

NOTITIA

ADNOVUM

BEMERKENSWERTES VON UND ÜBER ADNOVUM

Security: High-End oder keine

End-to-End-Lösungen mit Security Stack entsprechen einem realen Bedürfnis

IT-Sicherheit und was beim Kunden daraus wird

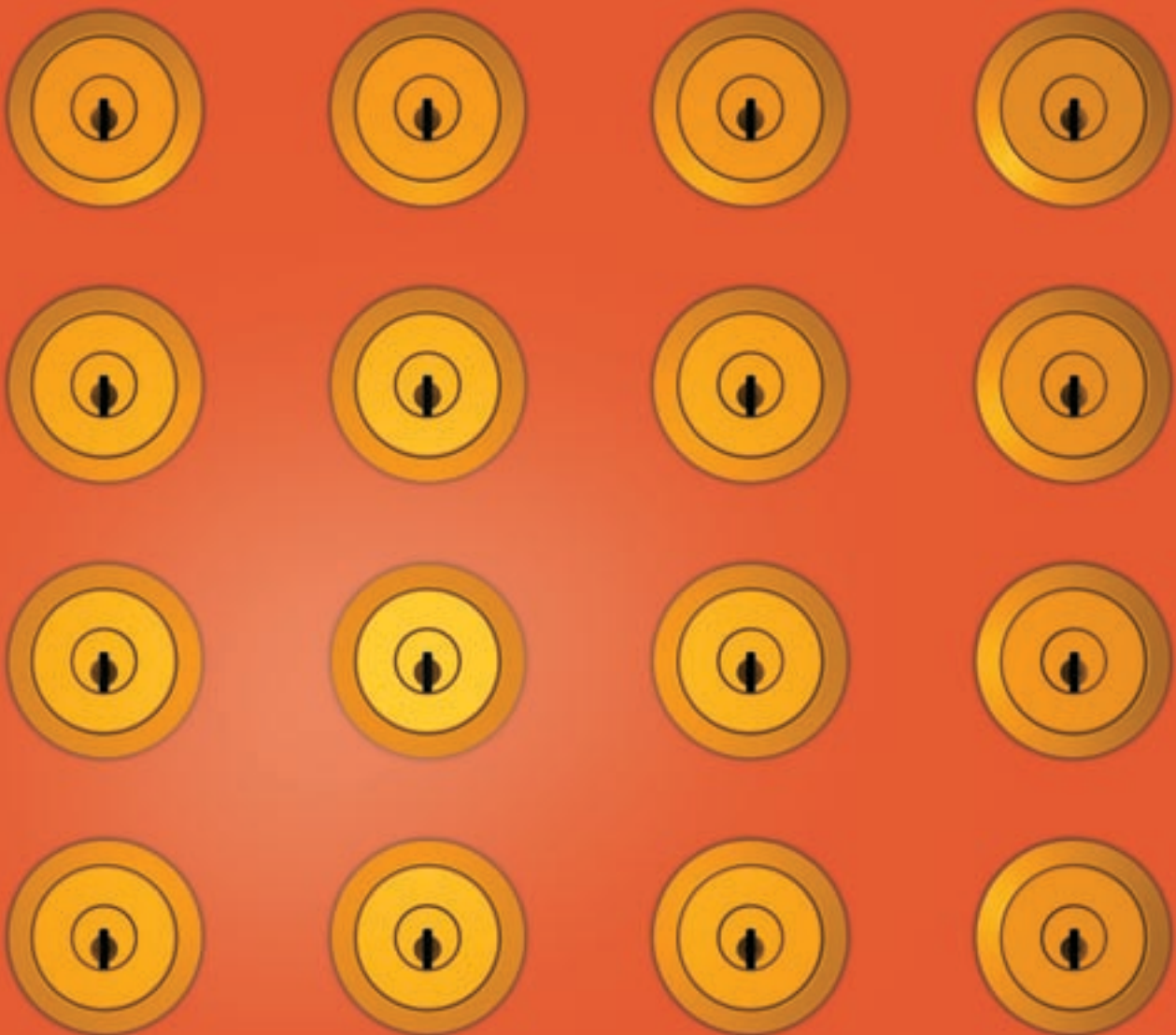
Gute Organisation ist das A und O

Outsourcing Schritt für Schritt

Der Weg zu einer effizienten Aufteilung der Verantwortung

HERBST 2003, NR. 5

SECURITY





Liebe Leserin, lieber Leser

Sicherheit im IT-Bereich umfasst viele Aspekte: Vertraulichkeit, Datenintegrität, Verfügbarkeit, Konsistenz, Kontrolle und Nachprüfbarkeit lauten derzeit die Schlagwörter. Sicherheit war zwar immer schon ein Thema, sie wird heute aber stärker gewichtet, und andere Aspekte stehen im Vordergrund als noch zu Anfangszeiten der IT. Der rasche Fortschritt des Internets löste einen Schub in der IT-Security-Entwicklung aus, denn die von vielen Seiten zugänglichen Daten brauchten

Security: High-End oder keine

HEUTE WERDEN IMMER MEHR GESCHÄFTE UND DIENSTLEISTUNGEN ÜBER ELEKTRONISCHE KANÄLE ANGEBOten. IN DIESE PROZESSE SIND HÄUFIG DATEN INVOLVIERT, DIE VOR MISSBRAUCH UND MANIPULATION DURCH UNBEFUGTE BESONDERS GUT GESCHÜTZT WERDEN MÜSSEN. UM DEN ERHÖHTEN ANFORDERUNGEN GERECHT ZU WERDEN, HAT DIE ADNOVUM DEN SECURITY STACK ENTWICKELT, DER END-TO-END-SICHERHEIT VOM CLIENT BIS ZUM MAINFRAME ERMÖGLICHT.

VON MARCEL VINZENS

Die Menge der Informationen, die in digitaler Form gespeichert und verteilt werden, nimmt stetig zu und umfasst immer mehr auch sehr sensible Daten. Dies gilt nicht nur für den Finanzsektor mit allen Kundensegmenten – Retail, externe Vermögensverwalter und institutionelle Kunden –, sondern in zunehmendem Masse auch für andere Dienstleistungsbereiche (E-Services) und die öffentliche Hand (E-Government), wo der verteilte Zugriff auf sicherheitskritische Daten ebenfalls stark gefördert wird. Der Internet-Boom hat dazu geführt, dass in den letzten Jahren der Schwerpunkt im Bereich Security auf Lösungen lag, die sichere Verbindungen vom Kunden bis in die Demilitarized Zone (DMZ) des Service Providers ermöglichten. Heute ist klar geworden, dass die Systeme nicht nur von aussen, sondern auch von innen gesichert werden müssen, zum Beispiel gegen interne

Man-in-the-Middle-Attacken. Deshalb geht man jetzt einen Schritt weiter und strebt hochsichere End-to-End-Security-Lösungen an, die eine Trust Chain vom Client bis zum Endziel, also etwa zum Mainframe,

DA DIE SYSTEME AUCH VON INNEN GESICHERT WERDEN MÜSSEN, STREBT MAN HEUTE END-TO-END-SICHERHEITSLÖSUNGEN AN, DIE EINE TRUST CHAIN VOM CLIENT BIS ZUM MAINFRAME ETABLIEREN.

etablieren. Die geheimen Schlüssel, auf denen die Sicherheit beruht, werden in Security-Modulen möglichst gut geschützt. Daneben ermöglichen diese Lösungen betriebliche Vereinfachungen und damit verbunden Kostenreduktionen, etwa mittels automatischer Zertifikatsmanagementsysteme.

