atsec the information security provider
NEWS 03/13

Vom Wert des Vertrauens

Als eines der weltweit aktivsten Prüflabore für Sicherheitsevaluierungen nach den Common Criteria war atsec mit einem großen Aufgebot und einigen Erwartungen zur diesjährigen International Common Criteria Conference (ICCC) nach Orlando, Florida, gereist. Eingeladen ins Heimatland von Micky Maus hatte die NSA, eben jener Nachrichtendienst, der in letzter Zeit selbst die Nachrichten füllt. Die NSA betreibt das amerikanische CC-Schema, stellt also in den USA die CC-Zertifikate aus. Diese sollen besorgten Kunden in aller Welt nachweisen, dass die geprüften IT-Produkte sicher und ihre Unternehmensdaten deshalb geschützt sind. Diese Zertifikate werden von 25 weiteren Nationen anerkannt, die zusammen das CCRA, also das Abkommen zur gegenseitigen Anerkennung solcher Zertifikate, unterschrieben haben.

Nachdem wir jetzt alle herzlich gelacht haben, verweilen wir noch etwas beim Kernproblem dieses Abkommens: Die Common Criteria definieren einen Prüfstandard, der es Unternehmen erlaubt, die Sicherheit ihrer IT-Produkte von einem unabhängigen und vertrauenswürdigen Dritten prüfen zu lassen, so dass nicht jeder Kunde diese Prüfung selbst durchführen muss. Mit anderen Worten: **Ein CC-Zertifikat transportiert Vertrauen vom Hersteller zum Kunden.** Voraussetzung dafür ist aber, dass der Dritte, der das Zertifikat ausstellt (und natürlich das Prüflabor, das die Prüfung durchgeführt hat), unabhängig und vertrauenswürdig ist. Was aber, wenn derjenige, der die Zertifikate ausstellt, weder unabhängig noch vertrauenswürdig ist? Was ist so ein Zertifikat noch wert? Welches Vertrauen transportiert es? Richtig: Gar keines.

Während der ICCC haben sich die CCRA-Mitgliedsstaaten auf einen ersten Entwurf für ein neues Abkommen zur gegenseitigen Anerkennung geeinigt. Es beschränkt die Anerkennung von Zertifikaten auf ein Minimalniveau, das für viele Kunden nicht mehr relevant ist. Gleichzeitig versuchen insbesondere die USA und ihre treuen Helfer, selbst die Nennung einer Vertrauenswürdigkeitsstufe (von EAL1 bis EAL7) aus den neuen Schutzprofilen und möglichst auch aus den Zertifikaten zu verbannen. Damit wissen die Kunden der Hersteller dann gar nicht mehr, wie viel Vertrauen sie in solche Zertifikate haben können.

Ist das nun schlimm und gar das Ende der Common Criteria? Ich meine nicht. Wer als Kunde das Zertifikat eines Herstellers erhält, musste auch bisher selbst entscheiden, wie viel Vertrauen er in das Zertifikat setzen sollte. Schon bisher gab es Nationen und Prüfstellen, bei denen man gewisse Zweifel hegte. Neu ist jetzt nur, dass ein paar Zweifel zur Gewissheit wurden.

Als Prüfstelle im deutschen Schema braucht atsec dies nicht zu fürchten, denn hier hat das Bundesamt für Sicherheit in der Informationstechnik sich über die Jahre den Ruf einer vertrauenswürdigen Instanz erarbeitet, den viele unserer internationalen Kunden jetzt noch viel mehr zu schätzen wissen als bisher schon. Vielleicht werden es einige europäische Staaten sogar schaffen, im SOGIS-Abkommen ein vernünftiges Gegengewicht zur Entwertung der Zertifikate zu schaffen, auch gegen den Widerstand der Five Eyes.

Wichtig ist vor allem zu erkennen, dass wegen ein paar fauler Äpfel nicht alle Zertifikate wertlos werden. Jeder muss genauer hinsehen und vor allem entscheiden, wem er sein Vertrauen schenkt, CCRA hin oder her.

In diesem Sinne hoffe ich, dass Sie uns auch in Zukunft Ihr Vertrauen schenken. Auf dieses Vertrauen sind wir stolz, weil es die Grundlage und die Frucht unserer Arbeit ist, heute und in Zukunft.

