Verletzliche Netze besser schützen

Autor(en): **Weber, Felix**

Objekttyp: **Article**

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

Band (Jahr): **81 (2003)**

Heft 9

PDF erstellt am: **31.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-876672

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://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 «bösartigen» 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.

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

Ungezählte 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 virtuelle 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 Benützer 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 heterogene 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 Massnahmen wie die oben erwähnten virtuellen privaten Netzwerke nicht mehr nötig. Die Sicherheit in der zusehends vernetzten IT-Welt ist eine hochkomplexe Angelegenheit, die selbst Experten herausfordert. Entsprechend gross sind der Wissensnotstand der gewöhnlichen Anwender und die Sicherheitslücken in ihren Systemen. Gezielte Aufklärung ist der erste Schritt, um diesem weit verbreiteten 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 bloss 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.

Schwächen beim Standard

Die meisten heutigen Funknetze arbeiten nach dem internationalen Standard 802.11b. Dieser Standard schreibt zwar eine Datenverschlüsselung vor, aber diese lässt sich relativ leicht knacken, und zwar mit Tools, die im Internet frei zugänglich sind.

Auch die Benutzer-Authentifizierung ist eine leicht überwindbare Hürde: Zwar sind die Wireless Access Points in der Regel mit Passwörtern geschützt, aber weil diese im Klartext übermittelt werden, ist der Schutz beinahe wirkungslos.

Teure Sicherheit

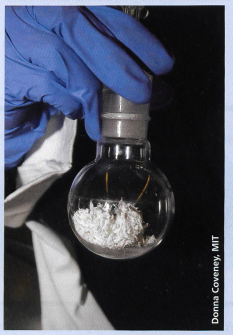
WLAN-Betreiber, die ihr Netz gut absichern wollen, müssen einiges an Aufwand in Kauf nehmen. Vor allem, wenn Lösungen unterschiedlicher Hersteller zum Einsatz kommen, wird es kompliziert und entsprechend teuer. 12

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

FORSCHUNG UND ENTWICKLUNG

Bald künstliche Spinnenfasern?

Seit langem faszinieren die fantastischen Eigenschaften von Spinnennetzen die Naturwissenschaftler: sie sind hoch elastisch, fast unzerreissbar, schockabsorbierend und sehr leicht. Wenn man nur eine solche Faser synthetisieren könnte. Das MIT sucht jetzt nach Wegen und hat erste Teilergebnisse realisiert (Bild). Associate Professor Paula Hammond aus der Chemieabteilung und Professor Gareth McKinley aus der Mechanik versuchen, den natürlichen Aufbau des Spinnwebpolymers zu imitieren. Einer der denkbaren Wege führt über die Synthese unterschiedlicher Materialzonen. Da wechseln sich winzige Regionen von weichem, elastischem Material ab mit Regionen von fester, kristalliner Form. Dazwischen liegen solche mit mittleren Eigenschaften, die als 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.



Donna Coveney, MIT

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