Die AdNovum arbeitet aktiv an der Realisierung solcher auf offenen Standards basierenden, integralen High-End-Security-Lösungen und hat hierfür zusätzlich zum Secure Reverse Proxy, der einen sicheren Zugriff auf das Intranet erlaubt, und zum generischen Authentisierungsservice einen Security Stack entwickelt.

High-End Security mit Security Stack

Um die Sicherheit auf und zwischen Knoten-Servern zu maximieren, wurde das Konzept eines Security Stack eingeführt, der unter der Middleware oder auch direkt unter Applikationen platziert wird. Der Security Stack besteht aus voneinander unabhängigen Komponenten, die je nach Anforderung zusammengesetzt werden können.

Dies funktioniert, da die einzelnen Komponenten auf offenen Standards basieren (GSSv2, PKCS#11, SSL, X.509 und anderen).

So greifen etwa GSS-fähige Applikationen wie auch SAP auf den gesamten Security Stack zu, Web-Server wie Apache typischerweise aber nur auf den PKCS#11-Teil. Der Einsatz von Hardware- oder Software-Sicherheits-Modulen (HSM oder SSM) oder beidem, wie er in der nebenstehenden Grafik im Security Module

einen besseren Schutz. In einer ersten Phase konzentrierte man sich vor allem darauf, den Zugang zum Intranet abzusichern, während andere Bereiche weniger Beachtung fanden. Heute muss eine IT-Architektur hingegen End-to-End-Sicherheit bieten, die alle Aspekte berücksichtigt.

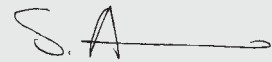
Diese neue Generation von Sicherheit bedeutet aber keine Revolution in diesem IT-Bereich, sondern ist das Resultat einer Entwicklung, die sich über die letzten Jahre

vollzogen hat. Die eingesetzten Sicherheitsmechanismen sind nicht völlig anders, es sind bewährte Konzepte auf einem höheren technischen Niveau. Neu ist, dass nicht mehr jeder Knoten für sich geschützt wird, sondern Sicherheit integriert ist, so dass vom Mainframe via Proxy bis zum Endbenutzer eine ununterbrochene, einheitliche Sicherheitskette entsteht. Dabei hat man sich weiter vom Konzept der «security by obscurity» weg bewegt und hin zur Offenlegung und damit

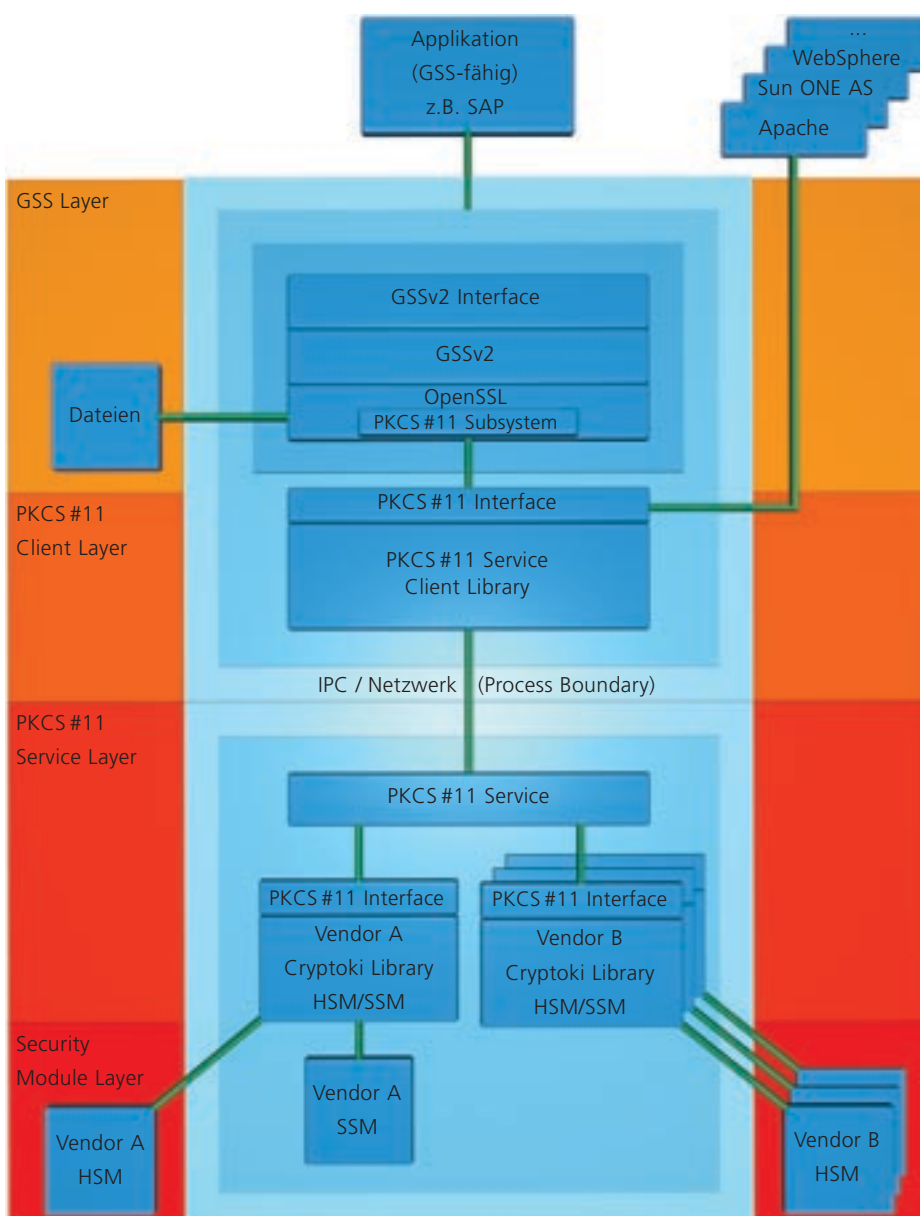
Beweisbarkeit der Sicherheitsmechanismen.

In dieser Ausgabe der Notitia versuchen wir aufzuzeigen, wie diese neue State-of-the-Art Security aussehen kann und dass es durchaus möglich ist, bezahlbare Lösungen zu finden, die höchsten Ansprüchen genügen.

Stefan Arn



CEO AdNovum Informatik AG



Die einzelnen Komponenten des Security Stack.

Layer dargestellt wird, ist ebenfalls frei wählbar. Dank der abgestimmten Architektur wird eine hohe Durchgängigkeit zwischen den grundsätzlich voneinander unabhängigen Modulen erreicht. So können die eingesetzten Komponenten etwa den zu verwendenden Log Channel für ein durchgängiges Logging von oben nach unten propagieren (von GSSv2 über OpenSSL und PKCS #11 bis zur Client Library). Alle Komponenten schreiben so ins gleiche Logfile und verwenden propagierte Log Levels.

Die Verwendung von Standards vereinfacht die Entwicklung neuer Applikationen und Tools und erlaubt es, auf diesen Standards basierende Applikationen und Tools zu integrieren. Dies gilt insbesondere für die Sicherheitsstandards, da diese einen gewissen Reifegrad erreicht haben und somit genügend Aussagekraft für die Praxis haben.

Im Folgenden soll kurz die Bedeutung der einzelnen Komponenten des Security Stack aufgezeigt werden.

