Outsourcing: Aus den Augen aus dem Sinn?

Die Sicherheitsproblematik beim IT-Outsourcing in privaten Unternehmungen

Peter R. Bitterli, CISA, Inhaber Bitterli Consulting AG, Zürich
prb@bitterli-consulting.ch

Immer mehr werden Informatikaufgaben an Dritte ausgelagert. Auch wenn es gute Gründe fürs Outsourcing gibt: Damit handelt sich das outsourcende Unternehmen erhebliche, oft sogar untragbare Risiken für die Informationssicherheit ein.

Es mag viele und auch gute Gründe dafür geben, bestimmte Informatikaufgaben auszulagern. Häufig werden aber zwei Aspekte des Outsourcings wenig, ja zu wenig beachtet. Dieser Artikel beschränkt sich auf diese beiden Aspekte: Auf die generellen Auswirkungen von Outsourcing auf die Informationssicherheit einerseits und auf das Outsourcing von sicherheitsrelevanten Tätigkeiten wie System- oder Firewall-Management andererseits.

Auswirkungen des Outsourcings auf Informationssicherheit

Am Beispiel von Putzdienst oder Bewachung sei das grundsätzliche Risiko von Outsourcing erläutert. Beide Bereiche gelten als besonders «gefährlich». Nicht etwa, weil sich in diesen Berufsgruppen überdurchschnittlich viel Kriminelle tummeln, sondern weil diese Personen erstens freien Zugang zu (fast) allen Räumen erhalten und zweitens zu Zeiten arbeiten, an denen sonst niemand anwesend ist. Dieser ungehinderte Zugang führt schon alleine, erst recht aber in Kombination mit der fehlenden Überwachung zu einem erhöhten Potenzial, einen Schaden zu erleiden, was durch Beispiele im Bereich von Wirtschaftsspionage oder Sabotage eindrücklich belegt ist.

Doch lassen sich diese Erkenntnisse auch auf die Auslagerung von Informatikdienstleistungen übertragen? Im Zusammenhang mit Outsourcing werden immer wieder dieselben Problembereiche genannt, welche nachfolgend auf ihre Auswirkungen auf die Informationssicherheit untersucht werden sollen. Es geht dabei nicht um Massnahmen zur Reduktion dieser typischen Probleme, sondern einzig und allein um die Frage der Sicherheit.

Schwer lösbare Haftungsfragen

Die komplexen Outsourcing-Vertragswerke enthalten typischerweise Haftungsausschlussklauseln. Besteht aber genügend Bereitschaft des Auftragnehmers für Investitionen in Qualität und Sicherheit, wenn er für die durch ihn verursachten Ausfälle nicht haftbar gemacht werden kann?

Unklare finanzielle Stabilität des Outsourcing-Partners

Durch den Einbruch unzähliger Dotcom-Firmen tauchte der Dienstleistungsbedarf weit unter die Vorjahreszahlen ab. Es musste an allen Ecken und Enden gespart werden. Das bedeutete Entlassungen, keine Schulung mehr für Spezialisten, Rückverkauf bereits gebrauchter Disks (mit vertraulichen Daten darauf[1]) bis zur Übernahme durch die Konkurrenz. Alle aufgeführten Beispiele erhöhen die bereits vorhandenen Risiken bezüglich Vertraulichkeit, Integrität und Verfügbarkeit. Im Extremfall stellt der Diensteanbieter von einem Tag auf den anderen den Betrieb ein und verkauft dann noch die Daten seiner Kunden an Dritte.

Massnahmen für Kontinuität der Verarbeitung nicht überprüfbar

Es ist schon schwierig genug, im eigenen Betrieb eine ausreichende Wiederanlaufpla-

nung für die IT- und Geschäftsprozesse aufzubauen und dann mit genügender Häufigkeit und Intensität zu testen. Wie aber soll ein Dienstleistungsrechenzentrum seinen eigenen Notfallplan ausreichend testen, wenn von so einem Test alle Kunden betroffen sind?

