Entscheidungshilfen und Beratungsangebot

G-ID Consulting bietet Ihnen das umfassende Beratungsangebot und **begleitet Sie sicher**, unkompliziert und kostengünstig **durch Ihre Informatik-Vorhaben und Sicherheits-Checks**.

Wenn Sie auf Basis der hier angeführten Informationen weitere Fragen haben oder in diesem Zusammenhang detailliertere Aspekte Ihrer Informatik und Organisation erörtern möchten, bieten wir Ihnen gerne ein **Beratungsgespräch** an, wo wir auf Ihre spezielle Situation eingehen können.
Ueber eine **Kontaktaufnahme** würden wir uns sehr freuen!
Bitte wenden Sie sich an:

Herrn Patrick Buser
Tel.Nr. 061/ 922 08 41
Natel-Nr. 079/ 439 61 33
E-Mail: p.buser@g-id.ch

Effiziente Planung und Realisierung Ihrer Organisations– und Informatik-projekte

G-ID Consulting GmbH
Benzburweg 18
CH-4410 Liestal BL

061/ 922 08 40
mail@g-id.ch

Was sind eigentlich Viren, Würmer, Trojaner etc. ?

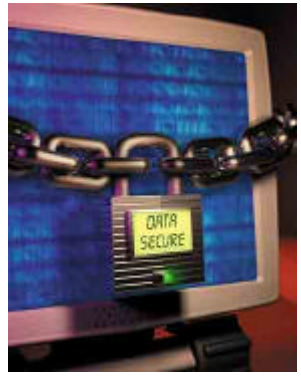
- **Computer-Viren**
  ☐ Kleine und kleinste Computer-Programme, die versuchen, sich selbst zu verbreiten und bestimmte oder alle Daten auf den Systemen zu zerstören.
- **DoS-Attacken (Denial of Service)**
  ☐ Daten-Bombardement auf einen Internet-Server mit dem Ziel, diesen durch grosse Datenmengen zum Absturz zu bringen.
- **Firewall**
  ☐ Hard– und/oder Software-System zum Schutz eines internen Netzwerks vor Angriffen aus dem Internet.
- **Hacker**
  ☐ Personen, welche mit Hilfe von Software (=Hacker-Tools) versuchen, in andere Netzwerke bzw. Computer einzudringen, um entweder Daten einzusehen, zu löschen, oder einfach die Systeme funktionsunfähig zu machen.
- **Hoax-Viren**
  ☐ „Spass"-Meldungen per E-Mail, die vor Viren warnen, die nicht existieren, und/oder Benutzer zum Löschen von Dateien mit bestimmtem Namen auf der Festplatte auffordern.
- **„Trojanische Pferde"**
  ☐ Kleine Programme, die nach aussen eine gewisse Funktionalität vortäuschen. In Wirklichkeit aber Passworte, Kreditkarten-Nummern etc. ausspionieren, und an einen Hacker zurücksenden. Sie können auch zur „Fernsteuerung" eines fremden Computers benutzt werden, um damit illegale Aktivitäten auf dem Internet auszulösen.
- **Würmer**
  ☐ Spezielle Art von Computer-Viren, welche sich meistens über Mailsysteme verbreiten, indem sie sich automatisch an alle Adressen eines Privat- oder Firmen-Adressbuchs versenden.

G-ID CONSULTING
GOOD IDEAS CONSULTING - WWW.G-ID.CH

Infos & Facts

Ausgabe 10/2003

Informatik - Sicherheit für KMU



Informatik-Sicherheit wurde bis jetzt immer als Angelegenheit der „grossen" Firmen angesehen. Vor allem Banken und Versicherungen, die bekanntermassen eine grosse Informatik-Abhängigkeit haben, widmen sich dem Thema schon seit längerem.
Kleine und mittlere Unternehmen sind häufig abgeschreckt durch die vermeintliche Komplexität der Massnahmen und den angenommenen hohen Kosten.

Wir zeigen Ihnen auf den folgenden Seiten, wie man einfach, schnell und kostengünstig die Sicherheit der Informatik erhöhen kann.

Oktober 2003

Informatik-Sicherheit in KMU und kleineren Organisationen

Umfrage-Ergebnisse zur Informatik-Sicherheit

In einer Umfrage der Zürcher Hochschule Winterthur (ZHW) wurden 205 Klein– und Mittel-Unternehmen mit sensiblen Daten (Treuhänder, Advokaten, Ärzte, Planungsbüros etc.) nach Ihrem Verhalten bezüglich Informatik-Sicherheit befragt. Dabei hat sich gezeigt, dass das Bewusstsein für diese Problematik vielerorts fehlt, und erst noch geweckt werden muss.

