

**Zeitschrift:** Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

**Herausgeber:** Swisscom

**Band:** 81 (2003)

**Heft:** 9

**Artikel:** Verletzliche Netze besser schützen

**Autor:** Weber, Felix

**DOI:** <https://doi.org/10.5169/seals-876672>

### Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 11.02.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

Orbit/Comdex 2003

# Verletzliche Netze besser schützen

Das Sicherheitsbewusstsein der Firmen im Bereich der IT ist zwar gestiegen, aber nur selektiv: Nach einer Studie der Meta Group bewerten insbesondere kleinere Unternehmen die Gefahr durch Virenbefall und «bösertigen» Code nach wie vor als grösstes Risiko. Am «Information Security Park» der Orbit/Comdex erfahren Besucher, wie es mit der Sicherheit von mobilen Anwendungen steht.

**U**nzählte Hackerangriffe, immer raffiniertere Computerviren und -würmer und durch Anfragelawinen blockierte Websites zeigen, dass die Sicherheit der IT-Systeme auf dem Spiel steht; und zwar nicht nur beim Staat und

FELIX WEBER

bei bekannten Grossfirmen, sondern auch bei den KMU. Praktisch alle Betriebe setzen heute auf irgendeine Form von Breitbandzugang zu ihrem Firmennetz – und dies mit gutem Grund: Die permanente Hochgeschwindigkeitsverbindung bietet ihnen signifikante Geschäftsvorteile. Gleichzeitig ist das Firmennetz aber auch umso mehr exponiert. Das kann bei all den Gefahren, die durch Fernzugriffe drohen, böse Folgen haben. Mitunter genügt ein einziger erfolgreicher Hackerangriff, um wertvolle Daten zu stehlen, zu verändern oder zu löschen; oder um das ganze Firmennetz lahm zu legen.

## Bequemlichkeit vor Sicherheit?

Seit immer mehr Verbindungen über fixe Kabel durch Funkverbindungen abgelöst werden – was für die Anwender zweifelsohne bequemer ist –, hat sich das Problem noch verschärft: Bei drahtlosen Netzen (Wireless Local Area Network, WLAN) ist die Angriffsfläche um ein Vielfaches grösser. WLANs können zum Albtraum der IT-Administratoren werden – erst recht, wenn Mitarbeiter beginnen, im Firmennetz ohne Erlaubnis eigene Funkzugänge (Wireless Access Points)

einzurichten, damit sie bequemeren Zugang zum Firmennetz haben. Wenn schon ein herkömmliches Firmennetz nicht einfach zu schützen ist, wie soll denn das bei einem WLAN-System geschehen? Die bisherige Praxis hat zumindest etwas klar gezeigt: Der aktuelle WLAN-Sicherheitsstandard mit der Bezeichnung Wireless Equivalent Privacy (WEP) reicht dazu bei weitem nicht aus. Zwar werden dabei die per Funk übertragenen Daten verschlüsselt, aber da alle Benutzer den gleichen Schlüssel verwenden, kann dieser leicht verraten werden. Dabei ist das nicht einmal nötig. Für einen guten Hacker ist es nämlich nur eine Frage der Zeit, ein WEP-verschlüsseltes Netz zu knacken: Er braucht dazu lediglich genügend Datenpakete einzufangen und diese mit einem einschlägigen Hacker-Tool (im Internet frei erhältlich) zu analysieren. Die Software eruiert daraus den Schlüssel und übersetzt die übertragenen Daten in Klartext. Jetzt braucht der Hacker nur noch zu warten, bis er aus dem Datenverkehr eine Benutzerkennung samt Passwort aufschnappen kann. Damit ausgerüstet, stehen ihm Tür und Tor des WLAN offen.

## Zusätzliche Sicherheit einbauen

Für eine ausreichende Sicherheit in einem WLAN sind technische und organisatorische Massnahmen nötig, die weit über WEP hinausgehen. Zu den technischen Massnahmen gehört mindestens eine Firewall, die das drahtlose Netz gegen die übrigen IT-Systeme abschottet und so zumindest die gängigsten Einbruchversuche abwehrt. Zudem sollte der Funkverkehr über so genannte virtu-



Je exponierter das Firmennetz, umso grösser sind die Gefahren, die durch Fernzugriffe drohen.

elle private Netzwerke (VPN) laufen, eine Technik, die sich bereits in Fixnetzen bewährt hat. VPNs sorgen für abhörsichere Verbindungen von den Mobilgeräten über den Wireless Access Point bis zum dahinter liegenden Firmennetz. Dort erfolgt dann auch die Authentifizierung der Benutzer.

