atsec the information security provider

NEWS 09/10

10 Jahre atsec!

10 Jahre Ideen, Enthusiasmus, Dynamik, höchste Qualifikation und Effizienz.

Wir danken unseren Kunden, Mitarbeitern und all denjenigen, die uns im Laufe der Jahre unterstützt haben, für die erfolgreiche und zukunftsweisende Zusammenarbeit.

Was vor zehn Jahren als Vision dreier Freunde und Kollegen mit einem kleinen Auftrag zur IT-Sicherheitsberatung in München begann, ist heute ein führender Dienstleister auf dem Gebiet der Informationssicherheit, der seine Kunden international mit Niederlassungen in Deutschland, USA, Schweden und China unterstützt.

Entscheidend für unseren Erfolg war die gemeinsame Leidenschaft für IT-Sicherheit und der Wunsch, neutrale und kundenorientierte Dienstleistungen anzubieten. Und zwar in einem Unternehmen das sich ausschließlich darauf spezialisiert und unabhängig von Produkten und Fremdkapital ist.

Es hat bei atsec in diesen zehn Jahren natürlich einige Veränderungen gegeben, um unser Wachstum als angesehenes internationales Unternehmen im Bereich der Informationssicherheit zu fördern. Aber im Kern sind die Eigenschaften, die uns von Anfang an ausgezeichnet haben, unverändert geblieben: unser Enthusiasmus, unsere Energie, der Teamgeist, der Wunsch nach Unabhängigkeit und unsere gemeinsame Leidenschaft für die IT-Sicherheit. Die Prinzipien, die wir an unserem ersten Tag als atsec information security formuliert haben, sind unverändert gültig und werden uns auch zukünftig begleiten:

- *Wir kennen unser Geschäft,*
- *wir konzentrieren uns auf unsere Kompetenzen,*
- *wir sind unabhängig*
- *und vor allen Dingen handeln wir mit Integrität.*

Es gibt nach wie vor viel zu tun: IT-Sicherheitsstandards sind laufend weiterzuentwickeln, Investitionen in die IT-Sicherheit wollen wir im Interesse unserer Kunden noch kosteneffizienter gestalten, die Ausbildung unserer Mitarbeiter ist uns wichtig und natürlich werden neue Herausforderungen durch moderne Technologien auf uns zukommen. Die Komplexität neuer Anwendungen bedeutet, dass wir uns auf Themen wie Sicherheits-Architektur, Cloud Computing, Virtualisierung und neue Sicherheits-Kriterien für das Risikomanagement und die Risikominimierung konzentrieren werden.

So wie sich die Ansprüche der IT-Welt an funktionierende Sicherheitskonzepte verändern, ist atsec bereit, eine Führungsrolle bei der Entwicklung neuer Dienstleistungen, Werkzeuge und Technologien einzunehmen.....für die nächsten zehn Jahre und darüber hinaus.

Vielen Dank,

Salvatore la Pietra, Staffan Persson, Helmut Kurth

Neues Schutzprofil für Betriebssysteme

Die Sicherheitsprüfung moderner, komplexer und vernetzter Betriebssysteme nach Common Criteria basiert noch immer auf teilweise überholten Konzepten für einzelne, isolierte Systeme. Mit dem *Operating Systems Protection Profile* (OSPP), einem Schutzprofil für Betriebssysteme, nahm atsec nun eine umfassende Erneuerung und Modernisierung der IT-Sicherheitsanforderungen für Server und Workstations vor. atsecs Spezialisten definierten zeitgemäße Anforderungen an sichere Betriebssysteme und wurden dabei von allen namhaften Betriebssystemherstellern, dem Bundesamt für Sicherheit für Informationstechnik (BSI) und deren amerikanischen Partnern (NIAP) unterstützt. OSPP definiert neben einem Satz obligatorischer Anforderungen eine Reihe optionaler Zusatzpakete und passt dadurch auf Laptops und Mainframes gleichermaßen.
Basisfunktionen sind dabei: sichere Anmeldung, Zugriffskontrolle auf alle Daten, Verschlüsselung der Netzkommunikation, Internet-Paketfilter, Audit und Sicherheitsmanagement.
Optionale Sicherheitsfunktionen sind beispielsweise rollenbasiertes Management, zentrales Audit, kryptographische Dienste, zentraler Anmeldeserver, Integritätsprüfung, Zugriffskontrolle mit Sicherheitslabeln, vertrauenswürdiger Boot und Virtualisierung.
Bei der Zertifizierung nach OSPP muss mindestens die Stufe EAL4 der Common Criteria erreicht werden.