- **Schutz der sensitiven Daten**
  Bei Informatik-Sicherheitsfragen stehen die Daten im Mittelpunkt. Von den befragten Firmen stufen 93% die Kundendaten, 90% die Personaldaten, 89% die dem Datenschutzgesetz unterstellte Daten, und 88% die Buchhaltungs-Daten als wichtig ein.
- **Was nützt ein „toter" PC ?**
  70% der Unternehmen geben an, bei einem Totalausfall auf manuelle Prozesse umzustellen. Dies verwundert sehr, sind doch viele Firmen praktisch vollständig von ihrer EDV abhängig. Bei einem Drittel aller Befragten steht bei einem Ausfall gar das ganze Unternehmen still !
- **Sicher ist nicht immer sicher**
  Datenverluste durch Hard– und Software-Fehler, Bedienungsfehler oder höhere Gewalt werden von 99% aller Firmen durch Backups begegnet. Nur, was nützt dieser, wenn nie ein Restore-Test gemacht wird, oder wenn die Backup-Medien direkt neben dem PC aufbewahrt werden ?
- **Bedrohung von Aussen und Innen**
  77% der Unternehmen glauben kaum an einen Angriff von Hackern oder Viren (Aussen), obwohl praktisch täglich solche Attacken erfolgen. Ganz unterschätzt wird auch die Bedrohung durch Mitarbeiter/innen, welche durch Sabotage, Fehlmanipulationen und Unachtsamkeit Daten vernichten oder preisgeben.

Lohnt sich der Aufwand für Informatik-Sicherheit ?

Sind Sie versichert ?

Diese Frage werden Sie höchstwahrscheinlich spontan mit Ja beantworten. Jedem ist heute klar, dass bestimmte Risiken versichert werden müssen, auch wenn es etwas kostet. Nur - bei den Risiken des Informatik-Einsatzes hat sich dieses Bewusstsein noch nicht vollständig durchgesetzt !

Ein Beispiel aus der Praxis

Nach 1-tägigem Ausfall eines Servers in einer Handelsfirma mit 5 Beschäftigten ergibt sich folgende Rechnung der direkten Aufwände:

- ☐ Fr. 3'000.00 Entgangener Bruttogewinn
- ☐ Fr. 1'500.00 Serverreparatur
- ☐ Fr. 3'500.00 Interne Daten-Wiederherstellung:
- ☐ **Fr. 8'000.00 Gesamtaufwand**

Die Kosten der Sicherheit

Informatik-Sicherheit heisst nicht, plan– und ziellos Geld zum Fenster hinauswerfen, sondern mittels transparenten Kosten-/Risiken-/Nutzen-Überlegungen zu ausgewogenen und den Bedürfnissen der Firma entsprechenden Sicherheitsmassnahmen zu gelangen.
Nur eine exakte individuelle Analyse der Risiken in Ihrem Unternehmen kann hier letzlich Klarheit bringen.
Für unser Beispiel der Handelsfirma würde dies etwa folgende Kosten (inkl. Installation) beinhalten:

- ☐ Fr. 1'000.00 Internet-Firewall
- ☐ Fr. 1'000.00 Anti-Virus-Software
- ☐ Fr. 2'000.00 Backup-System mit Medien
- ☐ **Fr. 4'000.00 Gesamtkosten**

So könnte also mit einer Investition, die 50% des potenziellen Schadens von Fr. 8'000.00 ausmacht, die Risiken auf ein Minimum reduziert werden.

Sicherheitsmassnahmen - einfach und effizient

Was gilt es sicher zu stellen ?

- **Verfügbarkeit**
  Ihre Mitarbeiter/innen sollen während Ihrer Arbeitszeit ungehindert und unterbruchsfrei mit den Informatik-Systemen arbeiten, und auf die notwendigen Daten zugreifen können.
- **Vertraulichkeit**
  Unautorisierte Personen inner– und ausserhalb Ihrer Unternehmung dürfen keinen Zugang zu Ihren Firmendaten haben.
- **Integrität**
  Niemand sollte Ihre Daten unbemerkt und unautorisiert manipulieren oder sogar löschen können.

Vorsorgen ist besser als Heilen !

Auch hier gilt: Eine 100%-ige Sicherheit gibt es nicht ! Dennoch können Sie relativ einfach die folgenden Schritte einleiten:

- **Bedrohungen erkennen**
  Jede Unternehmung ist einzigartig. Bestimmen Sie die für Ihre Firma relevanten Risiken von Aussen und Innen.
- **Gegenmassnahmen ergreifen**
  Stellen Sie einen Massnahmenkatalog gegen die Bedrohungen zusammen, und realisieren Sie diesen.
- **Notfall-Plan erstellen**
  Erarbeiten und testen Sie einen Notfall-Plan für Ihr Unternehmen.
- **Informieren und schulen**
  Informieren Sie Ihre Mitarbeiter/innen und schulen Sie diese bei Bedarf.
- **Regelmässig kontrollieren**
  Überprüfen Sie Ihre getroffenen Massnahmen in periodischen Abständen.