Herausforderungen jenseits der Technik

Sicherheitszertifizierung nach BSI IT-Grundschutz Standard

Kai Dietrich, Felix Friedrich, Milan Mehner

17. Juli 2009

Zusammenfassung

Die Firma *** baut in Kooperation mit der TU-Berlin ein nach BSI IT-Grundschutz zertifizierungsfähiges Informationssicherheitsmanagementsystem auf. Wir wollen hier einen kleinen Einstieg in das Thema IT-Grundschutz bieten, die bisher gewonnen Erfahrungen in dem Prozess teilen, die auftretenden Herausforderungen benennen sowie Lösungensvorschläge anbieten.

Einleitung

Die Firma *** beschäftigt zur Zeit einige tausend Mitarbeiter. Dabei wird auf einen schlanken „Wasserkopf“ gesetzt, so dass nur ca. 200 Mitarbeiter für Einkauf, Rechnungsstellung und andere zentrale Dienste zuständig sind. Um dies zu ermöglichen ist eine flexible und leistungsfähige IT unabdingbar. Im Umkehrschluß sind dadurch aber auch die Geschäftsprozesse von einer funktionierenden IT abhängig oder sensible Informationen einer möglichen Kompromittierung ausgesetzt – die Informationssicherheit des Unternehmens ist gefährdet.

Um diesen Bedrohungen aktiv zu begegnen wird bei der *** ein Informationssicherheitsmanagementsystem (ISMS) nach dem IT-Grundschutz Standard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingerichtet. Ein solches ISMS erkennt die Aufgabe Informationssicherheit als eine zentrale Aufgabe des Managements an und überlässt sie nicht mehr „den Technikern im Keller“.

Ein kleiner Ausflug in die Theorie der Informationssicherheit wird uns zuerst den Problemen Informationssicherheit und Informationssicherheitsmanagement ein wenig näher führen, bevor wir uns den Herausforderungen während der konkreten Umsetzung bei der *** zuwenden wollen.

Informationssicherheit als Aufgabe des Managements

Unter Informationssicherheit (auch: IT-Sicherheit) versteht man dabei die Abwesenheit von Risiken, die im Zusammenhang mit dem Einsatz von IT und dem Umgang mit sensiblen Informationen stehen. Informationssicherheit ist damit klar im Risikomanagement anzusiedeln. Ein Risiko lässt sich als das Produkt aus der Höhe eines möglichen Schadens und der Eintrittswahrscheinlichkeit dieses Schadens definieren. Es ist damit *zunächst theoretisch* quantifizierbar. Das übliche Wirtschaftlichkeitsprinzip bewirkt nun, dass Maßnahmen zur Senkung des Risikos nicht mehr kosten dürfen als sie einsparen.

Diese klare Sichtweise wird komplexer, wenn man tatsächlich versucht die Risiken für die Informationssicherheit in Euro auszudrücken. Die klassische Vorgehensweise dabei betrachtet einzelne Risiken für den Verlust von verschiedenen sog. Sicherheitszielen. Sicherheitsziele sind z. B. Vertraulichkeit, Integrität oder Verfügbarkeit (im Englischen auch als CIA - confidentiality, integrity, availability Prinzip bekannt) und werden auf bestimmte Objekte wie z.B. Server-Infrastruktur oder Datenbanken bezogen. Jedes dieser Sicherheitsziele kann durch technische oder organisatorische Mängel bedroht sein. Die Schadenshöhe müsste aus dem Verlust der Sicherheitsziele für die identifzierten Objekte abgeschätzt werden – eine an sich schon komplexe Aufgabe.

Es lassen sich nun eine Vielzahl von möglichen Bedrohungen für jede Komponente eines IT-Betriebs identifizieren. Ob beim Aufschlüsseln dieser Bedrohungen allerdings Vollständigkeit erreicht wurde ist zu keinem Zeitpunkt klar, denn komplexe Systeme und Organisationen lassen sich nicht oder nur kaum mit analytischen Methoden untersuchen, so dass ein Rest an unbekannten Bedrohungen verbleiben muss.

