Kammerseminar: e-business

e-shop: Stärken und Schwächen aus Revisorensicht

Software zum Betrieb eines Online-Shops im Internet gibt es in extremer Bandbreite: Von simplen Einstiegsprogrammen für einige Dutzend Franken, erhältlich im kommunen Buch- und Softwarehandel, bis zum ausgeklügelten Shopping-System mit voller Integration in die IT-Infrastruktur des Shop-Betreibers bietet der Markt Dutzende von mehr oder weniger geeigneten Produkten. Für unsere Untersuchung haben wir uns auf Produkte für den KMU-Bereich konzentriert, die im Preisbereich von unter 1000 bis etwa 15 000 Franken zu haben sind – dazu kommen jeweils noch die Kosten für die Planung und Umsetzung des Projekts.

Zehn e-shop-Pakete auf revisionsrelevante Aspekte untersucht

In gängigen Vergleichstests wird in erster Linie die Benutzerfreundlichkeit untersucht. Für die Revision wesentliche Aspekte wie Sicherheit und Anbindung an exerne IT-Systeme kommen kaum zum Zug. In einer nicht repräsentativen Studie wurden zwölf Hersteller mit einem sechsseitigen Fragebogen konfrontiert; zehn davon antworteten innerhalb der gesetzten Frist.

Bei näherer Durchsicht ergeben sich drei unterschiedliche Produktkategorien: Zusatzprodukte zu bestehenden KMU-Administrationslösungen ("Add-On"), Programme mit erheblichem Installations- und Konfigurationsbedarf, die man auch als Shop-Entwicklungstools bezeichnen könnte ("Software") sowie Komplettpakete mit weitgehend vorgefertigter Funktionalität, für die der Hersteller zudem meist auch das Hosting übernimmt ("All-In-One"). Wir haben folgende Produkte untersucht:

"Add-On"
- Abacus Abashop
- Navision Webshop
- Winware e-Shop

"Software"
- D3D Shopfactory Pro
- Hybris Shop Standard Edition
- Openshop Business
- Intershop enfinity

"All-In-One"
- SwissDigital ShopServer
- Think Software iShop Professional
- Eicom Easy-Shop Infinity

Schnittstellen wesentlich

e-shop-Software umfasst im allgemeinen die Funktionsbereiche Angebot (Präsentation der Waren oder Dienstleistungen im Online-Katalog), Auswahl (Bestellsystem mit Warenkorb), Bezahlung (per Rechnung oder Online-Buchung), Administration (Verarbeitung der Bestellungen, Bewirtschaftung der Stammdaten) und Analyse (Auswertung der Shop-Aktivität für finanz- und marketingtechnische Folgemassnahmen).

Damit ist klar, dass Schnittstellen zu anderen IT-Systemen essentiell sind: Warensortiment und Kundenstammdaten existieren bereits in anderen Datenbanken. Eine enge Anbindung an die Lagerbewirtschaftung ist nur schon zur Verfügbarkeitsanzeige erwünscht, und die Online-Kreditkartenbuchung funktioniert nicht ohne Beihilfe externer Systeme.

Sowohl bei den Schnittstellen zu Kunden- und Artikelstammdaten als auch bei der Anbindung zu den operativen Systemen sind die einfacheren Produkte klar limitiert: Die Add-Ons funktionieren nur mit dem ERP-System des gleichen Herstellers; die All-In-One-Lösungen setzen meist auf integrierte Datenbanken und bieten bloss einfache Import-/Exportschnittstellen für den periodischen Datenabgleich. Eine Online-Anbindung ist in der Kategorie "Software" durchaus möglich und sollte die Regel sein, ist aber mit erheblichem Implementationsaufwand im Umfang eines mittelgrossen IT-Projekts verbunden.

Sicherheit problematisch

Erhebliche Lücken zeigen sich auch punkto Sicherheit. Die wenigsten Produkte arbeiten im administrativen Bereich durchgängig mit verschlüsselten Daten. Bestellbestätigungen werden zudem meist obligatorisch – der Kunde hat hier keine Optionen – über e-mail verschickt, was etwa den gleichen Datenschutz bietet wie eine Postkarte.

Der Revisor sollte auch einige allgemeingültige Security-Aspekte beach-

ten: Die Zahlungsübermittlung erfolgt üblicherweise in einem geschützten Bereich und Kreditkarteninformationen werden damit verschlüsselt übertragen. Es muss jedoch von Fall zu Fall geprüft werden, ob keine geheimen Daten vor dem Aufbau der SSL-Verschlüsselung übermittelt werden.

Eine weitere Gefahr für die Sicherheit stellen Web-Adressen (URL) mit unverschlüsselten Kundenangaben wie Name oder Passwort dar, die während des Shop-Besuchs zwischen dem Web-Browser des Kunden und dem Web-Server des Shop-Betreibers ausgetauscht und überdies langfristig in den Router-Logfiles festgehalten werden.

Das Fazit: Ohne Fleiss kein Preis

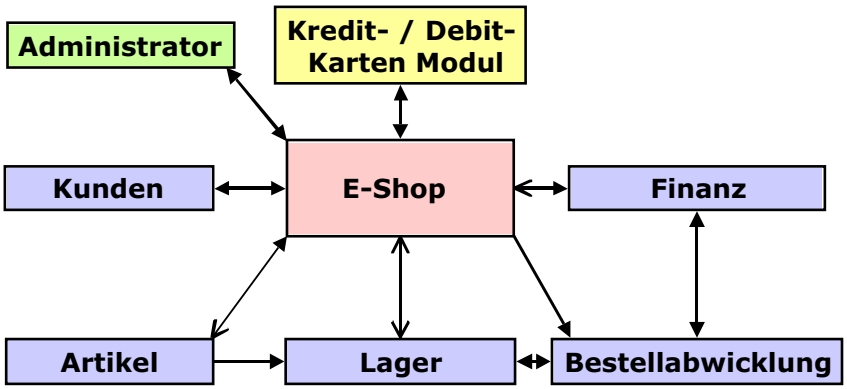
Aus unserer Untersuchung resultieren in erster Linie "Negativ-Erkenntnisse": Zwar bieten die meisten e-shop-Pakete eine gute Basisfunktionalität, kommen aber nicht ohne Schwachstellen daher: Keine, beschränkte oder zu allgemein gehaltene Schnittstellen, in der Grundkonfiguration mangelhafte Sicherheit sowie teils ungenügende technische Voraussetzungen, zum Beispiel fix installierte Datenbanken der einfacheren Klasse ohne Möglichkeit zum Einsatz höherwertiger SQL-Datenbankserver. Als Indiz für die Zukunftssicherheit von e-shop-Software kann die Unterstützung von offenen Standards wie XML, ODBC, SQL-Datenbanken und SSL dienen.

Für den Shop-Betreiber wichtig ist eine klare Strategie, was mit der Shop-Präsenz auf dem Internet überhaupt bezweckt werden soll: Handelt es sich um einen eher nebensächlichen zusätzlichen Verkaufskanal oder um einen wichtigen Grundpfeiler des Gesamtgeschäfts; arbeitet man in einem Nischenmarkt mit klar definierten Zielgruppen und wenig Konkurrenz oder im Massengeschäft mit zahlreichen Mitbewerbern, die ähnliche Sortimente anbieten? Diese strategischen Merkmale sollten auch vom Revisor in die Revisionsplanung einbezogen werden.

Eine genügende Revisionssicherheit erreicht eine e-shop-Lösung erst durch die konkrete Implementation, die nicht ohne sorgfältige Planung und erheblichen Entwicklungs- und Testaufwand denkbar ist: Ein Pflichtenheft ist buchstäblich Pflicht. Ohne detailliertes Know-how des eigenen Geschäfts und exakte Abstimmung des e-shops mit den übrigen Geschäftsprozessen resultiert allenfalls eine Lösung, die für niedrige Verkaufsvolumina mit nachträglicher manueller Behandlung aller elektronisch abgewickelten Geschäftsfälle geeignet ist.

Radim Svejda,
dipl. Wirtschaftsinformatiker,
Balsec GmbH, Basel
Urs Binder, Redaktor,
Infoweek, Basel

Der e-shop im Software-Umfeld



Logiciels e-shop : le point de vue de l'audit sur les forces et faiblesses des différents produits

Il existe une vaste palette de logiciels destinés à l'exploitation d'un shop online : du simple programme de base disponible pour une dizaine de francs dans les librairies informatiques, jusqu'au produit sophistiqué qui permet une parfaite intégration dans l'environnement informatique de l'entreprise, le marché offre des dizaines de programmes plus ou moins adaptés aux besoins. Notre étude s'est concentrée sur les logiciels destinés aux PME, vendus entre 1000 et 15 000 francs, frais de planification et de mise en place du projet non compris.

Etude de dix logiciels quant aux fonctionnalités importantes pour un réviseur

Les tests habituellement réalisés portent essentiellement sur la convivialité des produits. Des aspects essentiels pour l'audit, comme la sécurité ou les interfaces avec d'autres programmes, sont rarement évoqués. Dans une étude qui ne prétend ni exhaustive ni représentative, nous avons confronté douze fournisseurs à un questionnaire de seize pages. Dix d'entre eux ont accepté de répondre dans le délai fixé.

