linCK-IT GmbH & Co. KG

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
85521 Ottobrunn (Riemerling)

Netzwerklösungen
IT-Consulting
IT-Services
IT-Security

Katastrophenvorsorge
VoIP Telefonanlagen
Internetprojekte
Migrationen

Bei uns
ist Ihre IT
in guten Händen.

IT-Security im Mittelstand – Was Sie lieber nicht so genau darüber wissen wollten...

IT-Security – sie ist in aller Munde, wird aber nicht minder oft sträflich vernachlässigt – teils aus Unwissenheit, teils weil der Ernst der Situation schlicht unterschätzt wird.

Was soll sich ein Netzwerk-Administrator oder Unternehmer unter „IT-Security“ eigentlich vorstellen? Kurz gesagt geht es um die Sicherheit der Unternehmensdaten, also deren *Verfügbarkeit*, *Integrität* und *Vertraulichkeit*.

Die *Verfügbarkeit* der Unternehmensdaten, verbunden mit deren *Integrität* (frei: Korrektheit) ist eine elementare Voraussetzung für die Arbeitsfähigkeit der meisten Unternehmen. Man stelle sich zum besseren Verständnis einfach vor, im eigenen Büro wäre auf Grund einer Netzwerkstörung kein Zugriff auf die gespeicherten Informationen über Kunden, offene Rechnungen, laufende Projekte, und alle sonst irgendwie elektronisch erfassten Informationen mehr möglich.

Wäre Ihr Unternehmen dann noch arbeitsfähig? Wie hoch wäre der entstehende Schaden?

Bei den meisten Firmen wäre der Ausfall der IT[1] gleichbedeutend mit einem unternehmerischen Stillstand – oftmals verbunden mit schwer einschätzbaren Folgekosten aufgrund verlorener Aufträge, fehlender Rechnungslegung, fehlender Wahrnehmung von Terminen, etc.

Für Ihren Mitbewerber hat eine derartige Katastrophe in Ihrem Hause sogar einen Namen: *Jackpot*.

Hier nun alles Wesentliche, was Sie als Entscheider über IT-Security für Ihre Firma wissen sollten:

„Daten“ – was ist das?

Mit *Daten* sind in der IT üblicherweise all diejenigen Informationen gemeint, die in elektronisch gespeicherter Form vorliegen: Adressen von Geschäftspartnern und Mitarbeitern, Kontakte mit Telefonnummer und eMail-Adresse, Informationen zu offenen und erledigten Aufträgen, Rechnungen, Projekten, u.v.m. Kann auf diese Informationen plötzlich und ohne Vorbereitung nicht mehr zugegriffen werden, steht meist ein Großteil der Unternehmensabläufe still.
Dem gilt es so gut wie möglich vorzubeugen: durch Absicherung gegen Ausfall und die Bereithaltung ausgedruckter Informationen, die zumindest eine kurzfristige Fortführung der elementaren Geschäftsprozesse ermöglichen. Das „Papierlose Büro“ stellt nicht in *allen* Fällen einen erstrebenswerten und nützlichen Zustand dar...

Datenverfügbarkeit

Wie das Wort *Datenverfügbarkeit* bereits impliziert geht es dabei um die jederzeitige Möglichkeit des Zugriffs auf benötigte Daten.
Der Aufbau der IT-Infrastruktur eines Unternehmens muß u.a. darauf ausgerichtet sein, die Daten auch dann vorhalten zu können, wenn kleinere Defekte oder Störungen an der Hardware einer oder mehrerer Netzwerkkomponenten auftreten.
Ist ein Ausfall unvermeidlich, so sollte dieser zumindest möglichst kurz gehalten werden, die Daten müssen schnellstmöglich wieder im Zugriff sein.

1 IT: Informations Technologie

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: 089 5404748-0
info@linck-it.de
http://linck-it.de
http://mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

Datenintegrität

Informationen, die Sie heute in eine Datenbank oder schlicht Ihren elektronischen Terminkalender eingeben, sollten auch morgen noch korrekt sein und mit dem ursprünglich Erfassten übereinstimmen (sofern Sie nicht selbst und bewußt Änderungen vorgenommen haben).
Diese Korrektheit der Daten zu jedem beliebigen Zeitpunkt, das „nicht verändert worden sein“ – dies ist die Bedeutung des Begriffs „Datenintegrität“ im Sinne der Datenverarbeitung.

