

IT for you.



Acommit AG
IT for Wholesale, Retail, Production
www.acommit.ch



«Every function in my new house
is managed by the PC,
and sometimes it works.»

Bill Gates, 1997

Betriebsrisiko Informationstechnologie

Ohne Informationstechnologie – kurz IT – kommt keine moderne Unternehmung mehr aus. Sie ist zu einem wichtigen Teil des Wertschöpfungsprozesses geworden. Ihre Möglichkeiten verbessern Arbeitsprozesse, schaffen neue Unternehmensbereiche und prägen zukünftige Geschäftsmodelle.

Die Komplexität unserer IT-Systeme und -Landschaften wächst mit jeder neuen Generation. Entsprechend grösser werden die Betriebsrisiken bei IT-Störungen und Systemausfällen.

Als IT-Partner nationaler und regionaler Unternehmen sind wir für die Betriebsbereitschaft und Sicherheit von komplexen IT-Systemen verantwortlich. Wir sehen nicht nur die viel versprechenden Möglichkeiten von IT-Lösungen, wir erachten es auch als unsere Pflicht, mit Ihnen über die «Achillessehne» IT zu sprechen.

Im Sinne eines Checks möchten wir Sie auf den folgenden Seiten durch zentrale Themenbereiche der betrieblichen IT führen und Ihnen dabei einige kritische Fragen stellen. Gerne zeigen wir Ihnen, was Acommit punkto Betriebssicherheit und Risikominimierung für Sie tun kann.



Ist Ihre IT-Sicherheit gewährleistet?

Als IT-Gesamtanbieter denken wir in Systemen und Netzen: Auch wenn es um Sicherheit geht. Dabei ist es in jedem Fall nachhaltiger, wenn IT-Sicherheitsmassnahmen immer im Kontext zu anderen Bereichen konzipiert und umgesetzt werden.

Optimierter Nutzen Ihres Informatik-Netzwerks

Jede Büroumgebung nutzt heute ein Informatiknetzwerk. Seine Leistungsfähigkeit und seine Einsatzbereitschaft prägen den Arbeitsalltag. Was geschieht aber, wenn das Netzwerk ausfällt? Und was kann unternommen werden, um die Ausfallsicherheit so hoch wie möglich zu halten?

Zunehmend prägt das Internet unser Arbeitsverhalten am Bildschirm. Vor allem der Besuch von Foren und Social Communities wie Facebook oder Twitter nimmt stark zu. Eine immer grössere Anzahl von Arbeitsstunden wird mit privatem Web-Konsum zugebracht. Dies mindert die Produktivität deutlich.

In diesem Kontext stellen sich folgende Fragen:

- Wie lässt sich das Web nur selektiv nutzbar machen? Und wie kann dies einfach, transparent und stabil durchgeführt werden?
- Wie können Arbeitskräfte und Ressourcen global vernetzt und genutzt werden?
- Welche VPN-Technologie ist die richtige für meine Teleworker oder für den Aussendienst?
- Wie muss die Firewall konfiguriert sein, um den Arbeitsfluss nicht zu stören, aber ein hohes Mass an Sicherheit zu bieten?

Mehr Sicherheit für Ihre Server-Landschaft

In allen Unternehmen werden ein oder mehrere Server eingesetzt. Ihre Konfiguration und Arbeitsweise ist dabei so unterschiedlich wie es Firmen gibt. Meist sind Serverkonfigurationen das Produkt aus betrieblichen Bedürfnissen und technischen Möglichkeiten. Nicht immer wurde bei ihrer Einrichtung systematisch vorgegangen. Wo welche Software installiert ist und wie deren Zusammenspiel funktioniert, ist in der Regel komplex. Diese organisch «gewachsene» Komplexität stellt ein Risiko dar.

Fallen ein oder mehrere Server aufgrund eines Hardware- oder auch Betriebssystemschadens aus, kann dies die Unternehmung massgeblich beeinträchtigen. Damit solche Vorfälle minimiert werden, sind die Server, ähnlich wie ein Auto, pro-aktiv zu warten.