GSSv2 und SSL für den Aufbau des Security-Kontexts

Das Generic Security Service Application Program Interface (GSS-API) ist ein standardisiertes API, das Security Services auf eine generische Art zur Verfügung stellt. GSS ist unabhängig von darunter liegenden Technologien. Die Implementierung von GSSv2, die im Security Stack verwendet wird, basiert auf Public-Key-Kryptografie und verwendet eine Erweiterung von SSL (Secure Sockets Layer) als Authentisierungsprotokoll, um einen Security-Kontext zwischen zwei Peers

zu etablieren. Die Erweiterung von SSL ist vollständig kompatibel mit dem Standard-SSL. Somit kann auch ein Security-Kontext mit einem reinen SSL Peer etabliert werden.

Ein grosser Vorteil des GSSv2-API ist, dass es standardisiert und einfacher zu verwenden ist als beispielsweise das nicht standardisierte OpenSSL API selbst. Die Implementierung im Security Stack bietet zusätzlich flexible Log-Mechanismen.

OpenSSL wird verwendet, weil es im Bereich Web Security bereits grossflächig im Einsatz ist, gut auf Probleme hin geprüft wurde und SSL selbst eine breite Akzeptanz als sicheres, reifes Protokoll hat. Der Einsatz von X.509v3-Zertifikaten für die Credentials erlaubt es, für deren Verwaltung bestehende Public-Key-Infrastrukturen (PKI) zu verwenden. Diese sind heute State-of-the-Art.

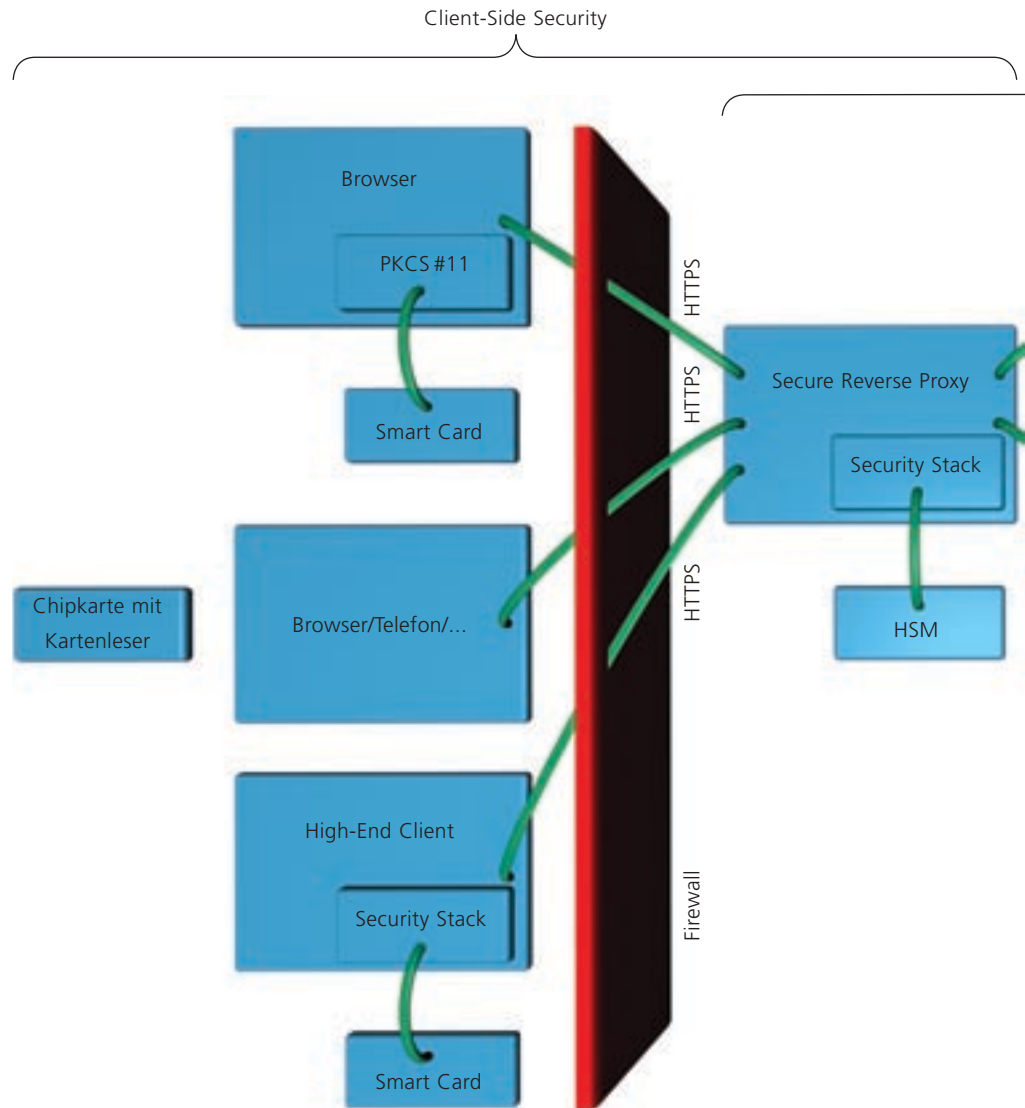
PKCS #11 Service und PKCS #11 Service Client Library

Der Cryptographic Token Interface Standard PKCS #11 spezifiziert ein API für den Zugriff auf Sicherheits-Module. Der PKCS #11 Service bietet einen «single access point» für SSMs und HSMs auf einer Maschine. Insbesondere löst er die bekannten Login- und Reinitialisierungs-Probleme, die im Umfeld von PKCS #11-Applikationen immer wieder auftreten. So bietet er beispielsweise Provider-unabhängige PINs oder automatisches Login an. Zudem erlaubt der Service, logische Sichten auf die internen Security-Module zu erstellen und selektiv bestimmten Applikationen zuzuweisen, zum Beispiel zu Migrationszwecken oder für Legacy-Applikationen, die die Slot-Identifikation oder Objekt-Labels fix verdrahtet haben. Ausserdem generiert der PKCS #11 Service automatisch ein Logfile für jede Applikation, welche die Client Library lädt, was die Problemanalyse vereinfacht.

DER MODULARE CHARAKTER DES SECURITY STACK MACHT ES MÖGLICH, DIE KOMPONENTEN JE NACH ANFORDERUNG EINZUSETZEN.

Sicherheits-Module

Security-Module enthalten sicherheitsrelevante Informationen und können kryptografische Operationen durchführen. Sie sind der sichere Aufbewahrungsort für die privaten Schlüssel, auf denen die PKI-Sicherheit beruht. Gelingt es, den Schlüssel eines Knotens zu kopieren, kann auch dessen Identität



Integrale Sicherheitslösung mit bestehenden Komponenten und Security Stack.

übernommen werden. Um dies zu verhindern, werden die Keys direkt auf dem Security-Modul generiert, das der private Schlüssel nie verlässt. Alle kryptografischen Operationen, die den privaten Schlüssel benötigen, werden auf dem Security-Modul ausgeführt.

