

Türöffner und Trendsetter

Die IT ist für die Erschliessung neuer Geschäftspotenziale und -prozesse immer wichtiger. Ob Outsourcing oder Eigenbetrieb, grundlegende Punkte müssen beachtet werden. Checklisten helfen dabei.

Bruno Morandi, Partner/Leiter Marketing und Verkauf, in4U AG

Gerade bei KMU wird vermehrt realisiert, dass der Eigenbetrieb der Informatik nicht zu den Kernkompetenzen gehört und somit keine Wettbewerbsvorteile bietet. Die Informatikleitung ist vielmehr vermehrt in die strategische Planung involviert, in welcher sie mit der Unternehmensleitung die applikatorische Umsetzung der Geschäftsprozesse analysiert und plant. Der Druck auf die IT-Abteilung erhöht sich. Eine rasche und flexible Umsetzung neuer komplexer Anforderungen wird seitens der Fachabteilungen gefordert. Oft fehlt es aber in vielen KMU an Zeit, Ressourcen, Geld und Know-how

Beim Serverbetrieb Supportaufwand einkalkulieren

für deren Realisierung. Neben erhöhter Sicherheit, Verfügbarkeit und Flexibilität steht der gesicherte Zugriff auf professionelle Ressourcen zur Beherrschung immer komplexerer Technologien im Vordergrund.

In solchen Situationen stellt sich oft die Frage, ob ein IT-Outsourcing an einen professionellen und zuverlässigen Partner nicht doch sinnvoll und angebracht wäre. Die Sicherheit in einer ASP-Umgebung im Datacenter ist

in der Regel umfassender gewährleistet als in einer lokalen Installation vor Ort. Unabhängig davon, ob der Entscheid auf eine Outsourcing- oder Inhouse-Lösung fällt, das Vorgehen und die Methodik sind immer dieselben. Wie aber soll vorgegangen werden? Welche Fragen müssen beantwortet werden? Grundsätzlich sollten für die folgenden drei Bereiche **Checklisten formuliert** und dazu Überlegungen angestellt werden: «Strategische Ziele», «Total Cost of Ownership (TCO)» und «Sicherheit und Verfügbarkeit».

TOTAL COST OF OWNERSHIP (TCO)

Server-Infrastruktur: Kosten für Serverraum (Strom, Kühlung) und Sicherheit (Zutrittskontrolle), Supportaufwand für Serverbetrieb, Kosten für Datensicherung und Outsourcing, Reduktion Hardwaresupport, Folgeinvestitionen für Hardware, Software und Support, Lizenzkosten, IT-Ausbildungskosten, Transparenz für IT-Kosten pro Monat und User, Umwälzung IT-Kosten auf Kostenstellen

Client-Infrastruktur: Limitierung der Betriebskosten pro Benutzer und Monat, tiefere TCO durch den Einsatz der Server-Based-Computing-Technik, Einsatz mehrfacher und günstigerer Geräte (Thin-Clients), Verlängerung des Lebenszyklus der aktuell installierten Clients, Standardisierung des lokalen Supports

SICHERHEIT UND VERFÜGBARKEIT

Bei den Sicherheitsvorkehrungen in einem Datacenter muss grosser Wert auf wirtschaftlich vertretbare Massnahmen zur Vermeidung von Sicherheitsrisiken gelegt werden.

Schutz vor Zerstörungen der Infrastruktur: bauliche Schutzmassnahmen für Serverräume (Feuer, Überflutung, Sabotage, Einbruch vermeiden), betriebliche Massnahmen (Zutrittskontrolle, Alarmsysteme), Klimatisierung und USV, Sicherungsmassnahmen gegen externe Bedrohungen (Viren, Eindringen von Unbefugten)

Schutz vor unberechtigtem Zugriff: Datensicherungskonzept mit externer Auslagerung entsprechender Datenträger, regelmässige Überprüfung der Wiederherstellbarkeit der gesicherten Daten, Wiederanlaufkonzept nach einer Katastrophe (Disaster Recovery), Sicherstellung der Vertraulichkeit der Daten, Einschränken des Zugriffs gemäss definierten Berechtigungen der Benutzer, Absichern der Risiken des Internets (laufend

aktualisierte Firewall-Funktionen), Personen und Benutzer gelten als Risikofaktoren

Sicherheit im Netzwerk: Verschlüsselung der Daten bei Übertragung, Sicherheitsmassnahmen im Zusammenhang mit dem Internet
Bauliche Standards: Geschlossene Zelle nach Brandschutznorm F120; USV (unterbrechungsfreie Stromversorgung), Dieselaggregate zur Notstromproduktion, redundante Klimaanlageanlagen, elektronisches Zutrittskontrollsystem, Alarmsysteme (Überwachung, Brand, Temperatur, Feuchtigkeit, Bewegung), zweiter Datacenter-Standort