Versicherungsausschlüsse

Ein vorsichtiges Unternehmen schliesst eine Betriebsunterbruchversicherung ab – oft in Unkenntnis der Tatsache, dass solche Verträge oft eine Deckung ausschliessen für den Fall, dass der Unterbruch in den ausgelagerten Geschäftsbereichen verursacht wurde. So dürften durch die Kombination der Haftungsausschlüsse in den Outsourcingverträgen und den Deckungsausschlüssen in den Versicherungsbedingungen derartige Schäden beim Unternehmen selber verbleiben[2].

Outsourcing innerhalb des Outsourcings

Es wäre illusorisch zu glauben, dass der beauftragte Dienstleister alle von ihm angebotenen Dienstleistungen selber erbringt. Auch er steht unter Kostendruck und muss sich auf seine Kernkompetenz konzentrieren. Er lagert daher seinerseits Tätigkeiten wie Bewachung und Monitoring an Dritte aus. Dieses sogenannte «Double Outsourcing» ist für den Auftraggeber kaum transparent und erst recht nicht kontrollierbar. In einer Untersuchung der InformationWeek[3] betrachtete mehr als die Hälfte der befragten Unternehmen die Existenz von Outsourcing-Unterauftragnehmern als problematisch. Folgende Punkte wurden in der Studie besonders kritisiert: Servicequalität 67%, Kosten 30%, Computerviren 17%, Sicherheit 10%. Im weiteren erwähnten 40% der Befragten im Zusammenhang mit Unterauftragnehmern Probleme wie das Fehlen technischer Fertigkeiten, die schlechte Kommunikation, die ungenügende Dokumentation und die zu langsame Reaktion. Kann man sich unter diesen Voraussetzungen vorstellen, dass die Anforderungen an Verfügbarkeit, Integrität oder Vertraulichkeit erfüllt werden?

Neue Risiken

Outsourcing erhöht zudem für ein einzelnes an sich ungefährdetes Unternehmen die Eintretenswahrscheinlichkeit bezüglich terroristischen Aktivitäten. In den verschiedenen Dienstleistungsrechenzentren stehen heute die Server der grössten und bekanntesten Unternehmen – was sie zu einem attraktiven Ziel für politisch oder wirtschaftlich[4] motivierten Terrorismus macht!

Outsourcing sicherheitsrelevanter Tätigkeiten

Der sichere Betrieb von Anwendungen setzt Kenntnisse und Ressourcen im IT-Sicherheitsumfeld voraus. Für viele Unternehmen ist es unmöglich, genügend Mitarbeiter mit dem notwendigen Spezialwissen zu finden, auszubilden oder zu halten. Zudem benötigen 7x24 Stunden verfügbare Systeme auch 7x24 Stunden an Monitoring und Support und damit personelle Ressourcen in bisher ungekannter Grösse[5]. Unter diesen Voraussetzungen ist es verständlich, dass auch grosse Unternehmen solche Tätigkeiten an Dritte auslagern.

Beim Outsourcing sind die Risiken bezüglich Informationssicherheit – vor allem bei geschäftskritischen Anwendungen – in den meisten Fällen nicht tragbar.

Doch mit der Auslagerung sicherheitsrelevanter Aktivitäten geht ein Unternehmen eine ganze Reihe neuer Risiken ein.

Monitoring und System-Management

Das Monitoring eines Systems erfolgt meist durch automatisierbare Funktionen wie das «Anpingen» von IP-Adressen oder bestimmten URL und stellt damit noch kein besonderes Risiko dar. Laufen jedoch die Systeme nicht korrekt, sind Eingriffe mit hohen Systemberechtigungen notwendig – vom Neustart bis hin zum komplett neuen Aufsetzen eines Systems mit Installation von Betriebssystem, Sicherheitsflicks usw. Das heisst letztlich, dass das Dienstleistungsunternehmen uneingeschränkte Kontrolle über die ausgelagerten Systeme, Anwendungen und Daten erhält!