Sichere Netzwerk-Zonen

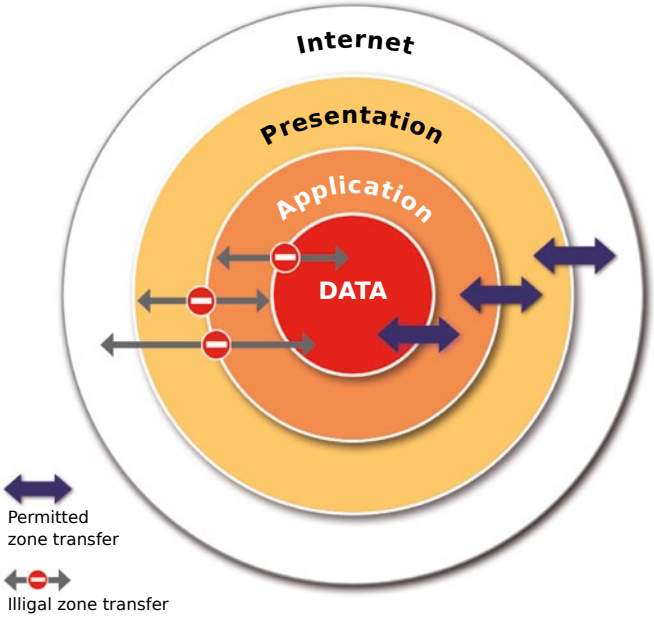
Große Netzwerke, die oft über mehrere Standorte verteilt sind, erfordern ein ganzheitliches Sicherheitskonzept. Ein Netzwerk, das in Zonen unterteilt ist, die sich einander umschließen, bietet ansteigende Sicherheitsstufen für die weiter innen liegenden, sicheren Zonen.

Der Fokus dieses Ansatzes liegt dabei auf der Datensicherheit, das heißt der Vertraulichkeit und der Integrität von Informationen. Daher ist es auch notwendig, Daten zu klassifizieren, zum Beispiel als öffentlich, intern oder vertraulich.

Zonenmodell

Generell werden drei interne Zonen definiert, gelb (außen) für öffentliche Daten, orange (Mitte) für interne und rot (innen) für vertrauliche Daten. Eine externe weiße Zone repräsentiert alle Netzwerke, die nicht von der Organisation kontrolliert werden – dies beinhaltet sowohl das Internet als auch „angeschlossene“ Netzwerke von Outsourcing-Partnern, Zulieferern und Dienstleistern.

Ansteigende Sicherheit wird sowohl durch die schützenden Schichten um sensitive Netzwerke, als auch durch zusätzliche Sicherheitsmaßnahmen gewährleistet. Diese reichen von grundlegenden Schutzmaßnahmen, wie Härtung und Firewalls, zu ausgefeilteren Maßnahmen wie Intrusion Detection und Verschlüsselung übertragener und gespeicherter Daten.



Weitere Sicherheitsmaßnahmen sind Authentifizierung, Protokollierung (zur Nachvollziehbarkeit) und Virenschutz. Ein Reverse-Proxy stellt Authentifizierung für externe Benutzer zur Verfügung; eine Web Application Firewall filtert als schädlich eingestuften Netzverkehr, etwa Sql-Injection-Angriffe. Organisatorische Sicherheitsmaßnahmen beinhalten Benutzerkontenverwaltung, Benutzer-Authentifizierung, aber auch physischen Schutz des Rechenzentrums, etwa durch Umzäunung, bewachte Zugänge und ständige Begleitung von Dritten durch eigene Mitarbeiter.

Das Zonenmodell fordert eine dreistufige Applikations-Architektur: Datenbanken in der inneren Zone, die eigentliche Applikation in der mittleren und Web Server, Reverse-Proxies und ähnliches in der äußeren Zone.