Herzlichst,
Gerald Krummeck
Leiter Prüfstelle

Messen und Konferenzen 2014

Die atsec information security wird in diesem Jahr auf folgenden Messen und Konferenzen vertreten sein:

- **DFN-Workshop in Hamburg: 18. bis 19.02.2014**
  Unser COO Matthias Hofherr wird am 19.02.2014 einen Vortrag zum Thema „Datenschutz – ein Lösch- und Sperrkonzept“ halten.

- **it-sa in Nürnberg: 07. bis 09.10.2014**
  Auf der größten IT-Sicherheitsmesse im deutschsprachigen Raum wird sich atsec auch im Jahr 2014 wieder mit einem eigenen Stand präsentieren.

- **MILCOM in San Diego: 06. bis 08.10.2014**
  Auf der wichtigsten internationalen Messe für Militärkommunikation wird atsec auch 2014 wieder vertreten sein.

atsec it security blog
Verfolgen Sie brandaktuell Diskussionen und Erlebnisse unserer Mitarbeiter auf http://atsec-information-security.blogspot.de

ISO 27001 im Wandel

Wer selbst ein Informationssicherheits-Management-System (ISMS) nach ISO/IEC 27001 (im weiteren kurz ISO 27001 bezeichnet) betreibt, kennt die Situation, dass jedes Jahr diverse Anpassungen und Überarbeitungen desselben fällig sind. Im September 2013 ist die Neuauflage der Standards ISO 27001 und ISO 27002 erschienen, was für die nächsten Überarbeitungszyklen zusätzliche Tätigkeiten nach sich zieht. Mit diesem Artikel geben wir einen Überblick über die Änderungen in den Standards und die Konsequenzen, die sich daraus ergeben.

Für wen sind diese neuen Standards denn nun von Interesse?

Diejenigen Firmen, die ein ISMS aufgebaut haben, das sich „grob an ISO 27001 anlehnt“, sind von den Änderungen nur unwesentlich betroffen. Dem Standard sind keine derart einschneidenden Veränderungen widerfahren, dass für diese Gruppe größere Maßnahmen notwendig sind (natürlich abhängig vom Grad der „groben Anlehnung“). Um aber die Nähe zum Standard beizubehalten, sollte hier zumindest ein Anpassung an die relevanten neuen Vokabeln erfolgen.

Firmen, die ein ISO 27001:2005 Zertifikat haben, sind von den Änderungen natürlich direkt betroffen. Grundsätzlich gibt es eine Schonfrist von 2 Jahren nach Erscheinen des Standards. Dies bedeutet, dass eine Umstellung auf ISO 27001:2013 bis zum September 2015 erfolgt sein muss. Sollte das bestehende Zertifikat bis September 2014 ablaufen (also, der 3-Jahres-Zyklus für die Gültigkeit des Zertifikats vollständig durchlaufen sein), dann gelten die neuen Anforderungen für die Re-Zertifizierung. Spezifische Vorgaben und Fristen der eigenen Zertifizierungsstelle sollten zur Sicherheit zeitnah erfragt werden.
Firmen, die gerade eine ISO 27001 Zertifizierung planen, aber den Termin für die Erstzertifizierung nicht innerhalb der nächsten Monate anstehen haben, sollten auf jeden Fall direkt den neuen Standard ISO 27001:2013 implementieren, um unnötige Migrationskosten zu vermeiden. Wenn die Implementierung des ISMS dagegen schon sehr weit fortgeschritten ist und auf dem alten Standard beruht, dann steht einer Zertifizierung nach ISO 27001:2005 normalerweise nichts im Wege.

