atsec the information security provider

NEWS 01/11

## atsec bei der ICCC-Konferenz

Die Zukunft der Common Criteria (CC) als dem Regelwerk zur Beurteilung der Sicherheit von IT-Produkten ist das Thema der alljährlichen, internationalen ICCC-Konferenz, die Ende September an der türkischen Riviera in Antalya stattfand.

atsec war als eines der führenden Prüflabors weltweit mit einer prominenten Delegation vertreten, die die gesamte Geschäftsführung und alle Leiter der Prüfstellen aus Deutschland, USA und Schweden umfasste. Insgesamt wurden knapp 300 Teilnehmer aus 25 Nationen gezählt. Die stärksten Delegationen kamen dabei neben der gastgebenden Türkei aus den USA, Deutschland, China, Japan, Frankreich, Südkorea, Spanien und Schweden und zeigen damit, wo die Anwendung der CC besonders intensiv betrieben und beobachtet wird.

Ein zentrales Thema der Konferenz waren dieses Mal die Bildung von Communities, d.h. Interessensgruppen, die zusammenarbeiten, um für bestimmte Produkttypen gemeinsame Sicherheitsanforderungen zu formulieren. Diese Zusammenarbeit existiert im Spezialbereich der Chipkarten schon lange auf europäischer Ebene. atsec hat entscheidend mitgeholfen, eine internationale Community für Betriebssysteme zu schaffen; dies wurde im Rahmen des BSI-Projektes zur Definition eines Schutzprofils für Betriebssysteme (OSPP) verwirklicht. Im Rahmen dieses Projektes haben atsec und das BSI auch grundlegende Neuerungen für Schutzprofile erarbeitet, die ein weiteres wichtiges Thema der Konferenz waren. Durch die flexible Struktur des OSPP-Schutzprofils mit einer vorgeschriebenen Grundfunktionalität und einer Reihe optionaler Zusatzfunktionen wurde erst die Möglichkeit für die Communities geschaffen, über einen Minimalkonsens hinaus gehende Spezifikationen für die Sicherheit von IT-Produkten zu definieren.

> *„Unfortunately, there are not enough atsecs in this world."*

Mit der Bildung produktspezifischer Interessengruppen und der daraus folgenden Definition von Schutzprofilen und Handreichungen für die Prüfung dieser Produkte wollen einige Zertifizierungsbehörden, insbesondere die der USA, offenbar auch gegen die Qualitätsprobleme in ihren eigenen Reihen vorgehen. Leider wird dabei die Kritik an einzelnen Evaluationen zum Teil als generelle Kritik an den CC missverstanden. „Unfortunately, there are not enough atsecs in this world" fasste ein bekannter Konferenzteilnehmer seine Erfahrung mit Evaluierungsproblemen durch mangelnde Expertise zusammen. Schön für uns!

Allerdings wird es für atsec noch einiger Überzeugungsarbeit bedürfen, um die internationale Gemeinschaft von einigen drohenden Irrwegen zur besseren Vergleichbarkeit von Evaluierungen abzubringen: IT-Sicherheit kann niemals alleine durch das sture Abhaken von Checklisten erreicht werden. „Messbar, aber irrelevant" kann nicht der Ersatz für eine fundierte Analyse sein. atsec zeigt immer wieder, dass solche Analysen effizient machbar sind, aber ohne Expertise geht es eben nicht.

***Gerald Krummeck***
Prüfstellenleiter atsec

## PCI und Mainframes – Zwei Welten treffen aufeinander

Einem Ruf der IBM Guide Share-Usergroup folgte atsecs Sicherheitsspezialist Andreas Siegert nach Whittlebury Hall, England, um über die Anwendung des PCI Data Security Standards auf Großrechnern zu referieren.

Die PCI DSS-Anforderungen der Kreditkartenindustrie passen auf typische Windows- und UNIX-Systeme. Trifft ein PCI-Auditor (QSA) bei einer Prüfung ohne entsprechendes Hintergrundwissen auf Mainframes, wird er mit diversen Schwierigkeiten konfrontiert. Aus diesem Grund entwickelte atsec mit IBM ein Whitepaper *(www.atsec.com/us/pci-lcs.html)*, auf das Siegert als einer der Autoren im Speziellen einging. Im Vordergrund seines Vortrags standen die wichtigsten Schlüsselpunkte, in denen sich der Umgang mit Mainframes vom Umfeld kleinerer Server unterscheidet, etwa die Anforderungen für die Implementierung multipler Funktionen und die Integritätsprüfung von Systemdateien, und wie sich diese auf Mainframes bezogen umsetzen lassen.

