atsec the information security provider
NEWS 01/12

Zwölf Jahre atsec information security

Im Januar feierte atsec information security zwölfjähriges Bestehen. Dieses Jubiläum nahmen wir zum Anlass, eine – nicht ganz ernste – Selbstreflektion zum Berufsstand des Beraters zu betreiben:

„... ungebeten erschienen, geliefert, was längst bekannt war, und keine Ahnung, worum es geht“

– dies ist meist die Quintessenz der Meinungen über Berater. Und wie so oft, ist natürlich auch hier ein wahrer Kern enthalten.

Dem fehlenden Fachwissen lässt sich noch am ehesten begegnen – bei atsec haben die meisten Kollegen über zehn, einige bereits auch über 20 Jahre Erfahrung in Sicherheits-Projekten gesammelt. Einige sind über Umwege, etwa nach einen Abschluss in Geschichte, Biologie, Mathematik oder Feinwerktechnik zur Informationssicherheit gelangt, somit ist auch für unterschiedliche Betrachtungswinkel gesorgt.

Der zweite Aspekt – dem Mandanten ist eigentlich klar, welcher Weg sinnvollerweise zu beschreiten wäre – begegnet uns tatsächlich immer wieder. Hier ist es Herausforderung und Ziel, einen unvoreingenommenen Blick auf die Aufgabe beizubehalten, die verschiedenen Optionen abzuwägen, und schließlich eine konkrete Empfehlung mit fundierten Argumenten zu liefern. So wird eine Entscheidung, die sich vielleicht vorher schon aus Instinkt und eigener Erfahrung abzeichnete, von neutraler Seite bestätigt und – insbesondere beim Thema Sicherheit – mit Hintergrundwissen und Projekterfahrung untermauert. Aufgrund unserer Erfahrung betrachten wir zudem Aspekte, die auf den ersten Blick nicht offensichtlich sein mögen, für den Erfolg eines Projektes jedoch ausschlaggebend sind.

> ***„Happy Birthday, atsec!***
>
> *You are not an ordinary 12-year-old! Your knowledge and wisdom extend well beyond your years. Some of the best people in the world work at atsec and make it what it is today. We at Fulbright & Jaworski LLP are honored to list atsec information security corporation among its clients.*
> *Our best wishes to you for many more years of success.”*
>
> ***R.G. „Jerry“ Converse***
> *Fulbright & Jaworski L.L.P.*

Als schwierigster Punkt verbleibt, wenn Auftraggeber und die eigentlichen Projektmitarbeiter unterschiedliche Ziele verfolgen. Während bei technischen Projekten eine komplette Ausführung durch Externe durchaus möglich ist, ist die Einführung von Richtlinien oder gar eines Management-Systems zur Informationssicherheit ohne intensive Mitwirkung der Verantwortlichen im Unternehmen meist aussichtslos. Ebenso entsteht sichere Software im Zusammenspiel von sicherheitsbewussten Entwicklern und sicheren Prozessen – eine Evaluierung bestätigt diese Sicherheit lediglich, kann sie aber nicht erzeugen. Die Voraussetzungen hierfür abzuklären liegt letztendlich auch in der Verantwortung der Berater, gerade weil wir nicht nur Konzepte liefern, sondern konkret Einführung und Umsetzung begleiten wollen, um ein erfolgreiches Projekt zu gewährleisten.

Sicherheit ist nie Selbstzweck, und Sicherheitsprojekte sollten immer mit klar formulierten Zielen angegangen werden. atsec hat in den vergangenen zwölf Jahren bewiesen, dass Sicherheit als integraler Bestandteil wirtschaftlichen Handelns Unternehmen nicht nur sicherer, sondern auch effizienter werden lässt. Dieses Ziel ist uns Herausforderung und Ansporn zugleich!

