

Weitere Geschäftsfelder

Organisation

Optimierung der Ablauforganisation.
Qualitätsmanagement (ISO 9000/9001).
Projektleitung (z.B. Einführung neuer Software).

Netzwerk (LAN, WLAN)

Netzwerkplanung / Serverplanung.
Installation.
Netzwerkadministration.
Entwicklung von Datensicherungskonzepten (z.B. Backup, Restore, Disaster Recovery).
Entwicklung von Schutzkonzepten (z.B. Firewall, VPN, Schutz vor Viren, Spyware u. Spam).

Betriebssysteme

Betriebssystem-Installation.
Automatisierte Betriebssystem-Aktualisierung.

Internet

Entwicklung von Internet Konzepten.
Gestaltung von Internet-Seiten.
Programmierung von Internet-Seiten.
Autoren-Systeme (CMS-Software).
Eintragung in Internet-Suchmaschinen (Web-Promotion).
Suchmaschinen-Optimierung (SEO).

Server-Software

Mail-Server (z.B. Microsoft Exchange).
Datenbank-Server (z.B. Microsoft SQL-Server).
Kaufmännische Software (ERP-Software wie z.B. von Microsoft, Sage oder Lexware).
Kundenmanagement Software (CRM-Software wie z.B. Act oder SuperOffice).

Office-Software

Microsoft-Office.
OpenOffice.

Training und Einweisung

Office-Software.
Kaufmännische Software.
Internet (z.B. Internet-Nutzung unter Sicherheitsaspekten).
Betriebssysteme.
Erstellung von Anleitungen und Dokumentationen.

Programmierung

Entwicklung von spezieller Individualsoftware (z.B. Datenbank-Abfragesoftware).
Programmierung von Makros (z.B. Microsoft Office).
Erstellung von Vorlagen, Druckmasken und Formularen (z.B. Microsoft, Sage oder Lexware).
Erstellung von Reports und Datenbankauswertungen (z.B. Access, SQL-Server, Crystal Reports).

Support

Wartungs- und Betreuungs-Verträge.
Hardware- und Software-Installation.
Hardware- und Software-Fehlerbeseitigung.

Dipl. Ing. J. Gehrke
IT-Beratung und Dienstleistung
Rahlstedter Straße 51 c
22149 Hamburg
Telefon: 040-670 44 123
Telefax: 040-670 44 124
E-Mail: info@gehrke.de

„First“ Sales & Marketing GmbH
Birtstrasse 16
22041 Hamburg
Telefon: 040-736163-0
Telefax: 040-73616311
E-Mail: info@f-s-m.de

IT-Sicherheit

- Analyse
- Konzeption
- Hardware
- Datensicherung
- Zugriffsschutz
- Training

Schützen Sie Ihre Daten und Investitionen.

Nutzen Sie die Chancen neuer Technologien.

Führen Sie Ihr Unternehmen erfolgreich in die Zukunft.

IT-Sicherheit

In dem Moment, wo Sie Ihr Netzwerk mit dem Internet verbinden, sind Sie bedroht. In dem Moment, wo sich ein Mensch an den PC setzt, erhöht sich das Risiko erheblich. Untersuchungen haben ergeben, dass Nachlässigkeit, Unwissenheit und Anwendungsfehler von Mitarbeitern die Hauptursache dafür sind, dass Schadprogramme in das Unternehmensnetzwerk gelangen. Dabei sind kleinere Unternehmen in der Regel stärker gefährdet als große. Besondere Aufmerksamkeit gebührt den unternehmenskritischen Daten, denn ihr Verlust kann zur Auflösung des Unternehmens führen.

Die Absicherung eines Netzwerkes ist, wegen der vielen Einflussfaktoren, äußerst komplex und kann auch niemals eine 100%ige Sicherheit bieten. Aber schon mit geringem Aufwand lässt sich vieles deutlich verbessern.

Wenn Sie einen kompetenten Partner für die Absicherung Ihres Netzwerkes suchen, sind wir Ihre erste Wahl.

Mögliche Bedrohungen

- Ausfall von Hardware.
- Verlust von Daten.
- Unberechtigter Zugriff auf Daten von außen.
- Unberechtigter Zugriff auf Daten von innen.
- Ausführen von Schadprogrammen.
- Fehlverhalten von Mitarbeitern.

Analyse

Vor jeder Absicherung erfolgt die Analyse der momentanen Situation. Weiterhin muss geklärt werden, gegen welche Bedrohung ein Schutz nötig ist und welche Ausfallzeiten akzeptabel sind.

Konzeption

Wir entwickeln gemeinsam mit Ihnen ein Schutz- und Sicherungskonzept, angepasst an Ihre Situation und Bedürfnisse.

Hardware

Die zentrale Hardware sollte vor Diebstahl und Feuer geschützt werden. Weitere Risiken werden durch eine unterbrechungsfreie Stromversorgung und Redundanz von wichtigen Teilen, wie z.B. Netzteilen, Festplatten u.s.w., minimiert.

Datensicherung

Basis aller Schutzmaßnahmen ist die Sicherung der unternehmenskritischen Daten. Dazu gehört ebenfalls die Möglichkeit einer kompletten Wiederherstellung - im Ernstfall auch auf andere Hardware.

Zugriffsschutz

Der Zugriffsschutz wird u.a. durch die Vergabe von eingeschränkten Benutzerrechten gewährleistet. Firewall, Proxy-Server, Anti-Viren- und Anti-Spyware-Programme sorgen dafür, dass nur erlaubte Aktionen ausgeführt werden.

Training

Der richtige und bewusste Umgang mit Internet-Programmen ist der wichtigste Schutz gegen Schadprogramme. Welche Internet-Seiten sollte man meiden? Welche Links und Buttons dürfen angeklickt werden?

Ist mein Netzwerk sicher?

Stellen Sie sich die folgenden Fragen:

- Was passiert, wenn der Strom ausfällt?
- Was passiert, wenn ein Server ausfällt?
- Was passiert, wenn eine Festplatte ausfällt?
- Was passiert, wenn Daten gestohlen werden?

- Was passiert, wenn Daten verloren gehen?
- Wie lange kann ich auf die EDV verzichten?

Realisierung

Wir installieren alle benötigten Hard- und Software-Komponenten. Wir schulen Ihre Mitarbeiter.

Maßnahmen

- Regelmäßige Datensicherung.
- Redundante zentrale Hardware.
- Notstromversorgung für die zentrale Hardware.
- Standardisierte Hard- und Software-Ausstattung der Arbeitsplätze.
- Regelmäßige Aktualisierung der Software.
- Sinnvolle Beschränkung der Zugriffsrechte.
- Einschränkung von mobilen Datenträgern.
- Regelmäßige Schulung der Mitarbeiter.
- Regelmäßige Anpassung der Maßnahmen an veränderte Bedrohungen.

Rundum-Betreuung

Wir entlasten Sie und bieten einen professionellen Service rund um Ihre IT-Sicherheit.

Wenn Sie mehr über unsere Produkte und Dienstleistungen erfahren möchten, rufen Sie uns an.