In diesem Zusammenhang stellen sich folgende Fragen:

- Sind alle schützenden Softwareprodukte (Virenschutz, Spamfilter usw.) aktiv und auf dem aktuellen Stand?
- Werden die notwendigen Betriebssystempatches regelmässig eingespielt und freigeschaltet?
- Könnten durch eine Server-Konsolidierung die Topografie und deren Unterhalt vereinfacht werden?
- Gibt es Hardwarekomponenten, welche an ihre Leistungsgrenzen gelangen (Speicherbelegungen, CPU-Auslastung)?

Reibungsloser Einsatz eines «IBM Power System i»

Die Produktlinie «IBM Power System i» zeichnet sich durch Stabilität, hohe Verfügbarkeit und geringe Betriebskosten aus. Alle diese Vorteile kommen aber nur dann zum Tragen, wenn das System fachgerecht gewartet wird.

Wartung bedeutet in diesem Fall: Einspielen von kumulativen PTF (Betriebssystem-Patches), überprüfen, ob die Serverleistung den Bedürfnissen der Anwender entspricht, und sicherstellen, dass die Hardware- und Softwarewartungsverträge noch gültig sind. Weiter ist darauf zu achten, dass das aktive Betriebssystemrelease wie auch die darauf eingesetzte betriebswirtschaftliche Applikation offiziell durch die Hersteller unterstützt wird.

Die ständige fachgerechte Wartung macht sich bei einem Schadensfall bezahlt. Muss nämlich die Applikation kurzfristig auf ein Ersatzsystem portiert werden, lässt sich dies bei einem gewarteten System effizient und mit kalkulierbarem Aufwand durchführen. Anderenfalls ist mit hohen Kosten und langen Ausfallzeiten zu rechnen.

In diesem Zusammenhang stellen sich folgende Fragen:

- Haben Sie sichergestellt, dass das Betriebssystemrelease aktuell, die Serverleistung genügend und die Wartungsverträge gültig sind?
- Können Sie sich vorstellen mehrere Tage ohne betriebswirtschaftliche Applikation auszukommen?

Unterbrechungsfreie Stromversorgung (USV)

Unterbrechungsfreie Stromversorgungen gewährleisten bei einem kurzen Stromunterbruch die Überbrückung der Stromversorgung. Bei einer länger anhaltenden Unterbrechung fährt die USV innerhalb einer definierten Zeitspanne die Serverlandschaft kontrolliert runter, so dass keine Datenschäden oder -verluste auftreten.

Der Einrichtung einer USV hat meist untergeordnete Priorität. Dies hat seine Gründe: Bei der Neuinstallation von Servern wird das Investitionsbudget oft sehr strapaziert, so dass keine Mittel mehr für eine USV zur Verfügung stehen. Bei der Investitionsplanung ist deshalb Umsicht gefragt.

Hat man sich für den Kauf einer USV entschlossen, wird diese nach der Installation meist vergessen. Eine USV ist jedoch eine Art Batterie, sie muss also gepflegt werden. Regelmässige Wartungen, entsprechende klimatische Voraussetzungen im Serverraum wie auch eine ausreichend dimensionierte Stromversorgung sind Kriterien, die für eine USV von zentraler Bedeutung sind.

Fragen, die in diesem Zusammenhang wichtig sind:

- Wann wurde die USV das letzte Mal kontrolliert und auch getestet?
- Genügt deren Auslegung den aktuellen Anforderungen des Strombedarfs aller Server?