Zwingendes Backup

Backups sind auch für ausgelagerte Systeme zwingend. Dabei müssen umfangreiche Datensicherungen lokal erfolgen. Da es aber viel zu umständlich ist, mittels direkt an die einzelnen Komponenten angeschlossenen

Backupsystemen diese Datensicherungen durchzuführen, werden üblicherweise alle wichtigen Komponenten an ein spezielles Backupnetz angeschlossen, bei dem die Daten verschiedener Kunden auf demselben System (!) gesichert werden.

Firewall-Management

Firewall-Management beinhaltet die Konfiguration und Administration der Firewall. Geregelt wird z.B. mittels Filterregeln, wer (welche Netzwerk-Absenderadresse) mit wem (welche Zieladresse) welche «Beziehung» (Dienst resp. Port-Nummer) aufnehmen kann[6]. Die mit der Administration beauftragte Person hat somit volle Kontrolle über den Zugang zu allen von der Firewall geschützten Systeme.

Intrusion Detection and Response

Präventive Massnahmen wie Firewall-Filter alleine garantieren noch keine ausreichende Sicherheit. Zahlreiche Ports (z.B. für http, https, DNS-Abfragen) müssen in jeder Firewall offen bleiben. Es gibt aber bestimmte Angriffe, welche durch diese Löcher in die geschützten Zonen eindringen und dort Unheil stiften können. Mit zusätzlichen Überwachungskomponenten (Sensoren) werden zu schützende Netzwerke und/oder die daran angeschlossenen Systeme permanent beobachtet und in Echtzeit auf verdächtige Verhaltensmuster überprüft.

VPN-Konfiguration und -Management

Virtuelle private Netze ermöglichen unter anderem durch Anwendung von Verschlüsselungsverfahren den sicheren externen Zugriff auf das firmeninterne Netz. Konfiguration, Implementation, Betrieb und Administration von VPN bedingt aber neben Fachkenntnissen wiederum hohe Berechtigungen. Auch hier erhält ein mit diesen Aufgaben Beauftragter die volle Kontrolle.

Für alle hier vorgestellten sicherheitsrelevanten Tätigkeiten benötigt die beauftragte Firma hohe Berechtigungen sowie einen ungehinderten (logischen) Zugriff auf die davon betroffenen Komponenten. Sie hat damit vollen – und von niemandem überwachten – Zugriff auf alle gespeicherten Daten und kann die Geschäftsprozesse fast beliebig manipulieren. Damit noch nicht genug: Weil ja von allen Servern die Daten gesichert, alle Server und Firewall administriert sowie alle Server und Firewall und die sie verbindenden Netze überwacht werden müssen, werden diese Komponenten mit zusätzlichen Kommunikationsnetzen miteinander verbunden – oder die Firewall-Regeln entsprechend geöffnet. Auf der einen Seite schottet man die eigenen Systeme mit mehrfachen Firewall von der «bösen» Aussenwelt ab und teilt sie sogar intern – wiederum mittels Firewall – in verschiedene getrennte Zonen. Auf der anderen Seite hängt man diese internen Zonen über die Überwachungssysteme nicht nur unter sich, sondern auch mit den Systemen des Dienstleistungsanbieters und allen Systemen seiner Kunden zusammen. Und das soll die Sicherheit verbessern?

Koppeln wir realistischerweise sämtliche hier aufgeführten Risiken mit denjenigen des Double Outsourcing, kann man die potentiellen Auswirkungen erahnen: Der Auftraggeber hat keine Ahnung mehr, wer wann woher und wie auf seine eigenen Systeme zugreift, ist den beauftragten Firmen und allen ihren Unterauftragnehmern auf Gedeih und Verderb ausgeliefert, kann im Ereignisfall aufgrund der (freiwillig) akzeptierten Vertragsbedingungen keinen Regress nehmen und hat zu guter Letzt auch keine Versicherungsdeckung.