Nous avons distingué trois classes de produits : des produits complémentaires aux logiciels de gestion utilisés par les PME ("Add-On"), des programmes nécessitant un considérable investissement pour leur installation et leur configuration – également considérés comme des caisses à outils de développement d'une plateforme e-shop ("Software"), et enfin les produits complets offrant sous une forme intégrée une solution prête à l'emploi que le fournisseur propose de surcroît souvent d'héberger ("All-In-One"). Nous avons examiné les logiciels suivants :

"Add-On"

- Abacus Abashop
- Navision Webshop
- Winware e-Shop

"Software"

- D3D Shopfactory Pro
- Hybris Shop Standard Edition
- Openshop Business
- Intershop enfinity

"All-In-One"

- SwissDigital ShopServer
- Think Software iShop Professional
- Eicom Easy-Shop Infinity

Les interfaces sont essentielles

Une application e-shop comprend généralement les fonctions d'offre des produits ou des services (catalogue online), de choix du produit (système de panier électronique), de payement (par facture ou par débit online), d'administration (traitement des commandes, mise à jour des données de base) et d'analyse (examen de l'activité e-shop dans un but de gestion ou de marketing).

Il est donc clair que les interfaces vers les autres logiciels sont essentielles : la base de données des clients et le catalogue des produits sont en principe déjà disponibles dans une autre application de l'entreprise. Un lien étroit avec le logiciel de gestion du stock est indispensable, ne serait-ce que pour vérifier la disponibilité des articles avant de confirmer la commande; et la vérification online de la validité des cartes de crédit ne fonctionne qu'à l'aide d'un système externe.

Les produits les plus simples n'offrent souvent pas de solution satisfaisante dans le domaine des liens avec des bases de données externes des clients ou des produits ou dans celui de la liaison avec le système de gestion de l'entreprise. Les produits "Add-On" ne fonctionnent qu'avec les produits de gestion du même fournisseur. Les solutions "All-In-One" sont généralement construites sur une base de données intégrée et n'offrent que des functions très simples d'import/export des données pour des réconciliations périodiques. Une intégration online est possible dans la catégorie "Software" – et devrait même être la règle – mais elle implique des travaux de développement importants qui ne peuvent être réalisés que dans le cadre d'un projet informatique de taille moyenne.

Une sécurité problématique

Des faiblesses importantes existent également dans le domaine de la sécu-

rité. In n'y a que très peu de produits qui travaillent systématiquement avec des données chiffrées dans le domaine administratif. Les confirmations de commande sont de plus envoyées de manière généralement obligatoire (le client n'a pas le choix) sous forme de courrier électronique, ce qui offre un degré de confidentialité comparable à celui d'une carte postale. Le réviseur devrait examiner quelques aspects généraux liés à la sécurité : la saisie des données relatives au payement est généralement effectuée dans un domaine protégé avant d'être transmise sous forme chiffrée. Il faudra cependant vérifier de cas en cas si des données secrètes ne sont pas transmises avant l'ouverture de la session chiffrée SSL.

Il existe des adresses Internet (URL) qui constituent également une menace pour la sécurité. Durant la visite du client sur le site de l'exploitant de l'e-shop, des données non chiffrées – comprenant par exemple le nom et le mot de passe du client – sont échangées entre le browser du client et le serveur de l'exploitant. De telles données demeurent durant des laps de temps importants dans les fichiers mouchards des différents routeurs.

Conclusion : pas de solution-miracle

Notre étude met surtout en avant des points négatifs : bien que la plupart des produits e-shop offrent une bonne fonctionnalité de base, celle-ci est accompagnée de faiblesses importantes. Des interfaces inexistantes, très limitées ou configurées de manière trop générale, des fonctions de sécurité insuffisantes dans la configuration de base, une base technique insuffisante, par exemple l'installation d'une base de données de classe inférieure sans possibilité d'y joindre un serveur base de données SQL. La mention des standards soutenus comme XML, ODBC, base de données SQL ou SSL constitue un bon indice de la capacité future du produit.

Pour l'exploitant d'un e-shop, il est essentiel de définir la stratégie de sa présence sur Internet. S'agit-il d'un canal de vente auxiliaire et accessoire ou d'une composante essentielle de la politique de l'entreprise ? Travaille-t-il dans une niche à l'abri de la concurrence et avec une clientèle précise ou est-il exposé à de nombreux concurrents offrant le même genre de produits ? Ces considérations stratégiques devraient également être prises en compte par le réviseur lors de la planification de sa mission.

Une application ne remplira les exigences de sécurité et de régularité qu'au prix d'un développement qui impliquera des investissements importants dans la gestion du projet, le développement et les tests. L'établissement d'un cahier des charges est donc incontournable.

Sans une bonne connaissance de son propre marché et une intégration soigneuse de l'application e-shop dans les autres processus, une entreprise installera un e-shop qui sera tout au plus à même de traiter manuellement les commandes électroniques des clients pour autant qu'elles n'atteignent pas un volume trop important…

Séminaire de la Chambre : e-business

Démarche d'audit informatique pour la révision d'une e-banque

Une e-banque fonctionne généralement comme une plaque tournante mettant en connexion différents partenaires regroupés sous une même raison sociale. Elle se caractérise par son caractère très hétérogène et un recours important à des contrats d'externalisation.

La démarche à suivre pour auditer une e-banque n'est pas fondamentalement différente de la démarche d'audit classique :

1. Avoir une vue d'ensemble sur le système
2. Identifier les processus les plus importants et en analyser le déroulement
3. Procéder aux vérifications en suivant le flux de la transaction à travers toutes les composantes du système

Chaque étape du processus présente des points critiques caractéristiques qu'il conviendra d'intégrer dans le programme d'audit. En voici quelques exemples :

Saisie des données par le client

■ Le client a-t-il une vision claire du type de transaction qu'il génère et le système garantit-il qu'un client n'a accès qu'aux types de transactions correspondant à sa relation bancaire ?

■ Le système procède-t-il à une plausibilisation des informations saisies, vérifie-t-il la solvabilité du client ?

■ Le système génère-t-il un procès-verbal de la session à l'attention du client ?

■ Une réconciliation entre la saisie par le client et l'enregistrement par le système avancé (front-end) est-elle possible ?

Enregistrement des données dans le système avancé (front-end)

■ L'exactitude et l'intégralité des données sont-elles assurées ?

■ Chaque transaction est-elle journalisée, y compris les données relatives à la transmission (date et heure, origine, autorisation, etc.) ?

■ Le système enregistre-t-il également les conditions (cours, etc.) valables à l'instant de la transaction, les transmet-il à l'application suivante ?

■ Moyens pour éviter une répétition erronée de la transaction ?

■ Une réconciliation est-elle effectuée entre le système avancé (front-end) et l'application suivante ? Quand et comment ?

Exécution de la transaction

■ Comment sont comptabilisées les transactions interrompues ?

■ Comment sont comptabilisées les transactions sur les comptes de la banque et les comptes des clients, par transaction, par client ? Réconciliations entre ces différentes comptabilisations ?

Liquidation de la transaction, payement et comptabilisation

■ Quand la transaction est-elle considérée comme achevée ?

■ Quels systèmes reçoivent-ils une annonce ? Comment réagissent les systèmes s'ils ne reçoivent pas d'annonce ?

■ Quand le nouveau solde du compte est-il transmis au système avancé (front-end) et au client ?

Cas spéciaux

■ Traitement des extournes (par exemple des ordres boursiers) ?

■ Traitement des retards d'exécution

■ Situation en cas de pannes d'une composante du système, synchronisation

Outsourcing

■ Le système de contrôle interne et les réconciliations entre les différentes composantes du système sont-ils assurés malgré l'externalisation d'une partie des activités ?

■ Pour le reste, les conditions de la Circulaire de la CFB (99/2) sont-elles respectées ?

Patrick Ludwig, lic. phil. II, dipl. Org., Infoguard, Zug
Christoph Protz, lic. iur., Arthur Andersen, Zürich

Einsatz der Informatik-Revision für eine e-bank

(Berichterstattung eines Seminar-Teilnehmers)

Vorgestellt wurde eine e-bank, welche sich in erster Linie als Drehscheibe und Verkaufskanal sieht. Sie bietet vor allem Dienstleistungen Dritter, unter eigenem Namen, an. Systementwicklung und Bankdienste werden entweder ausser Haus vergeben oder es wird mit Partnern zusammengearbeitet. Dies ergibt somit eine äusserst komplexe Informatik-Architektur.

Der Revisionsansatz im e-business ist nicht anders als bei herkömmlichen Informatikprüfungen (die Durchführung allerdings um einiges komplexer und aufwändiger):

1. Systemübersicht gewinnen
2. die wichtigsten Prozesse und Abläufe aufnehmen und analysieren
3. Durchgehende Prüfung des Transaktionsflusses

Zu den einzelnen Prüffeldern wurden beispielhafte Fragestellungen erläutert:

Prüffeld: Dateneingabe in Frontend-Systeme (Client)

■ Ist aus der Benutzerführung immer klar ersichtlich, welche Banktransaktion ausgelöst wird?

■ Ist die Benutzerführung so ausgelegt, dass der Kunde nur vereinbarte Transaktionen durchführen kann?