Ähnlich verhält es sich mit der Abschätzung der Eintrittswahrscheinlichkeiten für bestimmte Bedrohungen. Die Eintrittswahrscheinlichkeiten hängen in hohem Maße von der Motivation der potentiellen Angreifer ab – während das normale Aufkommen an Viren, Trojanern und anderen Angriffen aus dem Internet ungezielt ist und vorwiegend „leichte Beute“ befällt, wird beispielsweise ein fremder Nachrichtendienst sehr viel gezielter und mit deutlich komplexeren Methoden angreifen. Wie genau die Bedrohungslage für die eigene Organisation aussieht lässt sich höchstens abschätzen. Eine Quantifizierbarkeit zu erreichen ist also nahezu utopisch.

Nichtsdestotrotz gibt es ein reales Risiko dessen sich die Führungsebene eines Unternehmens bewusst sein muss und mit dem umgegangen werden sollte. Um im eben skizzierten Wald der Unbekannten nicht völlig ohne Orientierung zu sein, haben sich seit einigen Jahren Standards zur IT-Sicherheit etabliert. Der bekannteste darunter, der ISO-27001, setzt auf eine schlanke, flexible Formulierung der Sicherheitsanforderungen an einen IT-Betrieb und baut in erster Linie auf die Implementierung eines sog. Informationssicherheitsmanagementsystems auf. Wer ein solches Managementsystem in

seiner Organisation eingeführt hat, kann sich von einem Auditor zertifizieren lassen und darf dann das entsprechende Logo tragen. Der ISO-27001 hat allerdings einige Nachteile. Zum einen sind die Unterlagen der ISO generell nicht kostenlos verfügbar sondern müssen für einige hundert Euro erworben werden. Dies ist zwar für größere Organisationen meist kein Problem, für kleine bis kleinste Unternehmen kann das allerdings schon prohibitiv wirken, da der direkte Einstieg in das Sachthema vor einer Entscheidung für oder gegen eine Zertifizierung deutlich erschwert wird. Zum anderen ist der ISO-27001 deutlich Prozessorientierter. Eine Zertifizierung nach ISO-27001 sagt zwar aus, dass ein ISMS eingerichtet wurde, über den absoluten Stand der Informationssicherheit informiert das Zertifikat wenig.

Auf diese Schwächen reagieren die Informationssicherheits-Standards, BSI 100-1 bis 100-4, des BSI – auch besser bekannt als IT-Grundschutz. Sie sind kompatibel zum ISO-27001, jedoch sehr viel spezifischer, konkreter und zudem kostenlos verfügbar. Dadurch und weil sie zusätzlich zur deutschen Referenzausgabe auch in einer englischen Übersetzung vorliegen, finden sie zunehmend auch in ganz Europa Verwendung – sind also mehr als ein rein deutscher Binnenstandard. Die vier BSI IT-Grundschutz-Standards werden durch die IT-Grundschutz-Kataloge ergänzt. Die IT-Grundschutz-Kataloge stellen eine umfangreiche Sammlung von Gefährdungen und zugehörigen Gegenmaßnahmen dar und werden regelmäßig aktualisiert.

Ebenso wie der ISO-27001 baut auch der IT-Grundschutz auf der Einrichtung eines ISMS auf. Ein solches Managementsystem besteht aus einer Menge von Vorgehensweisen die regelmäßig zur Überprüfung der Adäquatheit der eigenen Informationssicherheitsmaßnahmen führen. Damit werden die Verantwortlichen allerdings nicht allein gelassen. Es werden zahlreiche konkrete Vorgaben zur Ausgestaltung der nötigen Arbeitsprozesse gegeben sowie Checklisten (sog. Bausteine) die abgearbeitet werden müssen. Vor der Abarbeitung der Bausteine steht die Modellierung des IT-Verbunds. Der IT-Verbund ist der zu zertifizierende Teilbereich einer Organisation inklusive aller seiner Mitarbeiter, Geschäftsprozesse und IT-Systeme. Er kann die gesamte Organisation umfassen, kann aber auch nur ein scharf abgegrenzte Teilorganisation sein. In der Modellierung werden alle relevanten IT-Komponenten, -Verfahren und -Anwendungen erfasst und bewertet. Anhand dieser Modellierung werden im Anschluss eine Menge von Bausteinen ausgewählt (z.B. *„B 3.209 Client unter Windows XP“*). Die Bausteine enthalten dann die zu betrachtenden Gefährdungen und die für ein *festgelegtes Sicherheitsniveau* adäquaten Maßnahmen. Durch die Festlegung auf ein mittleres Sicherheitsniveau „erspart“ das BSI den Verantwortlichen einen Großteil der komplexen Risikobewertung. Für höhere Sicherheitsanforderungen kann noch eine zusätzliche Risikoanalyse durchgeführt werden. An niedrigere Sicherheitsanforderungen können die Maßnahmen auch, jedoch schwerer, angepasst werden. Für Organisationen mit extrem niedrigen Sicherheitsanforderungen wird also unter Umständen ein etwas zu hoher Aufwand betrieben.