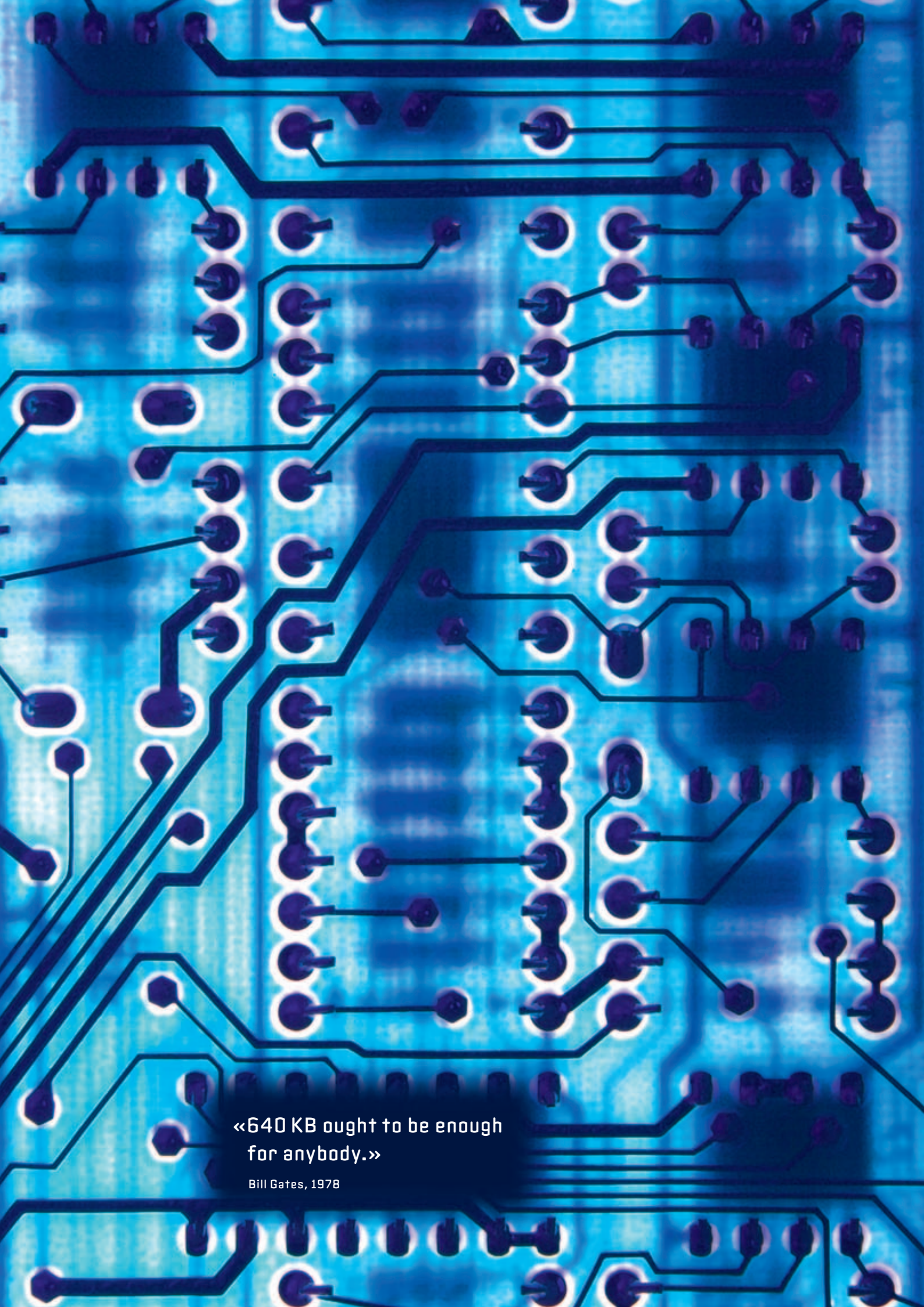
Ausfallsicheres E-Mail

E-Mails gehören zum Business-Alltag. Ohne E-Mail wäre der effiziente Verkehr mit Kunden, Lieferanten und Mitarbeitenden undenkbar. Längst geht man davon aus, dass E-Mails jederzeit und fast überall empfangen und gesendet werden können: sei es via WLAN oder Mobile Devices (Handy usw.).

Die Vielfalt von Remote-Access-Möglichkeiten mit Outlook Anywhere, Web-Mail und der Nutzung von Groupware-Funktionen (gemeinsame Kalender usw.) helfen, den betrieblichen Alltag effizient zu bewältigen. Doch was ist, wenn der E-Mail-Verkehr nicht mehr richtig fließt? Was geschieht, wenn Mitarbeitende wichtige E-Mails löschen?

Rund ums E-Mail taucht eine Vielzahl von wichtigen Fragen auf:

- Wie lange kann der Betrieb ohne E-Mail-Verkehr arbeiten?
- Was geschieht mit vertraulichen E-Mails, die man nur ungern anderen Personen zugänglich macht?
- Ist bekannt, wo und wie die gesamten E-Mails gespeichert werden?
- Und was, wenn der Revisor verlangt, dass bestimmte E-Mails revisionssicher archiviert werden müssen?