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

# Keine Angst vor eigenen Zertifikaten

**Das Verschlüsseln von E-Mail schreckt viele Unternehmen aufgrund der vermeintlich unwägbaren Komplexität ab. Dabei ist die Bereitstellung der notwendigen Mittel, wie etwa S/MIME-Zertifikate, äußerst simpel. Digitale Zertifikate bestätigen die Identität der Schlüssel und Zuordnung zu einer bestimmten Person, Organisation oder einem System. Bei der Versendung von E-Mail kommen S/MIME-Zertifikate zum Einsatz, für deren Kauf und Wartung viele Betriebe hohen Aufwand betreiben. Diese Zertifikate sind meist nur ein Jahr gültig und müssen dann erneuert werden. Dies führt nicht nur zu hohen Anschaffungskosten, sondern auch zu einem beachtlichen Verwaltungsaufwand. Eine einfache Lösung besteht in der Erstellung einer eigenen Certificate Authority (CA), um damit die externen Abhängigkeiten und Kosten zu reduzieren.**

Während technikorientierte Benutzer oft mit PGP/GPG arbeiten, um E-Mail zu verschlüsseln, sind reine Anwender ohne technischen Hintergrund oft damit überfordert. Auch die Integration in typische Unternehmens-Kommunikationslösungen, wie Lotus Notes oder Microsoft Exchange, stellt keine zufriedenstellende Lösung dar.

Für diese Anwender bieten S/MIME-Zertifikate eine wesentlich einfachere Möglichkeit zur Absicherung der Kommunikation.

Für die typische B2B-Kommunikation genügen einfache S/MIME-Zertifikate ohne Anspruch auf Rechtssicherheit gemäß Signaturgesetz. Durch den Einsatz einer eigenen CA spart man nicht nur Geld, auch die Anwendung ist flexibler als bei zugekauften Zertifikaten. Die regelmäßige Erneuerung erfolgt vollautomatisiert.

### Wie sieht ein typisches Anwendungsszenario für verschlüsselte E-Mail aus?

Üblicherweise wird eine 1:1-Kommunikation zwischen Partnern, die schon eine Geschäftsbeziehung unterhalten, verschlüsselt. Weder für Massenmails, noch für andere Formen der Kommunikation ohne bestehenden Kontakt, wird Verschlüsselung eingesetzt. Auch wenn mehrere Zielpersonen angesprochen werden, handelt es sich meist um übersichtliche Verteiler. Die Implementierung ist also, wenn man an Szenarien wie firmeninterne E-Mail oder Kommunikation mit Filialen und Partnern denkt, ohne große Infrastrukturanforderungen möglich.

### Welche Gründe gibt es, eine eigene CA aufzubauen, statt Zertifikate zu kaufen?

Je nach Menge der benötigten Zertifikate steigt der Anschaffungspreis schnell in die Tausende. Somit ist der Kostenaspekt ein wichtiger Gesichtspunkt.
Außerdem verfügt man über die Kontrolle, automatisiert neue Zertifikate zum selbst bestimmten Zeitpunkt zu generieren, anstatt auf bestellte möglicherweise warten zu müssen. Falls nötig, lassen sich Zertifikate über eine Certificate Revokation List (CRL) ohne Umstände sperren.

Auf Wunsch lassen sich interne Organisationszugehörigkeiten in den Zertifikaten mühelos abbilden.

**Wie erfolgt der Aufbau einer eigenen CA?**

Die Sicherheit der CA selbst wird durch einen minimalistischen Aufbau auf Basis eines portablen Systems, das nur bei Bedarf aus einem Safe genommen wird, erreicht. Je nach gewünschter Methode zur Schlüsselverteilung ist entweder überhaupt kein Netzwerk nötig, oder aber das CA-System agiert nur als Sender für die Verteilung der Zertifikate, um weniger Angriffsfläche zu bieten.

Um die sichere Kommunikation der Partner zu gewährleisten, ist zuerst die Durchführung einiger Tests angeraten, denn nicht jedes System verträgt jede Schlüssellänge oder beliebige Algorithmen. Sobald die Basisparameter festgelegt sind, wird mit dem Aufbau der eigentlichen CA begonnen. Auf Basis von OpenSSL (dessen Kryptographie schon nach FIPS-140 zertifiziert wurde) lassen sich alle Operationen der CA implementieren. Dies erfolgt am effektivsten über Skripte, die alle konstanten Parameter enthalten, um die Konformität der CA zur einmal festgelegten Richtlinie zu sichern. Dies setzt natürlich die Festlegung der Parameter für Algorithmen, Schlüssellängen und Laufzeiten und deren Umgang mit der CA in dieser Richtlinie voraus.