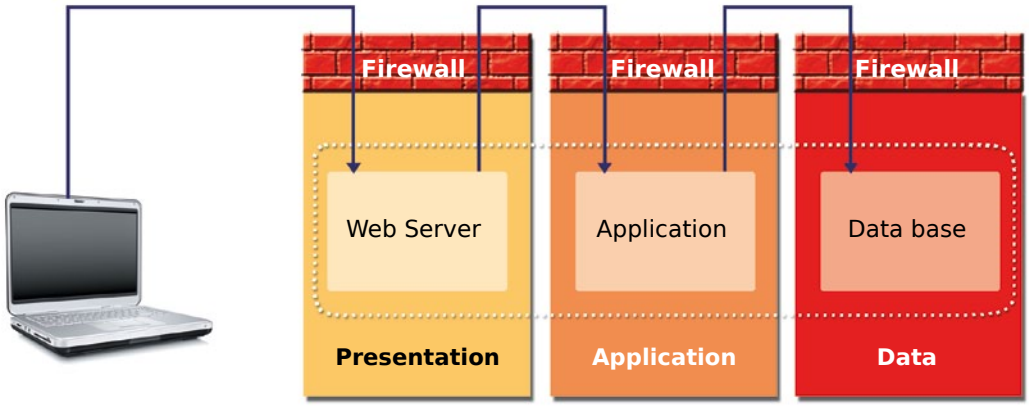
Zonen werden oft in Segmente, d. h. Subnetze, unterteilt, um kritische Applikationen voneinander abzuschotten und etwa DMZ und Endbenutzer zu trennen.

Anforderungen an Verfügbarkeit und Nachvollziehbarkeit werden individuell für jedes Segment definiert, unabhängig von der Vertraulichkeitsstufe. Beispielsweise erfordert ein öffentlicher Web Server sehr hohe Verfügbarkeit, während ein internes System mit vertraulichen Daten nur werktags erreichbar sein muss.

Datenfluss ist nur zwischen direkt aneinander liegenden Zonen gestattet, hierdurch wird eine direkte Verbindung zu sensitiven Daten von unsicher eingestuften Netzwerken verhindert. Diese Einschränkung gilt sowohl von außen nach innen, als auch umgekehrt. Obwohl die inneren Zonen als „sicherer“ (eigentlich: besser geschützt) angesehen werden, würde eine direkte Verbindung von einer Datenbank in der inneren Zone zum Internet einem Trojaner erlauben, vertrauliche Daten ohne weitere Hindernisse nach außen zu übertragen.

Die Erfordernis für Verschlüsselung ist wiederum unabhängig davon, in welcher Zone die Daten gerade verarbeitet oder gespeichert werden, da dies von der Klassifizierung des Datenschutzgesetzes vorgegeben wird.

Obwohl vertrauliche Daten in der innersten („sichersten“) Zone zu speichern sind, wird eine Untermenge dieser Daten immer von einer Applikation in einer Zone „darunter“ verarbeitet werden; diese wiederum reicht einen Teil dieser verarbeiteten Daten an die Präsentationsschicht in der angrenzenden darunter liegenden Zone weiter.



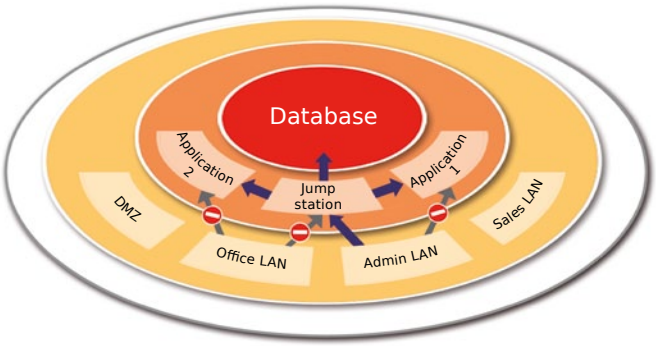
Die Klassifizierung der Information bestimmt, ob diese Daten bei der Übertragung zu verschlüsseln sind – somit werden vertrauliche Informationen verschlüsselt, insbesondere im Internet, aber auch in den sichereren Zonen.