Sind alle Bausteine abgearbeitet und alle notwendigen Unterlagen erstellt, so kann zusammen mit einem vom BSI akkreditierten Auditor eine Zertifizierung durchgeführt werden. Am Ende steht dann eine erfolgreiche Zertifizierung, mit der am Markt zuverlässig gezeigt werden kann, dass ein adäquates Maß an Informationssicherheit vorliegt. Obwohl vielen Verbrauchern und Handelspartnern dies noch nicht allzu wichtig scheint, wird dies in Zeiten von immer mehr Vernetzung und Datenschutz-Skandalen wohl zunehmend wichtiger werden. Wer sich also heute um seine Informationssicherheit kümmert, hat in Zukunft vielleicht einen sichtbaren Vorteil am Markt.

Die Einrichtung eines ISMS nach IT-Grundschutz ist ein Prozess, der nicht alle, aber viele Teile des Betriebes berührt. Ziel ist es eben die Risiken, welche durch den Einsatz von IT entstehen zu lokalisieren, abzuschätzen und angemessene Gegenmaßnahmen zu treffen. Das Wort Risiko selbst zeigt schon an: Informationssicherheit ist eine Managementaufgabe die eben nicht nur von der IT-Abteilung gemacht wird (und werden kann). In der Wissenschaft sowie bei Technikern ist zumindest eine Erkenntnis schon lange vorhanden: ohne entsprechende Bereitstellung von ausreichenden Ressourcen leidet die Sicherheit (meist wohl als erstes). Dem Management stellt sich im Gegenzug die Frage wie viel Sicherheit für die eigene Organisation richtig ist und wie viel Geld sie damit Wert ist, wie viele Ressourcen also ausreichend sind.

Standards zur Informationssicherheit, speziell der IT-Grundschutz des BSI, bieten sowohl Technikern als auch Managern eine Chance einen Teil dieses Problems zu lösen. Dem Management wird ein Werkzeug in die Hand gegeben mit dem auch von außen nachvollziehbar angemessen Sicherheit hergestellt werden kann. Technikern wird ein Werkzeug geboten mit dem sie sowohl ihr eigenes Vorgehen strukturieren, als auch dem Management gegenüber begründeten Anspruch auf zusätzliche Ressourcen geltend machen können.

Bevor die Entscheidung getroffen wird ein ISMS einzuführen sollten sich Techniker und Management einig sein, um gemeinsam an einem Strang ziehen zu können. Diese Entscheidung setzt auf beiden Seiten ein Verständnis der Materie voraus, um den bevorstehenden Aufwand und die möglichen Gewinne ungefähr abschätzen zu können. Es bedarf also im Voraus einer sachkundigen Entscheidung ob und wie ein ISMS tatsächlich sinnvoll ist. Dazu können die Beteiligten entweder auf die Primärquellen, den BSI-Standards, oder Sekundärliteratur zurück greifen als auch auf persönliche Erfahrungen. Diese Erfahrungen findet man bei Beraterfirmen, die sich im Bereich Informationssicherheitsmanagement spezialisiert haben.

IT-Grundschutz bei der ***

Wie der Titel *Herausforderungen jenseits der Technik* verspricht, wird sich dieser Artikel vorwiegend mit den nicht-technischen, den sog. Übergeordneten Aspekten einer IT-Grundschutz-Zertifizierung beschäftigen. Diese übergeordneten Aspekte sind die erste Schicht der Bausteine des IT-

Grundschutzes, die in insgesamt fünf Schichten gegliedert sind. Die Autoren haben die Umsetzung der Bausteine dieser ersten Schicht direkt begleitet. Die Umsetzung der geforderten Maßnahmen bedeutete im konkreten Fall einen Beitrag zur Organisationsentwicklung. Die Arbeit geht damit also weit über das normale Tagesgeschäft hinaus und beeinflusst dieses gleichermaßen.