Vertraulichkeit der Daten

Die Vertraulichkeit der Daten, also die Zugänglichkeit der Informationen nur für den Personenkreis, der auch tatsächlich autorisiert ist, diese Daten zu Gesicht zu bekommen, ist unabdingbar sowohl im Sinne des Datenschutzes[1], als auch aus Gründen der Wettbewerbsfähigkeit.
Mögliche „Lecks“ entstehen natürlich nicht nur durch den zeitlos populären Datenfeind Nr. 1 (das *Internet;* ⇨ *Firewall*), sondern oftmals durch ungenügenden Zugangsschutz (z.B. Passwörter, Rechtevergabe) und die fehlende Sperrung alternativer Speichermedien (CD-Brenner, USB-Stick, externe Festplatten).

Was soll ich tun? Konkrete Empfehlungen

Steigerung der *Datenverfügbarkeit*:

1. Weitestgehendes Ausschalten des so genannten „single point of failure“: ausfallgefährdete Punkte im Netz werden redundant[2] ausgelegt. Beispiele für das Schaffen von Redundanzen: Gespiegelte Server, Datenverteilung auf mehrere Festplatten (RAID-1/RAID-5), redundante Netzteile/Lüfter im Server, redundante Datenwege und Stromanschlüsse, etc.
2. Regelmäßige und möglichst automatische Anfertigung von Kopien unternehmensrelevanter Daten. Hierbei ist das tägliche Backup[3] auf Band oder Festplatten/NAS von zentraler Bedeutung. Die Funktion der automatischen Datensicherung sollte regelmäßig geprüft werden, denn auch bei angeblich erfolgreicher Sicherung können die gesicherten Daten ganz oder teilweise unlesbar sein.
3. Um auch bei einem Totalausfall des Netzwerkes zentrale Aufgaben im Unternehmen wahrnehmen zu können, empfiehlt sich das regelmäßige Anlegen von Datenausdrucken auf Papier (Adressliste von Geschäftspartnern und Mitarbeitern, Projektdokumentationen, offene Angebote, Terminkalender). Alternativ können diese Daten auch in elektronischer Form auf einer externen Festplatte im PDF-Format oder als Tabelle(n) vorgehalten werden.
4. Das zentrale Speichern geschäftlicher Daten auf einem Server ermöglicht sowohl den gemeinsamen Zugriff durch autorisierte Anwender im Netz, als auch eine zentrale Sicherung der Daten auf externe Speichermedien.
5. Katstrophenvorsorge (s.u.) treffen: nur die in einem Notfallplan festgehaltenen Informationen in Verbindung mit einem ausgelagerten Backup ermöglichen einen schnellstmöglichen Wiederanlauf der IT im Falle eines Totalschadens im Serverraum.

1 Der Schutz insbesondere personenbezogener Daten ist auf Bundes- (BDSG) und Ländererbene (LDSG) gesetzlich geregelt. Insbesondere dem betrieblichen Datenschutz *muss* ein Unternehmer seine Aufmerksamkeit widmen. Nähere Informationen sind zu finden unter http://www.datenschutz.de und http://www.bfdi.bund.de

2 Redundanz (lat.): „im Überfluss vorhanden sein“. Im Sinne der IT bedeutet dies das mehrfache Vorhandensein von Elementen derart, daß diese sich bei Ausfall gegenseitig ersetzten können.

3 Backup (engl.): „Datensicherung“, „Sicherungskopie“.

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: 089 5404748-0
info@linck-it.de
http://linck-it.de
http://mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

Datenintegrität bzw. Datenkonsistenz erfordert fehlerfrei arbeitende Systeme sowohl bei der Eingabe und Speicherung, als auch bei der Weiterverarbeitung der Daten. Ausgehend von technisch korrekt arbeitenden Datennetzen, Rechnern und Komponenten, muß aber auch Augenmerk gelenkt werden auf Virenschutz und Zugriffskontrollen (siehe *Vertraulichkeit* weiter unten). Konkret:

1. Verwendung von Business-tauglichen Servern und Arbeitsplatzrechnern.
2. Netzwerkweiten Virenschutz einrichten (Server und Arbeitsplatzrechner) mit regelmäßigen Updates der Virensignaturen.
3. Eigenständige Firewall aufstellen und regelmäßig prüfen/updaten lassen.
4. An mobilen Arbeitsplätzen (Notebooks) Desktop-Firewalls aktivieren und die Mitarbeiter in deren Bedienung einweisen (nicht ganz trivial, aber machbar).
5. Regelmäßiges Einspielen von Security-Updates/Patches für Server und PC/Notebooks.