■ Sind festgelegte Betrags-/ Eingabelimiten auch technisch implementiert? Wird die Bonität des Kunden technisch geprüft? Wann?

■ Existiert ein Verifikations/Kontrolldialog der vor endgültigem Absetzen der Transaktion durchlaufen werden muss?

■ Besteht kundenseitig ein Verfahren, das auf den Kundenterminal ein Protokoll über die abgesetzten Transaktionen erstellt?

■ Gibt es zwischen dem Kundenterminal und dem Eingabesystem transaktionsbezogene Abstimmkreise?

Prüffeld: Dateneingabe in Frontend-Systeme (Eingabesystem)

■ Ist sichergestellt, dass jede Transaktion vollständig und integer ins Eingabesystem weitergeleitet wird?

■ Wird jede Transaktion (einschliesslich Kurse etc.) im Eingabesystem vollständig und unveränderbar protokolliert? Sind auch Metadaten protokolliert (z. B. Transaktionszeitpunkt, Herkunft, Autorisierung)?

■ Wird die aktuelle Bonität des Kunden (um die neuesten Transaktionen bereinigt) geprüft? Per wann? Nachführung der abgeschlossenen bzw. pendenten Transaktionen?

■ Werden Transaktionen so weitergeleitet, dass die vereinbarten Bedingungen (Kurse etc.) auch gewahrt bleiben? Zeitstempel?

■ Welche Daten werden zur Transaktionsausführung weitergeleitet?

■ Gibt es Abstimmkreise zwischen dem Eingabesystem und Folgesystemen? Per wann wird abgestimmt?

Prüffeld: Transaktionsdurchführung

■ Wo und wann werden die abgesetzten Transaktionen verbucht?

■ Wann erfolgt die Verbuchung auf dem Kundenkonto? Auf den Bankenkonti?

■ Auf welche Weise werden Transaktionen, z. B. Wertschriften zusammengefasst bzw. konsolidiert? Pro Kunde? Pro Transaktionsart, beides?

■ Welche Abstimmungen existieren zwischen den verwendeten Abwicklungssystemen (z. B. Eingabe-Börse, Eingabe Abwicklung, Abwicklung – Börse-Zahlung)?

Prüffeld: Transaktionsabschluss, Zahlung, Verbuchung

■ Wann und wie erfolgt die Zahlung der Transaktionen?

■ Wann wird die Transaktion als abgeschlossen zurückgemeldet? An welche Systeme?

■ Wann und wie erfolgt die Aufteilung der Zahlungen sowie der Gesamttransaktionen an die Kunden?

■ Was geschieht bei (teilweise) erfolglosen Transaktionen?

■ Wann werden Zahlungen verbucht? Welche Abstimmungen zu Kundenkonti existieren?

■ Wann wird der Transaktionsstatus sowie der aktualisierte Kontostand an das Eingabesystem zurückgemeldet? Wann an den Kunden? Abstimmung mit Eingabesystem? Protokollierung?

Prüffeld: Spezialfälle

■ Wie werden Stornierungen – z. B. von Börsenaufträgen – gehandhabt? Zeitlicher Verlauf?

■ Wie wird vorgegangen, wenn wegen Verzögerungen Vereinbarungen nicht eingehalten werden können?

■ Wie ist der korrekte Buchungs- und Abstimmfluss im Nachhinein gewährleistet (z. B. im Falle von Systemausfällen)?

■ Wie werden die Teilsysteme synchronisiert (neue Transaktionen, Status alter Transaktionen, Storni etc.)? Was geschieht bei Ausfällen, Teilausfällen?

■ Welches ist der verbindliche Taktgeber für Transaktionen gegenüber dem Kunden? Gegenüber den Kontrahenten und Partnern?

Im Zusammenhang mit outsourcing stellen sich u. a. folgende Fragen:

■ Waren die grundsätzlichen Anforderungen der auszulagernden Geschäftsbereiche an den Leistungserbringer genau und vorgängig bestimmt?

■ Sind diese dokumentiert ?

■ Welche Anforderungskriterien dienen der Mess- und Beurteilbarkeit der Leistungserbringung?

■ Sind die Sicherheitsanforderungen klar definiert, beiden Parteien bekannt und im Vertrag festgehalten?

■ Werden die Anforderungen von beiden Parteien gleich verstanden?

■ Wer ist für die Überwachung und Kontrolle der Einhaltung durch den Dienstleister verantwortlich?

Auch wenn die Präsentationen der Architektur- und Prozessübersichten wohl nicht einmal mit einem starken Feldstecher lesbar gewesen wären, wurde uns ein sehr informativer Vortrag geboten, welcher aufzeigte, wie komplex und aufwändig eine Revision im e-business-Bereich sein kann. Die Verwischung von Grenzen (Systeme, Firmen, Länder, Gesetze) trägt ein wesentliches dazu bei.

Andreas Jordi, CISA

Kammerseminar: e-business

Revision von Schlüsselverwaltungs-Systemen

Einleitung

Bei der Revision von Schlüsselverwaltungs-Systemen haben wir es mit einem noch jungen Bereich innerhalb der Revision zu tun. Vor allem ist aber auch die Revision von Schlüsselverwaltungs-Systemen ein sehr komplexes Feld, bei dem es um weit mehr als um Technologie geht. Ich werde in meinen Ausführungen versuchen aufzuzeigen, warum dies so ist. Ganz am Anfang eine kurze Technologieeinführung.

Technologie-Einführung

Grundsätzlich unterscheiden wir zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Das dritte Verfahren, das hybride Verfahren kann aus den zwei anderen abgeleitet werden und wird in der Folge nicht weiter berücksichtigt.

Symmetrische Verfahren

Verschlüsselungsverfahren sind symmetrisch, wenn für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Symmetrische Verschlüsselungsverfahren sind in der Regel schneller als asymmetrische und können mit vergleichsweise kürzeren Schlüsseln eine hohe Sicherheit erreichen. Der Schwachpunkt ist jedoch die Kommunikation zwischen dem Sender und Empfänger, in der sich die beiden auf einen gemeinsamen Schlüssel einigen müssen (closed user group). Symmetrische Verschlüsselungsverfahren werden auch Secret-Key-Verfahren genannt. Wird diese Kommunikation abgehört, so ist der Schlüssel bekannt und die nachfolgende verschlüsselte Kommunikation unsicher. Für jede Gruppe von Personen, die geheime Nachrichten austauschen will, wird ein eigener Schlüssel benötigt, was die Schlüsselanzahl massiv erhöht.

Asymmetrische Verfahren

Ein asymmetrisches Verfahren ist ein Verschlüsselungsverfahren, bei dem für die Ver- und Entschlüsselung unterschiedliche Schlüssel verwendet werden. Das Schlüsselpaar wird aus einem privaten und einem öffentlichen Schlüssel gebildet. Der öffentliche Schlüssel kann frei verfügbar sein und wird in einer Art Telefonbuch (Directory) bereitgestellt. Mit dem öffentlichen Schlüssel läßt sich eine Nachricht für den Empfänger verschlüsseln. Die Kenntnis des öffentlichen Schlüssels allein reicht aber nicht aus, um die Nachricht wieder zu entschlüsseln. Der Empfänger entschlüsselt die Nachricht mit dem nur ihm bekannten privaten Schlüssel. Die asymmetrischen Verfahren werden auch Public-Key-Verfahren (PKI) genannt. Neben der Verschlüsselung können die asymmetrischen Verfahren auch zur Authentisierung eingesetzt werden. Wird eine Nachricht mit dem geheimen Schlüssel verschlüsselt, so kann sie nur mit dem dazugehörigen öffentlichen Schlüssel wieder lesbar gemacht werden. Dies heißt aber auch, daß sie von einer Person stammt, die über den zugehörigen geheimen Schlüssel verfügt. Eine weitere Anwendungsmöglichkeit von Public-Key-Verfahren ist die Digitale Unterschrift.

Der Nachteil der asymmetrischen Verfahren besteht darin, daß die verwendeten Schlüssel viel länger und rechenintensiver sind als bei symmetrischen Verfahren. So ist z. B. der symmetrische Algorithmus DES ca. 1000 mal schneller als vergleichbare asymmetrische Algorithmen (z. B. RSA). Heute gelten bei symmetrischen Verfahren Schlüssellängen von 128-Bit als sicher, während bei asymmetrischen Verfahren die Schlüssellänge dagegen mindestens 1024-Bit betragen sollte.

Anwendungsbereiche

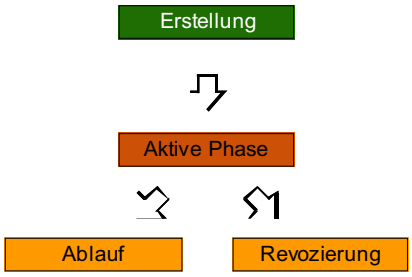
Beide Verfahren bedingen bei einem firmenweiten Einsatz eine mächtige Infrastruktur, die weit mehr als die Technologie tangiert. Während die symmetrischen Verfahren vor allem im Bereich File-/Folderverschlüsselung zum Einsatz kommen, sind grosse Public Key Infrastrukturen vor allem in grossen Unternehmen zu finden, viele jedoch noch im Pilot-Stadium.