«640 KB ought to be enough
for anybody.»

Bill Gates, 1978

Aktualisierung von Berechtigungsstrukturen

Jede Unternehmung ändert im Laufe der Zeit ihre Struktur: Neue Geschäftsbereiche werden kreiert, andere umfunktioniert oder ganz aufgehoben. Neue Mitarbeitende übernehmen neue Aufgaben, Arbeitsabläufe und Zuständigkeiten sind einem steten Wandel unterworfen.

Die ständigen innerbetrieblichen Veränderungen verlangen nach entsprechenden IT-Massnahmen:

- Sind alle Berechtigungsstrukturen immer auf dem aktuellsten Stand?
- Werden die Abläufe mit modernen Informatik-Hilfsmitteln wie zum Beispiel mit Workflows unterstützt? (Microsoft SharePoint und die Office-Produkte bieten dafür hervorragende Möglichkeiten.)

Die ständigen Veränderungsprozesse beanspruchen viel Aufmerksamkeit. Dies führt oft dazu, dass das firmenübergreifende Sicherungskonzept vernachlässigt wird. Offensichtlich werden die Sicherheitslücken vor allem dann, wenn einzelne oder mehrere Mitarbeitende ein Datenbackup anfordern. Beim Zurückspielen wird dann meist festgestellt, dass die gesicherten Daten entweder nicht lesbar oder schon mehrere Tage/Wochen alt sind.

Fragen, die Sie sich in diesem Kontext stellen müssen:

- Wie lange kann Ihre Unternehmung auf aktuelle Daten verzichten?
- Was geschieht, falls einmal die Zugangsdaten einzelner Mitarbeitender oder sogar der gesamten Belegschaft verloren gehen?
- Wie lange können Mitarbeitende Ihrer Unternehmung ohne PC das Tagesgeschäft bewältigen?
- Wie viel können Ihre Mitarbeitenden selbstständig wieder herstellen, ohne dabei fremde Hilfe in Anspruch nehmen zu müssen? (Self-Service-Lösungen helfen, den Arbeitsfluss nicht zu bremsen und Kosten zu sparen.)

Ein Service Level Agreement (SLA) ist sinnvoll

Service Level Agreements (SLA) sind ähnlich wie Versicherungen: Der Umfang der Leistung wird durch Sie bestimmt. Die Frage, die dabei ausschlaggebend ist: Mit wie viel Service sollen die Betriebssicherheit gesteigert und das Ausfallrisiko vermindert werden? Die Antwort auf diese Frage hängt nicht zuletzt auch von strategischen Überlegungen ab. Wie lange, so muss man sich in diesem Zusammenhang auch fragen, kann Ihre Unternehmung auf funktionierende Informatik verzichten?

Es gibt verschiedene Service Agreements. Grundsätzlich haben Sie die Wahl, wie viel Sie in IT-Service investieren wollen. Hinzu kommt, dass die Angebote von Anbieter zu Anbieter variieren.

Angebots-Beispiele

- 5 x 11 h, Aufnahme der Reparatur an Werktagen von 08.00 bis 19.00 Uhr.
- 7 x 24 h, Aufnahme der Reparatur jeden Tag von 00.00 bis 24.00 Uhr.
- 7 x 24 h (4 h), Aufnahme der Reparatur jeden Tag von 00.00 bis 24.00 Uhr und das System ist innert 4 Stunden wieder betriebsbereit.

Es zeigt sich, dass es notwendig ist, pro IT-Bereich eine Risikoanalyse durchzuführen. Dabei spielen Kriterien wie Ausfallwahrscheinlichkeit und mögliche Schäden bei Nichtverfügbarkeit einer Komponente eine wichtige Rolle.

Für den Abschluss eines Service Level Agreements ist es ratsam, auf spezialisiertes Know-how zurückzugreifen. Auch in diesem Bereich ist Acommit Ihr vertrauenswürdiger IT-Partner.



Acommit AG

IT for Wholesale, Retail, Production
Seestrasse 202 · CH-8810 Horgen
Phone +41 44 718 19 00
Fax +41 44 718 19 10
www.acommit.ch