeptanz und einfache Bedienung geht. Allerdings handeln Sie sich damit Nachteile aus Sicht der Administrierbarkeit und Sicherheit ein. Genau diese Vor- und Nachteile diskutieren wir in unserem Überblickspapier. Was wir jedoch feststellen ist, dass es in der öffentlichen Diskussion meistens gar nicht um „Bring-Your-Own-Device“ geht. Denn die wenigsten Firmen erlauben ein völlig freies Mitbringen von Endgeräten. Eher wird den Mitarbeitern Mitsprache bei der Auswahl der Geräte eingeräumt. Doch egal welche Strategie am Ende gewählt wird: Alle haben enorme rechtliche Implikationen, die viel schwieriger zu lösen sind als die Fragen der Informationssicherheit. Deswegen können wir den Institutionen beim tatsächlichen Einsatz nur im eng umrissenen Rahmen Hilfestellung geben.

Was würden Sie für die Informationssicherheit tun, wenn Sie unbegrenzte Mittel und unbegrenzten Einfluss zur Verfügung hätten?

Ich würde groß angelegte und nachhaltige Awareness-Maßnahmen starten und aufrechterhalten. Hier sehe ich die Mittel am besten angelegt. Verhalten ändert man nicht mit einem einzelnen Hinweis oder einem Zeitungsartikel. Es muss immer und immer wieder kommuniziert werden, was Nutzer tun können und was sie lassen sollten, da sehe ich einfach noch zu wenige Aktivitäten. Und außerdem würde ich die Ausbildung von viel mehr IT-Grundschutz–Experten finanzieren, damit es eine breite Basis von IT-Grundschutz-Anwendern und Ratgebern überall in den Institutionen gibt. ■

Impressum

Informationsdienst IT-Grundschutz
8. Jahrgang – ISSN 1862-4375

Herausgeber
Nina Malchus

Redaktion
Elmar Török, Fachjournalist
(verantw. für den redaktionellen Teil)
Tel.: +49 89 381578030
E-Mail: redaktion@grundschutz.info

Verlag
SecuMedia Verlags-GmbH
Lise-Meitner-Str. 4, 55435 Gau-Algesheim
www.secumedia.de

IT-Grundschutz in der Energiewirtschaft

Passt der BSI-Standard für Netzbetreiber?

Stefan Stumm, Geschäftsführer, Stefan Stumm IT-Sicherheit, Beratung & Schulung

IT-Grundschutz in der Energiewirtschaft wird zur Zeit heiß diskutiert. Es ist nicht unwahrscheinlich, dass der IT-Sicherheitsstandard auch die zukünftigen „smarten" Netze der Energieversorger vor Gefahren schützen soll. Doch lassen sich die IT-spezifischen Maßnahmen und Gefährdungen sinnvoll auf den neuen Einsatzbereich anwenden?

Kommt der IT-Grundschutz (oder BSI Standard 100) als verpflichtende Norm für Netzbetreiber oder nicht? Den Anlass liefert die Neuregelung des Energiewirtschaftsgesetzes, in der es heißt:

„§ 11 (1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. (...)"

Die Erfahrungen mit der Bundesnetzagentur und vor allem die ausdrückliche Beteiligung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), also dem Herausgeber des IT-Grundschutz, deuten sehr eindeutig darauf hin, dass die Frage eigentlich nur noch lautet: Kommt der IT-Grundschutz vollständig oder doch nur teilweise? Die Diskussion entzündet sich vor allem an der Bevormundung der Netzbetreiber durch den Gesetzgeber und den damit verbundenen Kosten. Weniger prominent ist die Fragestellung, ob die Methode für einen Schutz der Steuerelemente geeignet ist, obwohl hier vielfach das Argument zu hören ist, dass der IT-Grundschutz keine geeigneten Module (Bausteine) für die Netztechnik bietet. Aber trifft dieses Argument auch zu?