Illustrativ ist in diesem Zusammenhang ein Zitat des «Board of Governors of the Federal Reserve System» in Washington[7]: «Die Auslagerung der Informations- und Transaktionsver-

Kurz und bündig

Beim Outsourcing von Informatik-Dienstleistungen sind die Risiken bezüglich der Informationssicherheit gross und nicht abschliessend eruierbar – dies gilt insbesondere bei der Auslagerung von sicherheitsrelevanten Aktivitäten wie System- oder Firewall-Management. Neben einer klaren und detaillierten vertraglichen Regelung sämtlicher Aufgaben und Verantwortlichkeiten ist eine sorgfältige Auswahl des Outsourcing-Partners, aber vor allem eine permanente Kontrolle sämtlicher durch diesen ausgeführten Tätigkeiten unabdingbar. Dies ist jedoch vor allem im Fall von Subcontracting des Outsourcing-Partners an weitere Firmen kaum durchführbar. Wenn sensitive Daten an die Öffentlichkeit gelangen, wichtige Informationen verfälscht werden oder zeitkritische Geschäftsprozesse nicht verfügbar sind, ist einzig die Geschäftsleitung dafür verantwortlich! Aus Optik des Autors sind die Risiken bezüglich Informationssicherheit beim Outsourcing – vor allem bei geschäftskritischen Anwendungen – in den meisten Fällen nicht tragbar. Während kleinere Unternehmen kaum Alternativen haben, sollten sich grössere Unternehmen darauf besinnen, dass der Betrieb von Geschäftsprozessen ihre Kernkompetenz darstellt. Wenn sie diese Prozesse wirklich beherrschen wollen, gehört dazu auch eine Informatik-Umgebung, bei der das Unternehmen die Informationssicherheit im Griff hat.

arbeitung beinhaltet ähnliche operationelle Risiken wie wenn diese Funktionen intern ausgeübt werden [...]. Bei Outsourcing jedoch sind die üblicherweise zur Reduktion dieser Risiken eingesetzten Massnahmen (wie interne Kontrollen und Verfahren) ebenfalls unter der direkten operationellen Kontrolle des Dienstleistungsanbieters – und nicht beim Auftraggeber, der die damit verbunden Risiken von finanziellen Verlusten, Imageschaden oder andere negative Konsequenzen tragen muss.»

Und die Verantwortung?

Auch wenn dies viele Geschäftsleitungsmitglieder nicht gerne hören, wird man durch Outsourcing die Verantwortung nicht los[8]. Das zeigt auch das Bundesgesetz über den Datenschutz (DSG), das zum Thema Outsourcing erwähnt, dass der Auftraggeber für einen ausreichenden Datenschutz sorgen muss[9]. Noch deutlichere Worte findet die Eidgenössische Bankenkommission (EBK) in ihrem Rundschreiben zum Thema[10]: «Der ausgelagerte Geschäftsbereich ist in das interne Kontrollsystem der Unternehmung zu integrieren [...] Dessen [des Dienstleisters] Leistungen sind fortlaufend zu überwachen und zu beurteilen, so dass allfällig nötige Massnahmen sofort ergriffen werden können.»

Einverstanden: Nicht alle Unternehmen sind Banken – aber fast alle Unternehmen bearbeiten Personendaten (Angaben über natürliche oder juristische Personen) und unterstehen damit dem Datenschutzgesetz. Und an die klaren Grundsätze der EBK zum Thema Outsourcing sollten sich mindestens diejenigen Unternehmen halten, welche grössere Finanzgeschäfte tätigen.

Aus obigen Ausführungen lässt sich schliessen, dass der Auftraggeber die organisatorischen Abläufe des Dienstleistungsanbieters kennen und selber beurteilen können muss. Ebenso muss er laufend überwachen, ob Vertraulichkeit, Verfügbarkeit und Integrität der Daten sichergestellt sind. Auch der Abschlussprüfer muss sich mit den Aktivitäten des Outsourcing-Partners intensiv auseinandersetzen und die Sicherheitsmassnahmen des Anbieters selber prüfen[11].