Die Zertifizierung nach IT-Grundschutz birgt eine Menge technischer und nichttechnischer Herausforderungen. Im Folgenden beschäftigen wir uns mit einigen dieser Herausforderungen. Sind Herausforderungen bekannt, kann man besser mit diesen Umgehen. In Einzelfällen versuchen wir natürlich auch Lösungsansätze zu bieten.

Plan-Do-Check-Act

Die IT-Abteilung der *** ist mit den wachsenden Anforderungen an die IT des Unternehmens kontinuierlich und flexibel mitgewachsen. Auf Anforderungen von außen wurde schnell reagiert. Dieser reaktive Prozess setzt sich auch im normalen Tagesgeschäft fort. Entsteht ein neues Problem oder eine neue Anforderung wird sie unter Beachtung der Gegebenheiten direkt gelöst. Die Planung der Änderungen erfolgt mündlich oder implizit und wird erst im Nachhinein dokumentiert. Dieses Vorgehen führt unter Umständen dazu, dass die Dokumentation der Prozesse nicht vollständig ist oder Inkonsistenzen darin auftreten. Gerade wenn über einen bestimmten Zeitraum hinweg verschiedene Mitarbeiter mit der Betreuung der Systeme betraut sind steigert sich der Effekt. Diese Arbeitsweise dürfte sich nicht nur bei der *** sondern auch in den IT-Abteilungen vieler anderer mittelständischer Unternehmen wiederfinden lassen.

Eine IT-Grundschutz-Zertifizierung steht einer ständigen Erweiterung eines IT-Systems je nach Aufkommen neuer Anforderungen natürlich nicht im Weg, jedoch erfordert sie zwingend die Erstellung eines Plans für eine Änderungen an einem System. Nach der Planung kann dann erst in einem zweiten Schritt die Aktion umgesetzt werden. Bereits dieser erste Teil des größeren, sog. *Plan-Do-Check-Act* (PDCA) Zyklusses, kann eine enorme Änderung der Arbeitsmethode darstellen. In den wenigsten Fällen, wie auch bei der ***, wird das stringente PDCA-Vorgehen bereits übliche Praxis sein. Unternehmen die die Arbeitsweise ihrer IT schon an den Kriterien von etablierten Betriebsstandards (wie z.B. der ITIL – der „Information Technology Infrastructure Library“) ausgerichtet haben, werden dagegen schon weitestgehend die Kriterien des PDCA-Modells erfüllen.

Ist im reinen Betrieb der IT-Abteilung noch kein PDCA-Modell implementiert, so stellt dies eine der ersten großen Hürden für die Umsetzung von IT-Grundschutz dar. Es ist zu empfehlen schon vor dem Beginn einer IT-Grundschutz-Zertifizierung die eigene IT nach dem PDCA Modell mit expliziter Planungsphase und ausführlicher Dokumentation umzustellen.

Allerdings schreibt das BSI nicht nur vor die Umsetzung und Funktionsweise ein-

zelner IT-Komponenten zu dokumentieren, sondern verlangt auch die Dokumentation aller wesentlichen Arbeitsprozesse selbst. Der Druck oft nur implizit vorhandene Abläufe explizit niederzuschreiben, wird fast zwangsläufig fehlende Regelungen aufdecken. Meist hindern solche fehlenden Regelungen im Normalbetrieb die IT nicht daran zu funktionieren, denn auch informelle Regeln können für den reibungslosen Ablauf sorgen. Jedoch sind diese von außen nicht nachvollziehbar und damit nicht kontrollierbar. Existieren noch keine formellen Regeln für einen Arbeitsablauf, müssen diese natürlich dann auch entsprechend festgelegt werden. Dabei spielt auch die genaue Abgrenzung von Kompetenzbereichen einzelner Mitarbeiter eine Rolle. Die übergeordneten Führungsebenen müssen folglich mit einbezogen werden. Der dabei entstehende Prozess sorgt für nicht unerheblichen Kommunikations- und Organisationsaufwand aller Beteiligten.

