International Working Group
on Data Protection
in Telecommunications

675.28.17 15. April 2004

Arbeitspapier zu potenziellen Risiken drahtloser Netzwerke
Allgemeine Empfehlungen

- angenommen auf der 35. Sitzung am 14./15. April 2004 in Buenos Aires -

- Übersetzung -

Drahtlose Kommunikation bietet zahlreiche Vorteile wie Portabilität und Flexibilität, erhöhte Produktivität und niedrigere Installationskosten und wird zunehmend populärer. Drahtlose Technologie deckt eine breite Auswahl an unterschiedlichen Fähigkeiten ab, ausgerichtet auf verschiedene Anwendungen und Bedürfnisse. Vorrichtungen drahtloser lokaler Netzwerke (Wireless local area network – WLAN) erlauben den Nutzern zum Beispiel, ihre Laptops von einer Stelle zur anderen innerhalb ihres Büros oder zu Hause zu bewegen, ohne dass dafür Kabel notwendig wären und ohne dass die Netzwerkverbindung verloren geht.

Ad hoc Netzwerke, wie solche, die durch Bluetooth ermöglicht werden, erlauben den Datenabgleich mit Netzwerksystemen, die Anwendungsteilung zwischen verschiedenen Geräten und beseitigen die Notwendigkeit von Druckerkabeln und sonstigen Verbindungen zu Zusatzgeräten. Mobile Endgeräte wie Personal Digital Assistants (PDA) und Mobiltelefone erlauben Außendienstmitarbeitern den Abgleich von persönlichen Datenbanken und liefern den Zugang zu betrieblich bereitgestellten Diensten wie E-Mail und Internet. Drahtlose Technologie stellt für die Zukunft eine größere Funktionalität in Aussicht.

Dennoch gibt es Risiken bei der Nutzung von drahtloser Technologie, insbesondere weil das der Technik zugrundeliegende Kommunikationsmedium, die Funkverbindung, offen ist für Angriffe, wenn nicht angemessene Sicherheitsvorkehrungen getroffen werden.

Die Risiken umfassen:
- Das Abfangen von Standortdaten und anderen persönlichen Daten über den Netzwerknutzer;
- Unautorisierter und unbemerkter Zugang zu betrieblichen Netzwerken durch externe Nutzer;

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.datenschutz-berlin.de

- Umgehung von betrieblichen Firewalls und E-Mail-Filterung durch Nutzer drahtloser Netze, die auch Zugang zu Unternehmens- oder Behördennetzen haben, was zu einem Verlust des Schutzes vor Virusattacken und Spam führt;
- Abhören persönlicher Kommunikation und unentdeckte Verbindungen zwischen Nutzern drahtloser Netze, insbesondere auf öffentlichen Plätzen.

Die Arbeitsgruppe fordert sowohl die IEEE Task Group[1] und die WI-FI Alliance[2] als auch die Verkäufer von Produkten der drahtlosen Technologie auf, der Datensicherheit und dem Datenschutz einen hohen Stellenwert bei der gegenwärtigen und zukünftigen Entwicklung von drahtlosen Technologien einzuräumen[3].

Empfehlungen

A) Risikoanalyse und gewünschtes Sicherheitsniveau

Betreiber drahtloser Netzwerke[4] sollten sich der technischen und der sicherheitstechnischen Auswirkungen von drahtlosen und mobilen Technologien bewusst sein.

Betreiber drahtloser Netzwerke sollten eine Risikoeinschätzung durchführen und eine Sicherheitspolitik entwickeln bevor sie drahtlose Technik einsetzen, um sicherzustellen, dass sie die Risiken für ihre Informationen, Systemoperationen und die Kontinuität der Operationen überprüft haben, und diese handhaben und entschärfen können.

Nutzern drahtloser Netzwerke sollten die technischen und sicherheitstechnischen Auswirkungen drahtloser und mobiler Technologien bewusst gemacht werden.