Zweifel an Eignung des Grundschutz

Betrachten wir doch einmal die Methode etwas genauer: IT-Grundschutz ist zunächst einmal ein Sicherheits-Prozess, der aus den Schritten Planen – Umsetzen – Prüfen – Verbessern besteht. Wer schon einmal damit zu tun hatte, wird den kontinuierlichen Verbesserungsprozess aus dem Qualitätsmanagement nach ISO 9001 wiedererkennen. Als Planungshilfe stellt das BSI eine Vielzahl von typischen Maßnahmen bereit, mit den Bausteinen aufgeteilt auf typische Anwendungsbereiche im Zusammenhang mit dem Betrieb jeder Art von IT. Die Grundschutz-Methode besteht nun darin, festzustellen, welche Anwendungsbereiche im eigenen IT-Umfeld relevant sind, die entsprechenden Bausteine zuzuordnen und die damit verbundenen Maßnahmen als „Soll" zu akzeptieren. Maßnahmen können entbehrlich sein, wenn bereits gleichwertige andere Maßnahmen eingesetzt werden oder wenn die Maßnahme schlicht nicht gebraucht wird, weil im spezifischen Fall keine passende Bedrohung existiert. Anders ausgedrückt: auf eine Klimatisierung darf verzichtet werden, wenn die Überhitzung eines Raumes im konkreten Fall technisch nicht möglich ist.

Ob die Grundschutz-Methode für den Schutz des Netzbetriebes passt, hängt offensichtlich davon ab, wie viele der geschilderten Bausteine für die typischen Anwendungsfälle eines Energiedienstleisters passen und in welchem Grade. Wir müssen näher hinsehen, um dies

© SecuMedia Verlags-GmbH · D-55205 Ingelheim · IT-Grundschutz 2013/2

zu beurteilen. Die Bausteine des IT-Grundschutz sind in fünf Schichten aufgegliedert:

- Übergeordnete Aspekte
- Infrastruktur
- IT-Systeme
- Netze
- Anwendungen.

Zu den übergeordneten Aspekten gehören unter anderem Sicherheitsmanagement, Organisation, Personal, Notfallmanagement, Behandlung von Sicherheitsvorfällen, der Umgang mit Hard- und Software, Änderungsmanagement, Schulung und Compliance-Management. Für diese Bereiche werden allgemein gehaltene Regelungen gefordert, die auch auf Netzbetriebstechnik ohne Abstriche anwendbar sind. Dazu kommen IT-spezifischere Aspekte wie Datensicherung, Verschlüsselung oder Virenschutz. Spätestens der Stuxnet-Virus, der speziell für Steuerungssysteme programmiert war, sollte deutlich gemacht haben, dass dies durchaus Netzbetriebs-Themen sein können. Zusammenfassend lässt sich sagen, dass die komplette Schicht der übergeordneten Aspekte für den Netzbetrieb passt und dass sich – viel wesentlicher – das IT-Sicherheits-Management für den Netzbetrieb darüber gestalten lässt. Diese Behauptung lässt sich in diesem Rahmen nicht umfassend belegen, daher lade ich Sie ein, sich selbst ein Bild des IT-Grundschutz auf der Website des BSI zu machen: www.bsi.bund.de.

Mit den Infrastruktur-Bausteinen werden Vorgaben für die Sicherheit von Gebäuden, Räumen und Kabelwegen bereitgestellt. Also der gleichen Infrastruktur, die auch für den Netzbetrieb benötigt wird. Auch hier ist ein vollständiges Schutzkonzept unter Verwendung von IT-Grundschutz möglich. Dass die Bausteine zum Schutz von Netzen für den Schutz des Netzbetriebs geeignet sind, sei der Vollständigkeit halber erwähnt, ist aber nicht wirklich überraschend.

Im Zentrum der Kritik stehen die Schichten IT-Systeme und Anwendungen, die keine offensichtlich passenden Bausteine für Steuerungssysteme zur Verfügung stellen. Steuerungssysteme bestehen aber häufig aus Servern und Bedien-Clients, werden durch eine Firewall gegen andere Netze geschützt und benötigen Datenbanken oder mobile Datenträger. Für alle diese Aspekte stehen Grundschutz-Bausteine zur Verfügung. Das Fazit: Für den Netzbetrieb lässt sich bereits jetzt ein IT-Sicherheitskonzept nach IT-Grundschutz gestalten. Werden die Anforderungen durch die Bundesnetzagentur bestätigt, erarbeiten die Hersteller möglicherweise sogar eigene Bausteine für ihre Lösungen. So ist beispielsweise der Baustein SAP System auf diesem Wege entstanden.

Passend oder passend gemacht?