Zu den organisatorischen Sicherheitsmassnahmen gehört die Verpflichtung der Anwender, registrierte WLAN-Karten nicht weiterzugeben und entsprechende Verluste sofort zu melden – insbesondere, wenn die so genannten MAC-Adressen (Media Access Control) der Karten zur Authentifizierung der Anwender verwendet werden. In WLANs sollte zudem verboten sein, Laufwerke für andere Benutzer freizugeben, denn damit würde man Hackern einen besonderen Leckerbissen präsentieren.

Im Prinzip ist das technisch alles kein Problem: Auf dem Markt gibt es eine Vielzahl von entsprechenden Lösungen. Trotzdem ist die Aufgabe in der Praxis alles andere als trivial – vor allem, wenn die Sicherheitsausrüstung von unterschiedlichen Anbietern stammt. Solche heterogenen Systeme sind komplex, teuer und schwer zu managen. Gewitzt durch negative Erfahrungen, setzt sich bei den Anwendern langsam die Erkenntnis durch, dass auf dem Gebiet der WLAN-Sicherheit integrierte Lösungen vorzuziehen sind. Inzwischen haben das auch die Gremien erkannt, die für die Standardisierung der Telekommunikation zuständig sind. Das Resultat: In Zukunft sollen zwei neue Funknetz-Standards (802.11i und 802.1x) für mehr Sicherheit sorgen. Mit diesen wären dann aufwändige Mass-

breiteten Missstand und seinen gravierenden Folgen zu begegnen.

## WLAN-Schwachpunkte der drahtlosen Netze

Funksignale können grundsätzlich von allen Nutzern empfangen werden, ob sie nun berechtigte oder unberechtigte Nutzer sind. Damit laden drahtlose Netze geradezu ein zum so genannten «Drive-By Hacking». Auf Deutsch: Hacker machen sich einen Sport daraus, nach WLANs Ausschau zu halten und sich wenn möglich in diese einzuklinken. Dass Letzteres sehr viel öfter gelingt als den Betreibern lieb ist, liegt an den bekannten Schwachpunkten der noch jungen Technik:

## Mangelnde Zugangskontrolle

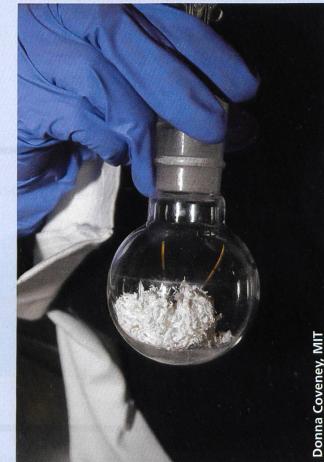
Viele WLANs arbeiten ohne oder blos mit leicht überlistbaren Zugangskontrollen. Das ist eine riskante Sache: Denn wer einmal in einem solchen Netz drin ist, kann schalten und walten wie er will – auch in Bereichen, wo er gar nichts zu suchen hat. Solche Netze sind leichte Beute für Hacker jeglicher Couleur – und diese lassen sich in der Regel nicht zweimal bitten.

## Teure Sicherheit

WLAN-Betreiber, die ihr Netz gut absichern wollen, müssen einiges an Aufwand in Kauf nehmen. Vor allem, wenn Lösungen unterschiedlicher Hersteller zum Einsatz kommen, wird es kompliziert und entsprechend teuer.

**Felix Weber,** dipl. Math. ETH, Wissenschaftsjournalist BR, Meilen

## FORSCHUNG UND ENTWICKLUNG



Donna Coveney, MIT

Verbindungselement zwischen den beiden Extremen wirken. In den Übergängen zwischen den kristallinen und den elastischen Zonen scheint die Problemlösung zu liegen. Wenn man eine solche synthetische Faser herstellen könnte, liessen sich neue Materialien für extreme Einsätze «designen», zum Beispiel eine sehr leichte kugelsichere Weste. Oder vielleicht ein Glashausdach, das bei Hagelschlag nicht zu Bruch geht.

**MIT**  
News Office  
77 Massachusetts Ave  
Room 5-111  
Cambridge MA 02139  
USA  
Tel. +1-617-258 5402  
Homepage:  
<http://web.mit.edu/newsoffice/www>