Es entsteht offensichtlich für viele Beteiligte ein Mehraufwand. Zunächst einmal werden diejenigen Mitarbeiter, welche direkt mit der IT-Grundschutz-Zertifizierung betraut sind, mit einem höheren Arbeitspensum konfrontiert. Eine erste Maßnahme muss sein, diese Mitarbeiter von anderen Aufgaben zu entlasten. Es gilt also auch die Frage zu berücksichtigen, ob die IT-Abteilung zusätzliche personelle Unterstützung benötigt. Sollte dies nicht berücksichtigt werden kann es leicht dazu kommen, dass das Projekt IT-Grundschutz-Zertifizierung nicht ernsthaft genug verfolgt werden kann. Führt dies zu Verzögerungen im Zeitplan kann es zu höheren Kosten kommen (z.B. durch mehr Beraterstunden o.ä.). Die komplizierte personelle Situation bei der *** ist z.B. ein großes Hindernis für die Einführung des ISMS gewesen, für das erst Lösungen gefunden werden mussten. Darüber hinaus betrifft die Zertifizierung allerdings nicht nur diejenigen Mitarbeiter, welche direkt für die Zertifizierung zuständig sind, sondern auch die Arbeit eines jeden Mitarbeiters des Betriebes. Spätestens wenn Arbeitsabläufe verändert, neue Maßnahmen umgesetzt werden oder Schulungen zu Sicherheitsbestimmungen anstehen ist die Mitarbeit aller gefordert. Dies setzt vor allem deren Bereitschaft und Motivation für das Projekt voraus.

Kommunikation

Um diese Motivation und Bereitschaft bei den Mitarbeitern zu erreichen, muss die Notwendigkeit eines erhöhten Aufwands für ein so abstraktes Ziel wie Informationssicherheit kommuniziert werden. Dazu ist ein funktionierendes Kommunikationsmedium nötig. Dieses Medium muss geeignet sein, den Fortschritt des Zertifizierungsprozesses und die konkreten Anweisungen, Prozessänderungen und Sicherheitsregelungen an alle Mitarbeiter zu vermitteln. Existiert noch keine effektive Kommunikationsinfrastruktur im Unternehmen, sollte diese, möglichst schon vor Projektbeginn, geschaffen werden. Das Management sollte dann die firmenintern geschaffenen Kommunikationsmedien intensiv dafür verwenden die Ziele des Projektes zu kommunizieren, jedem Mitarbeiter plausibel zu machen, sowie über den Stand

des Projektes zu informieren.

Wie bereits angedeutet, bietet es sich an, zumindest einen Teil der Einführung eines ISMS in einer projektartigen Arbeitsweise ablaufen zu lassen. Das vom Standard vorgesehene IT-Sicherheitsteam ist für die Einführung des ISMS zuständig. Das heißt es gibt ein Ziel an dem mehrere Mitarbeiter unterschiedlicher Unternehmenseinheiten gemeinsam arbeiten. Für die meisten Mitarbeiter bedeutet dies einen großen Unterschied zum normalen Tagesgeschäft. Im normalen Betriebsablauf eines Unternehmens wie der *** werden von den meisten Mitarbeitern mehr regelmäßige, gleichmäßige Aufgaben bearbeitet. Kommunikation und Koordination ist also unter Umständen nicht im gleichen Maße erforderlich, wie es bei projektbezogener Arbeit nötig ist, da die Mitarbeiter im Bezug auf ihre Aufgaben ein eingespieltes Team sind. Bei der IT-Grundschutz-Zertifizierung kommen allerdings ständig neue Probleme auf das Team zu. So ist es erforderlich, dass es regelmäßige Treffen des Teams gibt, in denen der aktuelle Stand besprochen wird und sich über aufgekommene Probleme ausgetauscht wird.

Diese regelmäßigen Team-Treffen oder andere Formen der Team-Kommunikation sind für die erfolgreiche Zusammenarbeit nötig, beanspruchen aber natürlich auch ungewöhnlich viel Arbeitszeit, welche im Zeitplan und in der Einschätzung des Arbeitspensums der einzelnen Mitarbeiter berücksichtigt werden muss. Hat ein Unternehmen bereits funktionierende Infrastrukturen und Vorgehensweisen für Projektarbeit ist dies ein deutlicher Vorteil für die Einführung eines ISMS.