Die Geschichte von ISO 27001 und ISO 27002

1995	Release des British Standards BS 7799:1995
1998	BS7799 wird aufgeteilt in BS 7799:1 (Best Practice Richtlinien) und BS 7799-2 (den eigentlichen Zertifizierungs-Standard)
2000	BS 7799-1 wird offiziell als ISO-Standard übernommen und firmierte fortan unter dem Namen ISO/IEC 17799:2000
2005	ISO 17799 wird stark überarbeitet und wird als ISO/IEC 17799:2005 neu veröffentlicht
2005	Der Zertifizierungs-Standard BS7799-2 wird offiziell als ISO-Standard unter dem Namen ISO 27001:2005 übernommen
2007	ISO 17799 erhält schließlich den Namen ISO 27002, allerdings ohne inhaltliche Änderungen
2013	ISO 27001:2013 und ISO 27002:2013 werden veröffentlicht

Das Migrations-Projekt

An dieser Stelle stellt sich nun die Frage: „Was muss ich eigentlich tun, um von ISO 27001:2005 auf ISO 27001:2013 zu migrieren?“. Dazu werfen wir zuerst einmal einen Blick auf die wichtigsten Änderungen zwischen den beiden Standards:

Risikomanagement: In ISO 27001:2013 wurden die Anforderungen an das Risikomanagement letztendlich vereinfacht und an den allgemeinen Risikomanagement-Standard ISO 31000 angepasst. Wo man früher Bedrohungen und Schwachstellen der Risiken betrachtet hat, genügt heute eine grundsätzliche Beschreibung des Risikos. Aus den alten Anforderungen, die Assets („Unternehmenswerte“) einer Organisation zu bestimmen und für diese einen Asset-Eigentümer festzulegen, wurde im neuen Standard die Anforderung, jeweils einen Risiko-Eigentümer (Risk Owner) festzulegen. Keine dieser Anforderungen bedeutet aber, dass man seine bestehende liebgewonnene Methodik zur Risikoanalyse ersetzen muss. Auch wenn aus einem bestehenden „Asset Owner“ jetzt formal ein „Risk Owner“ wird, dann gibt es hier eigentlich keinen Grund für einen Wechsel der Methoden.

Erstellung neuer Policies: Wer bisher keine dokumentierten Vorgaben für „Secure system engineering principles“ (A.14.2.5), „Supplier security policy“ (A.15.1.1), „Incident management procedure“ (A.16.1.5) und „Business continuity procedures“ (A.17.1.2) hat, der muss diese im Zuge der Migration erstellen. Wie üblich muss es sich dabei nicht zwingend jeweils um ein eigenes Dokument mit genau diesem Titel handeln, allerdings müssen die Inhalte in irgendeiner

dokumentierten Form niedergelegt sein. Auch wenn in ISO 27001:2005 die meisten dieser Dokumente nicht explizit gefordert sind, sollten die Inhalte bisher auch schon auf irgendeine Art und Weise behandelt worden sein.

Anpassung Annex A: Die bekannten Maßnahmen aus Annex A des Standards wurden in ISO 27001:2013 ebenfalls überarbeitet. Die Controls wurden dabei auch neu gegliedert, was dazu führt, dass das „Statement of Applicability" (SoA) komplett neu erstellt werden muss. Ebenso wurden einige Controls neu hinzugefügt:

- A.6.1.5 Information security in project management
- A.6.1.5 Information security in project management
- A.14.2.1 Secure development policy
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.8 System security testing
- A.16.1.4 Assessment of and decision on information security events
- A.17.2.1 Availability of information processing facilities

Diese müssen natürlich komplett neu bewertet werden. Hier kommt dann auch der neue Standard ISO 27002:2013 ins Spiel, der passenden zu den neuen Anforderungen auch neue „Best Practice"-Umsetzungen dafür liefert.

Kennzahlen: Das Thema Kennzahlen ist schon immer eines der etwas unschärferen Themen in der ISO 27001. Grundsätzlich ist der Gedanke, die Wirksamkeit von Maßnahmen mit Kennzahlen zu belegen durchaus nachvollziehbar. In der Praxis war es allerdings schon immer schwierig, hier Kennzahlen zu finden, die auch wirklich einen praktischen Mehrwert für die Sicherheitsorganisation haben. Hier hat leider auch der doch eher akademisch angehauchte Standard ISO 27004:2009 kein Licht ins Dunkel bringen können. In ISO 27001:2013 wurden die Anforderungen an Kennzahlen verschärft und präzisiert (siehe hierzu ISO 27001:2013 Kapitel 9.1).