In ihrem eigenen Interesse sollten alle Nutzer eine persönliche Risikoeinschätzung durchführen, bevor sie drahtlose Technologie oder Dienste kaufen, benutzen oder betreiben, weil ihre eigenen persönlichen Sicherheitsanforderungen bestimmen welche Produkte oder Dienste in Betracht kommen.

B) Netzwerkparametereinstellungen

Betreiber drahtloser Netzwerke sollten den Einsatz drahtloser Technologie sorgfältig planen und geeignete Parameter an den Geräten setzen, um sowohl die Netzwerkfunktion als auch die Sicherheit der Dienste zu garantieren. Insbesondere sollte der Netzwerkzugang durch hohe Sicherheitsstandards zusätzlich geschützt werden.

---

[1] IEEE 802.11 Working Group for Wireless Area Networks (WLANs). http://grouper.ieee.org/groups/802/11/. The IEEE (Eye-triple-E) is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc., although the organization is most popularly known and referred to by the letters IEEE.

[2] Wi-Fi Wireless Fidelity http://www.wi-fi.org/ The Wi-Fi Alliance organization, a nonprofit industry group, promotes the acceptance of 802.11 wireless technology worldwide, and ensures that all Wi-Fi CERTIFIED 802.11-based wireless networking gear works with all other Wi-Fi CERTIFIED equipment of the same frequency band and features.

[3] "NIST Publication 800-48: Wireless Network Security 802.11, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf. NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission in four cooperative programs.

[4] Englisch: “network manager” = anyone who wants to deploy and use wireless networks.

Nutzer sollten angeleitet werden und es sollte ihnen bewusst gemacht werden, wie sie ihr drahtloses Gerät konfigurieren müssen, um ein hohes Sicherheitsniveau und Vertraulichkeit herzustellen.

C) Sicherheitsmanagement

Betreiber drahtloser Netzwerke sollten Sicherheitsmaßnahmen einführen und kontrollieren, um die Sicherheit der drahtlosen Netzwerke zu erhalten.

Betreiber drahtloser Netzwerke müssen regelmäßig die inhärenten Sicherheitsmerkmale, wie z.B. die Authentifizierung und Verschlüsselung, die in drahtlosen Netzwerken existieren überprüfen. Die Authentifizierung ist in drahtlosen Netzwerken besonders wichtig und könnte auf einer strengeren Zugriffskontrolle mit regelmäßigem Wechsel der Passwörter basieren.

Betreiber drahtloser Netzwerke sollen die Nutzer über das Sicherheitsniveau in den Netzwerken und über die verfügbaren Maßnahmen zur Sicherstellung der Vertraulichkeit der Kommunikation informieren.

D) Weitere Erwägungen

Anbieter drahtloser Netzwerke sollten die rechtlichen Anforderungen[5] einhalten, die in den unterschiedlichen Rechtssystemen differieren können.

Die Arbeitsgruppe betont ferner, dass Sicherheitskonzepte für die Nutzer schwer zu verstehen sind. Die praktische Anwendung dürfte selbst für erfahrene IT-Spezialisten schwierig sein. Die Industrie als Ganzes sollte das Problem sowohl auf der technischen als auch auf der Informationsebene angehen, um das Vertrauen in die Technologie zu verbessern. Die Voreinstellungen sollten ein hohes Datenschutzniveau gewährleisten.

Internet-Diensteanbieter, insbesondere Web-Mailer, sollten die Möglichkeit zur Verschlüsselung auf Anwendungsebene bieten. Werden sensitive Daten über drahtlose Netzwerke übertragen ist eine starke Verschlüsselung unverzichtbar.

Nutzer sollten nicht davon abgehalten werden, öffentlich zugängliche Dienste anonym oder unter Pseudonym zu nutzen.

[5] Vgl. Art. 4 Richtlinie 2002/58/EC des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).