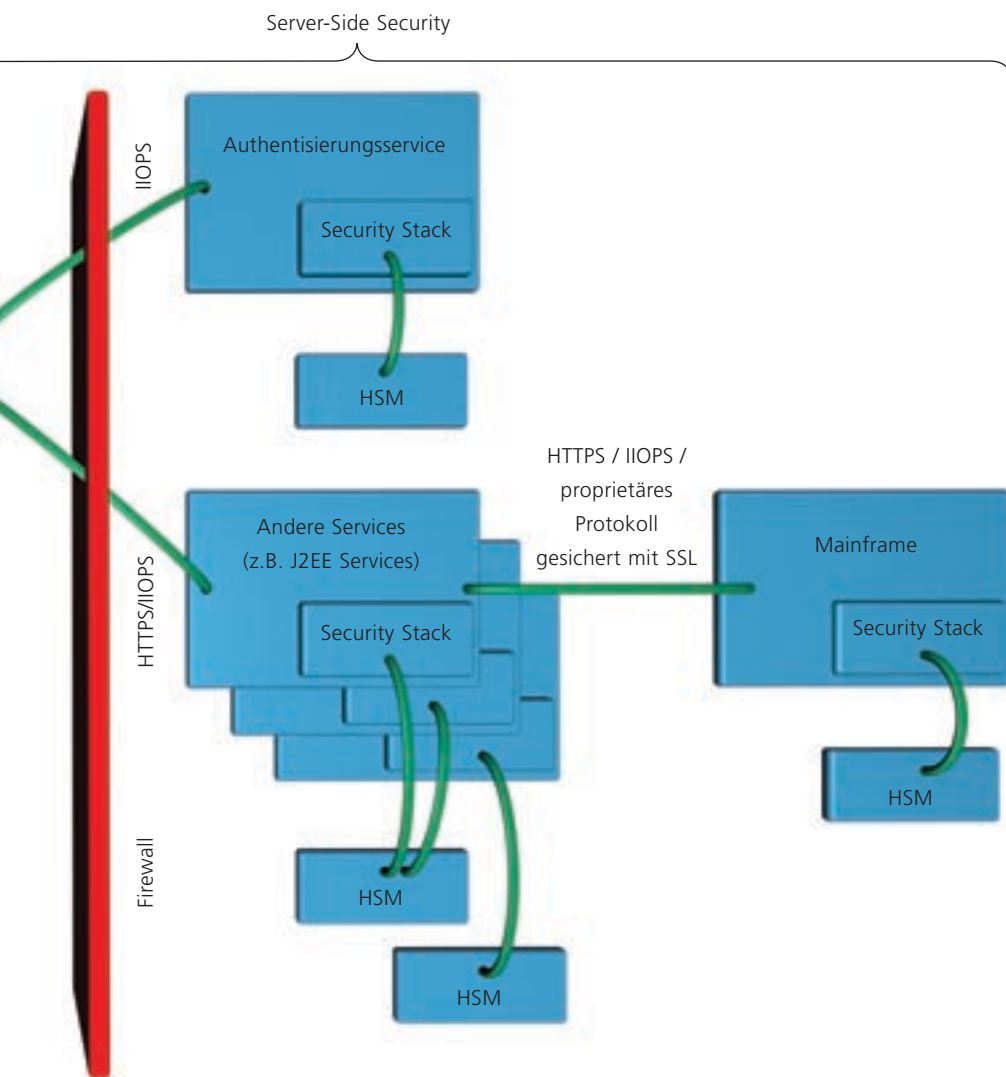
saubere Backup-Lösungen und sind normalerweise Security-zertifiziert.

Software Security Modules (SSM) sind eine Alternative zu HSMs. Sie sind billiger und bieten ein einfacheres Deployment, da es sich um Software und nicht um Hardware handelt, bieten aber keinen physischen Zugriffsschutz und auch keine Crypto-Beschleunigung.

Integrale End-to-End Security

Die Grafik oben zeigt, wie integrale End-to-End-Sicherheit mittels bestehender Komponenten und Security Stack erreicht werden kann. Links wird dargestellt, wie auf der Klienten-Seite die Identität verifiziert wird. Zu diesem Zweck werden zurzeit hauptsächlich die im Folgenden beschriebenen Verfahren eingesetzt.

Persönliche Authentifikationskarte (Smart Card): Der Benutzer hat eine persönliche Authentifikationskarte an seinen Rechner



angeschlossen. Der Browser greift über PKCS #11 direkt auf diese zu und etabliert mit den darauf gespeicherten Credentials (Private Key und X.509-Zertifikat) einen Security-Kontext mit dem Secure Reverse Proxy des Service Providers.

Challenge-Response-Authentisierung mit Chipkarte: Der Benutzer arbeitet mit einem Browser oder seinem Telefon, einer speziellen Chipkarte seines Service Providers und dem dazugehörigen Kartenlesegerät. Über ein Challenge-Response-Verfahren etabliert der Benutzer einen Security-Kontext mit dem Secure Reverse Proxy des Providers.

In Zukunft wird auch die Variante Security Stack und Smart Card möglich sein: Die Smart Card wird an den Rechner des Benutzers angeschlossen, und eine High-End-Applikation mit integriertem Security Stack greift über den PKCS #11 Service auf diese zu, um mit den darauf gespeicherten Credentials (Private Key

und X.509-Zertifikat) einen Security-Kontext mit dem Secure Reverse Proxy des Service Providers zu etablieren.

DIE FLEXIBLE ARCHITEKTUR VEREINFACHT DIE MIGRATION BESTEHENDER LÖSUNGEN UND DIE AUSBREITUNG AUF VERSCHIEDENE PLATTFORMEN.

Die rechte Seite der Grafik zeigt, wie der Security Stack in die bestehende Infrastruktur eingebunden wird. Grundsätzlich gibt es pro Maschine genau einen PKCS #11 Service mit mehreren Instanzen der GSSv2 Library und der PKCS #11 Service Client Library für verschiedene Applikationen und Services. Bereits der Reverse Proxy hat einen Security Stack mit HSM oder SSM oder beidem, und selbst auf dem Mainframe kann ein Security Stack mit HSM/SSM verfügbar sein.

Ein wichtiges, in der Grafik nicht eingezeichnetes Element sind signierte Tokens (SecTokens), die die Benutzeridentität an den Request binden. Bei jeder HTTPS-Anfrage überprüft der Secure Reverse Proxy, ob ein SecToken vorliegt. Ist keines vorhanden, wird der Authentisierungsservice aufgerufen, ansonsten wird das SecToken mit dem Request weitergegeben. Indem jeder beteiligte Knoten das SecToken überprüft, erreicht man nicht nur sichere Verbindungen zwischen benachbarten Knoten, sondern vom Benutzer bis zum Mainframe (End-to-End Security).

Migration und Plattformen

Wichtige Aspekte, die man schon vor der Realisierung einer High-End-Security-Lösung berücksichtigen muss, sind Migrationsszenarien von bestehenden Lösungen sowie die Ausbreitung der neuen Lösung auf verschiedene Plattformen. Deshalb wurde der Security Stack darauf ausgelegt, dass er einfach portierbar ist. So wird ein eigenes Runtime Environment verwendet, das die plattform-spezifischen Eigenheiten kapselt, was den Aufwand für eine Portierung reduziert. Der Security Stack ist auf z/OS, AS/400, DEC OpenVMS sowie den gängigen Unix-Derivaten (Linux, AIX, HP-Unix usw.) verfügbar.

Dank der flexiblen Architektur ist es möglich, bei «schwierigen» Plattformen, die sich stark von den Referenzplattformen Solaris und Windows unterscheiden, nur gewisse Teile des Security Stack zu portieren und die übrigen Komponenten auf einem Crypto-Server auf einer anderen Plattform laufen zu lassen (zum Beispiel Solaris). So kann der Schnitt zwischen dem PKCS #11 Client Layer und dem PKCS #11 Service Layer erfolgen. In diesem Fall laufen

nur die Applikation, der GSS Layer und die PKCS #11 Service Client Library auf der Zielplattform, der PKCS #11 Service und die SSM beziehungsweise die Cryptoki Library für die HSM aber auf einer anderen Plattform.