Peter Wimmer, COO

Messen 2012

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

- **RSA Konferenz 2012 in San Francisco**
  atsec beteiligt sich am deutschen Gemeinschaftsstand auf der RSA- Konferenz zur Informationssicherheit.
- **IKOM 2012 in München**

  Auf dem Karriereforum IKOM der Technischen Universität München bietet atsec Absolventen einen Einstieg in die spannende Welt der Sicherheitsberatung.
- **it-sa 2012 in Nürnberg**
  Auf der größten deutschen IT-Sicherheitsmesse wird sich atsec wie im letzten Jahr mit einem eigenen Stand präsentieren.
- **ICCC 2012 in Paris**
  Konferenz für Hersteller, Prüfstellen, Anwender sowie Behörden und Zertifizierungsstellen im Common Criteria Anerkennungsabkommen (CCRA).
- **MILCOM 2012 in Orlando**
  Auf der wichtigsten internationalen Messe für Militärkommunikation ist atsec wieder mit einem Stand vertreten.

Nutzen Sie die Gelegenheit, mit unseren Experten zu sprechen und sich über neueste Entwicklungen in der Informationssicherheit zu informieren.

Smart Meter – sicher ins Stromnetz der Zukunft

Eine neue Entwicklung auf dem Energiemarkt stellen Energie-Zähler, die tatsächliche Verbraucherdaten „intelligent“ per Datenfernübertragung an ein Energieversorgungsunternehmen übermitteln, dar. Sinn und Zweck dieser sogenannten Smart Meter besteht in der variablen Abrechnungsmöglichkeit und einer transparenten und somit effektiveren Ausnutzung der Versorgerinfrastruktur. Vereinzelt sind diese intelligenten Zähler schon in Pilotprojekten im Einsatz. Doch besteht die Gefahr, dass sich Schwachstellen in deren System für Manipulation und Überwachung missbrauchen lassen. Damit diese Smart Meter-Systeme schon vor dem flächendeckenden Einsatz einem einheitlichen Sicherheitsstandard genügen, wurde nun ein Schutzprofil nach Common Criteria für alle Hersteller verbindlich herausgegeben.

Wandel der Energiewirtschaft

Der stetig steigende Anteil regenerativer Energien wie Wind- oder Solarstrom erschwert zunehmend die Steuerung des heutigen Energienetzes. Windkraft und Sonnenenergie sind nicht ständig verfügbar und nur begrenzt speicherbar. Die Einspeisung und der tatsächliche Verbrauch müssen einander aber zu jedem Zeitpunkt entsprechen. Da die Zu- und Abschaltung von Kraftwerken teuer und unökonomisch ist, findet ein Wandel des Energienetzes in ein intelligentes Stromnetz (Smart Grid) statt. Hierfür wird das klassische Stromnetz um ein Kommunikationsnetz erweitert, welches die Steuerung des Energieverbrauchs in Abhängigkeit von der aktuell verfügbaren Strommenge ermöglicht. Der intelligente Stromzähler (Smart Meter) ist die erste sichtbare Komponente des Smart Grids.

Aufbau eines Smart Meter-Systems

Ein Smart Meter-System besteht im Wesentlichen aus zwei Funktionseinheiten. Der erste Teil ist der digitale Stromzähler (Smart Meter) selbst. Die Werte dieser Komponente werden an die eigentlich intelligente Einheit, das Gateway, weitergegeben. Das Smart Meter Gateway übermittelt die Werte anschließend an den jeweiligen Vertragspartner. Dies kann der Verteilnetzbetreiber, der Messstellenbetreiber oder der Stromerzeuger selbst sein.

Schutzbedarf

Verbraucherschutz

Da zwischen den Systemen des Betreibers und dem Smart Meter des Endkunden sensitive Daten übertragen werden, müssen diese gegen ein Auslesen und eine Manipulation durch Dritte sowohl auf dem Gerät, als auch während der Übertragung geschützt werden.

Seit Anfang 2010 müssen in jedem Neubau und total sanierten Gebäude per deutschem Gesetz und ab 2022 in jedem Haushalt nach einer EU-Richtlinie intelligente Strom- und Gaszähler installiert werden. Da der einzelne Verbraucher dabei nicht mehr die Wahl hat, einen herkömmlichen mechanischen Zähler zu verwenden, besteht für intelligente Zähler ein besonderer Schutzbedarf. Dies bewog das Bundesministerium für Wirtschaft und Technologie (BMWi) dazu, das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit einem Schutzprofil zu beauftragen, das für alle Hersteller von intelligenten Zählern verbindlich ist und die Sicherheitsbedürfnisse der Endkunden hinreichend abdeckt.