Lebenszyklus

Wichtig ist der Umstand, dass die Schlüssel einem Lebenszyklus unterworfen sind und dieser durch das System und die Management-Prozesse unterstützt werden muss. Während der

Ablauf bei der Erstellung des Schlüssels meist noch klar definiert ist, ist dies z. B. beim Austritt eines Schlüsselinhabers (z. B. Mitarbeiter) längst nicht so klar definiert und bietet Angriffsflächen. Wichtig ist deshalb die Überprüfung, ob allen Stadien des Lebenszyklus im Verwaltungsprozess Rechnung getragen wird. Auch die Bedingungen und Prozesse, unter welchen ein Schlüssel in einen anderen Status überführt wird, sind dabei zu berücksichtigen.

Unter Revozierung wird übrigens die "Ungültigerklärung" des Schlüssels bezeichnet, sei es durch den Austritt eines Mitarbeiters oder aber auch durch das Vermuten einer Sicherheitslücke.



Wichtig am Ende des Schlüssel-Lebenszyklus' ist insbesondere auch die Archivierung der Schlüssel.

Anwendungsbereiche von Verschlüsselung

Verschlüsselung, sei es symmetrisch oder asymmetrisch, kommt heute in den unterschiedlichsten Bereichen zum Einsatz (siehe nachstehende Tabelle).

Gruppe	Anwendungsbereich
Personen	In Verbindung mit asymmetrischen Verfahren (zertifikatsbasiert) im Bereich End-to-End-Security; mittels hybrider Verfahren (PGP) zum sicheren Austausch von Meldungen
Maschinen	In Verbindung mit einem Zertifikat bei der serverseitigen Verschlüsselung mit SSL/TLS (v. a. Authentisierung)
Übertragungskanäle	In Verbindung mit Zertifikaten im Bereich Virtual Private Network (VPN) oder Verbindungen zwischen Servern
Daten/Dateien	Daten-Verschlüsselung z. B. Kundendaten, File-/Folderverschlüsselung in Unternehmen (symmetrisch/asymmetrisch)
Applikationen	Mittels Kryptomodulen zur Verschlüsselung von Daten und Übertragungskanälen oder zur Authentisierung
Transaktionen	Mittels asymmetrischer Verfahren als Signatur
Meldungen	In Verbindung mit asymmetrischen Verfahren (zertifikatsbasiert) zur Verschlüsselung von Meldungen

Die unterschiedlichen Anwendungsbereiche, wie interner Gebrauch oder externer Gebrauch, bringen eine zusätzliche Komplexitätsdimension in die Problematik. Es muss definiert resp. abgeschätzt werden, welcher Grad von Sicherheit und welche Vorkehrungen und Prozesse für die jeweilige Anwendung implementiert werden müssen.

Kritische Komponenten

Gemäss unserer Erfahrung bei der Implementation von Verschlüsselungssystemen sind gewisse Komponenten resp. Prozesse kritisch für die Vertrauenswürdigkeit von Verschlüsselungssystemen. Wichtig ist jedoch immer, dass beachtet wird, wofür das System benutzt wird. Der Grad der getroffenen Vorkehrungen sollte also immer der Anwendung entsprechend gewählt werden.

Schlüsselerstellung/-speicherung

Jeder Schlüssel muss zunächst einmal erstellt werden. Dies kann unter unterschiedlichen Bedingungen geschehen:

- In hochsicherheitstrakt-ähnlichen Serverräumen mit speziell geschützter Krypto-Hardware, die sich nicht einmal am Netz befinden. Als Gegensatz dazu kann der Schlüssel auch lokal auf einem normalen PC erstellt werden, wo der Schlüssel als verschlüsselte Datei abgelegt wird. Alternativ dazu können die Schlüssel auch auf einem sogenannten Hardware-Token wie Smartcard abgelegt werden.
- Bei besonders vertrauenswürdigen Systemen wird z. B. die Erstellung des sogenannten Root-Keys, also des obersten Schlüssels in einer Hierarchie, mittels notarieller Beglaubigung erstellt und auf mehrere Personen aufgeteilt.
- Bei einigen Systemen haben nur gerade 3–5 Personen Zutritt zum Schlüsselserver. Bei anderen Systemen ist der Schlüsselserver ein "nor-

maler" Fileserver mit vielleicht noch speziell geschütztem Betriebssystem.

Schlüsselverteilung

Je nach dem, wie und wo der Schlüssel erstellt wurde, muss er nun zum Schlüsselinhaber gelangen. Auch hier gibt es völlig unterschiedliche Ansätze:

- Während bei einen das "Sneaker-Net" (Turnschuhnetzwerk) mittels Speicherung auf Diskette als Übertragungsmedium gewählt wird, wird bei anderen ein verschlüsselter Kanal zum Empfängen aufgebaut und der Schlüssel elektronisch übermittelt.
- Wie wird der Schlüsselinhaber identifiziert resp. welche Prozesse muss er durchlaufen, damit er den Schlüssel benutzen kann? Bei einigen Systemen werden zwei "Secrets" erstellt, wobei eines via e-mail übermittelt und das andere von einer vertrauenswürdigen Person direkt übergeben wird (z. B. noch mit Identitätsverifikation). Welche Stufe(n) hierbei eingeführt werden, hängt massgeblich von den Möglichkeiten der Infrastruktur und den Anwendungszweck des Schlüssels ab. So ist es in einigen Fällen durchaus genügend, wenn sich der Benutzer selber registrieren kann. Dies ist vor allem bei Grossfirmen der Fall, die bereits über eine umfassende Authentisierungsinfrastruktur verfügen und diese ebenfalls für den Registrationsprozess verwenden.

Schlüssel-Management

Zentral bei jeder Schlüsselinfrastruktur ist das Management der Schlüssel. Dabei stellen sich folgende Fragen:

- Wie lange ist ein Schlüssel gültig und wie erhält ein Inhaber einen neuen Schlüssel? Die Problematik lehnt sich teilweise an die Schlüsselerstellung resp. Schlüsselübermittlung an.
- Was passiert, wenn ein Benutzer annimmt, dass sein Schlüssel resp. sein Passwort bekannt ist? Wer kann diesen Schlüssel als ungültig erklären und wie wird der Inhaber überprüft? Was passiert darauf hin?
- Was passiert beim Austritt eines Mitarbeiters mit seinen Schlüsseln?
- Und folgender Punkt hat sich bei vielen Grossunternehmungen als Knacknuss erwiesen: Wie wird der Schlüsselinhaber auch über mehrere Jahre eindeutig identifiziert? Bei vielen Grossfirmen besteht zwar eine Mitarbeiternummer oder eindeutige Identifikation, während der Mitarbeiter in der Firma eingestellt ist. Diese Nummer wird aber nach dem Austritt oftmals wieder neu vergeben, sei dies sofort oder nach einigen Jahren.
- Welche Art von Backup-System ist sicher: bei einigen Systemen ist ein ebenso gesichertes Backup-System im Einsatz, während bei anderen Systemen die Schlüsselinformationen auf der gleichen Infrastruktur wie alle anderen Dateien gespeichert wird.
- Ein weiteres Problem ist der Umgang mit vergessenen Passwörtern. Für den Fall, dass ein User sein Passwort vergessen oder zu oft das falsche Passwort eingegeben hat, müssen Helpdesk-Prozesse bestehen. Dasselbe gilt für verlorene oder vergessene Smartcards: Was passiert, wenn ein User diese vergessen hat? Wie leicht kann eine fremde Person zu einem "neuen" Passwort resp. zu einer Smartcard kommen?

Weitere Sicherheitsaspekte

Weitere Fragen sind bei der Revision von Verschlüsselungssystemen zu beachten:

- Werden für alle kritischen Anwendungen Logs erstellt und ist klar definiert, wer sie in welcher Periodizität auswertet?
- Sind z. B. Systemadministrations- und Sicherheitsadministrations-Aufgaben auf mehrere Personen aufgeteilt? Diese Funktionen ist nach System (Windows NT/Windows 2000) nicht klar aufteilbar, so kann z. B. ein Systemadministrator die Sicherheits-Logs löschen.
- Wieviele und welche Personen können auf die Infrastruktur zugreifen und wer authorisiert diese Personen (Security Officer…)?
- Wie ist die Infrastruktur generell gesichert? D. h. steht sie in einem Serveraum resp. Rechenzentrum oder irgendwo unter einem Pult?
- Wird die Software immer auf den neuesten Stand gebracht, um allfällig bekannte Schwachstellen zu beheben? Dies gilt nicht nur für Verschlüsselungssoftware, sondern generell für Sicherheitssoftware (Viren-Scanner, Firewalls…).

Wogegen prüfen?

Wir haben im Moment eine Sammlung von kritischen Komponenten oder Prozessen, die eines genauen Augenmerkes bedürfen. Aber wogegen prüfen wir die Infrastruktur eigentlich? Welche Hilfsmittel bieten sich hier an? In diesem Bereich gibt es verschiedene Bereiche, wo wir uns Hilfe holen können.