Die Verwendung offener Standards macht es möglich, bestehende Komponenten für die Migrationsphase oder auch dauerhaft in die Lösung einzubetten. Besteht beispielsweise bereits eine GSS-Implementierung, die einen anderen Mechanismus als den im Security

Stack implementierten verwendet, kann ein GSS-Zwischenlayer realisiert werden, der je nach Peer zwischen der Verwendung der alten Implementierung über GSS und der neuen Security-Stack-Lösung hin- und herwechselt.

Wie bleibt High-End Security bezahlbar?

Für kleinere Unternehmen stellt sich schnell einmal die Frage, ob solche High-End-Security-Lösungen überhaupt bezahlbar sind. Selbstverständlich ist Sicherheit, die den heutigen Ansprüchen gerecht wird, nicht gratis, die Investitionen lassen sich aber durch den gezielten Einsatz von Komponenten, die auf Standards basieren, in einem kontrollierbaren Rahmen halten. So kann etwa für die Verwaltung der Zertifikate auf ein Standard-Zertifikatsmanagement zurückgegriffen werden.

In der Praxis hat sich herausgestellt, dass kleinere Unternehmen oft weniger Funktionalität benötigen und gewisse Security-Aspekte für sie weniger relevant sind, was eine günstigere und trotzdem noch sichere Lösung erlaubt. So sind allenfalls Einsparungen im Client-Bereich möglich, indem eine auf Challenge-Response-Verfahren basierende Chipkarten-Lösung implementiert wird, die einfacher und schneller zu realisieren ist als eine Lösung mit persönlicher Authentifikationskarte. Diese Variante der Client-Identifikation bietet allerdings auch weniger Funktionalität, etwa keine direkte Signierungsmöglichkeit, wie sie unter anderem für Mails verwendet wird.

Nicht zuletzt profitieren wir heute auch von der im Lauf der Zeit dazugewonnenen Erfahrung. Zusammen mit der Modularität der einzelnen Komponenten erlaubt uns dieses Wissen, Lösungen im Bereich der High-End Security günstiger zu realisieren. ■

Marcel Vinzens

Marcel Vinzens ist diplomierter Informatik-Ingenieur ETH und befasst sich in der AdNovum in erster Linie mit High-End-Sicherheitsaspekten. Als technischer Projektleiter war er massgeblich am Design und an der Entwicklung des Security Stack beteiligt.



IT-Sicherheit und was beim Kunden daraus wird

Ruedi Wipf sprach mit der Notitia darüber, was es alles braucht, damit High-Tech Security auch wirklich für Sicherheit sorgt.

INTERVIEW: BARBARA STAMMLER UND DORINA MAYRHOFER

NOTITIA: Warum reicht es nicht, sich in Sachen Sicherheit auf die Technik zu verlassen?

Ruedi Wipf: Unternehmen mit hohen Sicherheitsansprüchen geben Millionenbeträge für IT-Sicherheit aus. Ausgeklügelte Authentisierungs- und Verschlüsselungsverfahren werden implementiert. Spezielle Hardware wird angeschafft, die sich bei manipulativen Eingriffen selbst zerstört. Wird in einer Software-Komponente wie SSL ein Sicherheitsloch gefunden, reagieren Software-Lieferanten in Windeseile mit einer Patch-Lieferung.

Trotzdem kommt es täglich zu kleinen und grösseren Informationslecks und Sicherheitspannen. Diese verlaufen teilweise glimpflich, können aber unter Umständen ein Unternehmen – zum Beispiel im Falle eines Finanzdienstleisters – existenziell gefährden.

Wie ist dies möglich?

Ich sehe hauptsächlich zwei Gründe dafür, dass beim Einsatz von vernetzten IT-Systemen immer ein Restrisiko bleibt und Sicherheitsmanagement somit zum Risikomanagement wird:

1. Die technischen Aspekte der Sicherheit sind allgemein bekannt. Die Herausforderungen liegen vor allem im Bereich der Organisation.

« SICHERHEITSPANNEN KÖNNEN EIN UNTERNEHMEN UNTER UMSTÄNDEN EXISTENZIELL GEFÄHRDEN. »

2. Der Mensch ist das schwächste Glied in der Sicherheitskette. Seine natürliche Bereitschaft, anderen Leuten Glauben zu schenken und zu vertrauen, macht ihn angreifbar.

Ist IT-Sicherheit also technisch gesehen trivial?

Komplizierte Aspekte wie kryptografische Algorithmen sind zum heutigen Zeitpunkt

eine «commodity». Sie sind allgemein bekannt und in kommerziellen Produkten oder Open Source Software implementiert. Alle relevanten Komponenten müssen aber gezielt ausgewählt und geschickt kombiniert werden. Die Realisierung einer integrierten, durchgehenden Gesamtlösung ist nach wie vor anspruchsvoll.

« DIE HÄUFIGSTEN SICHERHEITSLÜCKEN IN UNTERNEHMEN ENTSTEHEN DURCH UNGENÜGENDE FESTGELEGTE UND UMGESETZTE SICHERHEITSRICHTLINIEN. »

Inwiefern ist die Organisation entscheidend?

Die häufigsten Sicherheitslücken in Firmen entstehen durch ungenügend festgelegte oder umgesetzte Sicherheitsrichtlinien. Fehlerhaft definierte Abläufe und ein sorgloser Umgang mit sensiblen Daten machen jede High-End Security wertlos.

Für eine Challenge-Response-Authentisierung etwa braucht der Benutzer ein spezielles Gerät und einen PIN-Code. Damit diese beiden Teile sicher zum Kunden gelangen, dürfen sie nicht im gleichen Paket verschickt werden, da dieses einer unbefugten Person in die Hände

fallen könnte. Ausserdem sollten sie nicht am gleichen Tag und auch nicht mit dem Firmen-Logo versehen verschickt werden. Für einen potenziellen Übeltäter in einer kleinen Poststelle wäre es sonst ein Leichtes, das Paket mit dem Gerät und den Umschlag mit der PIN an sich zu nehmen und so Zugriff auf das System zu erhalten.

Aber eine Firma kann die Abläufe in einem anderen Unternehmen doch gar nicht kontrollieren?

Allgemein ist bei Prozessen Vorsicht geboten, in die mehrere Firmen involviert sind. Lässt eine Bank Chipkarten für ihre Kunden extern personalisieren, darf der Chipkartenproduzent die Kundendaten nie sehen, denn sie unterstehen dem Bankgeheimnis und enthalten die geheimen initialen Passwörter. Der Hersteller muss aber die Kundendaten auf die Karte schreiben. Paradox? Nein. Mit der richtigen Verschlüsselungstechnik und den richtig umgesetzten Sicherheitsprozessen kann dieses Problem gelöst werden.

Damit sind die Probleme für die Bank aber noch nicht gelöst. Was geschieht, wenn eine Karte verloren geht?

Bereits bei einem kurzfristigen Kontrollverlust muss die Karte als kompromittiert betrachtet werden. Der betroffene Kunde muss die Karte dann so schnell wie möglich sperren lassen

können. Der Prozess zur Sperrung einer Karte muss daher im Idealfall rund um die Uhr zur Verfügung stehen.

Vereinfachen denn neue Technologien die Organisation?

Nicht unbedingt. Für elektronische Zertifikate, die beispielsweise zur E-Mail-Verschlüsselung verwendet werden, gilt Ähnliches wie für die oben erwähnten Chipkarten. Geht ein Schlüssel verloren, wird das Zertifikat zurückgenommen – das liegt auf der Hand. Auch im Falle, dass ein Mitarbeiter die Firma verlässt, muss sein Zertifikat sofort als ungültig betrachtet werden. Der Registrierungs- und Revokationsprozess muss deshalb in Unternehmen, die mit Zertifikaten arbeiten, in das alltägliche Personalmanagement integriert werden. Ich bezweifle allerdings, dass dies auch überall gemacht wird.