Eine Besonderheit des „Projektes“ IT-Grundschutz-Zertifizierung wird für die meisten Unternehmen sein, dass noch keiner oder nur wenige Mitarbeiter bereits Erfahrungen damit haben. Die erforderlichen Kompetenzen selbst zu erwerben kann sehr aufwändig und damit teuer werden. Externe Kompetenzen in das Unternehmen zu bringen spart dagegen viel Zeit und ist fast zwingend Vorraussetzung für die Einführung eines ISMS. Ein guter externer Berater kennt zudem die Notwendigkeiten, Dokumente und Bestandteile einer erfolgreichen IT-Grundschutz-Zertifizierung und kann mit diesem Wissen verhindern, dass in völlig falsche Richtungen gearbeitet wird.

Diese Gefahr ist alles andere als vernachlässigbar, denn die umzusetzenden Bausteine des BSI sind oftmals immernoch recht vage formuliert und vermitteln meist nur (mehr oder weniger hilfreiches) Wissen über eine bestimmte sicherheitsrelevante Problematik. Sie geben aber keine direkten Handlungsanweisungen wie die Umsetzung des Bausteins zu erfolgen hat oder aussehen könnte. Ein externen Berater mit entsprechenden Erfahrungen befreit an dieser Stelle die IT-Abteilung von der Interpretationsarbeit und kann viel direkter vermitteln, auf was bei der Zertifizierung am Ende Wert gelegt wird. Die IT-Abteilung kann sich so viel besser auf die Aufgaben konzentrieren, die ihrer technischen Kompetenz entsprechen.

Ein Problem welches ein erfahrener Berater lindern kann, ist auch die teilweise geringe Aktualität der einzelnen Abschnitte des IT-Grundschutz-Katalogs. Vielfach sind z.B. in den Gefahrenkatalo-

gen noch veraltete Beispiele angegeben. Neben überholten Teilen kennt ein externer Berater auch neuere Anforderungen und Entwicklungen, die in neue Versionen des IT-Grundschutzes einfließen werden und kann so bereits auf zukünftige Entwicklungen vorbereiten.

Mit der entsprechenden Erfahrung die ein externer Berater mitbringt, lässt sich auch ein realistischer Zeitplan für die Zertifizierung besser erstellen. Steht am Anfang der Einführung eines zertifizierungsfähigen ISMS eine Ausschreibung für Auditor und Berater, so ist damit unter Umständen ein solcher fester Zeitplan verbunden. Sollte sich herausstellen, dass dieser Zeitplan nicht eingehalten werden kann, so kann dies hohe Kosten nach sich ziehen. Besonders in die Festlegung solcher wichtigen Termine wie den Beginn des abschließenden Audits durch den Auditor sollte sehr viel Erfahrung und Informationsaustausch gesteckt werden. Es ist absolut zu empfehlen bereits zur Planung einer solchen Ausschreibung einen Berater hinzuzuziehen. Dieser hat den Vorteil sowohl die Seite des IT-Grundschutz als auch die Seite des Unternehmens zu kennen. Ihm ist damit die qualifizierte Aufstellung eines Zeitplans möglich.

Da der Verlauf des Einführungsprozesses nur schwer vorhergesehen werden kann, sollten (wenn möglich) die Termine sogar mit einer gewissen Flexibilität geplant werden. Sollte sich trotz aller qualifizierter Planung im Verlauf der Einführung des ISMS herausstellen, dass Termine nicht eingehalten werden können, so werden zusätzliche Kosten auftreten. Das Management muss zu jedem Zeitpunkt über den Verlauf des Projektes informiert sein um notfalls eingreifen zu können. Da die aufgewendeten Investitionen üblicherweise nicht wiedergewonnen werden können, handelt es sich um sog. versunkene Kosten (engl.: „sunken costs“). Die Forschung in Ökonomik und Psychologie hat gezeigt, dass Menschen in Gegenwart von versunkenen Kosten oft nicht ökonomisch rational handeln sondern der „Concorde Fallacy“ zum Opfer fallen, also immer mehr Kosten versenken anstelle das Projekt notfalls abzubrechen. Die Entscheidung ein Projekt fortzusetzen sollte auch im Falle der Einführung eines ISMS klassisch und ökonomisch rational ablaufen (siehe dazu auch die Arbeiten von Arkes u. Ayton, Garland u. Newport oder Kahneman u. Tversky im Literaturverzeichnis).