Schutz des Betreibers

Doch nicht nur die Endkunden benötigen einen Schutz der Messdaten und Smart Meter-Systeme. Auch die Betreiber solcher Anlagen müssen für einen korrekten Abrechnungsbetrieb und eine zuverlässige Stromversorgung Messdaten erhalten, bei denen sowohl die Integrität, als auch die Verfügbarkeit gewährleistet sind.

Der Umstand, dass in diesem Schutzprofil die zu schützenden Parteien zusätzlich voreinander geschützt werden müssen, stellt für die Verfasser des Schutzprofils im Vergleich zur Erstellung anderer Schutzprofile eine Herausforderung dar.

Angriffe auf das Smart Grid

Manipulation der Messwerte

Für das Abhören oder Manipulieren intelligenter Zähler gibt es eine Vielzahl unterschiedlichster Motivationen:

- Verringerung der Stromrechnung durch nach unten korrigierte Verbrauchszahlen
- Gleichzeitige Erhöhung des Stromverbrauchs eines Nachbarn zur Vermeidung von Auffälligkeiten in der Gesamtverbrauchssumme
- Vorgaukeln plötzlicher Verbrauchsspitzen und Provokation eventueller Notabschaltung eines ganzen Stadtteils bei Manipulation einer großen Anzahl Zähler. Denn durch die intelligenten Komponenten eines Smart Grids wird die Menge des einzuspeisenden Stroms automatisch reguliert. Melden tausende Zähler einen zu hohen Wert, besteht die Gefahr, dass einige Komponenten eine Notabschaltung durch Überspannung durchführen. Der volkswirtschaftliche Schaden wäre immens.

All diese Angriffe sind aber nur wahrscheinlich, wenn das Entdeckungsrisiko gering genug ist. Immerhin handelt es sich um Straftaten, für die drastische Strafen drohen.

Durch die Verschlüsselung der Kommunikation zwischen den Sensoren des Smart Meters und dem Gateway sowie zwischen Gateway und Anbieter wird das Abhören von Daten erschwert und damit die Privatsphäre der Verbraucher geschützt. Die Manipulation der Daten wird zudem durch digitale Signaturen, mit denen der Smart Meter oder der Sensor die Daten versieht, zuverlässig verhindert. Solche Signaturen sind rechenintensive Vorgänge und belasten die kleinen Prozessoren der Zähler stark. Es besteht allerdings keine Notwendigkeit, alle übertragenen Daten zu signieren. Manipulationen werden auch dann erschwert, wenn nur hin und wieder ein signierter und damit als „echt“ markierter Datensatz gesendet wird. Die Häufigkeit hängt letztendlich vom vereinbarten Tarif ab.

Unterbrechung der Stromzufuhr

Smart Meter-Systeme besitzen eine sogenannte Unterbrecherfunktion, um säumigen Zahlern ohne großen Aufwand die Stromzufuhr zu unterbinden. Erhalten Unberechtigte nun Zugriff auf diese Funktion, ist es bei gezielt oder willkürlich ausgewählten Haushalten möglich, den Strom abzuschalten. Eine Wiederherstellung eines störungsfreien Betriebs ist somit erst nach einem Update der Smart Meter auf eine Firmware möglich, bei der die ausgenutzte Schwachstelle entfernt wurde. Nicht nur die Entwicklung eines Securitypatches und die Analyse des Fehlers kann sich über Tage hin ausdehnen, auch darf nur zertifizierte Software auf den Smart Meter Gateways installiert sein. Eine Rezertifizierung des Produktes geschieht aber nicht ad hoc, sondern bedarf einer Anpassung der Dokumentationen und eines erhöhten Testaufwandes.