Damit archivierte, verschlüsselte E-Mails aber auch nach zehn Jahren noch gelesen werden können, müssen die privaten Schlüssel zur Entschlüsselung zu diesem Zeitpunkt immer noch verfügbar sein. Auch das ist kein technisches, sondern ein rein organisatorisches Problem.



Sie haben zuvor den Menschen als zweiten Risikofaktor erwähnt. Was meinen Sie damit?

Damit spreche ich das so genannte Social Engineering an. Wenn ich den Helpdesk meiner Bank anrufen kann und mir mündlich ein neues E-Banking-Passwort mitgeteilt wird, dann kann das jeder andere auch und damit auf mein Konto zugreifen.

Die psychologischen Aspekte sind beim Social Engineering zentral. Wenn ein Angreifer am Telefon nur genügend freundlich oder autoritär auftritt, kann er geheime Informationen erhalten. Viele Unternehmen machen den Fehler, nur auf der physischen, nicht aber auf der psychologischen Seite vorzubeugen.

« **VIELE UNTERNEHMEN MACHEN DEN FEHLER, NUR AUF DER PHYSISCHEN, NICHT ABER AUF DER PSYCHOLOGISCHEN SEITE VORZUBEUGEN.** »

Unsere Kunden müssen also als Erstes verstehen, dass all das Geld für Security Hardware, Software Patches und Penetration Tests umsonst ausgegeben wird, wenn nicht gleichzeitig adäquate Massnahmen gegen Social Engineering getroffen werden.

Steigt die Sicherheit also mit einer umfassenden Regelung aller Geschäftsfälle?

Klar müssen die Abläufe und Richtlinien lückenlos definiert werden. Wichtig sind aber vor allem auch die Auswahl und Schulung des Personals. Nur wenn die Richtlinien wirklich allen Beteiligten geläufig sind und ihr Sinn plausibel ist, werden sie auch befolgt. Einer der Vorteile von Richtlinien ist, dass sie dem Mitarbeiter die Verantwortung für gewisse Entscheide abnehmen. Wenn eine Richtlinie besagt, dass ein Passwort ausnahmslos nie herausgegeben werden darf, muss sich der Operator nie überlegen, ob er es nun weitergeben soll oder nicht.

Wie weit soll eine Firma bei der Festlegung der Richtlinien gehen?

Sicherheitsrichtlinien umfassen typischerweise offensichtliche Punkte wie: Wie wird ein gesperrtes Benutzerkonto wieder freigegeben, wie findet eine Passwortänderung statt,

welche Eigenschaften müssen Passwörter aufweisen? Vorsicht ist aber auch in ganz anderen Bereichen geboten, die in der Praxis oft vergessen werden. Wie werden beispielsweise Logfiles behandelt? Ein Finanzinstitut, für das wir tätig sind, durchsucht Logfiles nach sensiblen Kundendaten und entfernt diese, bevor es die Dateien zur Analyse freigibt. Das mag paranoid erscheinen, wenn ein

Ruedi Wipf

Ruedi Wipf, dipl. Inf. Ing. ETH, COO AdNovum, arbeitet seit 1998 in der AdNovum. Als Projektleiter war er für die Realisierung einer sicheren Online-Banken-Lösung für Wegelin & Co. Privatbankiers verantwortlich. Nebenbei organisiert er in einer Off-Galerie Ausstellungen für Nachwuchskünstler und steht an seinen Sommer-Partys mit bis zu 500 Gästen auch gerne mal selbst hinter der Bar.

Unternehmen aber davon ausgeht, dass ein Informationsleck im schlimmsten Fall seine Existenz gefährdet, kann es nur so handeln.

Sicherheit, und speziell IT-Sicherheit, kostet sehr viel. Lohnt sie sich für den Kunden?

Es ist richtig, dass Sicherheit viel kostet, aber nicht unmittelbar belohnt wird. Viele Firmen leben deshalb nach der Devise, dass ein wenig Sicherheit besser ist als gar keine, und implementieren keine durchgängigen Sicherheitskonzepte, die von Endpunkt zu Endpunkt, also vom Mainframe bis zum Endbenutzer, reichen. Auf ein Haus übertragen wäre das, wie wenn ich meine Türe mit Metallplatten verstärken, gleichzeitig aber den Hausschlüssel öffentlich herumliegen liesse. Das ist ein weiterer zentraler Punkt, den wir unseren Kunden zu vermitteln versuchen: Nur eine durchdachte, umfassende Sicherheitslösung ist ihr Geld wert.

Sie streben also 100%ige Sicherheit an?

Theoretisch gesehen sind Kompromisse im Gebiet Security fehl am Platz. In der Praxis zeichnen sich erfolgreiche Sicherheitsprojekte jedoch durch eine optimale Gewichtung von Technologie und Organisation aus. Die letzten Promille an Sicherheit sind praktisch unendlich teuer. Auch Grossbanken kommen nicht umhin, nach der Balance zwischen Kosten und Nutzen zu suchen.

Für unsere Kunden stellt sich die Frage, wie wertvoll die Daten sind, die beispielsweise per Internet zugänglich gemacht werden sollen. Oder anders ausgedrückt, wie gross der Schaden wäre, wenn die Daten entwendet, modifiziert oder gelöscht würden. Für viele

Unternehmen wäre ein solcher Schadensfall existenzbedrohend. Man entscheidet sich also entweder dafür, die Daten via Internet zugänglich zu machen, und implementiert die höchstmögliche Sicherheit, oder man schliesst eine Internetlösung aus.

Wie kann eine solche Balance in der Realität aussehen?

Ein Beispiel: Wir implementieren in Zusammenarbeit mit einem Kunden eine starke Authentisierung mit Zertifikaten. Es stellt sich die Frage, ob Software- oder Hardware-Zertifikate eingesetzt werden sollen. Natürlich sind Zertifikate auf einer Smart Card oder

oben erwähnte Gleichgewicht zu finden und das Resultat professionell zu implementieren. Die AdNovum als Sicherheitsspezialistin kann dem Kunden helfen, erstens technisch die richtige Lösung zu finden und zweitens organisatorisch die richtigen Massnahmen zu ergreifen.

Wie gehen Sie dabei vor?

Wir schlagen unseren Kunden zu Beginn eines neuen Projekts den Beizug einer Drittfirma vor, die als unabhängige Sicherheitsspezialistin ein Audit der Software und der vorgesehenen Sicherheitsmassnahmen durchführt. Die Spezialisten dieser Drittfirma haben die

« ERFOLGREICHE PROJEKTE IM SICHERHEITSBEREICH WEISEN EINE OPTIMALE GEWICHTUNG VON TECHNOLOGIE UND ORGANISATION AUF. »

einem anderen Hardware Token sicherer als Soft-Zertifikate. Die Nachteile sind aber deutlich: Erstens verursacht das zusätzliche Gerät höhere Kosten, zweitens nimmt die Benutzerfreundlichkeit entscheidend ab und drittens wird die Organisation rund um die Zertifikate viel komplizierter. Für eine Internetbank überwiegt wahrscheinlich der Sicherheitsaspekt, für einen Online-Konsumgüter-Shop dürfte die Usability im Vordergrund stehen.

Was kann die AdNovum zu einer optimalen Sicherheitslösung beitragen?

