News

Objekttyp: **Group**

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

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

Heft 4

PDF erstellt am: **21.07.2024**

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

Gefahrenmeldungen

Panikmache oder Wirklichkeit?

Bis zum Ende des Jahres 2004 greifen wahrscheinlich mehr als hundert Millionen drahtlose Geräte auf das Internet zu. Dies gibt Anlass zu den folgenden Fragen: Wie anfällig sind wir gegenüber den heutigen Viren und welche praktischen Massnahmen können wir zu ihrer Abwehr in der nahen Zukunft ergreifen?

Zurzeit sind die Gefahren für Verwender drahtloser Technologien noch relativ gering und nicht sehr komplex. Einige Hersteller bieten bereits Anwendungen an, mit denen drahtlose Geräte gegen diese Gefahren geschützt werden können. Bisher gilt die Bedrohung jedoch noch nicht dem gesamten Funktionsumfang der entsprechenden Betriebssysteme und zugehörigen Übertragungsplattformen wie beispielsweise Bluetooth, GPRS oder UMTS (3G).

Das Risiko steigt

Mit der Verbreitung drahtloser Technologien steigt auch das Risiko. Das gesamte Ausmass der potenziellen Gefahren wird wohl erst deutlich, wenn einige dieser neuen Technologien gemeinsam mit bereits etablierten Systemen verwendet werden können. Sobald die PDA-Betriebssysteme wie EPOC, Palm OS und Windows CE nicht mehr nur auf Standalone-Geräten, sondern auch auf den neuen «intelligenten» Telefonen und drahtlosen PDAs eingesetzt werden, steht zu erwarten, dass Benutzer und Unternehmen auch entsprechende neue Anwendungen fordern werden. Dieser Übergang von Terminals mit sehr eingeschränkter Funktionalität hin zu flexiblen Plattformen mit umfassenden Funktionen und der Fähigkeit zum drahtlosen Herunterladen und Ausführen von Drittanbieteranwendungen öffnet jedoch auch das Tor für einen umfassenden bösartigen Angriff.
Genauso wie Standardanwendungen, wie Outlook und Windows, schnell zum Hauptziel von Hackern und Virenprogrammierern wurden, werden sich diese beiden Gruppen mit zunehmender Ausbreitung den drahtlosen Geräten zuwenden. Zu den sehr wahrscheinlichen Gefahren der Zukunft wird gehören, dass virusinfizierte Dateien von Gerät zu Gerät «gebeamt» und dass ausgewachsene Würmer sich über sämtliche vorhandenen Kommunikationssysteme verbreiten werden.

Was tun?

Die neuen drahtlosen Technologien sind sehr interessant, ihr wahres Potenzial wird sich jedoch erst wirklich zeigen, wenn sie etwas an Neuigkeitswert verloren haben. Bis dahin sollte schon einmal über eine Sicherheitsstrategie zum Schutz der drahtlosen Geräte nachgedacht werden. Es ist vorerst zu überlegen, wie geplant ist, die drahtlosen Technologien im Unternehmen einzusetzen, welche Mindestanforderungen erfüllt sein müssen und welche Erfolgserwartungen vorhanden sind. Der Anbieter kann darüber Auskunft geben, welche Massnahmen er zum Schutz gegen die neuen Gefahren ergriffen hat bzw. zu ergreifen gedenkt. Vor allem sollte zuerst abgeklärt werden, wie anfällig die derzeitige Infrastruktur gegenüber bösartigen Angriffen ist, bevor das gesamte Budget in neue Schutzmassnahmen investiert wird. Erst dann sollte der geeignete Partner gesucht werden, der bei der langfristigen Minimierung dieser Bedrohungen behilflich sein kann. [4]

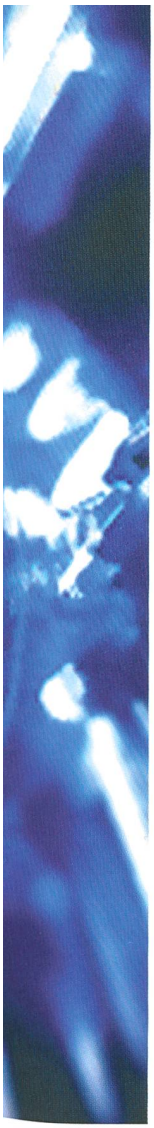
Frost & Sullivan
Stefan Gerhardt
Clemensstrasse 9
D-60487 Frankfurt a. Main
Tel. +49 (0)69 770 33 11
E-Mail: stefan.gerhardt@frost.com
Homepage: www.wireless.frost.com

