XXII. GP.-NR
1120/J
2003 -11- 21

ANFRAGE

der Abgeordneten Mag. Johann Maier
und GenossInnen
an den Bundesminister für Wirtschaft und Arbeit
betreffend Wireless Lan; Sicherheits- und Datenschutzprobleme

Nach einem Verordnungsentwurf des BM für Verkehr, Technik und Innovation wird hinsichtlich der in der Anlage genannten Funkanlagen, die generelle Bewilligung zur Errichtung und zum Betrieb erteilt. Es liegen zwar die Gerätebeschreibungen vor, es ist allerdings unbekannt, ob diesen Gerätebeschreibungen auch Verhaltensvorschriften beigefügt wurden bzw. werden, die bei der Ausübung der Bewilligung zu befolgen sind. Dies betrifft nicht nur die Sicherstellung der zulässigen Strahlungsleistung, sondern auch sonstige telekommunikations- sowie auch datenschutzrechtliche Bestimmungen.

In der dem Verordnungsentwurf beigefügten Anlage findet sich unter A (Funksendeanlagen für bestimmte Schnittstellen) in der Tabelle 2 der Gerätekategorie auch „Wireless-Lan" (FSP-LD 047). **Die Aufnahme von Wireless Lan in diese Verordnung muss allerdings hinterfragt werden.**

Begründet wird diese Verordnung generell mit der technischen Weiterentwicklung, wobei insbesondere die Liste der Schnittstellenbeschreibungen ergänzt und einzelne Schnittstellenbeschreibungen aufgrund international zu beachtender Vorgaben geändert wurden. Datenschutzrechtliche Problemstellungen wurden dabei nach unserem Informationsstand – die Verhaltensvorschriften sind uns bedauerlicherweise nicht bekannt – nicht berücksichtigt. Dies gilt insbesondere für „Wireless–Lan".

So wird derzeit keiner der zahlreichen dieser „illegalen Zugriffe" von Hackern auf Datenbestände von Unternehmen und öffentlichen Einrichtungen, die Wireless Lan verwenden, dokumentiert und kann somit im nachhinein nicht nachvollzogen werden. Ohne entsprechende Sicherheitsmaßnahmen mutiert Wireless-Lan zu einem Selbstbedienungsladen für fremde Daten, mit allen Konsequenzen. Aus der Sicht der

Fragesteller wäre es noch interessant in Erfahrung zu bringen, welche öffentlichen Einrichtungen (Bund, Länder, Gemeinden sowie deren nachgeordneten Dienststellen und ausgegliederte Unternehmen) Wireless Lan verwenden und welche Sicherheitsmaßnahmen in diesen Bereichen getroffen wurden.

Die datenschutzrechtlichen Kontrollmaßnahmen weisen in Österreich insgesamt ein großes Defizit auf. Während es bei Produkten (z.B. Lebensmittel) vorgeschriebene Kontrollen gibt (z.B. Proben- und Revisionsplan), gibt es keine präventiven bzw. laufenden Kontrollen von Datensicherheitsmaßnahmen. Auch die Datenschutzkommission hat dafür keine Zuständigkeit.

Notwendig wäre daher durch eine entsprechende Behörde derartige Datenschutz- und Sicherheitskontrollen– unter Berücksichtigung des letzten Standes der Technik – sicherzustellen.

Viele Unternehmen, die mit einem Wireless-Local-Area-Network (Wireless-Lan) arbeiten, vergessen auf die notwendigen Sicherheitsmaßnahmen. Nach Presseberichten sind zwei von fünf Unternehmensfunknetzwerken ungeschützt und damit für Hacker besonders leicht angreifbar. Unternehmen, die auf die notwendigen Sicherheitsmaßnahmen verzichten, schaffen damit ein neues Sicherheitsrisiko für ihre Daten. Das Aufspüren, Knacken und Mitbenutzen schlecht geschützter Funknetzwerke hat sich unter dem Namen „War driving" mittlerweile zu einer Art Hackersport in Europa und in den USA entwickelt.

Diese Sicherheitslücken ermöglichen Hackern, sich in fremde Netzwerke einzuwählen und so z.B. nicht nur kostenlos im Internet zu surfen, sondern auch eventuell Straftaten unter einer IP-Adresse des angegriffenen Netzwerkes zu begehen.