Es empfiehlt sich, eine CA immer nach dem Vier-Augen-Prinzip zu betreiben. Dies wird technisch beispielsweise durch Aufteilung des Passwortes für Festplattenverschlüsselung in zwei Teile durchgesetzt.

Der Root-Schlüssel sollte nach der initialen Inbetriebnahme auf einer CD oder als Ausdruck im Bankschließfach gesichert werden. So ist im Falle eines Defekts oder der Zerstörung des CA-Rechners oder dessen Festplatte die Funktionsfähigkeit der CA weiterhin gewährleistet. Für den Betrieb der CA ist ein Logbuch in Papierform ausreichend, um die Nutzung nachzuvollziehen.

**Risikoanalyse**

Anwendungsbezogen ist sicherzustellen, dass die CA-Lösung den Sicherheitsanforderungen entspricht. Dies geschieht zweckmäßigerweise mittels einer Risikoanalyse. Diese bewertet die potentiellen Risiken durch den CA-Betrieb im Vergleich zu gekauften Zertifikaten neutral. Gleichzeitig dient sie als Grundlage für die Abnahme durch das Management. Anhand der Risikoanalyse werden folgende kritischen Fragen geklärt:

- Sind die Sicherheitsmaßnahmen für die CA ausreichend?
- Welche Risiken entstehen im Vergleich zu gekauften Zertifikaten?
- Wie werden existierende Risiken durch Design und Implementierung reduziert und ist die Reduktion ausreichend?

Diese Informationen dienen zum einen dazu, gegebenenfalls notwendige Verfeinerungen an der CA-Policy, dem Design und der Implementierung vorzunehmen. Zum anderen wird das Restrisiko erfasst und bewertet, um eine verlässliche Grundlage für die Entscheidung zum Einsatz der CA zu erhalten.

Nach Einarbeitung der Resultate der Risikoanalyse in Richtlinie und Design erfolgt nun die eigentliche Implementierung. Hierzu ist keine aufwendige Infrastruktur nötig, die Verwendung eines Laptops ist beispielsweise denkbar.

**Schlüsselverteilung**

Während der Design-Phase gilt dem Punkt Schlüsselverteilung vordringliche Aufmerksamkeit. Einerseits ist zu beachten, dass nur berechtigte Benutzer den Schlüssel erhalten. Gleichzeitig ist die sichere Verteilung zu gewährleisten. Sobald Benutzer einmal einen Schlüssel besitzen, lassen sich neue, aktualisierte Schlüssel unkompliziert in verschlüsselter Form bereit stellen.

Die initiale Verteilung ist dagegen etwas komplexer. Je nach Organisationsgröße setzt man hier verschiedene Mechanismen ein, beispielsweise die Verteilung der Schlüssel ans Management eines Unternehmens via USB-Stick. Sobald diese Manager über einen sicheren Kommunikationspfad verfügen, kann er für den Empfang der Schlüssel der Mitarbeiter verwendet werden.

Der öffentliche Teil des CA-Schlüssels wird per Webserver zur Verfügung gestellt, um so externen Kommunikationspartnern die Möglichkeit zu geben, die Schlüssel der Mitarbeiter zu verifizieren. Der Webserver sollte den CA-Schlüssel über eine SSL-Verbindung anbieten. Bei dieser wird ein von einer externen Stelle gekauftes Zertifikat verwendet, um hier eine Vertrauenskette aufzubauen.

Die hier beschriebene Methodik für den CA-Aufbau konzentriert sich auf die Erstellung von S/MIME- Zertifikaten für den E-Mail-Verkehr. Eine weitere, geläufige Verwendung der CA findet sich etwa in der Erstellung von Zertifikaten für interne Webserver und Benutzerauthentisierung.

Der Aufbau einer eigenen CA bietet also unter Beachtung der genannten Voraussetzungen Vorteile gegenüber gekauften Zertifikaten: die Implementierung ist ohne aufwendige Infrastruktur möglich, durch rechtzeitige Generierung der Zertifikate und Möglichkeit der Sperrung wird die Kontrolle erhöht, vollautomatische Erneuerung stellt einen komfortablen Zusatz dar.

Die Sicherheit der Unternehmenskommunikation wird somit durch flexible, kostengünstige und praktikable Art und Weise gewährleistet.