Eine gute Ausgangsbasis für eine erste Risikoreduktion bietet der Leitfaden «Outsourcing of IS Activities to Other Organisations»[12]. Dieser Leitfaden enthält grundlegende Aussagen zur Dienstleistungsvereinbarung sowie zum Management der ausgelagerten Bereiche. Eine grosse Hilfe sind auch die in der Schweiz von einer ISACA-Arbeitsgruppe zu Themen wie Outsourcing-Vertrag, Sicherheit, Prüfung zusammengestellten Unterlagen[13]. ■

Fussnoten und Links

1 BEAT HOCHULI, Datenschatzinseln, Computerworld Nr. 35/2001; Zitat: «In Occasions-PC konkursiter Dotcoms finden sich oft geschäftskritische Informationen».

2 Durch den Ausfall des Swisscom-GSM-Netzes entstanden bei Unternehmen, welche ihre Logistik mit Hilfe von SMS abwikkeln, riesige ungedeckte Kosten.

3 BRUCE CALDWELL ET AL., Hidden Partners, Hidden Dangers - Security and service quality may be at risk when your outsourcing vendors use subcontractors, in: Informationweek Issue 614.

4 Es gibt in Literatur, Film und unter Fachspezialisten Szenarien, bei denen durch terroristische Angriffe auf Ziele wie Flughäfen, Telecom- oder Rechenzentren die Börsenkurse manipuliert werden – mit möglichen Gewinnen bis zum mehrhundertfachen des eingesetzten Kapitals. Diese Szenarien wurden durch die Einflüsse der Attentate vom 11. September 2001 auf die Kurse von Fluggesellschaften, Tourismusunternehmen, Baufirmen, Goldproduzenten usw. leider bestätigt.

5 Überschlagsrechnung: pro zu besetzende Stelle (z.B. für Help-Desk, Monitoring) benötigt man für einen 7x24 Stunden Betrieb mindestens 5 Personen (3 Schichten, 2 Freitage pro Woche, Krankheit und Ferien).

6 Weitere Einschränkungen und Zusatzfunktionen (Authentisierung, Verschlüsselung, Virenscanning usw.) sind möglich.

7 Supervisory Letter SR 00-4 (Sup) on outsourcing of information and transaction processing, Februar 29, 2000.

8 S. YVONNE SCOTT, IS Audit and Control of IS Outsourcing, in: IS Audit & Control Journal VI 1996: «While tasks and duties can be delegated, responsibility for the results produced with information services remains with the organization's management. As a result, outsourcing cannot relieve the organization, or its management, of its responsibility to provide information services for its internal and external customers». Das gilt auch für Outsourcing der öffentlichen Hand: vgl. hierzu BEAT RUDIN, IT-Outsourcing in der Verwaltung, in: digma 2001.4, 176 ff.

9 DSG Art 14: Absatz 1: «Das Bearbeiten von Personendaten kann einem Dritten übertragen werden, wenn: a. der Auftraggeber dafür sorgt, dass die Daten nur so bearbeitet werden, wie er es selbst tun dürfte [...]». Vgl. hierzu auch JEAN-PHILIPPE WALTER, Outsourcing et protection des données, in: digma 2001.4, 166 ff.

10 EBK-RS 99/2. Randziffer 24.

11 Grundsatz zur Abschlussprüfung Nr. 18 der Schweiz. Treuhandkammer: Ziff. 3.3 «[...] hat er sich über den Outsourcing-Partner und seine Tätigkeit genügend Informationen zu beschaffen, um die Auswirkungen auf die Interne Kontrolle der Gesellschaft hinreichend feststellen und beurteilen zu können.»

12 Information Systems and Control Association: IS Auditing Guideline.

13 Verschiedene Hilfsmittel in Englisch und Deutsch herunterladbar von http://www.isaca.ch.