Maßnahmen zur Sicherheit

Zur Absicherung der Zonen werden übliche Best-Practice-Maßnahmen implementiert. Diese umfassen Firewalls, Systemhärtung, Virenschutz und Protokollierung wichtiger Systemereignisse für alle Zonen, zusätzlich Zugriffskontrolle und Angriffserkennung (IDS) für die orange Zone.

Sonderfälle

Systemadministration und Backup-Szenarien sind natürlich auch im Zonenmodell abzubilden.



Systemadministration
Zur Systemadministration wird ein „Jump Host“ in der mittleren Zone platziert, der so Zugriff auf alle drei internen Zonen hat. Administrativer Zugriff auf andere Systeme ist ausschließlich über diesen Jump Host erlaubt, Administratoren müssen sich also erst auf diesem anmelden. Der Jump Host verwaltet SSH-Schlüssel und Zertifikate, die zur Authentifizierung auf anderen Systemen verwendet werden. So ist eine zentralisierte Kontrolle über Zugangsdaten sowie Nachvollziehbarkeit durch Protokollierung gewährleistet.

Backup
Die Vertraulichkeit von Daten ist auch auf Backup-Servern zu schützen, daher werden diese in einer Zone platziert, welche mindestens die gleiche Vertraulichkeitsstufe wie die zu sichernden Daten hat. Zudem ist oft ein separates Backup-Netzwerk sinnvoll, um eine Überlastung des Produktiv-Netzes zu vermeiden. Allerdings dürfen solche Netzwerke nicht die Grenzen zwischen Zonen und Segmenten umgehen.

Migration

Das Zonenmodell wird üblicherweise in bestehenden Rechenzentren mit einer Vielzahl von Alt-Anwendungen und einer flachen Netzstruktur eingeführt. Eine Migration beginnt mit der Pilot-Umstellung einer typischen Applikation als Proof-of-Concept, um sich mit der neuen Architektur vertraut zu machen und mögliche Schwierigkeiten rechtzeitig zu erkennen. Applikationen sind in ihre drei Schichten (Präsentation, Logik, Daten) aufzuspalten und Protokolle gegebenenfalls auf ihre sicheren Äquivalente (z. B. HTTP / HTTPS) umzustellen. Eine gewisse Zahl von Alt-Applikationen wird allerdings nicht migriert werden können.

Sichere Netzwerk-Zonen schützen also sensitive Daten und wichtige Systeme durch ein mehrschichtiges Sicherheitsmodell. Die Auswirkungen von Schadcode und Angriffen werden effektiv eingedämmt, und der einheitliche Ansatz für die sichere Implementierung von Applikationen erhöht die Effizienz in Rechenzentren.

atsec NEWS

FIPS 140 – Geprüfte Kryptographie

Der *Federal Information Processing Standard* (FIPS) 140 definiert ein US-Schema zur Prüfung von Kryptographie-Implementierungen. Die aktuelle Version FIPS 140-2 ist ein international anerkanntes Schema, das weltweit als Standard zur Prüfung von Kryptographie etabliert ist. atsec führt FIPS 140-Prüfungen durch und bietet dazu Beratungen in USA und Europa an. Da atsec aktiv an der neuen Version FIPS 140-3 mitarbeitet, können diese Neuentwicklungen bereits jetzt bei Beratungen und Prüfungen eingebracht werden, um Entwickler auf diese Neuerungen vorzubereiten.

Bei der Prüfung nach FIPS 140 ist die Analyse der kryptographischen Algorithmen, derer sich ein kryptographisches Modul bedient, Voraussetzung. Dies geschieht mittels einer Referenzimplementierung aller erlaubten kryptographischen Algorithmen, die durch das *Cryptographic Algorithm Validation System* (CAVS) bereitgestellt wird und auch die erlaubten kryptographischen Algorithmen in einem geprüften Modul bestimmt. Beispielsweise sind für symmetrische Algorithmen ausschließlich AES und Triple-DES erlaubt. Als Zufallszahlengeneratoren werden nur deterministische Algorithmen zugelassen, also rein auf mathematischen Verfahren basierende Algorithmen. Nicht-deterministische Methoden eignen sich nicht für den Test mit einer Referenzimplementierung.