Intern bestehen bei grossen Firmen mittlerweile umfangreiche Regelwerke, wie Weisungen und Policies im Bereich Anforderungen an die Sicherheitsinfrastruktur. Oftmals sind diese jedoch generell, das heisst der Revisor muss das konkrete System gegen die oftmals generischen Weisungen überprüfen. Auch branchenübliche Vorschriften, wie z. B. das Bankengesetz, geben Auskunft über den Qualitätsgrad einer Infrastruktur und können als Massstab genommen werden.

Im Bereich von PKI gibt es die sogenannten Certificate Policy und das Certification Practice Statement. Das Problem ist, dass diese Dokumente nicht einheitlich verwendet werden. Auch welches veröffentlich wird und welches eher intern gehalten wird, ist nicht überall einheitlich, wobei man selten die genaue Implementation einer Sicherheitsvorkehrung beschreibt (dies auch wieder aus Sicherheitsgründen). Diese Dokumente können sehr umfangreich sein und in ihrer internen Fassung sehr genau Auskunft über die Anforderungen an ein solches System geben. Bei der Implementierung dieser Verschlüsselungsinfrastrukturen sind diese jedoch oft noch nicht bereit und eine "Nachbesserung" der Infrastruktur findet aus Kostengründen oft nicht statt. Vor allem im Bereich der PKI sind in Zukunft weitere Vorschriften auch auf Bundesebene zu erwarten, da diese vor allem auch im Zusammenhang mit der Digitalen Signatur und deren Gleichsetzung mit einer "normalen" Unterschrift geregelt werden. Links auf die entsprechenden Seiten sind auf folgenden Seiten zu finden:

- Entwurf zum Bundesgesetz über die elektronische Signatur (BEGS) (http://www.admin.ch/ch/d/sr/7/784.103.de.pdf)
- Ausführungsbestimmungen zur Zertifizierungsdienstverordnung (ZertDV) und BEGS sind als erster Entwurf erhältlich; (http://www.bakom.ch/ger/subpage/?category_104.html)

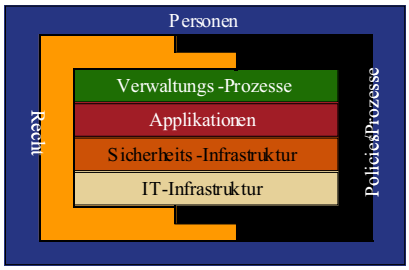
Der Bund führt dabei die sogenannte SAS (Schweizerische Akkreditierungsstelle) ein. Diese ernennt Certification Bodies (Zertifizierungsstellen), die die Zertifizierungsdienstanbieter (Certification Authorities) abnimmt resp zertifiziert.

Weitere Regelwerke, vor allem auch mit internationalem Charakter, sind folgende:

- RFC2527 von IETF (www.ietf.org)
- ANSI X9.79 Financial Services PKI Practices and Policy Framework
- SAS-70 von AICPA (Statement on Audit Standards vom American Institute of Certified Public Accountants); http://www.sas70.com
- CS-2 gemäss Common Criteria (National Institute of Standards and Technology)
- CobiT BS7799 Framework
- WebTrust für die Beurteilung von Internet Service Providers

Zusammenfassung

Bei der Revision von Verschlüsselungssystemen geht es um viel mehr als um die reine Technologie und ich hoffe, ich konnte aufzeigen, warum. Der untenstehende Baukasten soll aufzeigen, in welchem Umfeld sich Verschlüsselungssysteme bewegen.



Diese Bausteine sind von einander abhängig. Die verwendete Schlüsselstärke kann noch so gut und sicher sein. Wenn die dazugehörigen Registrationsprozesse nicht gelebt werden, ist davon das ganze System betroffen. Nachfolgend noch einmal eine kurze Zusammenfassung von prüfenswerten Fragen aus der Sicht des Baukastens:

IT-Infrastruktur

- Wie gut ist die Infrastruktur physisch und logisch gesichert?
- Sind die Betriebssysteme "hardened", d. h. speziell gesichert?

Sicherheits-Infrastruktur

- Wie gut ist die Infrastruktur physisch und logisch gesichert?
- Wer hat Zutritt zu der Sicherheitsinfrastruktur?
- Sind die unterschiedlichen Verantwortlichkeiten auf verschiedene Personen aufgeteilt?
- Wofür wird die Sicherheits-Infrastruktur eingesetzt?

Applikationen

- Besteht für die Applikationen eine "Hintertür" über APIs?
- Welche Authentisierungs-/Authorisierungsmöglichkeiten sichern die Applikationen?
- Sind die Applikationen mit Toolkits gesichert?
- Wie sind die Applikationen in die Sicherheitsinfrastruktur eingebunden?

Verwaltungsprozesse

- Sind die definierten Verwaltungsprozesse im System abgebildet und nachlebbar?
- Sind alle notwendigen Prozesse definiert und dokumentiert?

Recht

- Welche rechtlichen Vorschriften bestehen?
- Welches ist die rechtliche Situation in verschiedenen Ländern?

Policies/Prozesse

- Welche Policies und Prozesse bestehen?
- Werden diese auch gelebt?
- Wer kontrolliert diese regelmässig?

Personen

- Wie sind die Personen im Unternehmen auf sicherheitsrelevante Fragen sensibilisiert?
- Werden die Personen, die mit sicherheitsrelevanter Infrastruktur zu tun haben, einer speziellen Prüfung unterzogen?
- Wie sind Personalbewegungen in den Prozess integriert?

All diesen Fragen sollte bei der Revision Rechnung getragen werden, d. h. sie müssen gegenüber den vorhandenen Definitionen/Weisungen/Regelungen geprüft werden.

Fazit

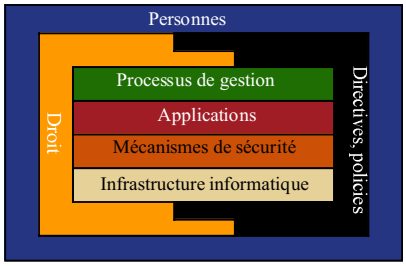
Der Bereich der Revision von Verschlüsselungssystemen ist noch jung und vor allem auch noch Änderungen unterworfen (siehe Bundesregelungen). Hier sind noch Änderungen resp. Konkretisierungen zu erwarten, vor allem auch wegen dem Gebrauch der Digitalen Signatur. Im Bereich von Branchenvorschriften, internen Vorschriften und Vorschriften von Gremien sind aber sehr wohl bereits heute Dokumente und Standards erhältlich, gegen die geprüft werden kann. Wichtig ist es meines Erachtens, vor allem die umliegenden Prozesse und deren Einhaltung genau zu überprüfen. Für die Revisoren eröffnet sich meines Erachtens ein sehr interessantes und zukunftsträchtiges Tätigkeitsgebiet.

Monika Josi,
dipl. Wirtschaftsinformatikerin,
PricewaterhouseCoopers, Zürich

Résumé

Audit des systèmes de gestion des clés de chiffrement

L'audit des systèmes de gestion des clés de chiffrement constitue un domaine nouveau pour les auditeurs. Ce champ est multidisciplinaire et très complexe. Le schéma suivant illustre les différents aspects que l'auditeur doit prendre en compte :



Les techniques de chiffrement sont utilisées aujourd'hui dans différents domaines : l'échange de communications chiffrées, protection par chiffrement du canal de transmission, chiffrement de données enregistrées. L'importance et la priorité de ces différents aspects varient selon le type d'utilisation.

L'auditeur appelé à examiner la gestion de ces technologies devra d'abord vérifier que leur mise en œuvre correspond aux différentes directives et "policies" édictées par l'entreprise dans le domaine de la sécurité. S'agissant de la régularité de la gestion des clés, les Certificate Policy et Certification Practice Statement élaborés par les fournisseurs de ces prestations contiennent des indications importantes sur les mesures de sécurité à respecter. Sur le plan du droit fédéral, les dispositions d'exécution des dispositions régissant la signature électronique contiendront probablement des conditions supplémentaires, dont l'auditeur devra vérifier le respect. Les différents projets sont actuellement en consultation. Sur le plan international, l'auditeur trouvera enfin des modèles et des exemples de meilleures pratiques, ainsi que des recommandations sectorielles, dont il pourra s'inspirer.

Le domaine est nouveau et des adaptations du droit sont attendues ces prochains mois mais l'approche d'audit reste immuable :

1. identifier les risques et les obligations légales
2. vérifier que les procédures mises en place couvrent de manière adéquate ces risques et tiennent compte des obligations légales
3. vérifier que ces procédures sont respectées

Séminaire de la Chambre : e-business

Start-up.com

Approche lors d'un audit informatique d'une *Start-up* dans *l'e-commerce*

L'exposé traite de l'approche effectuée lors d'un audit informatique (cas pratique) d'une nouvelle société de la *Net-économie*.

Introduction

Nous parlerons des différents points sensibles liés directement ou indirectement à l'informatique qui doivent être pris en considération. En premier lieu, après avoir décrit l'activité de cette nouvelle "e-société", nous parlerons des risques et des contrôles à vérifier. Ensuite, nous évoquerons les observations réelles rencontrées lors de l'audit de cette entreprise.