Gleichzeitig wird die Datensicherheit gefährdet. Hacker könnten beim Eindringen in ein Funknetz sensible Daten einsehen oder sogar manipulieren. Für die Unternehmen selbst wird durch unbefugte Netzwerknutzer ein Teil ihrer Bandbreite eingeschränkt.

Vorgeschrieben werden müssten daher technisch aktuelle Sicherheitsapplikationen zum Schutz der sensiblen Unternehmensdaten. WEP (Wired Equivalent Privacy) ist zwar der gegenwärtig gebräuchliche Sicherheitsstandard, aber seine nachgewiesenen

Sicherheitslücken haben Unternehmen zu einem erneuten Umdenken über die Schutzstrategien bewegt.

Nachdem die WEP-Verschlüsselung schon seit einigen Jahren als nicht mehr wirklich sicher gilt und beim Unternehmenseinsatz deshalb zusätzliche Verschlüsselungsmaßnahmen getroffen werden sollten, soll auch der WEP-Nachfolger „Wi-Fi Protected Access" (WPA) eine gravierende Schwäche haben: Werden nur kurze Passwörter auf Basis normaler Wörter eingesetzt, so reicht – auf Grund einer Schwäche in der Passwort-Eingabe von WPA-fähigen Access-Points und WLAN-Adapter – eine Wörterbuch-Attacke, um das Netz anzugreifen, ohne dass dazu ein direkter Zugriff auf WLAN notwendig ist, so Robert Moskowitz von TruSecure.

Kurz gesagt können kurze textbasierte WPA-Schlüssel geknackt werden, ohne dass dazu ein Fehler im WPA-Protokoll nötig ist. Nutzt man die Standardschnittstelle für die Eintragung von WPA-Schlüsseln und wählt ein reines textbasiertes Passwort mit weniger als 20 Buchstaben, kann ein Hacker den nachfolgenden, ersten Schlüssel-Austausch belauschen und anschließend das Passwort über eine Wörterbuch-Attacke herausfinden. Dazu soll die entsprechende Software nur leicht modifiziert werden müssen, um als Werkzeug für eine „weak-WPA-key attack" dienen zu können.

Datenschutzrechtlich ist daher zu befürchten, dass Wireless Lan als drahtlose Schnittstelle unter anderem für Datenmissbrauch genutzt wird. Die Rechtslage ist an und für sich in Österreich eindeutig (Zivilrecht, StGB, Telekommunikationsgesetz, Datenschutzgesetz 2000 bzw. Datenschutzrichtlinie für elektronische Kommunikation 2002/21/EG): Die in Medienberichten oftmals proklamierte Ansicht, dass (ungesicherte) Wireless Lans von findigen Usern ohne (rechtliche) Konsequenzen genutzt werden können, entspricht nicht den juristischen Gegebenheiten. Die bestehenden und auch für leitungsgebundene Kommunikation geltenden Regelungen sind grundsätzlich sowohl für den Missbrauch von Wireless Lan für als solche, wie auch für mittels Wireless Lan übertragenen Daten anwendbar und ziehen in der Regel zivil- bzw. (verwaltungs)strafrechtliche Konsequenzen nach sich (siehe Wireless Lan – drahtlose Schnittstelle für Datenmissbrauch? ÖJZ 2003/07 Seite 253 ff.).

Sicherheitslücken haben Unternehmen zu einem erneuten Umdenken über die Schutzstrategien bewegt.

Nachdem die WEP-Verschlüsselung schon seit einigen Jahren als nicht mehr wirklich sicher gilt und beim Unternehmenseinsatz deshalb zusätzliche Verschlüsselungsmaßnahmen getroffen werden sollten, soll auch der WEP-Nachfolger „Wi-Fi Protected Access" (WPA) eine gravierende Schwäche haben: Werden nur kurze Passwörter auf Basis normaler Wörter eingesetzt, so reicht – auf Grund einer Schwäche in der Passwort-Eingabe von WPA-fähigen Access-Points und WLAN-Adapter – eine Wörterbuch-Attacke, um das Netz anzugreifen, ohne dass dazu ein direkter Zugriff auf WLAN notwendig ist, so Robert Moskowitz von TruSecure.