Es gibt derzeit nur eine Norm, die für den Umgang mit Informationssicherheit international anerkannt ist: ISO 27001. Allerdings führen zwei Wege zum Ziel, diese Norm zu erfüllen: über eine Anwendung von ISO 27002 (der ehemaligen ISO 17799-2) oder mittels IT-Grundschutz. Dabei erfüllt IT-Grundschutz die Anforderungen der ISO 27002, konkretisiert sie aber in großem Umfang. Im Anforderungskatalog von ISO 27002 sind auf ca. 50 Seiten generische Anforderungen festgehalten, was für Informationssicherheit zu beachten ist. Im IT-Grundschutz werden diese Anforderungen in Bezug zur Praxis verdeutlicht. Die generische Anforderung nach einem Datensicherungskonzept wird beispielsweise durch zwölf Einzelmaßnahmen, alle detailliert beschrieben, vertieft.

Beide Wege bieten entsprechend ihrer Grundtendenz Vor- und Nachteile. Der große Vorteil von ISO 27002 ist ein hohes Maß an Bewertungsfreiheit, was zur Erfüllung der Anforderung notwendig ist. Dies kann Kosten und Aufwand für die Umsetzung der Einzelmaßnahmen reduzieren. Nachteilig ist, dass diese Bewertungsfreiheit auch einem Auditor oder Gutachter zur Verfügung steht. Im schlimmsten Fall kann der Nachweis der ausreichenden Sicherheit nicht erbracht werden, weil der Auditor aufgrund einer anderen Einschätzung das Zertifikat verweigert oder sogar ein Zertifikat neu erbracht werden muss, weil ein Gegen-Gutachter eine andere Auffassung vertritt.

Diese Situation könnte bei einer Anwendung des IT-Grundschutz zwar auch eintreten – nämlich dann, wenn man eine geforderte Maßnahme als entbehrlich einschätzt – im Regelfall wird aber lediglich festzustellen sein, dass die beschriebene Maßnahme erfüllt ist. Dies ist tatsächlich der Regelfall, da die IT-Grundschutzmaßnahmen, obwohl von einer Behörde zusammengestellt, meistens sehr praxisnah sind. Ein Auditor oder Gegen-Gutachter müsste gegen den Standard argumentieren, nicht gegen eine andere Auffassung des Standards.

Der Nachteil des IT-Grundschutz wird durch die Möglichkeit, auf Einzelmaßnahmen begründet zu verzichten, teilweise aufgehoben. Es entsteht in diesem Falle aber ein höherer Dokumentationsbedarf. Man kann also festhalten: IT-Grundschutz ist für den Einsatz beim Netzbetrieb geeignet und auch mindestens so effizient, wie die einzige Vergleichslösung. Wird der BSI-Standard von der Bundesnetzagentur für verbindlich erklärt, wird das nicht zum Schaden der Netzbetreiber sein.

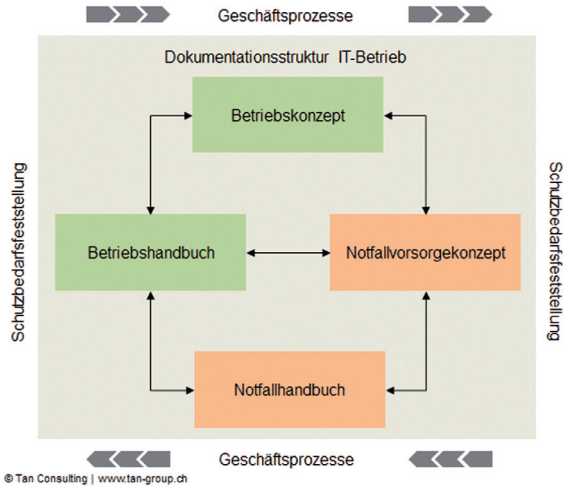
IT-Grundschutz nach BSI strategisch planen

Teil 3: Warum scheitern viele Sicherheitskonzepte?

Felix Widmer, Inhaber, Tan Consulting

Viele Sicherheitskonzepte sind immer noch rein statische Bestandsaufnahmen, die einmal erstellt werden und dann sich selbst überlassen bleiben. Die IT-Grundschutzmethode erwähnt zwar die Prozessmodellierung, die Grundschutzkataloge bieten dazu aber keine eigentliche Hilfestellung. Schwachstellen der Sicherheitskonzepte sind die oft mangelhafte Dokumentation und die zu enge Fokussierung der Sicherheitsthematik.

