ccc 2004

Vortrag “IT-Sicherheitsstandards”
Viola Bräuer
IT Security- und Technologieberatung
me@vbraeuer.de

Abstract:
“Und hinterher machen wir das noch schnell sicher” - daß das nicht funktioniert, ist allgemein bekannt. Um Sicherheit in IT-Systeme von Anfang an zu integrieren, bedarf es “Kochrezepte”, niedergeschriebene Erfahrung anderer und vor allem allgemein anerkannter Prinzipien um Vertrauen beim Anwender herzustellen. Genau das liefern IT-Sicherheitsstandards. Je nach gewünschtem Sicherheitsziel - Verfügbarkeit, Vertraulichkeit, Integrität oder/ und Nicht-Abstreitbarkeit - werden über die ganze Palette von IT-Technik – Hardware, Netzwerk, Betriebssystem, Applikation- und die Organisation von Unternehmen Sicherheitsmaßnahmen und Prozesse zu deren Umsetzung und Kontrolle beschrieben. Standards wie BSI Grundschutzhandbuch, Common Criteria, BS 7799 und ITIL haben unterschiedliche Sichtweisen und behandeln unterschiedliche Aspekte. Summasummarum bietet gerade die Vielfalt von IT Sicherheitsstandards ein umfassendes Bild.

1 Einleitung

Standards sind trocken, IT-Standards sind noch trockener und IT-Standards für Sicherheit erst recht. Wofür IT-Sicherheitsstandards trotzdem brauchbar sind, beleuchtet der Vortrag. Es werden die Standards BSI Grundschutzhandbuch, Common Criteria, ITIL und BS 7799 vorgestellt, deren Einsatzgebiete erläutert und die einzelnen Standards miteinander verglichen.

2 Sinn und Zweck von IT-Sicherheitsstandards

Die Komplixität, die IT-Systeme erreichen können, erfordert eine methodische Herangehensweise. Die angestrebten Ziele sind immer diesselben: eine Mischung aus Vertraulichkeit, Verfügbarkeit, Integriät und Nicht-Abstreitbarkeit. Zudem wirken sie sich immer auf die komplette Technik aus - von der Hardware, über das Betriebssystem bis zu Netzwerk und Applikationen. Ein weiterer wiederkehrender Aspekt ist Unternehmensorganisation, personelle Zuständigkeiten und menschliche Schwachstellen (und Stärken).
Standards sind Orientierungshilfen, Mischungen aus best practise und dem Versuch, der Sache von vorn herein Vollständigkeit und Übersicht zu verleihen. Dem kommt das Ziel, IT-Sicherheit von Anfang an zu integrieren, entgegen.
Neben dem Design ist vor allem die Prüfung und Bewertung von bestehenden IT-Systemen ohne international anerkannte Standards undenkbar.
Methoden für das Mangement von IT Sicherheit werden als Information Security Management System (ISMS) bezeichnet.

3 Die Standards im Einzelnen

- BSI Grundschutz

Das Bundesamt für Informationssicherheit (BSI) in Deutschland hat das Grundschutzhandbuch herausgegeben. Es betrifft technische und organisatorische Aspekte der IT-Sicherheit, wobei es sehr detaillierte Maßnahmen bereithält. Im Gegensatz zu anderen Standards verzichtet es aber auf eine Risikoanalyse – die Maßnahmen werden quasi gießkannenmäßig niedrig verteilt - ohne Beachtung höherer Risiken, die einen höheren Schutzbedarf nach sich ziehen würden.

- Common Criteria (CC)

Die Common Criteria sind ein internationaler Standard, der “gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit in der Informationstechnik” beschreibt. Was schon der Titel durchscheinen läßt: es handelt sich um ein theoretisches Werk, das in etwa dem Umfang des Bürgerlichen Gesetzbuches nahekommt und ihm in der allgemeinen Verständlichkeit in nichts nachsteht. Dafür umfassen die Common Criteria ausführlich alle bekannten Sicherheitsziele bis hin zu Privatheit und Anonymität. Ein weiteres Pro ist die internationale Anerkennung der Prüfzertifikate. Nach – oder Vorteil: die CC müssen auf den jeweils vorliegenden Fall “übersetzt” werden.