Kurz gesagt können kurze textbasierte WPA-Schlüssel geknackt werden, ohne dass dazu ein Fehler im WPA-Protokoll nötig ist. Nutzt man die Standardschnittstelle für die Eintragung von WPA-Schlüsseln und wählt ein reines textbasiertes Passwort mit weniger als 20 Buchstaben, kann ein Hacker den nachfolgenden, ersten Schlüssel-Austausch belauschen und anschließend das Passwort über eine Wörterbuch-Attacke herausfinden. Dazu soll die entsprechende Software nur leicht modifiziert werden müssen, um als Werkzeug für eine „weak-WPA-key attack" dienen zu können.

Datenschutzrechtlich ist daher zu befürchten, dass Wireless Lan als drahtlose Schnittstelle unter anderem für Datenmissbrauch genutzt wird. Die Rechtslage ist an und für sich in Österreich eindeutig (Zivilrecht, StGB, Telekommunikationsgesetz, Datenschutzgesetz 2000 bzw. Datenschutzrichtlinie für elektronische Kommunikation 2002/21/EG): Die in Medienberichten oftmals proklamierte Ansicht, dass (ungesicherte) Wireless Lans von findigen Usern ohne (rechtliche) Konsequenzen genutzt werden können, entspricht nicht den juristischen Gegebenheiten. Die bestehenden und auch für leitungsgebundene Kommunikation geltenden Regelungen sind grundsätzlich sowohl für den Missbrauch von Wireless Lan für als solche, wie auch für mittels Wireless Lan übertragenen Daten anwendbar und ziehen in der Regel zivil- bzw. (verwaltungs)strafrechtliche Konsequenzen nach sich (siehe Wireless Lan – drahtlose Schnittstelle für Datenmissbrauch? ÖJZ 2003/07 Seite 253 ff.).

In den Printmedien fanden sich bereits gedruckte Karten über ungesicherte drahtlose Netzwerke – für Hacker geradezu eine Einladung!

In Anbetracht der geschilderten Gefahren des Wireless-LAN´s ergeben sich zahlreiche Fragen, wie in den einzelnen Bundesministerien und Behörden diese Problemstellung gesehen und behandelt wird.

Die unterzeichneten Abgeordneten richten daher an den Bundesminister für Wirtschaft und Arbeit nachstehende

Anfrage

1. Wird in Ihrem Ministerium bzw. in einer nachgeordneten Dienststelle oder in einem ausgegliederten Unternehmen ein W-LAN verwendet (ersuche um Aufschlüsselung)?

2. Wann wurde dieses jeweils in Betrieb genommen?

3. Welche Kosten fielen jeweils bei der Installation an?

4. Wie sind diese drahtlosen Netzwerke jeweils gesichert?

5. Welche zusätzlichen Sicherheitsvorkehrungen (zu denen eines „Standard"-Netzwerkes) wurden jeweils getroffen?

6. Wurden für die Verwendung von W-LAN auch Verhaltensvorschriften erlassen?

7. Wenn ja, wie lauten diese?

8. Wenn nein, warum nicht?

9. Welche Personen erhalten Zugang zum W-LAN?
   Wie viele Personen haben einen Zugang?

10. Ist eine Bewilligung dafür notwendig?

11. Wer bewilligt diese Zugänge?

12. Wer vergibt die Passwörter für solche Zugänge?

13. Ist es für den Benutzer möglich, sein Passwort selbst zu ändern?

14. Welche Kriterien müssen diese Personen erfüllen, um einen Zugang zum W-LAN bewilligt zu bekommen?

15. Werden diese Personen gesondert auf Ihre Pflichten bezüglich des W-LAN´s hingewiesen (Weitergabe des Passworts, etc.)?

16. Haben diese Personen durch das Einloggen über das W-LAN Zugang zum ganzen Netzwerk, oder nur Teilen davon?

    Wenn nein – Zu welchen Teilen erhält man Zugang und wie sind die anderen Bereiche des Netzwerks vor unberechtigten Zugang geschützt?