Sonstige Anpassungen: ISO 27001:2013 enthält verschiedene kleinere Anpassungen und Formulierungs-Änderungen, die Modifikationen in bestehenden Dokumenten nach sich ziehen. Eine Aufzählung aller Details würde allerdings den Rahmen dieses Artikel sprengen. Generell sollte beachtet werden, dass es den PDCA-(„Plan-Do-Check-Act") Zyklus (auch besser bekannt als Demming Kreislauf) nicht mehr explizit gibt. Dieser wurde durch den allgemeinen Begriff „Continuous improvement" ersetzt. In der Praxis hat dies allerdings keine großen Auswirkungen; es bietet sich hier aber die Möglichkeit, statt PDCA andere Methoden zur kontinuierlichen Verbesserung umzusetzen.

Ebenso sollte beachtet werden, dass es keine expliziten Anforderungen für „Preventive Actions" mehr gibt. Hier sollte geprüft werden, ob man sich von bestehenden Policies/Richtlinien, die man erstellt hat, trennen möchte. Faktisch wird das Thema „Preventive Actions" im Rahmen des bestehenden Risikomanagements abgehandelt, wo es praktisch auch schon immer stattgefunden hat.

Auswirkungen auf BSI IT-Grundschutz

Auf Betreiber von Systemen, die nach BSI IT-Grundschutz zertifiziert sind, dürfte die Anpassung des Standards mittelfristig sicher auch Auswirkungen haben. Um weiterhin eine Kompatibilität zum Standard ISO 27001 aufrechtzuerhalten, werden auch hier in absehbarer Zeit Anpassungen an den IT-Grundschutz-Standards notwendig werden. Zertifikatsinhaber sollten hier regelmäßig die einschlägigen Mailinglisten prüfen bzw. sich vom Grundschutz-Auditor ihres Vertrauens unterrichten lassen.

Fazit

Abgesehen von der Tatsache, dass eine Anpassung an den neuen Standard Aufwand erzeugt, sind die Änderungen alles in allem positiv zu bewerten. Sehr spezifische Anforderungen wurden entfernt und die Anforderungen wurden allgemein so gestaltet, dass zertifizierte Unternehmen eine größere Gestaltungsfreiheit bei der Umsetzung haben. Die Schonfrist für eine Migration ist so gewählt, dass jedes Unternehmen ausreichend Zeit haben sollte, sein ISMS entsprechend anzupassen. Die Änderungen sollten sich jeweils im Rahmen des bestehenden kontinuierlichen Verbesserungsprozesses zwischen zwei Audits im Rahmen eines kleineren Projekts umsetzen lassen.

atsec NEWS

Zertifizierte IT-Sicherheit – welcher Standard ist der richtige?

Informations-Sicherheitsstandards schaffen die Basis für ein einheitliches, angemessenes Sicherheitsniveau innerhalb einer Organisation, können aber auch die Entwicklung sicherer Produkte begleiten und Vertrauen in deren Einsatz begründen. Durch die Prüfung und Zertifizierung wird der Nachweis einer vergleichbaren und einheitlichen Umsetzung des Standards erbracht. Ein vertrauenswürdiger Nachweis ist ein schlagkräftiges Argument im umkämpften Markt für IT-Sicherheitsprodukte und -Dienstleistungen. Das Vertrauen in die Prüfergebnisse steht und fällt mit der Vertrauenswürdigkeit der prüfenden und zertifizierenden Instanzen. atsec beschäftigt sich insbesondere mit den folgenden Sicherheitsstandards:

ISO 27001 mit und ohne BSI IT-Grundschutz

Der internationale Standard ISO/IEC 27001 definiert Anforderungen für ein Informationssicherheitsmanagementsystem (ISMS). Die Anforderungen beschreiben einen prozessorientierten Ansatz, der die Planung, Umsetzung, Durchführung, Überwachung und Überprüfung sowie die Wartung und Verbesserung des ISMS beinhaltet. Sowohl Behörden als auch Unternehmen können ihr ISMS nach diesem Standard auditieren und zertifizieren lassen. Der Geltungsbereich des ISMS kann ein geschäftsrelevanter Teilbereich aber auch eine komplette Organisation sein. Man unterscheidet zwischen nativen ISO 27001 Zertifizierungen durch anerkannten Zertifizierungsstellen und Zertifizierungen nach ISO 27001 auf der Basis von IT- Grundschutz (ITGS) durch das BSI. ITGS ersetzt dabei zunächst die Risikoanalyse mit einem Standard-Sicherheitsniveau, für das ein detaillierter Katalog von Standard-Maßnahmen bereitsteht. Für höheren Schutzbedarf können weitere individuelle Maßnahmen anhand einer detaillierten Risikoanalyse definiert werden. Im Gegensatz zu den sehr spezifischen ITGS Maßnahmen definiert ISO 27001 einen grundsätzlichen Rahmen an Anforderungen, die jeweils mit individuellen Maßnahmen adressiert werden. Das Abarbeiten konkreter ITGS-Maßnahmen ist meist mit einem deutlich höheren Aufwand verbunden, als der risiko- und anforderungsgetriebene Ansatz des nativen ISO 27001.