Description de l'activité de l'entreprise

Le but de cette start-up est la vente de biens de consommation par Internet. Toutes les commandes sont traitées directement depuis le site Web et les livraisons sont réalisées par une société de logistique indépendante. La structure de la société est la suivante :

- Marketing
- Achats
- Client Relation Management (Help Desk & Support client)
- Contrôle des commandes client et facturation
- Comptabilité/Finances
- Informatique

Analyse de risques

Les risques inhérents au personnel, à la propriété intellectuelle des logiciels et à la dépendance technologique sont des caractéristiques majeures des sociétés dans l'e-commerce. Vous trouverez ci-après la liste des risques identifiés lors de cette intervention, soit :

1 La confidentialité, l'intégrité et la sécurité des données
2 Le hacking
3 La disponibilité du S.I. (Système d'Information, soit le Site Web et la production)
4 La catastrophe
5 La dépendance sur les ressources humaines
6 Les facteurs d'influence externes (propriété intellectuelle…)
7 La dépendance technologique

Revue des Contrôles

Les risques étant posés, nous allons survoler quels seraient les contrôles à mettre en place dans le but de maîtriser les risques énoncés précédemment, à savoir :

1 Comment est gérée la sécurité (logique, physique) ?
2 Quelles sont les procédures de contrôle des transactions, des sauvegardes ?
3 Quelles sont les procédures mises en place pour assurer la disponibilité du système et du site Web ainsi que la surveillance de hacking ?
4 Quels aspects doit-on tenir compte pour la gestion des ressources humaines? Le système est-il bien dimensionné, quel est son cycle de vie ?
5 Comment est préparé le plan de secours (BCM) ?

Observations rencontrées

Ensuite, nous traiterons des observations et des recommandations que nous avons évoquées lors de l'audit de cette PME.

Conclusion

Nous avons constaté que les points suivants nécessitent une attention particulière:

- L'appartenance de la propriété intellectuelle
- Le niveau de dépendance technologique (du site Web, des outils utilisés et de la mouvance du marché Internet)
- Les procédures de sauvegarde
- La sécurité physique et logique
- Le plan de secours (quasi inexistant dans la plupart des cas)
- La dépendance et la fidélisation des ressources humaines

La *Net-économie* a vu naître beaucoup de société et de services supplémentaires apportant une nouvelle dimension au consommateur, mais va-t-elle tout bouleverser ? L'avenir nous le dira…

Stéphane Vigna,
dipl. informaticien de gestion,
KPMG, Genève

e-business und e-commerce

WebTrust – unabhängige Validierung von e-business-Anwendungen

Die Veränderungen, die durch die Einführung von internet-basierten Geschäftsprozessen (e-business) in Unternehmen geschehen, stellen das Management und die Revision vor neue Herausforderungen.

Für den IT-Revisor stellt sich in der Regel die Frage nach den spezifischen Risiken durch die Verwendung dieser neuen Technologien. Durch die Vernetzung der IT-Systeme und -prozesse ist sowohl der Datenfluß durch das gesamte Unternehmen als auch die Abarbeitung "konventioneller" Geschäftsprozesse betroffen. Für das Management wesentlich ist aber auch die Sicherheitsperzeption von außen, denn Misstrauen seitens der Geschäftspartner und potentieller Kunden kann den unternehmerischen Erfolg im e-business insgesamt gefährden.

Mit der Einführung der WebTrust-Prüfung durch die internationalen Berufsorganisationen der Wirtschaftsprüfer ist es den Unternehmen möglich, in Form eines Siegels (Seal) und eines im Internet veröffentlichten Kurztestats nach außen zu dokumentieren, dass wesentliche Sicherheitsaspekte der e-business-Anwendung einer unabhängigen Prüfung unterzogen wurden. Nähere Informationen zu WebTrust können auf www.webtrust.org gefunden werden.

Bei WebTrust-Prüfungen erfolgt eine echte, sozusagen "klassische" IT-Revision bezüglich folgender Aspekte/Module:

- Sicherung des Zugangs zu den Daten (Security)
- Schutz personenbezogener Daten (Privacy)
- Vertraulichkeit (Confidentiality)
- Vereinbarungsgemäße Vertragsabwicklung (Transaction Integrity)
- Verbindlichkeit (Non-Repudiation)
- Verfügbarkeit (Availability) oder
- spezifischer Aussagen des Betreibers (Customized Disclosures)

Neu in der im wesentlichen ab 1. März 2001 in Kraft getretenen Version 3.0 der WebTrust-Programme ist der modulare Aufbau, der es ermöglicht, WebTrust-Prüfungen auf die Bedürfnisse der spezifisch beim Unternehmen vorliegenden Geschäftsprozesse im e-business zu optimieren. So wird ein Unternehmen mit Endkundenproduktgeschäft an der Prüfungsaussage zum Schutz personenbezogener Daten interessiert sein, während es keinerlei Anforderungen an Verfügbarkeit seiner Dienste stellt. Für einen Application-Hosting-Dienstleister gilt das genaue Gegenteil, während für den Online-Broker – der für Endkunden Intra-Day-Trading ermöglicht – beide Aspekte von hoher Wichtigkeit sind.

Die Prüfkriterien sind international einheitlich und ebenfalls im Internet veröffentlicht (www.aicpa.org, www.cica.ca), so dass der Qualitätsstandard objektiv nachvollzogen werden kann. Allen Kriterien gemeinsam ist, dass eine Prüfung des für den jeweiligen Aspekt eingerichteten Internen Kontrollsystems erfolgen muss. Inhaltlich wird der oft vernachlässigte Bereich IT-Audit hiermit stark aufgewertet, da eine Art Wirtschaftsprüfertestat für Aspekte der IT-Sicherheit erteilt wird.

Die WebTrust-Prüfung muss entsprechend anerkannter Prüfungsstandards geplant und durchgeführt werden; diese sind international ähnlich und weitgehend deckungsgleich mit den Standards für IT-Revision von ISACA. Prüfer müssen über Kenntnisse der anwendbaren Standards sowie der technischen Grundlage der IT-gestützten Geschäftsprozesse verfügen. Als Prüfer bieten sich hier insbesondere CISAs an, da sie diese Kenntnisse und Erfahrungen bereits nachgewiesen haben.

Während die Erteilung des WebTrust-Seal aus lizenzrechtlichen Gründen nur durch dafür zugelassene Wirtschaftsprüfer erfolgen darf, können die WebTrust-Kriterien natürlich auch von internen Revisoren oder IT-Sicherheitsberatern als anerkannter Qualitätsmaßstab für eigene Tätigkeiten herangezogen werden. Insbesondere bietet es sich an, im Rahmen eines Vorprojektes zur eigentlichen WebTrust-Zertifizierung das Einhalten der Kriterien zu bewerten.

Darüber hinaus könnte es sein, dass ein Wirtschaftsprüfer bei der Durchführung der WebTrust-Prüfung auf entsprechende Prüfungsergebnisse der IT-Innenrevision zurückgreift oder einzelne Prüffelder durch externe Spezialisten bearbeiten lässt. Notwendig bleibt in jedem Fall die "Prozessunab-

hängigkeit" des Auditors – der zuständige Firewall-Administrator kann nicht objektiv die Zugriffssicherheit des Unternehmensnetzes gegenüber dem Internet prüfen. Auch klar ist, dass das Management des Unternehmens letztlich die Verantwortung für die IT-gestützten Geschäftsprozesse und deren Kontrolle behält. Der Prüfer beurteilt, ob dieser Verantwortung angemessen nachgekommen wurde.

Das German Chapter des ISACA hat die Thematik WebTrust als fachlichen Akzent im Rahmen der Mitgliederversammlung am 2. März 2001 gesetzt. Als Referenten standen Dr. Gross, Geschäftsführer des Instituts der Wirtschaftsprüfer e.V., und der Verfasser zur Verfügung. Die Vorträge – hier wird auch auf Fragen der Haftung des WebTrust-Prüfers und auf exemplarische Prüfungshandlungen zu den einzelnen Modulen eingegangen – stehen den Mitgliedern auf www.isaca.de zum Download bereit.

Michael Schneider, CISA, CIA,
Arthur Andersen, München

e-business und e-commerce

Ergänzung der Sicherheitsarchitektur durch ein Intrusion Detection System

Management Summary

Entwicklungen in der IT-Sicherheit haben deutlich gezeigt, dass eine Firewall alleine keinen ausreichenden Schutz vor Hackerangriffen bietet. Deshalb ergänzt heutzutage ein Intrusion Detection System (IDS) eine zeitgemässe IT-Sicherheitsarchitektur. Die Einbindung eines IDS in das Unternehmensnetzwerk – sowohl auf der Ebene der entsprechenden Policies als auch auf der Ebene der technischen Implementation – stellt die verantwortlichen Personen aber vor keine leichte Aufgabe. Dabei verlangen die folgenden Bereiche ein spezielles Augenmerk:

- Platzierung der Sensoren
- Konfiguration der einzelnen Sensoren
- Alarmierungsmechanismen
- Aktualisierung der Signatur-Datenbank

Bei einer erfolgreichen Implementation eines IDS werden die meisten gefährlichen Angriffe erkannt und gleichzeitig die Anzahl falscher "Positivmeldungen" so gering wie möglich gehalten. Dies ist eine zentrale Voraussetzung für die Akzeptanz und die Wirksamkeit eines IDS und erlaubt proaktives Handeln.