Die Datensicherheit als Ganzes kann nicht an Externe delegiert werden. Wir sind aber ein optimaler Partner, wenn es darum geht, das

Aufgabe, nach potenziellen Schwachstellen in den vorgeschlagenen Prozessen zu suchen. Das macht uns das Leben nicht leichter, erhöht aber die Qualität und Zuverlässigkeit der Lösung.

Die AdNovum ist eine Technologie-Firma und kann deshalb in erster Linie in technischen Bereichen in Zusammenarbeit mit den Kunden die richtigen Sicherheitslösungen finden. Das ist aber noch lange nicht alles. Wir versuchen, bei den Unternehmen, mit denen wir Projekte realisieren, das Sicherheitsbewusstsein auf sämtlichen Stufen zu fördern. Nur wenn alle Beteiligten am gleichen Strang ziehen, kann letztlich eine sichere, erfolgreiche Applikation entstehen. ■





Von links nach rechts: Daniel Bates, Manuel Kauf, Lars Sörensen, Andrea Induni, Chris Tanner und Markus Grimm.

Outsourcing Schritt für Schritt

BEI DEN IT-DIENSTLEISTUNGEN IST ZURZEIT EIN TREND ZUM OUTSOURCING FESTSTELLBAR. GROSSE UND MITTLERE BETRIEBE VERSUCHEN SO, IHRE EXPLOSIONS-ARTIG GESTIEGENEN IT-KOSTEN ZU KONTROLLIEREN. DIE ZÜRICH VERSICHERUNG HAT FÜR IHRE ZÜRICH INVEST BANK DIESE MÖGLICHKEIT GENUTZT UND DEN BETRIEB DER BANKAPPLIKATION AN DIE ADN OVUM AUSGELAGERT.

VON RAPHAEL SCHMIDIGER UND CHRIS TANNER

Das Besondere am Outsourcing der Zurich Invest Bank ist, dass für den Betrieb der IT-Systeme sowie Backup und Recovery auf Betriebssystemebene, System Engineering und

Hardware-Betrieb das Rechenzentrum der Zürich Versicherung verantwortlich ist. Für die Aufrechterhaltung des Service sind mehrere Parteien zuständig, verschiedene Zürich-interne und das Banken-Betriebs-Team (BBT) der AdNovum.

Damit der Betrieb unter diesen Umständen optimal funktionieren kann, musste vor

durchgeführt. Das so entstandene Dokument diente als Grundlage für einen Request for Proposal, anhand dessen ein Service Level Agreement (SLA) ausgearbeitet wurde.

Die AdNovum hatte dabei den grossen Vorteil, dass sie die betroffene Software sehr gut kannte, da bis auf den zentralen Banking-Teil alle Produkte des Zurich-Invest-Bankensystems von der AdNovum selbst entwickelt worden waren. Diesem Umstand ist es auch zu verdanken, dass bei Problemen sehr schnell am richtigen Ort eingegriffen werden kann.

Die Zusammenarbeit der Outsourcing-Partner verlief problemlos. Beiden Parteien war bewusst, dass ein solches Vorhaben nur erfolgreich sein kann, wenn alle Beteiligten mit absoluter Professionalität vorgehen und Vertrauen zueinander vorhanden ist.

Andere Sorgen bereiteten anfänglich die zwischenmenschlichen Aspekte. Eine Woche nachdem die für den Betrieb Verantwortlichen über das Outsourcing informiert worden waren, befanden sich bereits zwei Mitarbeiter

Raphael Schmidiger

Raphael Schmidiger, eidg. dipl. Wirtschaftsinformatiker und seit 1999 Leiter System Engineering der AdNovum, wurde aufgrund seiner langjährigen Betriebserfahrung mit dem Aufbau des BBT betraut.

Chris Tanner

Chris Tanner, dipl. El. Ing. HTL, gehört seit 1995 zur AdNovum und war technischer Leiter des Projekts Finance Point der Zurich Invest Bank.

FÜR DIE AUFRECHTERHALTUNG DES EFFEKTIVEN SERVICE SIND MEHRERE PARTEIEN ZUSTÄNDIG.

der eigentlichen Übergabe der Bestand sämtlicher Services und der betroffenen Software- und Hardware-Komponenten aufgenommen werden. Anhand dieser Liste wurde nach einer möglichst praktikablen Aufteilung der Verantwortung gesucht. Im Falle der Zurich Invest Bank wurde eine erste Bestandesaufnahme durch eine unabhängige Drittfirma

der AdNovum permanent bei der Zürich. Während dieser für alle Beteiligten nicht immer einfachen Zeit ging es darum, von den Erfahrungen der Vorgänger zu profitieren und ihr Vorgehen zu verstehen. Nur dank dem professionellen Verhalten und der Mithilfe aller Beteiligten konnte die Übernahme des Betriebes reibungslos durchgeführt werden.



Schritte in Richtung Übergabe

Nach diesen Vorarbeiten erfolgte die eigentliche Übergabe an die neuen Outsourcing-Partner in den folgenden drei Schritten:

In der ersten und heikelsten Phase ging es um eine Bestandsaufnahme vor Ort und Mithilfe im Betrieb. Ziel dieses Einsatzes war es, möglichst genau zu erfassen, wie das System bis dahin betrieben worden war. Die Mitarbeiter der AdNovum protokollierten während dieser Zeit jeden Handgriff am und um das System. Die Erkenntnisse wurden wöchentlich ausgewertet und die Änderungen priorisiert, die für den späteren Betrieb von der AdNovum aus nötig waren. Dabei entstanden die konkreten Anforderungen, anhand derer die Entwickler während der Übergangszeit gewisse Applikationen und Tools anpassten.

In der nächsten Phase, als die Infrastruktur (Virtual Private Network, Firewall usw.) und die Arbeitsplätze des BBT eingerichtet waren, wurde der Betrieb der Bank von den bisherigen Mitarbeitern in der AdNovum weitergeführt. Dieser Schritt war notwendig, um zu überprüfen, ob ein Betrieb mit den bereitgestellten Hilfsmitteln überhaupt machbar ist. Während dieser Phase konnte das BBT seine Erfahrung und sein Wissen ausbauen und den Know-how-Transfer von den alten Betreibern zum neuen Team sicherstellen.

Eigentliche Betriebsübergabe

Nach Abschluss der beiden oben beschriebenen Phasen konnte die Betriebsübergabe stattfinden. Damit alle im Verlauf der Nacht angefallenen Pendenzen noch abgearbeitet

Banken-Betriebs-Team (BBT)

Das Banken-Betriebs-Team stellt den Betrieb der Bankapplikationen sicher, welche die AdNovum Operations AG im Auftrag ihrer Kunden betreut. Diese Verantwortung nimmt das BBT im Rahmen der im entsprechenden Service Level Agreement spezifizierten Aufgaben wahr. Der Betrieb der Applikationen ist physisch und logisch völlig von der AdNovum-Infrastruktur getrennt, und die Mitarbeiter arbeiten über ein VPN (Virtual Private Network) im Netzwerk des Kunden. Die BBT-eigene Kommunikationsinfrastruktur stellt sicher, dass die Mitarbeiter für Kunden immer optimal erreichbar sind.

Das aus Andrea Induni, Markus Grimm und Lars Sörensen bestehende BBT arbeitet unter der Leitung von Raphael Schmidiger, der es im Rahmen seiner Funktion als Leiter System Engineering der AdNovum aufgebaut

und etabliert hat. Die grosse Selbständigkeit des Teams garantiert den professionellen und gesicherten Betrieb der Applikationen.