Common Criteria und FIPS 140-2

Common Criteria (CC) und FIPS 140-2 sind Standards zur Bewertung von IT-Sicherheitsprodukten. Sie unterscheiden sich wesentlich in Bezug auf den Prüfgegenstand, den Schwerpunkt der Prüfung, ihre Abstraktheit und nicht zuletzt hinsichtlich ihrer Anerkennung. Während es bei CC um die Prüfung und Bewertung von allgemeinen Sicherheitseigenschaften von IT-Produkten geht, beschäftigt sich FIPS 140-2 mit der Bestätigung von Sicherheitsanforderungen kryptographischer Module. CC und der entsprechende ISO Standard (ISO/IEC 15408) sind international anerkannt, wogegen es sich bei FIPS 140-2 um einen US-Standard des National Institute for Standards and Technology (NIST) handelt. Die FIPS 140-2 Validierungs- und Testprogramme sind in Zusammenarbeit von NIST und dem Communications Security Establishment Canada (CSEC) entstanden. CC-Zertifikate werden von Zertifizierungsbehörden herausgegeben und weltweit von verschiedenen Ländern anerkannt. Ein FIPS Zertifikat wird nur von NIST oder von CSEC erteilt. Beide Länder erkennen ihre Zertifikate gegenseitig an. Amerikanische Bundesbehörden sind verpflichtet, für die Verarbeitung sensitiver Daten ausschließlich kryptographische Systeme einzusetzen, die FIPS 140-2-validierte kryptographische Module implementieren.

FIPS 140-2 definiert Anforderungen an kryptographische Module in verschiedenen Bereichen (wie z. B. physische Sicherheit, Schlüsselmanagement, Selbsttests etc.) und Stufen. Bei der Modul-Validierung geht es um reines Compliance Testing: das kryptographische Modul wird gegen die vordefinierten Sicherheitsanforderungen geprüft. Es werden nur von NIST / CSEC anerkannte Standardalgorithmen zertifiziert. Voraussetzung für eine erfolgreiche Modul-Validierung ist der Nachweis der korrekten Implementierung dieser Algorithmen.

Bei einer CC-Evaluierung erfolgt die Bewertung eines IT-Produktes hinsichtlich funktionaler Sicherheitsanforderung und Anforderungen an die Vertrauenswürdigkeit. Um Vergleichbarkeit und Unabhängigkeit der Prüfergebnisse zu schaffen, werden Klassen für beide Aspekte von den CC vorgegeben. Dadurch lässt sich einerseits die tatsächliche Sicherheitsfunktionalität des Produktes vergleichbar modellieren, andererseits die Prüftiefe für die Evaluierung allgemeingültig und vergleichbar festlegen. Die CC definieren auch Sicherheitsanforderungen für kryptographische Funktionen. Kriterien für die Bewertung der Qualität kryptographischer Algorithmen und Protokolle sind jedoch nicht enthalten; sie liegen in der Verantwortung des CC-Zertifizierungsschemas. Im deutschen Schema werden z. B. zusätzliche Prüfaspekte im Rahmen der Schachstellenanalyse für kryptographische Algorithmen, Protokolle und Zufallszahlengeneratoren definiert. In anderen CC-Schemata kann ggf. ein FIPS-Zertifikat für das kryptographische Modul als Vertrauenswürdigkeitsmaßnahme herangezogen werden.

IMPRESSUM

atsec information security GmbH
Steinstraße 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com

Vertretungsberechtigte
Geschäftsführer:
Salvatore la Pietra
Staffan Persson
Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG:
DE205370914
Verantwortlich für den Inhalt:
Staffan Persson (Anschrift s.o.)