Die Maturität von neuen IT-Technologien

Martin Dietrich, lic. oec. HSG, CISA

«Es gehört zu den anerkannten Merkwürdigkeiten der Realität, dass die Integration wohlbekannter Subsysteme in ein komplexes System zu neuen, unvorhersehbaren Eigenschaften des Gesamtsystems führen kann», schreibt Prof. Dr. Andreas Menzl am Schluss seines Beitrages in diesem Jahresbericht. In der IT kann diese Merkwürdigkeit häufig beobachtet werden. Hier wird zudem die Sicherheit teils unnötig gefährdet, weil die Maturität einer verlockenden neuen IT-Technologie gerne überschätzt wird. Bei der Implementierung neuer IT-Systemtechnologien ist es deshalb besonders wichtig, die Einführungsphase gut vorbereitet und überlegt anzugehen, eigene Tests durchzuführen und nicht – im Eifer des Gefechts – die Technologie sofort breit auszurollen – was durchaus lukrativ sein könnte.

Solche kritischen Situationen haben wir im Rahmen unserer ITSEC Audits vorgefunden; sie betreffen im vergangenen Jahr folgende Bereiche:

- SAN für Datenspeicherung
- Server-Virtualisierung
- Zentralisierung der IT
- Web-basierte Applikationen / Unternehmensübergreifende Prozesse

Aus Sicht der IT-Sicherheit befinden sich diese Technologien in einer Vor-Phase der Maturität, die besonders heikel ist, weil hier noch viele Fehler erstmals gemacht werden [können]. Die Komplexität verkompliziert und verunmöglicht viele herkömmliche Arbeitsweisen, denn grundsätzlich führt eine Ausweitung der technischen Möglichkeiten, in den oben erwähnten Bereichen, zu komplexeren Systemen, die aus immer mehr Teilsystemen und Einzelkomponenten bestehen. Die Teilsysteme und die damit verbundenen Tücken sind gut beschrieben und werden auch oft den Empfehlungen folgend umgesetzt. Die Sicherheit des Gesamtsystems entspricht hingegen nicht einfach der Summe der Sicherheiten der Teilsysteme. Bei der Synthese der Teilsysteme zu einem Gesamtsystem nehmen die Anzahl der (möglichen) Fehler (wie auch Nutzen und Komplexität) exponentiell zu. Deshalb ist es unerlässlich, die Sicherheit der Teilsysteme und diejenige der Einzelkomponenten von Beginn an in einem Sicherheitskonzept aufeinander abzustimmen. Fehler in den konzeptionellen Überlegungen lassen sich nachträglich technisch kaum mehr oder nur zu horrenden Kosten beheben.

Einige dieser konzeptionellen Überlegungen möchten wir hier erwähnen:

Datenspeicherung auf SAN

Storage Area Networks (SAN) ermöglichen heute die Speicherung einer sehr grossen Datenmenge auf kleinem Platz. Zusätzlich kann das gesamte zur Verfügung stehende Speichervolumen jederzeit und ohne Umlagerung von Daten ausgebaut, oder auch der Platzbedarf einzelner Systeme variabel angepasst werden. Da ein SAN in sich als relativ sicher gilt (vorausgesetzt, die Sicherheitsmassnahmen sind richtig umgesetzt), verzichten viele Unternehmen vor allem aus Kostengründen auf ein durchgehendes Sicherheitskonzept. Oft wird dabei nicht nur auf ein zweites SAN an einem entfernten Standort verzichtet, sondern zusätzlich auch auf das regelmässige Auslagern der Daten an einen entfernten Standort.
Da der Neuaufbau eines SAN, im Verhältnis zur Neuinstallation und zur Datenrecovery eines einzelnen Servers, sehr (zeit-)aufwendig ist, müssen die Verfügbarkeitsanforderungen der Geschäftsprozesse für die Entscheidung, ob ein redundantes SAN notwendig ist, unbedingt betrachtet werden. Ein zusätzliches Backup der Daten, mit Lagerung an einem entfernten Ort, ist aber auf jeden Fall zwingend nötig, denn auch redundante SAN schützen nicht vor gewollten oder ungewollten Benutzerfehlern, wie dem (un-)absichtlichen Löschen geschäftskritischer Daten oder dem berühmten Wasserschaden im Rechenzentrum.