Für die Auswahl eines IDS stehen viele Kriterien zur Auswahl – auch einige, die sich diametral entgegenstehen. Es ist deshalb wichtig, dass vor jedem Kauf und jedem Einsatz eines IDS eine gründliche Evaluation vorangeht, in der eine Priorisierung und Gewichtung der Anforderungen auf die spezifischen Bedürfnisse hin vorgenommen werden sollte. Dies legt den Grundstein für eine zeitgemässe und erfolgreiche Erweiterung der Sicherheitarchitektur durch ein Intrusion Detection System.

Einführung

Firewalls sind ein bewährtes und bekanntes Mittel, um den Zugang eines Unternehmensnetzes an das Internet sicher zu gestalten. Während die Firewall diesen Auftrag erfüllt, ist sie jedoch nur ein Glied in einer Kette von verschiedenen Sicherheitsmassnahmen.

Viele Angriffe nutzen Applikationsfehler (Web-, FTP-, Mailserver usw.) aus, die mit einer Firewall nicht erkannt bzw. verhindert werden können. Mit der Implementation eines IDS wird eine zusätzliche Ebene der Sicherheit errichtet, um die verschiedensten Arten von Angriffen besser erkennen und so schneller handeln zu können.

Um einen "Einbruch" erkennen zu können, muss vorgängig definiert werden, was als Angriff zu werten ist. Eine Implementierung eines IDS ist erst auf der Basis einer Security Policy möglich. Denn nur wenn vorgängig definiert wurde, was auf den Systemen

erlaubt bzw. nicht erlaubt ist, können Abweichungen davon festgestellt oder noch besser, die Systeme davor geschützt werden. Grundsätzlich kann jede Aktion, die die Vertraulichkeit, Integrität und Verfügbarkeit von Ressourcen gefährdet, als Einbruch bzw. als Angriff verstanden werden.

Die heutigen IDS lassen sich grob in zwei Arten unterteilen:
Netzwerkbasierende IDS. Solche Systeme untersuchen und analysieren den Datenverkehr ihres Netzwerksegments und vergleichen diesen mit den implementierten Regeln. Jedes Datenpaket wird dabei auf bestimmte Signaturen eines bekannten bzw. typischen Angriffes hin untersucht. Mögliche Signaturen können z. B. sein:

- String Signaturen: Eine Zeichenkette, die auf einen möglichen Angriff hindeutet (z. B. cat/etc/passwd)
- Port Signaturen: Ein Verbindungsaufbauversuch zu einem bekannten Port usw.

Hostbasierende IDS. Solche Systeme untersuchen und analysieren den Zugriff auf ein bestimmtes System und vergleichen es mit den implementierten Regeln. Sie sind bei Systemen im Einsatz, auf denen schützenswerte Daten abgelegt sind und die deshalb einen besonders hohen Schutz benötigen (z. B. Web-, Datenbank- und Mailserver, Domain Controller, usw.). Bei hostbasierenden IDS muss wiederum zwischen zwei Arten unterschieden werden:

- Netzwerkmonitore – Diese Systeme analysieren nur den eingehenden Datenverkehr des zu schützenden Systems. Damit können z. B. Verbindungsanfragen nur zum überwachten System auf bestimmte Ports erkannt werden. Sie unterscheiden sich somit von einem netzwerkbasierenden IDS in dem Sinne, dass nicht der gesamte Datenverkehr auf dem Netzwerksegment überwacht werden kann.
- Hostmonitore – Sie überwachen Dateien, Dateisysteme und Aktionen der Benutzer auf dem System selbst, um ungewöhnliche Aktivitäten oder bereits erfolgte Einbrüche festzustellen.

Die Komponenten, mit denen Abweichungen von den vordefinierten Regeln erkannt werden, werden häufig als Sensoren bezeichnet. Die Konfiguration dieser Sensoren sowie die Aufzeichnung und Auswertung der eingehenden Alarmmeldungen erfolgt von einer Management-Station aus. Je nach Implementation der festgelegten Policy können entsprechende Gegenmassnahmen eingeleitet werden (z. B. Trennen der Verbindung, Alarmierung eines Mitarbeiters, usw.)

Die Aktion jeder einzelnen IDS-Komponente (ob netzwerk- oder hostbasierend), die nach einer Verletzung der implementierten Regeln erfolgt, kann meist unabhängig von anderen Systemkomponenten erfolgen. Dabei wird zwischen einer aktiven und einer passiven Reaktion des IDS unterschieden.

- Die meisten IDS sind passiv, d. h. falls eine Abweichung von der Policy erkannt wird, erfolgt eine Alarmierung in einer frei wählbaren Form (e-mail, Telefon, SMS, usw.). Die Gegenmassnahmen müssen dann von den alarmierten Mitarbeitern eingeleitet werden.
- Im Gegensatz zu den passiven IDS leiten aktive IDS je nach Konfiguration die Gegenmassnahmen selbstständig ein. Als Gegenmassnahmen kommen dabei sowohl die Umkonfiguration des zu schützenden Objektes und dessen Umfeld, als auch der Versuch das Angreifersystem selbst ausser Gefecht zu setzen, in Frage.

Stärken und Schwächen

Die Implementation eines IDS stellt die verantwortlichen Personen vor keine leichte Aufgabe. Idealerweise sollten alle gefährlichen Angriffe erkannt und gleichzeitig die Anzahl falscher "Positivmeldungen" so gering wie möglich gehalten werden. Dies erweist sich in der Praxis als schwieriges Unterfangen. Deshalb stellt die Implementation der Security Policy die grösste Schwierigkeit bei der Einführung eines IDS dar. Um einen hohen Schutzgrad zu erreichen, müssen die Policies für jeden einzelnen Sensor der Situation angepasst werden. Wird dies unterlassen, kann z. B. eine Flut von Alarmmeldungen (z.B. via e-mail, usw.) generiert werden und somit den Mail-Server überlasten.

Den Stärken eines IDS (zentral verwaltbar und konfigurierbar, automatische Updates und vielseitige Alarmierungsmöglichkeiten) stehen teilweise erhebliche Schwächen gegenüber. Bei den meisten Systemen werden nur bekannte Angriffsmuster erkannt. Eine ständige Aktualisierung der Signatur-Datenbank ist damit – wie bei Virenscannern – zwingend erforderlich.

Der Nutzen eines IDS hängt stark von dessen Planung und entsprechender Implementation und Integration in das Netzwerkumfeld ab. Ein schlecht integriertes IDS wiegt den Benutzer in falscher Sicherheit und kann somit mehr schaden als nützen. Im Integrationsprozess sollte auch die Problematik der Vorbereitung des Umfeldes

wie Security-Konzepte, Netzwerk-Konzepte, Policies, Organisation, Abläufe usw. behandelt werden. Trotz den dafür notwendigen Aufwendungen stellt ein IDS eine nützliche und gewinnbringende Ergänzung jeder Sicherheits-Architektur dar.

Zur Zeit können nicht alle Attacken (z. B. verschlüsselte Attacken, usw.) durch Firewall, IDS, Virenscanner und die Netzwerkstruktur abgedeckt werden. Dennoch lassen sich in einer optimalen Verbindung der verfügbaren Möglichkeiten eine nach heutigen Gesichtspunkten (mit kontinuierlicher Anpassung und Funktionserweiterung), "sicherere" Umgebung schaffen.

Erfolgsfaktoren für die Einführung

Um einen möglichst hohen Nutzen aus der Implementation eines IDS erzielen zu können, müssen im Minimum folgende Faktoren in der Konzeption beachtet werden:

- Platzierung der Sensoren
- Konfiguration der einzelnen Sensoren
- Alarmierungsmechanismen
- Aktualisierung der Signatur-Datenbank

Der Platzierung der einzelnen Sensoren kommt eine grosse Bedeutung zu. Denn wie bereits erwähnt wurde, kann mit Netzwerk-Sensoren nur der Datenverkehr im eigenen Netzwerksegment überwacht werden. Wird der Sensor im internen Netzwerk platziert, identifiziert das IDS Angriffe "von innen" und Firewall-Regeln, die nicht korrekt arbeiten oder falsch konfiguriert sind. Die hostbasierenden Sensoren überwachen die Benutzeraktivitäten auf den jeweiligen Systemen und sollten auf allen kritischen und wichtigen Systemen, die einen speziellen Schutz benötigen (zum Beispiel Web- und Datenbankserver usw.), platziert werden.

Jedes IDS steht und fällt mit der Art und Weise, wie es auf Ereignisse reagiert, weshalb der Implementation der Alarmierungs-Policy eine entscheidende Rolle zukommt. Da die einzelnen Sensoren unterschiedliche Systeme und Netzwerksegmente überwachen, müssen die Policies für jeden einzelnen Sensor der jeweiligen Situation angepasst werden. Dies beinhaltet sowohl die Abstimmung der Angriffsarten auf das zu schützende System, als auch die Festlegung der Regeln, wann ein Alarm ausgelöst werden soll. Dabei ist es wichtig, dass die Anzahl falscher "Positivmeldungen" minimiert wird, denn bei allzu häufigen Fehlalarmen sinkt die Akzeptanz des IDS beträchtlich.