# atsec NEWS

## Vier IEEE-Schutzprofile für Multifunktionsdrucker von atsec evaluiert

Sicherheitsrisiko Bürodrucker? Die Möglichkeiten eines Multifunktionsgerätes, das im Büroalltag zum Drucken, Scannen, Kopieren und Faxen eingesetzt wird, sind weitaus vielfältiger als vermutet. Je nach Bauart verfügen diese Geräte über eindrucksvolle Funktionen, wie beispielsweise das Speichern und sichere Ausdrucken vertraulicher Schriftstücke, die vorher per Mail oder Druckauftrag an den Drucker gesendet wurden. Die Autorisierung erfolgt am Gerät durch eine Passwort- oder PIN-Eingabe. Dieser Multifunktionsdrucker ist also Druck-, Mail- und FTP-Server in einem, der insbesondere vertrauliche Dokumente auf einer Festplatte zwischenspeichert, und somit äußert angreifbar ist.

Angesichts dieser Problematik entwickelte das Institute of Electrical and Electronics Engineers (IEEE) in Zusammenarbeit mit Sponsoren aus dem Kreis der Druckerhersteller sogenannte Schutzprofile. Diese definieren die Sicherheitsanforderungen an ein solches Multifunktionsgerät in unterschiedlichsten Umgebungen. Durch die Beteiligung aller großen Hersteller entstanden sinnvolle und vor allem von der Industrie akzeptierte Sicherheitsstandards in Bezug auf Funktionalität und Vertrauenswürdigkeit der Drucker. Diese Standards berücksichtigen alle Aspekte der IT-Sicherheit, wie Authentifizierung, Autorisierung, Geheimhaltung, Datenschutz, Integrität, Gerätemanagement, physikalische Sicherheit und Informationssicherheit.

Alle vier dieser Schutzprofile, auch PPs (Protection Profiles) genannt, wurden nun von atsec im Auftrag der IEEE evaluiert. Durch seine Akkreditierung beim Bundesamt für Sicherheit in der Informationstechnik (BSI), der amerikanischen NIAP CCEVS sowie der schwedischen CSEC war atsec für diese Aufgabe prädestiniert.

Für den sicherheitsbewussten Verbraucher bedeutet dies, dass ihm die Anschaffung eines nach diesen Standards qualifizierten Multifunktionsgeräts die größtmögliche Sicherheit für seine Daten bietet.

## atsec bei Datenschutzfachtagung vertreten

Informationssicherheit ist gerade im Bankensektor ein wichtiges Thema. Der Bankenfachverband, die Vereinigung der Kreditbanken in Deutschland, lud im September 2010 nach Berlin zur Fachtagung „Datenschutz“ ein. Peter Wimmer, COO von atsec Deutschland, hielt dort den Vortrag „Zertifizierung von Informationssicherheits-Management-Systemen (ISMS) nach ISO 27001“. Er betonte darin die Notwendigkeit, die Balance zwischen Compliance-Anforderungen und verfügbaren Ressourcen zu finden. Wichtig sei in diesem Bereich die Entwicklung schlanker Lösungen, trotz hoher Komplexität. Ohne Risikomanagement sind keine fundierten Entscheidungen möglich, wo reelle Gefahren abzuwehren sind und wo Restrisiken akzeptiert werden können.

Die 56 Kreditbanken des Bankenfachverbandes finanzieren privaten Konsum und gewerbliche Investitionen, darunter vor allem Kraftfahrzeuge. Der Verband vertritt die Interessen seiner Mitglieder gegenüber Politik, Bankenaufsicht, Verbraucherschutz und der Öffentlichkeit.

## MilCom 2010 und AFCEA

Alljährlich findet in San Jose, Kalifornien, die MilCom *(Military Communications)*, die wichtigste internationale Messe für Militärkommunikation, statt. Auch dieses Jahr beteiligte sich atsec wieder mit einem gut besuchten Stand.

Unter anderem führten wir zukunftsweisende Gespräche mit Vertretern der AFCEA *(Armed Forces Communications and Electronics Association)*. Dies ist eine internationale Vereinigung von Fachleuten aus Staat, Militär, Sicherheitsbehörden, Industrie, Wirtschaft und Wissenschaft, die sich mit den Themenbereichen Kommunikation, Information, Elektronik und Sensorik im Bereich militärischer und sicherheitsrelevanter Anwendungsfelder beschäftigt.

atsec entschloss sich zu einer Mitgliedschaft in der AFCEA. Auf der internationalen Plattform mit über 35.000 Mitgliedern besteht die Gelegenheit zu intensivem Gedankenaustausch und Kontakten zu Fachkollegen in aller Welt. Die Präsenz auf diesem Marktsegment stellt einen wichtigen Schritt für zukünftige Zusammenarbeit dar.


### IMPRESSUM

atsec information security GmbH
Steinstr. 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:
Peter Wimmer (Anschrift s.o.)