Trotz der vielen Vorteile die der IT-Grundschutz mit sich bringt, gibt es auch Aspekte die noch nicht ausreichend untersucht sind. Einer dieser Aspekte ist die Rolle von Vertrauen für die Informationssicherheit eines Unternehmens und den Einfluss des IT-Grundschutzes darauf.

Vertrauen

In vielen kleinen Unternehmen ist das Thema Informationssicherheit schlichtweg kein Thema. Es werden Passwörter offen hin- und her gereicht, Accounts von mehreren Personen verwendet und vor allem die Administratoren genießen das Privileg omnipotenten Zugriffs auf nahezu alle Daten des Unternehmens. Erstaunlicherweise funktioniert die IT dieser Unternehmen dann trotzdem. Der Administratoren löscht nicht bösartig Da-

ten von anderen Mitarbeitern oder liest die E-Mails der Kollegen mit, auch wenn ihm das unter Umständen zum eigenen Vorteil gereichen könnte. Erfasst man das erwünschte („gute“) Verhalten eines Mitarbeiters in einem ökonomischen Modell, so wird man wohl oft zu dem Schluss kommen, dass was für die Organisation richtiges Verhalten ist noch lange nicht für den Mitarbeiter ökonomisch optimal ist. Hat ein Administrator z.B. die Möglichkeit sich selbst über das Lohnabrechnungssystem *unbemerkt* mehr Urlaubstage zu geben, wird er dies nach dem Standardmodell der Ökonomik auch tun. Üblicherweise passiert dies aber genau nicht. Es lassen sich unzählige Situationen skizzieren in denen sich Administratoren ökonomisch gesehen völlig irrational verhalten.

Ein Grund dafür ist, dass wir Menschen, entgegen dem Standardmodell der Ökonomik, nicht völlig egoistisch zu sein scheinen, oder wenn, dann auf eine andere Art. Vor allem der Punkt Vertrauen scheint eine eine große Rolle zu spielen. So haben unter anderem die Arbeiten von Roland Bénabou und Jean Tirole gezeigt, dass Vertrauen eines Vorgesetzten in seinen Angestellten unter bestimmten Voraussetzungen dessen Arbeitsweise stark positiv beeinflussen kann. In kleinen Unternehmen kann ein Vertrauensverhältnis zwischen allen Mitarbeitern und vor allem den Vorgesetzten und Mitarbeitern möglich sein. Ist dies der Fall, so zeigt der aktuelle Stand der Forschung, dass möglicherweise genau dieses Vertrauensverhältnis zu einem Großteil dafür verantwortlich ist, dass sich die Mitarbeiter nicht völlig egoistisch verhalten.

Dies trifft vermutlich in besonderen Maße auch für das Verhältnis zwischen Führungsebene und Administratoren zu. Vertraut die Führung ihren Administratoren, so sorgt sie damit auch dafür, dass sich die Administratoren im Sinne der Organisation verhalten. Beginnt die Führungsebene den Administratoren dieses Vertrauen zu entziehen, so kann sehr schnell der Gegenteilige Effekt auftreten. Beim IT-Grundschutz ist an einigen Punkten vorgesehen, dass besonders wichtige Systeme nur unter Vier-Augen-Prinzip administriert werden dürfen. Das Vier-Augen-Prinzip hat dabei einen ambivalenten Charakter: Auf der einen Seite stellt es auch für die Administratoren eine wirksame organisatorische Sicherheitsmaßnahme dar um Fehler zu vermeiden, auf der anderen Seite signalisiert es aber auch die Sorge vor einem möglichen Missbrauch. Es bedarf äußerstem kommunikativem Fingerspitzengefühl um den letzteren Charakter nicht die Oberhand gewinnen zu lassen. Wenn nämlich durch die sture Einführung eines Vier-Augen-Prinzips ohne Klärung und Kommunikation der Notwendigkeiten den Administratoren ein Vertrauensentzug signalisiert wird, kann dies sehr schnell dazu führen, dass auch ihre sonstige Motivation kippt und „unterm Strich“ weniger Sicherheit heraus kommt.

