## HINWEISE ZU DEN ORGANISATORISCHEN FRAGEN

**Gesetzliche Vorschriften** (z.B. §14 Datenschutzgesetz) verpflichten jedes Unternehmen, das Computer einsetzt, angemessene Maßnahmen zur Gewährleistung der Datensicherheit und den Schutz der Daten zu treffen.

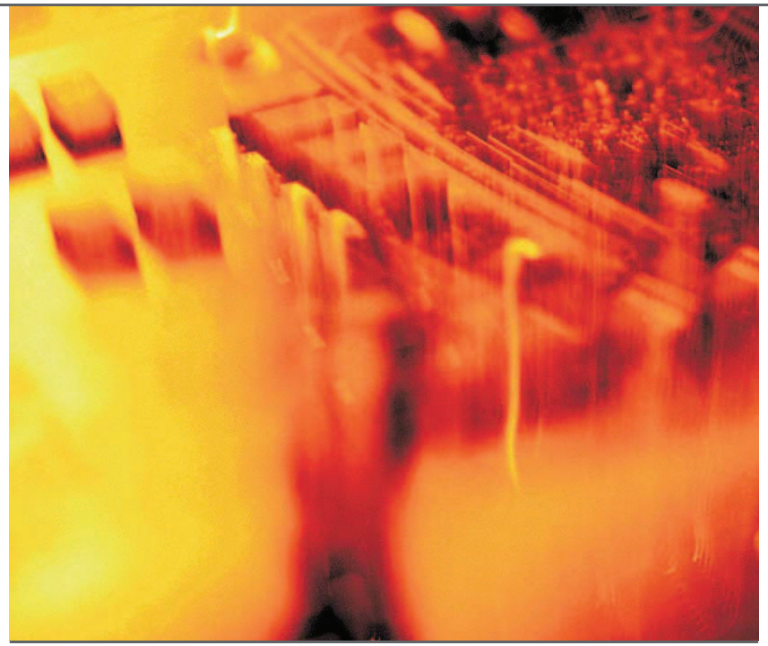
**Sicherheitskonzepte** können ihre Wirkung nur dann entfalten, wenn alle Computerbenutzer im Unternehmen entsprechend geschult sind und auf klare schriftliche Anweisungen zurückgreifen können.

Unzulänglich konzipierte und administrierte **Computernetzwerke** sind potentielle Schwachstellen und bieten **Angriffsflächen** für unbefugten Zugriff auf Unternehmensdaten.

**Schadsoftware** wird oft über harmlos scheinende Programme eingeschleppt, wobei dies sowohl über Internet als auch über Speichermedien erfolgen kann (Disketten, CD-ROM, USB-Stick, externe Speicher, PDA, Digitalkameras, etc.).

Mit funktionierenden umfassenden **Datensicherungs- und Notfallskonzepten** können Sie im Falle des Falles den Schaden in Grenzen halten.

**Impressum**
Fachverband Unternehmensberatung und Informationstechnologie
1045 Wien | Wiedner Hauptstraße 63
http://wko.at/it-security | it-security@wko.at
Druck: Druckerei Pillwein, 1040 Wien



# 10 FRAGEN
## an die Geschäftsleitung zur Abwehr von Schadprogrammen

IT-Security Experts

WIRTSCHAFTSKAMMER ÖSTERREICH
Unternehmensberatung·IT

## 10 FRAGEN an die Geschäftsleitung zur Abwehr von Schadprogrammen

Es gibt sie überall - die Schadprogramme.
Manchmal sind sie einfach lästig (z.B. Spam-Mails), manchmal werden Sie eine echte Bedrohung: (z.B. Trojaner). Je mehr das Internet ins tägliche Leben Einzug hält, desto größer wird die Gefahr, dass Schadprogramme in Ihre Computersysteme kommen,

- von denen Sie vielleicht nicht einmal wissen, dass sie bereits in Ihrem Rechner sind,
- von denen Sie nicht wissen, was sie anstellen,
- die Ihnen hohe Kosten verursachen können.

Die Zeitungen sind voll von Meldungen über Schadprogramme, die sogar Kontrolle über fremde EDV-Systeme ermöglichen. Wenn Sie nichts dagegen tun, hat das den selben Effekt, wie wenn Sie den Schlüssel in der Haustür stecken lassen und auf Urlaub fahren. Würden Sie das tun?