Alle Manipulationen an den applikatorischen Banksystemen werden vom BBT streng nach den Qualitätssicherungsvorgaben des Kunden ausgeführt und dokumentiert. Dank der genauen Kenntnisse der Abläufe und Schnittstellen im Bankwesen (SIC, SWIFT, SWX usw.) kann dem Kunden ein optimaler Service geboten werden.

Die Endverarbeitungen und die Dokumentenproduktion stellen eine besondere Herausforderung für das Team dar, da es sich um weniger häufige Aufgaben handelt und die Systeme durch die grossen Mengen schnell an ihre Grenzen stossen, so dass es innovative Lösungen braucht, um entstehende Probleme und Engpässe umgehen zu können.

werden konnten, wurde der Termin auf zwölf Uhr mittags angesetzt. Dabei entstand das Übernahmeprotokoll, in dem genau festgehalten ist, welche Aufgaben nur mit und welche ohne Vorbehalt übernommen werden konnten.

In Absprache mit allen Vertragspartnern wurden während der Übergabe verschiedene ursprünglich geplante Prozesse und Vorgaben zugunsten einer günstigeren und angemesseneren Lösung fallen gelassen. Nur durch aktives Nachfragen und dank einem gesunden Mass an Flexibilität konnten gewisse zuvor als

unabdingbar oder unveränderbar angesehene Prozesse angepasst oder ganz weggelassen werden.

Das BBT war mit Unterstützung von erfahrenen System Engineers von Anfang an am Übernahmeprozess beteiligt. Im ersten Monat konnten die Verfügbarkeit und die Kundenzufriedenheit dank dem unermüdlichen Einsatz beider Outsourcing-Partner markant gesteigert werden.

Ende August 2003 wurde ein Teil der Bankprodukte der Zurich Invest Bank an die AIG Privat Bank übertragen. ■

Innerhalb der Grenzen

DER FINANZIELLE SCHADEN, DER UNTERNEHMEN DURCH DEN VERLUST DER KONTROLLE ÜBER SENSIBLE DATEN ENTSTEHT, BELÄUFT SICH AUF MEHRERE MILLIONEN, WENN NICHT MILLIARDEN EURO JÄHRLICH. DIES VERLANGT NACH EINEM NEUEN SICHERHEITS-KONZEPT FÜR SERVER-BASIERTE SYSTEME, DAS AUCH INSIDER-ANGRIFFE IN BETRACHT ZIEHT.

VON CHRIS DUNN (VP ENGINEERING CHRYSALIS-ITS)

Mittel zum Schutz der Netzwerkübergänge von Unternehmen (Perimeter Security) wie Firewalls, Viruswalls, Intrusion Detection, VPNs (Virtual Private Networks) und DMZs (Demilitarized Zones) als Frontlinie werden oft diskutiert. Externe Angriffe ziehen die Aufmerksamkeit der Medien auf sich und verschlingen das IT-Sicherheitsbudget, während die Server vor Insider-Angriffen ungeschützt bleiben. Diese wohl grösste Bedrohung der IT-Sicherheit der Unternehmen wird trotz der gravierenden Auswirkungen vernachlässigt. In einer im Jahr 2001 durchgeführten Umfrage bezifferten 267 Unternehmen den Verlust, der ihnen durch nicht autorisierte Zugriffe der eigenen Mitarbeiter und den Missbrauch von Zugriffsprivilegien durch Insider entstanden war, auf über 41 Millionen Euro.

Obwohl Techniken zur Gewährleistung der Perimetersicherheit in Kombination mit

einer starken Authentisierung und Verschlüsselung einen wirksamen Schutz der IT-Systeme gegen externe Angriffe bieten können, sind sie gegen interne Attacken weitgehend nutzlos. Deshalb stellt sich die Frage, wie Server-basierte Systeme von der mehrstufigen Sicherheit profitieren können, wie sie in der hochsicheren Welt der kryptografischen Verarbeitung eingesetzt wird, so dass eine Infrastruktur entsteht, die sowohl gegen Insider-Angriffe als auch gegen Gefahren von aussen gefeit ist.

DER INSIDER-ANGRIFF, DIE WOHL GRÖSSTE BEDROHUNG DER IT-SICHERHEIT DER UNTERNEHMEN, WIRD TROTZ DER GRAVIERENDEN AUSWIRKUNGEN VERNACHLÄSSIGT.

Betriebs-, Software- und physische beziehungsweise Hardware-Sicherheit sind die drei Aspekte, die zu berücksichtigen sind, wenn es um die Schaffung einer wirklich sicheren IT-Plattform geht. Genau diese Prinzipien wurden bei einem der sichersten Computing-Module auf dem heutigen Markt erfolgreich angewandt, dem Luna SA HSM Server.

Die Anwendung dieser Konzepte auf das Design eines Servers für allgemeinere Aufgaben ergibt ein System, das gegen Angriffe äusserst widerstandsfähig ist, da es von der Sicherheit der Übergänge zum Datacenter und den Verarbeitungsfähigkeiten des Hardware-Sicherheitsmoduls weniger abhängig ist. Im Wesentlichen sorgt jeder sichere Server für seine eigenen Sicherheitsgrenzen, kryptografischen Verarbeitungen und operativen Kontrollen. Ein so konzipierter Server stellt ein eigentliches «Datacenter im Datacenter» dar. Diese neue Systemgattung wird die Definition von Sicherheitsanforderungen an Datacenter

Chrysalis-ITS Inc.

Chrysalis-ITS ist ein führender Hersteller von Hardware-Sicherheitsprodukten, die der Absicherung und Geschwindigkeitsoptimierung von Applikationen dienen, die beispielsweise Finanztransaktionen auf elektronischer Basis, SSL, die Herausgabe von Smart Cards, Dokumentensicherheit und das Management von digitalen Identitäten umfassen.

Die 1994 gegründete Chrysalis-ITS hat ihren Hauptsitz in Ottawa, Kanada, und Niederlassungen in den USA, Grossbritannien, Deutschland, Japan und Hongkong. Weitere Informationen finden Sie unter: www.chrysalis-its.com

und Managed Security Service Provider massgebend beeinflussen, da sie einerseits hochsichere Server ermöglicht, die bestehende

Sicherheitseinrichtungen aufwerten können, und andererseits vor Manipulation geschützte Systeme für den Einsatz an weniger sicheren Standorten zur Verfügung stellt.

Sichere Server bilden die Grundlage für den Einsatz vertrauenswürdiger Netzwerk-knoten und führen einen Schritt näher an das Ziel, das Potenzial einer hochverteilten, Web-basierten Computing-Umgebung voll auszuschöpfen.

AdNovum und Chrysalis-ITS sind im Dezember 2002 eine strategische Partnerschaft eingegangen, um gemeinsam kombinierte Software- und Hardware-Sicherheitslösungen kundenspezifisch anbieten zu können.

Den vollständigen Beitrag «Innerhalb der Grenzen: Sicherheitsdesign für Next-Generation Server» finden Sie auf der Chrysalis Homepage: http://www.chrysalis-its.com/news/press_releases/press_2003/inside_the_perimeter_DE.htm

Impressum

Herausgeber:

AdNovum Informatik AG
Corporate Marketing
Röntgenstrasse 22
CH-8005 Zürich
Telefon 01 272 61 11
Telefax 01 272 63 12
E-Mail info@adnovum.ch
www.adnovum.ch

Verantwortlich und Redaktion:

Barbara Stammler
Dorina Mayrhofer

Gestaltung und Realisation:

Rüegg Werbung, Zürich

Fotografie:

Matthias Auer, Zürich