- ITIL

Der de-facto Standard ITIL beschreibt einen best practise-Ansatz für die Einrichtung und den Betrieb von IT Infrastrukturen aus Sicht eines Dienstleisters: Service Level Agreements (SLA's) stehen hier im Vordergrund. Weitere Stichworte sind Incident Management, Problem Management, Configuration Management, Change Management und Release Management, um nur einige zu nennen. ITIL konzentriert sich auf die Verläßlichkeit und Verfügbarkeit der bereitzustellenden IT-Infrastrukture unter den vereinbarten Bedingungen (SLA's). Risikoanalyse steht nur am Rande im Blickwinkel des ITIL, technische Details fehlen bewußt.

- BS 7799

  Der britische Standard BS 7799 besteht aus zwei Teilen: der erste Teil wird auch als ISO 17799 bezeichnet. Der BS 7799 konzentriert sich auf organisatorische Aspekte, technische Details fehlen ganz. Dafür bringt er banale aber wichtige Anforderungen mit, wie zum Beispiel die Forderung der Unterstützung der IT-Sicherheitspolitik durch die Unternehmensleitung – wer jemals in einem Projekt zu tun hatte, das diesen Vorschlag nicht beherzigte, wird den Wert solcher scheinbar trivialer Forderungen zu schätzen wissen. Risikoanalyse ist für BS 7799 genauso selbstverständlich wie die Einbeziehung des Layers 8 (des Menschen) durch Schulung. Hauptziel des BS 7799 ist die Dokumentation des Information Security Management Systems (ISMS).

4 Vergleich der Standards

Alle Standards zu IT Sicherheit beschäftigen sich mit dem gleichen Thema; was den Vergleich erschwert ist die unterschiedliche Verwendung von Begriffen und die unterschiedliche Einteilung. Um Groben kann aber gesagt werden, daß das BSI Grundschutzhandbuch am detailliertesten ist, was den Nachteil hat, das es auf Neuerungen wie mobiles Arbeiten nicht selbständig angepaßt werden kann. Die Common Criteria hingegen müssen ob ihrer Allgemeinheit immer angepaßt werden, was eine gewisse Neigung zu Abstraktion voraussetzt. ITIL ist DAS Werk für die Administration von IT-Infrastrukturen für einen Dienstleister und der British Standard (BS 7799) stürtzt sich ganz auf organisatorische Aspekte. Je nachdem, welches Anliegen verfolgt wird, ist der eine oder der andere Standard der geeignete.
Es gibt weitere Standards auf dem Gebiet wie den Technical Report 13335 und Cobit, die hier nicht näher beleuchtet werden.

5 Fazit

Ab einer bestimmten Komplexität ist das Design, die Entwicklung, der Betrieb oder gar die Einschätzung eines IT-Systems nicht mehr aus dem Bauch heraus machbar. In den beschriebenen Standards sind immer wiederkehrende Punkte allgemein dargestellt. Das betrifft insbesondere die technischen Aspekte wie Hardware, Netzwerke, Betriebssysteme und Applikationen als auch die organisatorischen Aspekte wie Zuständigkeiten und Prozesse.
IT-Sicherheitsstandards haben als Basis die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität, Nicht-Abstreitbarkeit und, je nach Betrachtung, auch Authentifizierung im Visier. Der einzelne

Standard umfaßt aber oft nur technische oder nur organisatorische Aspekte, oder betrachtet nur eine Teilmenge der Sicherheitsziele. Es ist somit immer notwendig zu fragen: Was soll erreicht werden? Bei Bedarf können mehrere Werke gleichzeitig Verwendung finden, da die Grundgedanken immer diesselben sind, auch wenn oft in Form von verschiedenen Begriffen, Betrachtungswinkeln und Einteilungen.
Summasummarum: IT-Sicherheitsstandards sind brauchbare Orientierungshilfen. Die Abstrahierungen haben allerdings einen Nachteil: in der Mehrzahl handelt es sich um komplexe, umfangreiche und theoretische Werke. Abstraktes Herangehen sowie die Umsetzung in den jeweils vorliegenden Fall erfordert breites und tiefes IT-Wissen in Theorie und Praxis.

7 Literatur

- BSI: www.bsi.de
- BSI: http://www.bsi.de/literat/index.htm
- Studie zu ISO-Normungsaktivitäten ISO/BPM:http://www.bsi.bund.de/literat/studien/gshb/ISO-BPM-Zertifizierung_040305.pdf
- BSI Grundschutzhandbuch:http://www.bsi.bund.de/gshb/deutsch/index.htm
- Common Criteria:http://www.bsi.de/cc/index.htm
- ITIL: www.itil.org
- BS 7799: http://www.secorvo.de/whitepapers/secorvo-wp10.pdf