**Hacker-Angriffe**

**Wie sich kleine Unternehmen schützen können**

19.07.2012 - Laut einer Studie wurde jedes zehnte kleine oder mittlere Unternehmen (KMU) schon einmal Opfer eines Hacker-Angriffs. Lesen Sie hier wertvolle Sicherheitstipps.

Die Studie des britischen IT-Spezialisten Hiscox förderte nicht nur alarmierende Zahlen über die Zahl der Opfer von Hackerangriffen zu Tage. Sie ergab auch, dass 90 Prozent der befragten Unternehmen über keinen Versicherungsschutz gegen Internetkriminalität verfügen.

Der würde im Zweifel für die finanziellen Schäden, Betriebsunterbrechungsschäden und Rechtskosten aufkommt, wenn Unternehmen Opfer einer Cyber-Attacke werden.

Wie Hiscox herausfand, sind vier von zehn KMU-Inhabern (41 Prozent) besorgt, dass sich Hacker unberechtigten Zugang zu ihren Computersystemen verschaffen könnten. Aber nur 25 Prozent von ihnen hätten großes Vertrauen in die Sicherheitsmaßnahmen ihres Unternehmens.

Die Studie zeigte außerdem, dass Inhaber kleiner Unternehmen die Risiken von Internetkriminalität, wie Hacker-Angriffe (39 Prozent) oder Phishing (36 Prozent), stärker befürchten als die Gefahr, dass materielle Gegenstände (Laptops, Kundenunterlagen) aus dem Büro entwendet werden.

Hiscox gibt die folgenden Sicherheitstipps, wie sich KMU gegen Online-Risiken schützen können:

**1. Holen Sie sich professionelle Hilfe**

Die Führung eines Unternehmens ist eine Vollzeittätigkeit. Wenn Sie selbst kein IT-Fachwissen haben, sollten Sie eine professionelle Sicherheitsberatung in Anspruch nehmen. Das spart langfristig Zeit und Aufwand, indem sichergestellt wird, dass die Sicherheitsmaßnahmen den geschäftlichen Anforderungen genügen.

**2. Schützen Sie Ihre Daten mit einer internen "Need-to-know"-Richtlinie**

Wenn die Daten auf einem zentralen Dateiserver gespeichert werden, sollte geregelt sein, wer Zugang zu diesen Dateien hat. Auch dies kann vor versehentlichem oder vorsätzlichem Datenverlust schützen.

**3. Verschlüsseln Sie Ihre Daten**

Verschlüsseln Sie wichtige Informationen als zusätzliche Sicherheit, damit nur berechtigte Benutzer darauf zugreifen können. Daten auf mobilen Endgeräte sollten immer verschlüsselt werden.

**4. Achten Sie besonders auf den E-Mail-Verkehr**

Sobald Sie Internet und E-Mail geschäftlich nutzen, erhöht sich das Risiko eines Datenverlustes. Entwickeln Sie eine klare E-Mail-Richtlinie, sensibilisieren Sie die Mitarbeiter für das Thema Sicherheit und verfolgen Sie verdächtige E-Mails, selbst wenn es sich um einmalige Vorkommnisse handelt.

**5. Sorgen Sie für bessere Passwörter Ihrer Mitarbeiter**

Führen Sie die unternehmensweite Vorschrift ein, dass Mitarbeiter in ihren Passwörtern eine Kombination aus Zahlen und Buchstaben verwenden, die einen weitaus besseren Schutz vor Online-Kriminellen bieten.

**6. Sichern Sie Ihre Dateien**

Führen Sie Datensicherungen Ihrer Dateien durch und prüfen Sie Ihren Versicherungsschutz, damit Ihr Unternehmen nach einem Vorfall schnell wieder funktionsfähig ist.

**7. Achten Sie auf Ihre Hardware**

Gegenstände wie Laptops und Computermonitore sind häufig Ziele von Dieben. Die eigentlichen Kosten eines gestohlenen IT-Geräts betreffen nicht die Hardware, sondern entstehen durch den Datenverlust und die entgangene Produktivität. Schließen Sie die Server in einem Raum ein und räumen Sie Laptops am Ende eines Arbeitstags in eine sichere Schublade.