Vertraulichkeit erfordert sowohl generelle Maßnahmen im Netzwerk, als auch die Beachtung gewisser Spielregeln für die einzelnen Anwender:

1. Der Zugang zu Serverraum und Karteikästen/Ordnern sollte durch geeignete Maßnahmen gesichert sein (Serverschrank und Aktenschränke abschließbar, bespielte Sicherungsmedien unter Verschluß halten).
2. Der Zugang auf Netzwerkressourcen sollte durch hinreichend komplexe Passwörter (Buchstaben, Zahlen und Sonderzeichen) für jeden Anwender separat gesichert sein.
   Der Name von Ehefrau/-mann, Kind, des Lieblingshaustieres oder der bevorzugten Zigarettenmarke sind ebenso ungeeignet, wie „start“, „1234“, der eigene Vor- oder Nachname, oder ähnlich simple Begriffe. Derart einfache Passwörter sind innerhalb kürzester Zeit automatisiert herauszufinden.
3. Die unter *Datenintegrität* genannten Punkte stellen, im Verbund mit einem Schutz vor Spyware, Trojanern und Würmern, auch hier eine wesentliche Voraussetzung dar.
4. Mails können auf ihrem Weg durchs Internet mit entsprechenden Mitteln abgefangen werden. Auf dem Firmen-Mailserver sind sie ein offenes Buch für den Administrator, der ja systembedingt auf *alle* Netzwerkressourcen Vollzugriff benötigt. Streng vertrauliche eMails sollten deshalb nur verschlüsselt versendet werden (z.B. mit GnuPG[1], oder PGP[2]). Dies erfordert immer eine erstmalige Abstimmung zwischen Absender und Empfänger der Mails. Vorteil dieser Verschlüsselungsmethode: die Mail bleibt nicht nur auf ihrem Weg durchs Internet vor unbefugten Zugriffen weitgehend geschützt, auch im Firmennetz des Empfängers angekommen kann die Mail nur von demjenigen gelesen werden, für den die Nachricht tatsächlich bestimmt ist.
   Oft ist bei Mailservern eine verschlüsselte Verbindung bereits eingerichtet. Diese funktioniert leider nur zwischen dem Mailprogramm der Anwender und dem Firmen-Mailserver zuverlässig. Eine verschlüsselte Übermittlung zwischen den Mailservern von Absender und Empfänger kommt leider nur selten zustande: sprechen beide Mailserver unterschiedliche „Verschlüsselungssprachen“, so kommt häufig als gemeinsamer Nenner die unverschlüsselte Übertragung der Nachricht zum Einsatz.
5. Verbindungen zwischen Niederlassungen, vom Büro zu einem mobilen Anwender oder Heimarbeitsplatz (neudeutsch: Home Office) werden mittlerweile fast ausschließlich über das Medium *Internet* realisiert. Hierbei sollte unbedingt auf eine verschlüsselte Verbindung per VPN[3] geachtet werden. Die einigen Betriebssystemen dafür beiliegende Software ist dabei nicht immer die geeignete Wahl...

---

1 GnuPG: kostenfreies Verschlüsselungs-Tool für eMails: http://www.gnupg.org
2 PGP: kommerzielles Verschlüsselungs-Tool für eMails, Festplatte und BlackBerry: http://www.pgp.com/de
3 VPN: **V**irtuelles **P**rivates **N**etz (mit verschlüsselter Verbindung)

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: 089 5404748-0
info@linck-it.de
http://linck-it.de
http://mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

Katastrophenvorsorge

Stellen Sie sich vor, in Ihrem Serverraum hat es gebrannt – Totalschaden für die Daten Ihrer IT. Die üblicherweise im Serverraum gelagerten Sicherungsbänder sind natürlich ebenfalls verbrannt, zusammen mit Passwortlisten, Datenträgern und Lizenzen.

Was nun?

Für viele Unternehmen unterschiedlichster Größe hat eine solche oder ähnliche Katastrophe schon das unternehmerische „Aus“ bedeutet.

Lassen Sie es nicht so weit kommen – Vorsorge ist einfacher und preiswerter, als Sie denken.