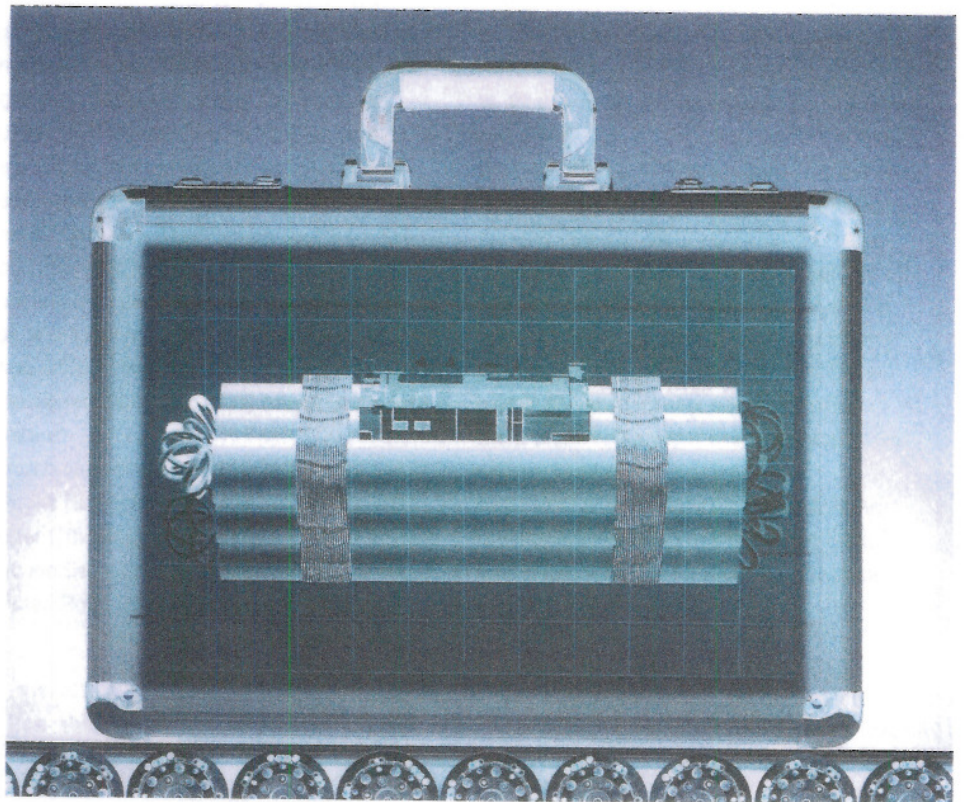
Vertraulichkeit und Sicherheit der Daten und Organisation: Datensicherung inkl. regelmässiger Prüfung der Wiederherstellbarkeit, Vertraulichkeit der Daten sollte regelmässig durch externe Audits überprüft werden, Abschottung der Daten gegenüber Dritten, sämtliche Mitarbeitende müssen zur Vertraulichkeit verpflichtet werden, mit ISO-Prozessen sollten die entsprechenden Massnahmen regelmässig überprüft werden

STRATEGISCHE ZIELE

Die Unternehmung: Konzentration auf Kernkompetenzen, schnellere Reaktion auf Veränderungen, optimale Datensicherheit und Datenschutz, Sicherstellung vor Katastrophen (Business Continuity), IT-Betrieb auf technologisch neuem Stand

Die Mitarbeiter: Mobilität der Arbeitsplätze und Daten, Flexibilität durch Fernzugriff, möglicher Produktivitätsgewinn für Endbenutzer, Skalierbarkeit bei Fluktuationen, höhere Leistung bei zentralisierten Servern, Überbrückung von Mangel an IT-Know-how, Standardisierung der lokalen Infrastruktur

Die IT-Abteilung: Puffer bei Überlastung der IT-Mitarbeiter, Delegation von Routineaufgaben, Unterstützung Kerngeschäft durch die IT, Aufbau und Sicherstellung von geschäftskritischem Know-how mit IT (z.B. ERP), Konzentration der IT auf Strategie, Projekte und Prozessoptimierung



Die Sicherheit in einer ASP-Umgebung im Datacenter ist in der Regel umfassender gewährleistet als in einer lokalen Installation vor Ort

ERSTELLUNG EINES PFLICHTENHEFTS

- Auswahlprozess festlegen
- Status quo definieren
- Vorauswahl treffen
- Pflichtenheft versenden
- Angebote einholen
- Referenzprojekte prüfen
- Verhandlungen
- Vertragsabschluss

Anbieter die beste und wirtschaftlichste Lösung bietet. Der Markt ist unübersichtlich, die angebotenen Lösungen sind komplex. Es empfiehlt sich eine sehr sorgfältige Auswahl des Dienstleisters, der das Projekt realisiert. Als Basis für Produkt- und Anbieterauswahl ist es empfehlenswert, ein Pflichtenheft zu erstellen. Das IT-Pflichtenheft mit den darin enthaltenen funktionalen und systemtechnischen Anforderungen ist ein wichtiger Projektschritt im Rahmen der Zielfindung und Konzeptionsphase eines Projekts.

Die Anforderungen an eine neue IT-Infrastruktur müssen sorgfältig definiert werden. Es gilt zu evaluieren, welcher

KONTAKT: in4U AG
Werkstrasse 36
3250 Lyss
Tel. 032 387 81 00
Fax 032 387 81 11
info@in4u.ch
www.in4u.ch

Ihre Sicherheit, unsere Datacenter!

Überlassen Sie uns Ihre ICT und kümmern Sie sich um Ihre Kernkompetenzen. Mit zwei geografisch getrennten, hochverfügbaren Datacenter erfüllen wir sämtliche Ansprüche bezüglich Datensicherheit und Datenschutz.

Microsoft
GOLD CERTIFIED
Partner

in4U

in4U AG | Werkstrasse 36 | CH-3250 Lyss
Tel. +41 32 387 81 00 | Fax +41 32 387 81 11
info@in4u.ch | www.in4u.ch