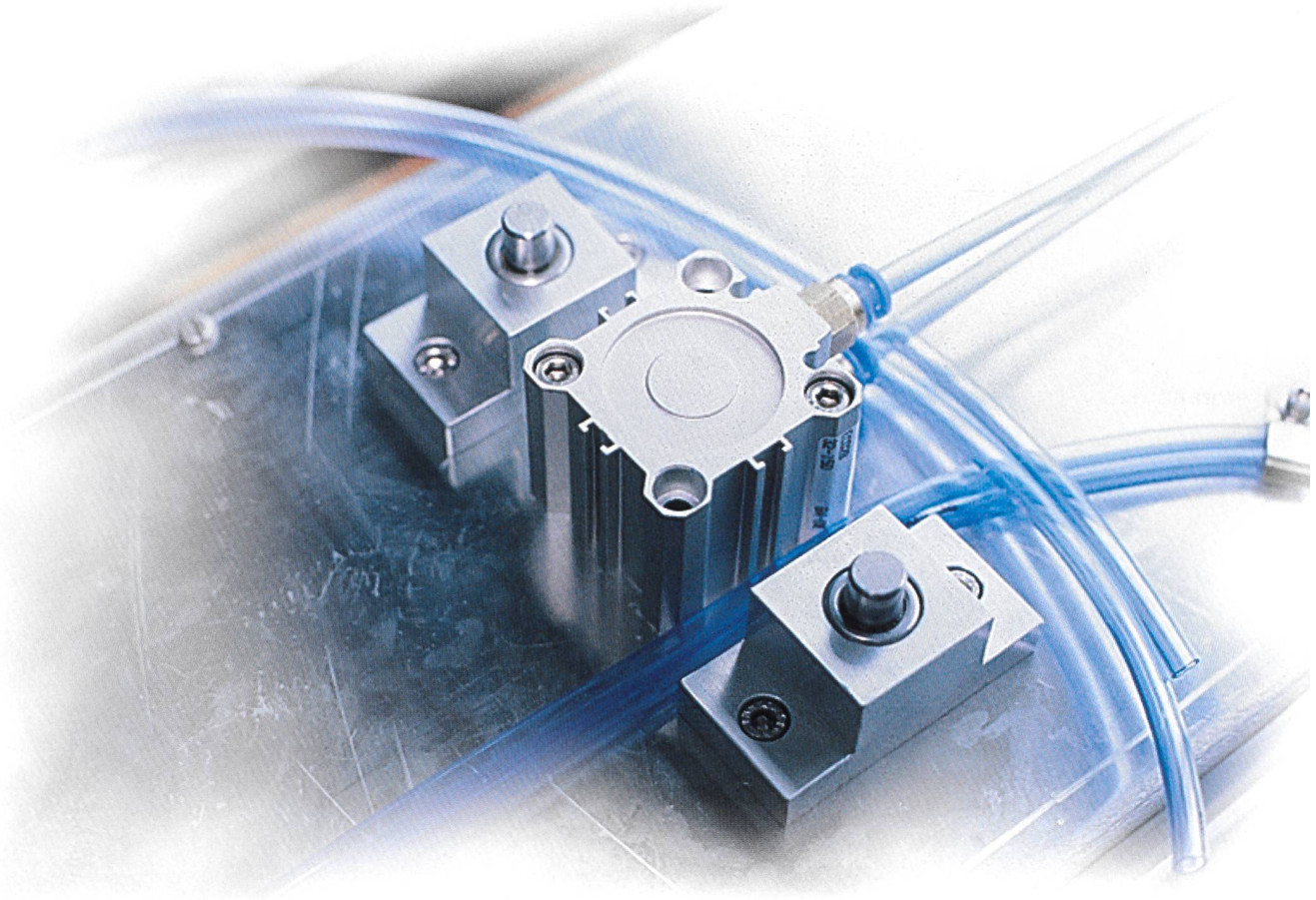
Drahtloses Internet: zu grosser Wirrwarr?

WLAN (oder WiFi, Wireless Fidelity, wie die Amerikaner sagen), irritiert die Anwender. Der Grund liegt in drei nebeneinander existierenden Normen, die alle die gleiche Bezeichnung tragen (IEEE 802.11) und sich nur durch den Endbuchstaben unterscheiden: b, a und g. Die bereits laufende b-Variante liefert theoretisch 11 Mbit/s bei 2,4 GHz. Doch da liegen viele andere Dienste auch, und die amerikanische FCC befürchtet zu Recht Interferenzen. Die Version a arbeitet bei 5 GHz, könnte theoretisch 54 Mbit/s anbieten, doch auch hier haben sich schon andere Dienste breit gemacht. Die g-Variante (u. a. vertreten durch Apple) liegt irgendwo zwischen a und b. Die Anbieter der künftigen Mobilfunksysteme (3. Generation) sehen das alles mit Misstrauen, nehmen die WiFi-Dienste ihnen doch Übertragungsbänder weg.

Zahl der DSL-Anschlüsse in Japan kräftig gestiegen

Nach Angaben des japanischen Postministeriums gab es Ende 2002 in Japan 5,64 Mio. DSL-Anschlüsse (Digital Subscriber Lines). Gegenüber dem Vorjahr ist dies ein Zuwachs von 370%.





HIGH QUALITY

www.schillingag.com

Ihr kompetenter Partner für fertigungsgerechte Konstruktion, marktgerechte Produktion und termingerechte Lieferung.

Your competent partner for manufacturing-oriented machine design and market-oriented production – delivered on time.

PSA
PAUL SCHILLING AG

Präzisionsmechanik und Maschinenbau, Konstruktionsbüro.
Werkstrasse 7, CH-9434 Au/SG
Telefon +41 (0)71 747 51 51, Fax +41 (0)71 747 51 61
psa@schillingag.com www.schillingag.com