Wer ist die größere Bedrohung? Mitarbeiter oder Cyber-Kriminelle?

Brisante Informationen landen auf dem Schreibtisch des Mitbewerbers, gestohlene Daten werden zum Verkauf angeboten. Ein Horrorszenario? Mitnichten, denn die eigenen Mitarbeiter können Unternehmen unter Umständen das Fürchten lehren. Von den eigenen Angestellten geht ebenso eine Bedrohung aus wie von Kriminellen aus dem Cybernet. Denn gerade in einer kleinen oder mittelständischen Firma haben die Mitarbeiter häufig Zugang zu vertraulichen Informationen.

Laut IDC („IT Security in Deutschland 2010“) fehlt es vielen Betrieben in Deutschland an einem ganzheitlichen Sicherheitskonzept.

Wussten sie zum Beispiel, dass:

- laut CERT, eine der wichtigsten Computer-Organisationen in den USA, Unternehmen ihr Hauptaugenmerk auf interne Bedrohungen richten sollten?
- ‚interne' Internetkriminalität einen viel größeren Schaden anrichtet als die von externen Cyberverbrechern?
- eine FBI-Studie zu dem Schluss kam: 80 Prozent aller Angriffe auf die IT-Sicherheit gehen auf das Konto von Insidern?
- laut einer Study des US-Sicherheitsanbieters Cyber-Ark 41 Prozent der IT-Mitarbeiter ihre Administrator-Rechte nutzen, um auf vertrauliche Informationen zuzugreifen?
- laut der selben Studie bei einer Kündigung jeder zweite Arbeitgeber Unternehmesdaten stehlen würde?

Und was bedeutet das für Sie und Ihre Kunden?

Egal ob Gefahr von „innen“ oder „außen“: Unternehmen müssen dringend Sicherheitsvorkehrungen treffen.

Dazu brauchen sie drei Dinge: Richtlinien, Technologien und Prozesse. Und die richtige Sicherheitssoftware.

AVG

So schützen Unternehmen ihre wertvollen Informationen

1. Definieren Sie Nutzerrichtlinien sowohl für Laptops, Netbooks und stationäre Rechner sowie für alle Medien, auf denen Daten gespeichert oder transportiert werden.

2. Um betriebsintern Akzeptanz zu finden, sollten diese Regeln möglichst einfach sein.

3. Definieren Sie Richtlinien auch für die Passwörter. Wählen Sie starke Passwörter

4. Sorgen Sie dafür, dass grundsätzlich alle PCs und IT-Systeme passwortgeschützt sind.

5. Setzen Sie stets eine aktuelle Sicherheitssoftware auf allen PCs und Servern ein, um ein Eindringen von Außen zu verhindern.

Warum glauben viele IT-Sicherheitsexperten, dass unzufriedene Mitarbeiter eine viel größere Sicherheitsbedrohung darstellen als ‚professionelle' Internetverbrecher?

- Sie haben legitimen Zugang zu Informationen, Systemen und dem Unternehmensnetzwerk.
- Sie müssen nicht wie ein Internetverbrecher per Hackerangriff ins System einbrechen, sie loggen sich ganz normal mit ihrem Passwort ein.
- Sie wissen in der Regel genau, wie sie ihrem Unternehmen am meisten schaden können – etwa, wenn sie Mitbewerber mit brisanten Informationen versorgen.
- Mitarbeiter mit finanziellen Problemen können einfach die Systeme, die sie jeden Tag für ihre Arbeit nutzen, für betrügerische Aktivitäten missbrauchen.
- Das Geschäftsumfeld hat sich in den letzten zwanzig Jahren stark verändert:
  - Unternehmensgrenzen werden immer durchlässiger.
  - Der Zugang zu vertraulichen Informationen beschränkt sich nicht mehr ausschließlich auf die eigenen Mitarbeiter, er umfasst auch Dienstleister, Berater, Lieferanten und manchmal sogar Kunden.

Ihr Fachhändler:

AVG