

CAcert und das Audit



CAcert und das Audit

- Um CAcert Root-Zertifikate in Browser zu bekommen
 - => wird ein Audit benötigt
 - => das erfordert
 - Management
 - Policies + Verfahrensanweisungen
 - Audit der Geschäftsabläufe & Systeme
 - gegenüber diesen Richtlinien und Verfahren.

CACert und das Audit

- CACert hat zwei wesentliche Tätigkeitsbereiche
 - ➔ Assurances
 - ➔ Systeme.

CAcert und das Audit

a. Assurance

- Assurance Policy ist nun in
=> vollem POLICY-Status
- **Verbindlich** für alle Assurer
- Der Prozess der Assurance kann nun Ge-Audited werden.

CAcert und das Audit

a.i Auditor auf (ATE) Tour

- Assurer sollen Auditor prüfen
- == ein Beleg für Assurance im Einklang mit der Policy
- verifiziert die Qualität der Assurance
- (Steigerung der Qualität des Assurens?)

CAcert und das Audit

a.ii Auditor Vertretung (co-Auditors)

- Erfahrene Assurer vertreten den Auditor und sollen stattdessen von Assurern geprüft werden
- (Wurde bereits assured, überwacht er das Assuren eines anderen Assurers)
- Im Bericht ein Statement:
„Assurance wurde gemäß Policy durchgeführt.“
- Gilt als "weiterer Nachweis" für das Audit.

CACert und das Audit

a.iii Assurance Audit

- Abschluß für Nachweise:
war der 16. Mai '09 München

CAcert und das Audit

b. Systeme

- Verzögerung des System-Audits mangels sicheren Hosting-Dienstes
- Serverumzug am 1. Oktober 2008
- von Wien
- ins sichere Datenzentrum BIT einer Firma in Ede, NL

CAcert und das Audit

b. Systeme (Fortsetzung)

- Neues Team von Systemadministratoren
- Freigabe Security Policy in DRAFT-Status
 - => Verbindlich für die Systemverwalter und Techniker mit Zugangsrechten
 - => System-Audit gegenüber dieser Richtlinie jetzt möglich.

CACert und das Audit

b.i Audit Vorort Inspektion

- 1. Besuch am 4., 5., 6. Mai 2009
warm-up: personnel, Roots, Access, inventory
- Voraussichtlich 1. von 3 Besuchen.
- Nächster Besuch: Mitte Juni

CAcert und das Audit

b.ii Zertifizierungs-Verfahrensanweisung
(Certification Practice Statement, CPS)

Seit Juli 2009 im Draft Status
und somit verbindlich.

CAcert und das Audit

b.iii Audit der Software

- Innsbruck Softwarecamp
Woche 20. April 2009
- Ernsthafte Schwierigkeiten bei der Wartung
Optimierung und Absicherung
- keine verlässliche Aussage möglich
- Neues Software Entwicklungsteam,
neues Design, Neuaufbau

Hintergründe zum Audit



Hintergründe zum Audit

- Der Maßstab für das Audit nennt sich **DRC** for "**D**avid **R**oss **C**riteria".
- David ist ein Qualitäts-Ingenieur im Ruhestand
- Er startete das CACert Audit
- Er hat eine andere Aufgabe übernommen

Hintergründe zum Audit

- Die DRC haben eine solide Eigenschaft:
- sie verlangen, daß
 - alle Risiken,
 - jegliche Haftung und
 - alle Verpflichtungen
- klar gegenüber jedermann dargelegt werden!

Hintergründe zum Audit

- Dies errichtete etliche gewaltige Hürden für die CA:
 - Was genau sind die Risiken/Haftung/Pflichten?
 - Auf wen beziehen sie sich?
 - Sind sie zumutbar?
 - Und wie soll mit ihnen umgegangen werden?

Hintergründe zum Audit

Ein wichtiges Ergebnis der Überlegungen:

wir benötigen

- eine Vereinbarung der CAcert-Gemeinschaft
- und sie muß folgendes leisten:

Hintergründe zum Audit

- a. Mitglieder in beidseitig verpflichtende Gemeinschaft einbinden
- b. die Risiken/Haftung/Pflichten festzulegen.
- c. die Haftung zu begrenzen
 - 1000 Euro
 - die Haftung an die Mitglieder zurück zu geben

Hintergründe zum Audit

- Wie können wir die Verbindlichkeiten zurückgeben?
 - Durch unser eigenes „Forum der Streitbeilegung“,
 - Zustimmung dieser Form der Streitbeilegung
 - Schreiben einer Policy um den Prozess zu kontrollieren:
 - ==> Arbitration.

Hintergründe zum Audit

- Zusammenfassung: Das ursprüngliche „Warum“ der Arbitration:
 - Audit (DRC) zwingt die Offenlegung der Verbindlichkeiten
 - Einfacher Fix: *Limitierung*
 - Komplexer Fix: *Verteilung*
 - die sichere und günstige Lösung zur Verteilung:
 - eine eigene Arbitration nutzen
- (Das letzte Kapitel diskutierte das „Wie“.)