So ist es bei unsorgfältiger Implementation der Alarmierungs-Policy möglich, dass der Administrator wegen eines gewöhnlichen Portscans mitten in der Nacht einen automatischen Anruf auf sein Mobiltelefon erhält, was mit der Zeit eine Deaktivierung der Alarmierung zur Folge haben könnte.

Abhängig vom Bedrohungspotential des Angriffs können bei den meisten IDS verschiedene Alarmierungsmechanismen aktiviert werden, die ebenfalls vor der Inbetriebnahme mit dem unternehmensweiten Sicherheits-Konzept abgestimmt werden sollten.

Folgende Alarmierungsmechanismen finden sich in den meisten IDS:

- Auf einer zentralen Konsole werden die Meldungen der verschiedenen dezentralen Sensoren gesammelt, entsprechend des Gefahrenpotentiales priorisiert und danach dargestellt. Dies ist die visuelle (akustische) Alarmierung an der Management-Konsole.
- Eine Fern-Alarmierung des Administrators ist in fast allen Fällen über e-mail, Telefon, oder SMS möglich.

Die meisten IDS bieten noch diverse andere Alarmierungsmöglichkeiten an, die aber nur in seltenen Fällen benutzt werden.

Um Angriffe wirksam identifizieren zu können, ist eine ständige Aktualisierung der Datenbank mit den neuesten Signaturen unumgänglich. Zusätzlich müssen die Logdateien und System-Reports periodisch überprüft werden. Wird dies unterlassen, so könnten Hacker durch die neuesten Sicherheitslücken ins Netz gelangen oder durch eine Denial-Of-Service-Attacke das Netz ausser Gefecht setzen, weil dieses Angriffsmuster im IDS noch nicht aktualisiert ist. Der Betrieb eines IDS erfordert deshalb ständige Überwachung, intensive Wartung (Change- und Release-Management) und ist sehr arbeitsintensiv. Das System muss häufig manuell gepflegt und unterhalten werden, da noch wenige Automatismen vorhanden sind. Ausserdem ist es wichtig, dass die aktuelle Konfiguration des IDS nur einem begrenzten Personenkreis bekannt ist (Berechtigungskonzept, "Need-to-Know" Prinzip).

Sollte trotzdem ein Angriff erfolgen und entdeckt werden, so sind die Urheber von Angriffen meist nur schwer zu identifizieren. Findige Hacker melden sich zunächst nacheinander an

unverdächtigen Rechnern an. Die begrenzten Möglichkeiten zum Aufspüren des Angreifers sind:

- Ermittlung des Eigentümers der IP-Adresse z. B. über Dienste whois oder einen DNS-Lookup.
- Rückverfolgung der Route bis zur angreifenden IP-Adresse mittels traceroute.
- Nutzung der verschiedenen Informationsdienste wie finger oder who, um weitere Daten über die IP-Adresse zu erhalten.

Gegenangriffe sind eine zweite Möglichkeit der Abwehr, von der wir aber dringend abraten möchten. In den meisten Fällen werden mit solchen Gegenangriffen die Falschen getroffen, da Angriffe meist über ahnungslose Dritt-Systeme getätigt werden.

Verfügbare Systeme

Auf dem Markt gibt es zur Zeit diverse Anbieter von IDS-Lösungen. Alle grösseren Anbieter von Sicherheitslösungen haben ein entsprechendes IDS im Programm. Sie unterscheiden sich in verschiedenen Bereichen. Es kann keine generelle Aussage über die "beste" Wahl eines Produktes gemacht werden. Die Evaluation der IDS-Produkte sollte der aktuellen Situation, dem jeweiligen Einsatzort sowie dem Umfeld angepasst werden. IDS-Produkte sind in allen Preisklassen verfügbar, wobei das Preisspektrum von gratis bis zu mehreren tausend Franken reicht. Dabei triff die Regel, je höher der Preis, desto besser das Produkt, nicht automatisch zu.

Grundsätzlich können folgende Kriterien (unabhängig von deren Einsatz und Ausführung und/oder Netzintegration) für die Beurteilung eines IDS herangezogen werden:

- Das IDS sollte ohne menschliche Überwachung fortwährend laufen. Das IDS sollte genug zuverlässig sein, um im Hintergrund des Systems ohne Beobachtung laufen zu können.
- Das IDS sollte gegenüber Störungen wenig anfällig sein. Ein Systemabsturz sollte verkraftet werden können, ohne dass die manuelle Rekonstruktion der IDS-Informationsdatenbank notwendig wird. Ist dies nicht der Fall, so würde der System-Wiederanlauf unnötigerweise verzögert.
- Das IDS selbst sollte Angriffen widerstehen. Das System sollte sich selbst überwachen, um sicherzustellen, dass es nicht selber einem Angriff erlegen ist.
- Das IDS sollte minimale Zusatzaufwendungen (Kosten, Aufwand, Verkehr, usw.) verursachen (Kosten-Nutzen-Betrachtung).
- Das IDS sollte Abweichungen vom normalen Verhalten zuverlässig beobachten und melden.
- Das IDS sollte einfach ins Netzwerk integrierbar sein. Da jedes System unterschiedliche Charakteristiken hat, sollte sich das IDS an diese Systeme leicht anpassen lassen.
- Das IDS sollte sich änderndem Systemverhalten über die Zeit hinweg anpassen können, da sich die Systemprofile ändern können und somit die Angriffs-Identifikation angepasst und aufdatiert werden können sollten.
- Das IDS sollte nicht getäuscht werden können.
- Das IDS sollte verständlich und benutzerfreundlich in der Bedienung und im Unterhalt sein und entsprechend zuverlässige und präzise Meldungen liefern (besonders wichtig bei unerfahrenen Mitarbeitern und in kleinen Firmen).
- Ein IDS sollte einfach konfigurierbar und integrierbar sein. Die Konfiguration sollte jederzeit nachvollziehbar sein. Die Dokumentation der Umgebung muss einfach und für Dritte nachvollziehbar und kontrollierbar sein.
- Das IDS sollte eine hohe Erkennungsdichte haben. Die Anzahl der erkannten Angriffe muss breit abgestützt sein und im Hinblick auf künftige Situationen adaptierbar sein.
- Ein IDS sollte skalierbar sein. Speziell die Leistungsfähigkeit des Systems sollte skalierbar sein, um potentielle Anwendungen, Weiterentwicklungen und Situationen unterstützen zu können.

Aus der oben aufgeführten Liste ist ersichtlich, dass sich die einzelnen Kriterien häufig diametral gegenüberstehen. Deshalb ist es wichtig, dass jedem Kauf und jedem Einsatz eines IDS eine gründliche Evaluation vorangeht, in der eine Priorisierung und Gewichtung der Anforderungen auf die spezifischen Bedürfnisse hin vorgenommen werden sollte.

Allgemein – wenn es die Mittel zulassen – sind mehrfache IDS-Lösungen zu empfehlen, die netzwerk- und hostbasierende Sensoren miteinander koppeln. Mit mehreren solchen "Stufen", kann die Sicherheit massgeblich erhöht werden (was mit der Situation bei Antivirussoftware, Firewall, usw., verglichen werden kann).

Ausblick

Die aktuellen Entwicklungen in der IT Sicherheit haben gezeigt, dass eine reine Firewall-Lösung keinen absoluten Schutz vor internen und externen Angriffen bietet. Intrusion Detection Systeme sind ein wichtiger Bestandteil einer zeitgemässen Unternehmenssicherheitsstrategie. Das IDS war lange Zeit nur am Rande ein Thema, das nun aber immer stärker in der Praxis Einsatz findet. Für den Einsatz auf breiter Basis muss sich das IDS noch weiter entwickeln, da die zur Zeit verfügbaren Systeme noch einige Schwachpunkte haben. Die Zuverlässigkeit und die Automatismen müssen verbessert sowie die Möglichkeiten der Definition von Verstössen weiter verstärkt werden.

Ein Alarm sollte erst dann ausgelöst werden, wenn es sich um eine ernstzunehmende Attacke handelt. Das System sollte mehr "Intelligenz" erhalten, um sich ändernden Situationen anpassen zu können. Damit würde die Konfiguration vereinfacht und es wäre möglich eine Reaktion zu erlauben, die der jeweiligen Gefährdung angepasst ist. Die Definition der Regeln ist heute aber noch recht rudimentär und grob, so dass der Einsatz wissensbasierter oder neuronaler Netze für die Erkennung von neuen Angriffsarten wünschenswert wäre.

Trotzdem sind heutige IDS – sofern deren Einsatz durch geeignete Policies festgelegt und das IDS richtig integriert ist – ein wichtiger Bestandteil einer unternehmensweiten Sicherheits-Architektur. Somit darf man gespannt sein, welche Entwicklungen in diesem – einem doch zumindest für Europa noch jungen – Bereich in nächster Zukunft auf uns zukommen wird.

Markus Limacher, Esther Pines, PricewaterhouseCoopers

Die Autoren arbeiten bei PricewaterhouseCoopers im Bereich "Telecom and Network Services", wo unter anderem Dienstleistungen in den Bereichen Konfiguration, Integration, Implementation und Review von IDS-Systemen angeboten werden.