Server-Virtualisierung

Die Server-Virtualisierung dient vielerorts der Kostenreduktion durch die bessere Auslastung der eingesetzten Hardware und damit Reduktion der benötigten Hardware. Zusätzlich wird die Wartbarkeit der Hardware erhöht, indem die Applikationen und Services mit wenig Aufwand von Server zu Server verschoben werden können. Zur Erhöhung der Verfügbarkeit können virtuelle Server neu gestartet werden, ohne gleichzeitig andere Applikationen zu stoppen und somit dahinterstehende Geschäftsprozesse zu beeinträchtigen. Die Server-Virtualisierung führt aber oft dazu, dass die Hardware-Redundanz auf ein absolutes Minimum zurückgefahren wird, um die Kosteneinsparungen

Rorschacher Strasse 150
Silberturm, 9006 St. Gallen
Telefon 071 243 57 57
Telefax 071 243 57 43
E-Mail: m.dietrich@bsg.ch
Internet: www.bsg.ch

sparungen zu maximieren, oder weil das Vorhalten von grossen Ersatzmaschinen die ganze Kostenreduktion auffrisst. Ein Hardware-Defekt beeinträchtigt in diesem Falle gleich verschiedene Applikationen und Geschäftsprozesse. Fehlende Kapazität auf der vorhandenen restlichen Hardware oder fehlende Testsysteme führen dazu, dass heute Ersatzgeräte beschafft werden müssten. Das grosse Warten ist für die Benutzer die spürbare Folge.

Zentralisierung der Informatik

Nachdem sich die Informatikorganisation mit dem Wechsel von Host-Systemen zu Client-Server-Architekturen dezentralisiert hatte, ist seit einiger Zeit der gegenläufige Trend, hin zur Zentralisierung, zu beobachten. Dies hat vor allem mit dem unkontrollierbaren Wildwuchs der dezentralen Informatik und den daraus entstehenden Kosten zu tun, aber auch die neuen Technologien (z.B. Citrix Metaframe, Virtualisierung) tragen ihren Teil zu dieser Entwicklung bei. Die Zentralisierung führt zu einer Standardisierung und zu einer Professionalisierung, was in jedem Fall zu begrüssen ist. Auf organisatorischer Seite ist allerdings die Zentralisierung häufig schwierig, gerade dann wenn die Arbeitsplätze über mehrere Standorte, Zeitzonen oder Kontinente verteilt sind. Die Kunden in Asien werden wohl wenig Verständnis für eine unerfüllte Lieferung aufbringen, nur weil das (einzige) Rechenzentrum in Europa ausser Funktion ist. Während die allgemeinen technischen Massnahmen in der Regel zentral einfacher und durchgehender umgesetzt werden können, sind insbesondere das Katastrophenszenario (Ausfall des zentralen Standortes oder dessen Anbindung an die grosse weite Welt) und die dazugehörenden Notfallpläne in der Zentrale und in den dezentralen Einheiten zu beachten.

Web-Applikationen / Unternehmensübergreifende Prozesse

Die Forderung nach unternehmensübergreifenden Prozessen führt dazu, dass die Systeme und Netzwerke für Benutzer, Kunden, aber auch für unerwünschte Trittbrettfahrer geöffnet werden. Die klassische Isolierung der Informatik gegen aussen entspricht heute in den wenigsten Fällen den Anforderungen – «immer und überall» steht heute in jedem Pflichtenheft. Der Standard «innen = sicher, aussen = feindlich» gilt nicht mehr. Sicherheitsmassnahmen wie Firewalls sind zwar weiterhin notwendig, aber nicht mehr ausreichend. Web-Applikationen mit Zugriff vom Internet, vom Partnernetz und von allen x-hundert Geschäftsstellen in zig Ländern führen zwangsläufig dazu, dass wir weder die Benutzer der Web-Applikation noch deren Eingaben und schon gar nicht deren Absichten «unter Kontrolle» haben. Da hier verschiedenste Komponenten (Applikationen, Datenserver, Zugriffssysteme, Netzwerkkomponenten) immer richtig zusammenarbeiten müssen, genügt es ebenfalls nicht, nur die einzelnen Komponenten für sich im Griff zu haben. Mehr denn irgendwo sonst ist es in solchen Fällen notwendig, dass die Sicherheit der Einzelkomponenten, des Netzwerks, des Netzwerk-Übergangs (LAN – WAN), der eingesetzten Technologie, der Qualität der Implementierung, der Logik des Workflows, der Semantik des Benutzerinterfaces (inhalts- und kommunikationsbezogene Aspekte) und der organisatorischen Vorschriften sowie Bestimmungen als Ganzes betrachtet und aufeinander abgestimmt wird. Erfolgt diese Abstimmung nicht bereits während der Konzeptphase, sind sicherheitstechnische Mängel vorprogrammiert.

Man sagt, der Teufel liege im Detail. Bei komplexen Technologien liegt der Teufel aber zuallererst in der fehlenden umfassenden System-Konzeption und den unvollständigen Lösungen. Die Maturität der neuen IT-Technologien wird (zu) leicht überschätzt, was die IT-Sicherheit gefährden kann. ☐

Rorschacher Strasse 150
Silberturm, 9006 St. Gallen
Telefon 071 243 57 57
Telefax 071 243 57 43
E-Mail: m.dietrich@bsg.ch
Internet: www.bsg.ch