

Bessere Datensicherheit dank Auslagerung der IT

Es gibt viele Gründe, warum man seine IT auslagern soll, doch was für einen Mehrwert bringt die Auslagerung in puncto Datensicherheit und welches sind die Konsequenzen einer Auslagerung? Kaspar Geiser



Kaspar Geiser
ist Managing Director und
Mitinhaber der Aspectra AG

Was bedeutet eigentlich «Datensicherheit»? Die Erläuterung dieser Frage muss in verschiedene Teilaspekte gegliedert werden. Auch verlangen die einzelnen Aspekte unterschiedliche Schutzmassnahmen. Als Erstes kann der Schutz vor unberechtigtem Zugriff genannt werden. Ein weiterer Aspekt ist das unbemerkte Verändern der Daten und ein dritter Punkt ist die Lesbarkeit der Daten auch nach einer unbestimmten Zeit und dies ebenfalls mit der Garantie, dass diese in der Zwischenzeit nicht verändert wurden.

Der Zugriff auf die Daten muss sowohl physisch wie auch virtuell stattfinden. Das heisst, die Datenträger, also die Rechner, CDs/DVDs sowie Backup-Tapes müssen vor Dritten geschützt werden. Einen physischer Schutz erreicht man, indem man seine Rechner in eigens dafür vorgesehenen Räumen betreibt und den Zugang zu diesen schützt. Dies ist vergleichbar mit einem Safe, zu dem nur der Chef einen Schlüssel hat. Um im Katastrophenfall noch immer die Möglichkeit zu haben, auf Daten zugreifen zu können, empfiehlt es sich, Kopien der Daten regelmässig an Drittstandorten zu lagern. Dabei sorgt der Datenverantwortliche dafür, dass die Datenträger regelmässig an einen sicheren Standort gebracht werden. Selbstverständlich muss auch dieser Standort physisch geschützt sein. Der Schutz vor unberechtigtem Zugriff via Computernetzwerk gestaltet sich da schon etwas schwieriger. Dass man sich von Zugriffen aus dem Netz schützen muss, versteht sich von selbst. Wie sieht dies jedoch innerhalb der eigenen Firma aus? Hier empfiehlt es sich, Schutzmassnahmen umzusetzen, die es erlauben, den Zugriff auf Daten für einzelne Abteilungen und Mitarbeiter einzuschränken. Mit dem Schutz des Zugriffs ist es noch lange nicht getan. Sind die Daten einmal geschrieben, gehen wir davon aus, dass diese sich nicht ändern. Und falls sie doch verändert werden, muss dies erkennbar sein. Um dies umzusetzen, ist ein erheblicher technischer Aufwand nötig.



Ihr Geld legen Sie auch nicht unters Kopfkissen.

Wann ist eine Auslagerung sinnvoll?

Der nächste Punkt im Zusammenhang mit der Datensicherheit ist die Lesbarkeit nach einer unbestimmten Zeit. Sind die Daten beispielsweise auf einer Floppy-Disk gespeichert, muss sichergestellt sein, dass auch nach x Jahren noch ein Floppy-Laufwerk da ist, mit dem die Diskette gelesen werden kann. Die Haltbarkeit der Datenträger ist endlich. Somit muss auch bei deren Wahl bereits überlegt werden, auf welches Medium die Daten für eine Langzeitsicherung gespeichert werden sollen. Neben dem Medium muss auch berücksichtigt werden, wie die Daten gespeichert werden. Sind diese beispielsweise verschlüsselt, muss ich auch nach x Jahren noch über die Codierung der dazu nötigen Hard- und Software verfügen, um die Daten wieder lesen zu können.

Obige Ausführungen lassen unschwer erkennen, dass ein guter und sicherer Schutz von Daten aufwendig, kompliziert und mit Kosten verbunden ist. Da die Kernkompetenz einer Firma in den wenigsten Fällen im Sichern und Halten von Daten besteht, liegt es auf der Hand, dass hierfür Dritte beigezogen werden, die diese Massnahmen umsetzen. Bei dieser Umsetzung stellt sich die Frage, ob und warum eine Auslagerung sinnvoll ist.

Vorteile der Auslagerung

Durch die Auslagerung bezieht man sämtliche zum Schutz der Daten notwendigen Leistungen von einem dafür spezialisierten Anbieter. Dieser befasst sich tagtäglich mit sämtlichen Massnahmen und möglichen Gefahren, die die Daten schützen beziehungsweise gefährden. Des Weiteren besteht die Kernkompetenz eines Outsourcers darin, dies nicht bloss für einen, sondern für mehrere Kunden zu tun. Dies bedingt, dass dieser über spezialisiertes Personal und die notwendigen Mechanismen verfügt, die die Daten schützen. Die dazu nötigen Res-

sourcen und Prozesse und damit deren Kosten können dabei auf mehrere Kunden verteilt werden. Somit sind die einzelnen Schutzmassnahmen bei für den spezifischen Kunden gleichbleibenden Kosten ein Vielfaches besser, als wenn die IT und Daten intern gehalten werden. Mit der Auslagerung wird die Datenhaltung und die damit verbundene Sicherheit auch ver-

traglich mittels eines Service Level Agreements (SLA) geregelt. Damit wird sichergestellt, dass der Outsourcer trotz technologisch be-

dingter Veränderungen die Daten stets zur Verfügung stellen kann. Damit wird der Outsourcer verpflichtet, die Daten falls nötig von einem «alten» auf einen «neuen» Datenträger zu portieren.

Verantwortung bleibt in den eigenen Reihen

Wer nun allerdings denkt, mit einer Auslagerung sei man von allen Pflichten und Verantwortungen entlastet, der irrt. Die finalen Entscheide und Qualitätskontrollen müssen in den eigenen Reihen gefällt und durchgeführt werden. Es ist somit sinnvoll, dass sich Anwender mit den Technologien, Prozessen und dem Vertragswerk auseinandersetzen und sich nötigenfalls ausbilden. Die Outsourcing-Anbieter wiederum müssen geeignete Werkzeuge und Prozesse wie Cockpits zur Verfügung stellen, in denen die für den Kunden erbrachten Dienstleistungen überprüft werden können. Da sich die eigenen Bedürfnisse über die Jahre ändern können, sollte auch regelmässig überprüft werden, ob der gewählte Outsourcing-Partner diese auch zufriedenstellen kann, und ob die Kosten im Verhältnis zu einem möglichen Schaden stehen. Des Weiteren gilt es zu beachten, ob der Outsourcer die eigenen Revisionsbedingungen erfüllt und eventuell gar eigene Berichte, zum Beispiel im Bereich FINMA, zur Verfügung stellt. ■

«Es sollte regelmässig überprüft werden, ob der gewählte Outsourcing-Partner die eigenen Bedürfnisse auch zufriedenstellen kann.»