Zu dieser Problemstellung gibt es bisher noch keine Lösung, die ein flexibles und schnelles Beheben der Schwachstelle erlaubt. Hier besteht Handlungsbedarf, da die Schwachstelle nicht nur bei einem Haushalt ausgenutzt wird, sondern eine Vielzahl an Haushalten, öffentlichen Einrichtungen oder Firmen davon betroffen sind. Bei lediglicher Unterbrechung der Stromzufuhr entsteht ein Schaden ausschließlich bei den betroffenen Anschlüssen. Werden allerdings tausende Anschlüsse gleichzeitig und fortwährend aus- und wieder eingeschaltet, reduziert sich zum einen die Lebenserwartung vieler angeschlossener Geräte, zum anderen wird auch die Stabilität des gesamten Stromnetzes stark beeinträchtigt. Eine Abschaltung aller betroffenen Versorgungsbereiche ist unumgänglich. Die wirtschaftlichen Folgen sind auch hier gravierend.

Preisgabe der Leistungsdaten

Im Gegensatz zu bisherigen Messeinrichtungen wird der Verbrauch in Echtzeit an den zuständigen Messstellenbetreiber übermittelt. Anhand dieser Daten erstellen die Energieversorger anschließend ein anonymisiertes Lastprofil für die jeweiligen Versorgungsbereiche. Diese werden benötigt, um die vorhandenen Energieressourcen optimal einzusetzen und Preismodelle zur Reduktion von Lastspitzen zu generieren. In einem vom Bund geförderten Projekt wurde herausgefunden, dass mit diesen übermittelten Daten nicht nur Lastprofile, sondern auch Nutzungsprofile erstellt werden können. So ist es anhand der in Echtzeit übermittelten Daten beispielsweise möglich, das eingeschaltete TV-Programm oder den im Moment laufenden Film zu identifizieren. Ermöglicht wird dies durch die Analyse von Hell-Dunkel-Abschnitten und dem sich dadurch ändernden Stromverbrauch. In der Theorie könnten Stromanbieter so recht genaue Konsumprofile ihrer Kunden erstellen und diese zielgerichtet für Werbung nutzen. Auch wenn dies in der Realität recht unwahrscheinlich ist, zeigt es trotzdem, dass für einen sicheren Einsatz solcher Geräte eine gewisse Sensibilität notwendig ist.

Das Schutzprofil des BSI und geplante technische Richtlinien sind die Basis für ein sicheres Smart Grid. Um allerdings eine datenschutzfreundliche und sichere Nutzung der Smart Meter zu erreichen, bedarf es einer gesetzlichen Regelung für die Erhebung, Verarbeitung und Nutzung der durch die digitalen Zähler erhobenen Verbrauchsinformationen. Denn technisch ist eine Profilbildung möglich und aufgrund der Abrechnungsnotwendigkeit auch nicht zu vermeiden.

Bilderbuch-Evaluierung bei Stonesoft

In Zusammenarbeit mit CSEC, der schwedischen Zertifizierungsbehörde, schloss atsec information security die Evaluierung der StoneGate Firewall/VPN 5.2.5. der Fa. Stonesoft erfolgreich ab. Das Sicherheitszertifikat nach den Vorgaben der Common Criteria wurde auf der Stufe EAL4+ erteilt; dies ist die höchste Vertrauenswürdigkeitsstufe im Rahmen der weltweiten gegenseitigen Anerkennung von Zertifikaten. Mitarbeiter von atsec Deutschland und Schweden waren an der Evaluierung beteiligt, in der das Produkt bis auf die Ebene seines Quellcodes analysiert wurde. Sowohl die Zertifizierungsbehörde als auch die Evaluatoren waren von der Qualität der Entwicklung bei Stonesoft außerordentlich beeindruckt. So gestaltete sich diese Prüfung zu einer Bilderbuchevaluierung, die in kürzester Zeit durchlaufen wurde. Zum Erfolg trug dabei auch die Kompetenz und sehr schnelle Reaktionszeit der schwedischen Zertifizierungsstelle bei. „Die Evaluierung bei Stonesoft zeigt, dass bei einer kompetenten und engagierten Zusammenarbeit aller Beteiligten, also Hersteller, Prüflabor und Zertifizierungsstelle, eine Zertifizierung unter Beachtung aller Kriterien der Common Criteria schnell vonstatten gehen kann“, erklärt Staffan Persson, Prüfstellenleiter atsec Schweden.