Konkrete Präventiv-Maßnahmen zur schnellstmöglichen Wiederherstellung der Arbeitsbereitschaft Ihrer IT nach einem GAU[1]:

1. Regelmäßiges Auslagern von Sicherungsmedien an einem entfernten Ort (Heimatadresse des Geschäftsführers oder Administrators, Bankschließfach, etc.) – zumindest möglichst weit entfernt von der Hausanschrift Ihres Unternehmens.
2. Erstellung einer Netzwerkdokumentation durch den Administrator oder IT-Betreuer.
   Hier sollten alle für eine Wiederherstellung der IT-Landschaft benötigten Informationen wie IP-Adress-Bereiche, Admin-Passwörter, Internetzugangsdaten, etc. gelistet sein.
3. Aufstellen einer „Einkaufsliste“ für die Neubeschaffung von Hard- und ggfs. Software.
   Diese kann im Ernstfall schnell für die Ersatzbeschaffung als Vorlage verwendet werden.
4. Abschluß einer Elektronikversicherung, die möglichst auch Brand-, Blitz- und Wasserschäden abdeckt, sowie Vandalismus und Einbruchdiebstahl.
5. Abschluß einer Betriebsunterbrechungs- bzw. Betriebsausfallversicherung.

1 GAU: aus dem Bereich der Kernenergie bekannte Abk. für „**G**rößter **A**nzunehmender **U**nfall“.

Zusammenfassung

Die Sicherheit in Firmennetzen sollte durchaus ernst genommen werden. Über die rein wirtschaftlichen Risiken von Betriebsausfällen auf Grund eines Stillstandes oder Totalausfalls der IT hinaus sind auch einige datenschutzrechtliche Aspekte zu beachten, für die Geschäftsführer und Administrator in der Haftung stehen.

Keiner der oben angesprochenen Punkte zur Prävention stellt ein wirkliches Problem dar – das Problem entsteht erst dann, wenn Security-Lücken zu Folgeschäden führen (Informationen gelangen in die falschen Hände, Daten gehen verloren oder können nicht wieder hergestellt werden).

Befragen Sie im Zweifelsfall Ihren IT-Betreuer zu den Themen IT-Security und Katastrophenvorsorge – bevor es zu spät ist.

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: 089 5404748-0
info@linck-it.de
http://linck-it.de
http://mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny

linCK-IT GmbH & Co. KG

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
85521 Ottobrunn (Riemerling)

Netzwerklösungen
IT-Consulting
IT-Services
IT-Security

Katastrophenvorsorge
VoIP Telefonanlagen
Internetprojekte
Migrationen

Bei uns
ist Ihre IT
in guten Händen.

Gerne beraten wir Firmenkunden zu diesem oder weiterführenden Themen bei einem persönlichen Gespräch.

Die linCK-IT ist ein IT-Dienstleistungsunternehmen mit Firmensitz in Ottobrunn (bei München) und fokussiert auf kleine und mittelständische Unternehmen (Netzwerke ab einem dedizierten Server bis hin zu ca. 20 Serversystemen). Unseren Kunden bieten wir herstellerneutrale Beratung/Konzeption, Installation und Wartung im IT-Umfeld (Windows/Linux).

Gerne unterstützen wir auch Ihr Unternehmen in allen Fragen der Informations-Technologie – damit Sie den Kopf frei haben für Ihr *eigentliches* Business.

Ihr Ansprechpartner:

Dipl.-Kfm.
Thomas Carlile
IT-Berater

Telefon: 089 5404748-10
tc@linck-it.de

www.linck-it.de

John Ruskin (englischer Sozialkritiker, 1819 – 1900) zum Thema "billig einkaufen":

„Es gibt auf der Welt fast nichts, was man nicht ein wenig schlechter machen und billiger verkaufen könnte. Wer nur auf den Preis achtet, wird zu Recht Beute solcher Geschäftspraktiken.

Es ist unklug, zu viel zu zahlen, aber es ist auch unklug, zu wenig zu zahlen. Zahlt man zu viel, verliert man ein bisschen Geld, mehr nicht. Zahlt man zu wenig, verliert man manchmal alles, weil der gekaufte Gegenstand seinen Zweck nicht erfüllt.

Die Marktgesetze verbieten es, dass man für wenig Geld viel Leistung erhält - das ist unmöglich. Kauft man vom billigsten Anbieter, muss man für den eventuellen Ärger etwas Geld zurücklegen. Und wenn man das tut, hat man auch genug Geld, um etwas Besseres zu kaufen.“

linCK-IT GmbH & Co. KG
Otto-Hahn-Str. 28-30
D-85521 Ottobrunn (Riemerling)
HRA 83410 München
USt.-ID-Nr.: DE232672954

Telefon: 089 5404748-0
info@linck-it.de
http://linck-it.de
http://mittelstands-it.de

Pers. haftende Gesellschafterin:
linCK-IT Verwaltungs GmbH
HRB 150743 München
Geschäftsführer:
Dipl.-Kfm. Thomas Carlile,
Eidg. Dipl.-Inf. Manuel Kleinhäny