Die größten Themenkomplexe der Modul-Prüfung (CMVP) nach FIPS 140 umfassen:

- die Modul-Definition mit ihren physikalischen und logischen Grenzen,
- die Schnittstellen des Moduls mit der Einsatzumgebung,
- bei Hardware-Modulen die physische Absicherung des Moduls gegen das Auslesen sensitiver Informationen (zum Beispiel private Schlüssel, Status des Zufallszahlengenerators),
- alle Aspekte der Schlüsselverwaltung und
- die Implementierung der Selbsttests, welche sowohl die Integrität des Moduls zur Startzeit prüfen, als auch die korrekte Funktionsweise der kryptographischen Algorithmen.

Da nur die CAVS-getesteten Algorithmen verwendet werden dürfen, ist nur ein Teil (Subset) der Funktionen oder Algorithmen eines Moduls im Rahmen von FIPS 140 nutzbar. Weiterhin werden gegebenenfalls Einschränkungen für die Konfiguration eines Moduls spezifiziert, damit es FIPS 140-konform ist. Üblicherweise wird ein FIPS-Modus des Moduls definiert, der in der sogenannten Security Policy erläutert wird. Die Security Policy stellt Anwendungs- und Konfigurationshinweise sowie Informationen zur Einsatzumgebung bereit. Weiterhin definiert sie die physischen und logischen Grenzen des Moduls für den Anwender, spezifiziert die erlaubten kryptographischen Algorithmen und definiert genau die getestete Version des Moduls.

Ansprechpartner für weitere Informationen: info@atsec.com

GRC – Governance, Risk & Compliance

Diese drei Schlagwörter beschreiben den mittlerweile wichtigsten Rahmen für unternehmerisches Handeln:
„Governance“ meint die Minimierung von IT-Risiken, sowie die Kontrolle und Transparenz von Geschäftsprozessen. „Risk“ bezieht sich auf die Analyse von Risiken, ihrer Schadenshöhe und Eintrittswahrscheinlichkeit, um kostenbewusst geeignete Gegenmaßnahmen zu ergreifen. „Compliance“ bedeutet Einhaltung verschiedenster Regelwerke bei der Informationsverarbeitung, etwa gesetzlicher Vorschriften.

Vielfältig und durchaus unübersichtlich zeigen sich diese einzuhaltenden Vorgaben – KontraG, BiMoG, SOX bzw. EuroSOX, Datenschutz sind nur einige davon. Die beiden wichtigen Instrumente für GRC sind dabei universell – ein adäquates Risikomanagement und ein Internes Kontroll-System (IKS). Richtig eingesetzt, stellen diese Werkzeuge sicher, dass effektive und sinnvolle Maßnahmen ausgewählt werden. Dabei schlanke und kostengünstige Prozesse zu wählen, sorgt gleichzeitig für effizientere Abläufe und

lässt so das Unternehmen als Ganzes profitieren.
Einen aussagekräftigen Überblick über den aktuellen Stand in Ihrem Unternehmen bietet das „GRC Readiness Assessment“ von atsec. Es dokumentiert Übereinstimmungen und Defizite, beziffert die internen sowie externen Aufwände und zeigt eine Roadmap zur Umsetzung auf.

PCI Compliance für Mainframes

Zusammen mit IBM und anderen Großrechner-Experten hat atsec ein White Paper verfasst, das einen Überblick über die Herausforderungen und Herangehensweisen bei der Anwendung des PCI Data Security Standards auf Großrechnern gibt.
Das Dokument unterstützt Kunden und PCI-QSAs (Qualifizierte Sicherheitsprüfer) im Umgang mit den speziellen Anforderungen der Mainframe-Umgebung.
atsec stützt sich dabei auf die langjährige Erfahrung mit der Evaluierung entsprechender Systeme und Anwendungen, wie beispielsweise z/OS, z/VM, PR/SM, System SSL, DB2.

Das White Paper finden Sie unter: http://www.atsec.com/us/pci-lcs.html

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.)