Wie kann man sich aber dagegen schützen? Kann man das überhaupt als KMU (Kleine und Mittlere Unternehmen)? Kann man sich so etwas leisten?

Die Antwort heißt „JA". Natürlich gibt es keinen 100%igen Schutz. Der würde jedes vernünftige Arbeiten unmöglich machen und jedes Budget sprengen. Aber man kann mit planbarem Aufwand das Risiko drastisch vermindern.

Die folgenden 10 Fragen sollen Ihnen helfen, einen Minimalschutz zu erreichen.

***Sollten Sie auch nur eine der 10 Fragen mit NEIN beantworten: so tun Sie etwas! Reden Sie mit einem Sicherheitsexperten Ihres Vertrauens!***

## ORGANISATORISCHE FRAGEN

1) Ist die Verantwortung für die Datensicherheit in Ihrem Unternehmen eindeutig festgelegt? Wird diese mit der erforderlichen Sachkenntnis und Sorgfalt wahrgenommen?

2) Verfügt Ihr Unternehmen über klare schriftliche Anweisungen zum Gebrauch von Computer, Netzwerk, E-Mail und Internet und sind diese allen betroffenen Mitarbeitern nachweislich bekannt?

3) Wenn in Ihrem Unternehmen ein Netzwerk verwendet wird - wissen Sie zuverlässig, dass es fachgerecht installiert wurde und liegt die laufende Administration in entsprechend qualifizierten Händen?

4) Ist in Ihrem Unternehmen durch ein angemessenes Berechtigungssystem sichergestellt, dass die Installation von Programmen nur von fachkundigen Administratoren vorgenommen werden darf und kann?

5) Haben Sie umfassende Datensicherungs- und Notfallskonzepte und werden diese in regelmäßigen Abständen (zumindest 1x jährlich) einem Test unterzogen?

## TECHNISCHE FRAGEN

6) Ist sichergestellt, dass in Ihrem Unternehmen die Betriebssystemkomponenten aller Computer laufend und systematisch aktualisiert werden?

7) Haben Sie auf allen Computern Virenschutzprogramme und werden diese laufend (täglich oder wöchentlich) aktualisiert?

8) Im Falle, dass Sie E-Mail benutzen: sind Sie sich der damit zusammenhängenden erhöhten Risiken und der Notwendigkeit von Abwehrmaßnahmen bewusst (Virenschutzprogramme, Mitarbeiterschulung, Updates)?

9) Im Falle, dass Ihre Computer Zugang ins Internet haben, - sind Sie sich der Gefahren und der Notwendigkeit von Abwehrmaßnahmen bewusst (Firewall, Virenschutzprogramm, Mitarbeiterschulung, Updates)?

10) Haben Sie ein fachmännisch installiertes und laufend gewartetes Firewallsystem im Einsatz, dessen Protokolle (Logfiles) regelmäßig überprüft und ausgewertet werden?

## HINWEISE ZU DEN TECHNISCHEN FRAGEN

Mit regelmäßigen **Updates** (Fehlerkorrekturen) der Betriebssystemkomponenten können bekannte Fehler behoben werden, bevor sie von Schadprogrammen ausgenutzt werden.

**Virenschutzprogramme** schützen - sofern sie laufend aktualisiert werden - Ihre Computer und Daten vor bereits bekannten Schadprogrammen.

Die meisten **Schadprogramme** werden über **E-Mail Verkehr** eingeschleust. Daher sollten hier spezielle Schutzmaßnahmen und Mitarbeitersensibilisierung vorhanden sein.

Über das **Internet** können Sie die ganze Welt erreichen. Aber ist Ihnen bewusst, dass auch jeder Hacker in der ganzen Welt Ihren Computer erreichen und für kriminelle Zwecke missbrauchen kann? Dagegen sollten Sie Maßnahmen ergreifen.

Firewalls sind spezielle Systeme, die unerwünschte Verbindungen verhindern und Angriffe erkennen können. Dafür ist allerdings erforderlich, dass sie fachmännisch installiert und laufend gewartet werden.

***Jede Änderung Ihrer Systemlandschaft (WLAN, Notebooks, etc…) birgt neue Sicherheitsrisiken in sich. Fragen Sie Ihren Sicherheitsexperten!***