

Nachrichten für Meinungsbildner für 95.885 Abonnenten | 127.883 Meldungen | 40.621 Pressefotos


**Verwandte Meldungen**

Algorithmus für robusteres WLAN entwickelt

"Datenschlamperei muss bestraft werden"

**Weitere Meldungen**

Digitale Revolution für Bibliotheken und Museen

Grafikqualität von Film-Spezialeffekten erobert PCs

Tausende verzichteten auf CeBIT-Besuch

Hybrid-Scanner ordnet Dokumente nach Chaos-Prinzip

**Sponsored Links**

 Sie haben die Webseite  
Wir haben die Inhalte

**Monster Jobcorner**

SCHAUEN SIE DOCH MAL...

 Suche: 

 PLZ: 

Detailsuche

**Werbung**

 pte090309030 **Computer/Telekommunikation, Medien/Kommunikation**

Share |



## WLAN-Sicherheit erfordert klare Richtlinien

Alte Protokolle und Angestellte wesentliche Risiken für Unternehmen

Mountain View

(pte/09.03.2009/13:55) -

Angesichts der großen Verbreitung von drahtlosen Netzwerken wie insbesondere WLAN werden verbesserte

Sicherheitsmaßnahmen immer wichtiger, warnen Analysten von Frost & Sullivan. Große Risikofaktoren für Unternehmen umfassen dabei die Verwendung alter, unsicherer Protokolle sowie die eigenen Mitarbeiter.

"Angestellte werden als größtes Risiko für die drahtlose Sicherheit gesehen, da viele nicht wissen, was auf dem Spiel steht, wenn Daten auf Smartphones oder Laptops kompromittiert werden oder verloren gehen", so Frost-&-Sullivan-Analyst Achyuthanandan S. Auf Firmenseite wiederum würde oft der Wert klarer Sicherheitsrichtlinien nicht verstanden.



Drahtloser Netzwerkzugriff - User und Protokolle als Risiken (Foto: pixelio.de, Kigoo Images)

"Viele Unternehmen begreifen nicht, wie wichtig es ist, eine zentral verwaltete Richtlinie für den drahtlosen Netzwerkzugriff zu definieren und durchzusetzen", sagt Achyuthanandan. In der Praxis seien die Richtlinien und nicht die Technologie in Sicherheitsbelangen ausschlaggebend. Dabei reichen Frost & Sullivan zufolge klare Richtlinien in Kombination mit grundlegenden Sicherheitsvorkehrungen meist aus, um drahtlose Netzwerke vor den meisten Problemen zu schützen. Für Unternehmen wäre es laut Achyuthanandan auch wichtig, höheres Augenmerk auf die Erziehung der Mitarbeiter zu legen. "Sie umgehen oft Sicherheitsregeln und liefern damit die ganze Organisation Angreifern aus", erklärt der Analyst.

Einen weiteren großen Risikofaktor in Sachen drahtloser Netzwerke sieht Frost & Sullivan darin, dass viele Unternehmen weiterhin auf standardisierte Protokolle vertrauen würden, bei denen viele Schwachstellen bekannt sind. Als Beispiel wird etwa "Wired Equivalent Privacy" (WEP) genannt. Dieser Algorithmus zur Sicherung von WLAN-Übertragungen wird vom Institute of Electrical and Electronics Engineers <http://www.ieee.org> bereits seit 2004 offiziell abgelehnt, da er die Sicherheitsziele nicht erreicht. In der Praxis sollten also längst sicherere Nachfolger wie "Wi-Fi Protected Access" (WPA) zum Einsatz kommen.

Wichtig ist entsprechende Sicherheit angesichts der steigenden Bedeutung von Smartphones und Laptops im Geschäftsleben. Der Internet-Zugriff über teils öffentliche WLANs ist bei solchen Geräten praktisch nicht mehr wegzudenken. "Es wird geschätzt, dass über 90 Prozent aller heute eingesetzten Laptops mit WLAN ausgerüstet sind", sagt Yin Fern Ko, Frost & Sullivan Technical Insights Research Analyst. Entsprechend häufig sind Nutzer den damit verbundenen Gefahren durch immer neue Hacker-Angriffe ausgesetzt. Die wachsende Verbreitung von WLAN und das Nahen des Übertragungsstandards 802.11n haben aber auch die Entwicklung im Bereich entsprechender Sicherheitstechnologien vorangetrieben, so Frost & Sullivan. (Ende)

email: [pichler@presstext.com](mailto:pichler@presstext.com)  
Tel. +43-1-81140-303



presstext  
ist jetzt  
börsenfit.

Versenden Sie Ihre  
Pflichtmitteilungen  
kostenfrei!

adhoc

Mehr Info

[Startseite](#) | [Abo](#) | [Aussendung](#) | [Termine](#) | [Pressefotos](#) | [Adhoc-Dienst](#) | [Fotodienst](#) | [Toplocations](#) | [Archiv](#) | [Produkte](#) | [presstext4Joomla](#)  
© 1997-2010 Presstext | [Nutzungsbedingungen](#) | [AGB](#) | [Impressum](#) | [Österreich](#) | [Schweiz](#) | [Europa](#) | [Corporate](#) | [Kontakt](#)