Eine ordnungsgemäße Dokumentation des IT-Betriebs ist die Voraussetzung für die IT-Sicherheit. Die traditionelle Trennung zwischen



Zusammenhang im Überblick: Konzepte für das „Was" und Handbücher für das „Wie"

Sicherheitshandbuch und Betriebshandbuch ist überholt. Sicherheit muss im Betrieb integriert sein. Notfallvorsorge und das Überleben im Notfall sind eigenständige Bereiche. Die Geschäftsprozesse bestimmen, was die Informatik leisten muss. Eine wichtige aber nicht die einzige Schnittstelle ist die Schutzbedarfsfeststellung. Betrachten wir die praxisbezogene Inhaltsstruktur des Betriebshandbuchs: Die beiden Kernteile sind die Systemdokumentation und die Prozessdokumentation. Die Systemdokumentation beschreibt die eingesetzte Hard- und Software.

Systeme und Prozesse zur Umgebung passend dokumentieren

Wer bereits ITIL eingeführt hat oder die Einführung plant, nutzt die Configuration Management Database (CMDB) mit den Configuration Items als Schnittstelle zu den Systemakten der Systemdokumentation. Kleinere Unternehmen verstehen das oft falsch: Weder die CMDB noch das Betriebshandbuch sind monolithische Gebilde. Die Systemdokumentation kann für eine kleinere IT-Landschaft eine CMDB vollwertig ersetzen. Eine komplexe Umgebung wird hingegen mit einer CMDB dokumentiert und nicht mit einem Word-Dokument oder einer Excel-Tabelle.

Die Prozessdokumentation strukturiert die Prozesse auf der Basis des Qualitätskreises nach Deming (PDCA-Modell). Mit den vier Prozessgruppen Planung und Änderung (Change Management), Regelbetrieb, Supportmanagement und Optimierung des IT-Betriebs entsteht eine skalierbare, transparente und nachvollziehbare Betriebsdokumentation. Sie ist in ihrer Logik kompatibel zu den Standards ISO 9001 (Qualitätsmanagement), ISO 20000 (IT Service Management), ISO 27001 (Information Security Management System, ISMS), BSI 100-1 (ISMS) und 100-4 (Notfallmanagement).

Für die entsprechenden Zertifizierungen werden durch die Dokumentation wichtige Vorarbeiten geleistet, unabhängig davon, ob letztlich eine Zertifizierung angestrebt wird.

Wo steht der IT-Grundschutz?

Einige typische Prozesse des Regelbetriebs sind Benutzerverwaltung, Netzwerkmanagement, Datensicherung und Wiederherstellung sowie das Sicherheitsmanagement. Für diese Bereiche und natürlich auch für das Notfallvorsorgekonzept und das Notfallhandbuch sind die IT-Grundschutz-Kataloge ein unverzichtbares Hilfsmittel.

Die prozessorientierte Dokumentation führt zu zielorientierten und nachvollziehbaren Handbüchern für den IT-Betrieb und die Notfallbewältigung. Eng mit den Prozessen verbunden sind die funktional definierten Informationen. Prozesse werden mit Anleitungen, den funktionalen Elementen, gelebt. Ein funktionales Element enthält immer ein Handlungsziel, die Voraussetzungen, benötigte, manchmal optionale, Hilfsmittel, Handlungsaufforderungen als Kern der Anleitung und ein überprüfbares oder messbares Resultat.

Die Integration der Sicherheitsaspekte in das IT-Betriebshandbuch stärkt das Sicherheitsdenken und gewährleistet einen sicheren IT-Betrieb. Aus der Polarisierung Notfall vs. IT-Betrieb resultieren klare Schnittstellen zu den Anforderungen der Geschäftsprozesse und der Schutzbedarfsfeststellung.

Der IT-Betrieb wird schrittweise kompatibel zu den Grundsätzen der relevanten ISO-Normen und De-Facto-Standards wie ISO 9001, ISO 20000, ISO 27001, ITIL® und BSI 100-1/-4. Vorstand/Verwaltungsrat und Management erfüllen damit die rechtlichen Anforderungen (Compliance) und vermeiden Klagen zur Durchgriffshaftung in einem Schadensfall.

© SecuMedia Verlags-GmbH · D-55205 Ingelheim · *IT-Grundschutz 2013/2*