Wie werden Start-ups und kleine und mittelständische Unternehmen sicherer?

Immer mehr Geschäftsprozesse laufen online – von Internet-Banking bis zur Bestellung von Büromaterial oder der elektronischen Steuererklärung. Wer diese Prozesse nutzt, hat Vorteile, muss aber auch mit den Risiken richtig umgehen. Denn kleine Unternehmen können es sich einfach nicht leisten, dass ihre Systeme stundenlang wegen eines Virenbefalls ausfallen oder gar selbst zum Verbreiter von Schadsoftware werden.

Wussten sie, dass es laut IDC („IT Security in Deutschland 2010“) vielen Betrieben an einem ganzheitlichen Sicherheitskonzept fehlt?

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.

Richtlinien für den Faktor Mensch
Alle Mitarbeiter müssen wissen, dass sie ein große Verantwortung tragen und nicht leichtfertig mit Passwörtern und Zugangsdaten hantieren dürfen. Verpflichten Sie auch alle Mitarbeiter, eine Sicherheitsverletzung oder ein scheinbares Sicherheitsproblem auf einem Computer zu melden. Denn der Faktor Mensch ist entscheidend für den Erfolg jeder Sicherheitsstrategie.

Technologie
Jeden Tag werden neue Sicherheitslücken in Programmen und Systemen entdeckt. Sorgen Sie dafür, dass Betriebssysteme und Anwendungen regelmäßig die neuesten Patches erhalten. Die meisten Systeme verfügen dazu über eine automatische Update-Funktion. Nutzen Sie diesen Vorteil – das spart Zeit und erhöht die Sicherheit.

Prozesse
Viele Probleme lassen sich von Grund auf vermeiden, wenn ein Unternehmen sich einige grundsätzliche Regeln im Umgang mit der Sicherheit gibt. Legen Sie beispielsweise fest, wer zu welchen Daten Zugang haben muss. Überprüfen Sie, ob Backups angelegt sind und sichern Sie den Zugang zu diesen Medien. Legen Sie ein Vorgehen zum Umgang mit Sicherheitsproblemen fest, das jeder im Unternehmen so gut kennen sollte wie den Fluchtweg bei Brandgefahr.

AVG

Zehn Basis-Tipps zur Internetsicherheit

1. Einsatz einer Antivirensoftware, die mehr leistet als lediglich bekannte Viren, Würmer und Spyware vom System fernzuhalten. Sie muss Webseiten auf Malware untersuchen, bevor der Nutzer sie anklickt.

2. Verantwortungsvoller Umgang mit E-Mails, insbesondere bei unbekannten Absendern oder unvermuteten Nachrichten.

3. Vorsicht bei Links und Daten, die über Internet Messaging kommen. Erst prüfen, dann öffnen.

4. Endet ein Lieferantenvertrag oder hat ein Mitarbeiter gekündigt: nach dem letzten Arbeitstag alle Zugänge zum Netzwerk sperren.

5. Sicherheitsrichtlinien für alle Rechner implementieren, besondere Vorkehrungen treffen, wenn mobil genutzte Geräte wieder ans Firmennetz angeschlossen werden.

6. Dafür sorgen, dass mobile Geräte automatisch mit aktueller Antivirensoftware überprüft werden.

7. Keine unnötigen Downloads auf Firmen-Handys, -Smartphones, und -PDAs.

8. Bluetooth-Funktion ausschalten, wenn sie nicht benötigt wird.

9. Durch die Installation und regelmäßige Aktualisierung der Sicherheitseinstellungen der Firewall Schutz in WiFi-Netzen und -Zonen gewährleisten.

10. Firewalls direkt auf mobilen Geräten aktivieren oder installieren.

Ihr Fachhändler:

AVG