atsec prüfte die Kernfunktionalität der Firewall mit Schwerpunkten bei der Netzwerksicherheit und der Hochverfügbarkeit. Die Evaluierung wurde beim Kunden Stonesoft in Helsinki, Finnland, und im Prüflabor von atsec in Stockholm durchgeführt.
In der Fortführung der erfolgreichen Zusammenarbeit von Stonesoft und atsec prüft das US-Labor von atsec jetzt die StoneGate-Kryptomodule nach dem Standard FIPS 140-2, Level 2.

Shoppen mit Virtual Credit Cards

Sie sind in den USA seit fast einem Jahrzehnt im Einsatz, jedoch nur einer Minderheit der „Online-Shopper“ bekannt. Die Rede ist von Kreditkarten, die nur für Zahlungen im Internet oder übers Telefon entwickelt wurden und seit einiger Zeit auch in Deutschland Einzug halten. Da der Benutzer keine Plastikkarte, sondern nur die benötigten Daten, wie Kreditkartennummer, Gültigkeit, Karteninhabername und Sicherheitsprüfnummer vom Kreditkartenunternehmen erhält, spricht man von „virtuellen“ Kreditkarten.
Die Vorteile einer VCC sind mannigfaltig. Zum einen gestaltet sich der Erhalt wesentlich einfacher, denn anders als bei der klassischen Kreditkarte wird keine Bonitätsprüfung vorgenommen. So steht sie auch Kunden ohne regelmäßiges Einkommen offen. Die virtuelle Kreditkarte hat keine Kreditfunktion und kann deshalb mit einer Prepaid-Kreditkarte verglichen werden. Mittels einer Weboberfläche erhält der Kunde Zugriff auf die virtuelle Kreditkarte. Das zugehörige Guthabenkonto wird per Banküberweisung aufgeladen und kann online überwacht werden. Durch die Möglichkeit, sich für jeden Kauf eine neue VCC erstellen zu lassen, also eine Gültigkeit für jeweils nur einen Einsatz festzulegen, wird Betrug verringert. Sobald der Online-Händler die Zahlung abgebucht hat, ist die dafür generierte VCC gesperrt. Auch eine zeitliche Begrenzung der Kartengültigkeit, beispielsweise auf ein Jahr, ist möglich. So sind monatliche Abbuchungen für einen bestimmten Zweck, wie Zeitschriftenabos oder Kursgebühren, für die Laufzeit von 12 Monaten möglich. Anschließende, nicht autorisierte Abbuchungen werden durch den Ablauf der VCC nicht mehr stattfinden.
Ein weiterer, nicht zu vernachlässigender Vorteil einer virtuellen Kreditkarte bietet der Schutz vor Diebstahl und Verlust – von der Reduzierung des Umfangs unserer Geldbeutel, die heutzutage von Plastikkarten überquellen, ganz abgesehen.

Company Meeting atsec information security 2011

Drei neue CC-Evaluatoren bei atsec

Die letzte Chance, sich an einer Schulung des Common Criteria-„Urgesteins“ beim BSI, Herrn Marcel Weinand, zu erfreuen, nutzten drei unserer angehenden Evaluatoren im vergangenen Herbst. Beim Workshop Common Criteria 3.1 mit den Themen „Erstellung von Schutzprofilen und Sicherheitsvorgaben“ und „Einführung in die Evaluierung“ schlossen alle mit Bravour ab. Gratulation an unsere engagierten Mitarbeiter Peter Wimmer, Robert Hoffmann und Reimar Barthel zur bestandenen Evaluatoren-Prüfung! Dem scheidenden Schulungsleiter Marcel Weinand, dessen kompetent, sympatisch und sehr enthusiastisch geführte Kurse Schulungsteilnehmer seit Anbeginn der Common Criteria mitrissen, wünschen wir alles Gute im verdienten Ruhestand.

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.)