Dieser, Ihnen als Leser vielleicht trivial erscheinende Umstand, ist von der Wissenschaft um Informationssicherheits-Management jedoch bisher weitestgehend nicht aufgenommen worden. Und so findet man auch nirgends in den BSI- oder ISO-Standards dazu einen Notiz. Bevor Sie jedoch vielleicht auch in Ihrer Organisation an die Einführung eines ISMS denken, denken Sie auch an ihre

Administratoren. Machen Sie Ihnen klar, dass ohne ihre Zuverlässigkeit auch kein zuverlässiger Betrieb der IT möglich ist und schon gar kein sicherer.

Fazit

Die IT-Grundschutz-Zertifizierung ist ein umfangreiches Projekt. Der organisatorische Aufwand vor und während der Zertifizierung sollte nicht unterschätzt werden. Dazu ist es notwendig, dass die Arbeitsweise der IT auf ein planvolles Vorgehen (Plan-Do-Check-Act) umgestellt wird. Die wesentlichen Arbeitsprozesse des Unternehmens müssen dokumentiert bzw. erst einmal explizit formuliert werden. Dies ist unter Umständen ein erheblicher Aufwand. Nicht nur für die IT-Abteilung sondern für alle Mitarbeiter, muss der zusätzliche Zeitaufwand berücksichtigt werden, sonst droht eine Vernachlässigung des Einführungsprozesses des Informationssicherheitsmanagementsystems. Um die anstehenden Änderungen an die Mitarbeiter zu vermitteln muss eine unternehmensinterne Kommunikationsinfrastruktur vorhanden sein bzw. geschaffen werden. Ziele und Bedeutung der Zertifizierung muss den Mitarbeitern plausibel gemacht werden, damit die erforderliche Motivation für den Erfolg des Projektes erreicht wird. Liegt innerhalb des Unternehmens bisher keine Erfahrung mit IT-Grundschutz vor, ist externe Kompetenz in Form eines Beraters unverzichtbar. Dies erleichtert die Planung und die Konkretisierung der Grundschutz-Anforderungen sowie in einer frühen Phase bereits die zeitliche Auslegung des Prozesses. Schließlich sollte bedacht werden, dass die Zertifizierung auch mit einer Kompetenzeinschränkung der Administratoren verbunden sein kann. Es ist wichtig, diesen wesentlich am Projekt beteiligten Mitarbeitern zu vermitteln, dass Sicherheitsmaßnahmen nicht einem Vertrauensentzug gleichkommen.

Die Einführung eines ISMS wirkt sich nicht nur auf den IT-Betrieb aus sondern auf das gesammte Unternehmen: dessen Kommunikation, Organisation und Firmenkultur. Nur Unternehmen, die bereit sind sich in allen diesen Aspekten zu verändern, werden bei der Einführung eines ISMS erfolgreich sein und davon auch profitieren.

Literatur

Arkes u. Ayton 1999
ARKES, Hal R. ; AYTON, Peter: The sunk cost and Concorde effects: Are humans less rational than lower animals? In: *Psychological Bulletin* 125 (1999), S. 591–600

BSI 2005
BSI: *BSI-Standards 100-1 bis 100-4*. Bundesamt für Sicherheit in der Informationstechnik, 2005–2008 http://www.bsi.de/literat/bsi_standard/

Burgartz u. Röhrig 2007
BURGARTZ, Dieter (Hrsg.) ; RÖHRIG, Ralf (Hrsg.): *Information Security Management*. TÜV Media / TÜV Rheinland Group, 2007

Bánabou u. Tirole 2000
BÁNABOU, Roland ; TIROLE, Jean: Self-confidence and social interactions. In: *NBER working paper No. W7585* (2000). Verfügbar über SSRN: http://ssrn.com/abstract=218750

Bénabou u. Tirole 2002
BÉNABOU, Roland ; TIROLE, Jean: Self-Confidence and Personal Motivation. In: *Quarterly Journal of Economics* 117 (2002), Nr. 3, S. 871–915

Garland u. Newport 1991
GARLAND, Howard ; NEWPORT, Stephanie: Effects of Absolute and Relative Sunk Costs on the Decision to Persist with a Course of Action. In: *Organizational Behaviour and Human Decision Processes* 48 (1991), February, Nr. 1, S. 55–69

Kahneman u. Tversky 1979
KAHNEMAN, Daniel ; TVERSKY, Amos: Prospect Theory: An Analysis of Decision under Risk. In: *Econometrica: Journal of the Econometric Society* (1979), S. 263–291