17. Zu wie vielen Versuchen unberechtigt auf Teile des Netzwerks zuzugreifen kam es inzwischen (über interne sowie externe Computer)?

18. Mit welchen Sanktionen muss eine Person rechnen, die ihr Passwort und Login an Dritte weitergibt? Werden die Personen gesondert darauf hingewiesen?

19. Werden diesen Personen W-LAN fähige Computer zu diesem Zweck zur Verfügung gestellt oder können diese ihre privaten Geräte verwenden? Im Falle der Bereitstellung der Geräte – Wie viele Geräte wurden zur Verfügung gestellt und auf wie viel beliefen sich die Kosten dafür?

20. Wer installiert die Zugänge zum W-LAN auf diesen externen PC´s (privat wie auch zur Verfügung gestellte)?

21. Wie werden diese Computer vor Hacker-Angriffen geschützt?

22. Erfolgt die Anmeldung dieser externen Computer mittels einfachem Login und Passwort, oder wird zusätzlich eine „Whitelist" mit fixen IP-Adressen dieser Geräte geführt?

23. Wird das VPN (Virtual Private Network) -Protokoll von Microsoft verwendet?

24. Werden in nachgeordneten Dienststellen (z.B. Behörden) Ihres Bundesministeriums Wireless-LAN´s verwendet?

25. Wenn ja – in welchen? Auf wie viel Euro beliefen sich die Kosten der Installationen (Erbitte Aufschlüsselung auf BM, nachgeordnete Dienststellen, ausgegliederte Unternehmen und Kosten)?

26. Wurde eines dieser Netze (Ministerium, untergeordnete Behörden, ausgegliederte Unternehmen) bereits angegriffen?

    Wenn ja – welche, wie oft und wann (Erbitte Aufschlüsselung nach Monaten seit Inbetriebnahme des Netzes)?

    Wenn nein – Sehen Sie hierin die Möglichkeit eines erfolgreichen Missbrauchs, d.h. daß das Eindringen nicht bemerkt wurde – oder sind Sie der Meinung, das dies mit aller Gewissheit auszuschließen ist?

27. Wie oft waren die Angriffe erfolglos (Aufschlüsselung auf Gesamtattacken)?

28. Welche Manipulationen wurden begangen, bzw. versucht zu begehen?

29. Wurde Anzeige erstattet?

    Wenn nein – warum nicht?
    Wenn ja – konnte(n) der (die) Täter zweifelsfrei identifiziert und angezeigt werden?

30. Falls Täter identifiziert wurden – aus welchen Berufskreisen stammen die Täter?

31. Falls der/die Täter nicht ausgeforscht werden konnten – Warum war dies nicht möglich?

32. Gibt es derzeit diesbezüglich anhängige Strafverfahren, bzw. rechtskräftige Straferkenntnisse?

33. Wird Ihr Computer-Netzwerk von externen Unternehmen auf die Sicherheit hin geprüft?

    Wenn ja – Durch welches Unternehmen und welche Kosten fallen dadurch an?
    Wenn nein – Warum nicht?

34. Wann erfolgte die letzte Sicherheitsprüfung Ihres gesamten Computer-Netzwerkes?

35. Was war das Ergebnis dieser Prüfung?

36. Konnten Schwachstellen gefunden werden? Wenn ja – welcher Art?

37. Wird Ihr Netzwerk regelmäßig auf die Sicherheit geprüft? Wenn nein – Warum nicht?

38. Sind Sie für oder gegen die Einrichtung einer Behörde, die staatliche Computernetzwerke auf deren Datensicherheit hin überprüft?
    Wenn nein – Warum nicht?

39. Falls in Ihrem Ministerium und den untergeordneten Dienststellen und Behörden derzeit keine W-LANs betrieben werden: Sind welche in Planung?
    Wenn ja – wie viele und für welche Stellen?

40. Welche Notwendigkeit besteht dazu?

41. Welche Vorteile erwartet man sich dadurch? Welche Nachteile sehen Sie in der Verwendung eines W-LAN?

42. Welche Personengruppe soll Zugang zum geplanten W-LAN erhalten?

43. Welche Kriterien werden Personen erfüllen müssen, um einen Zugang zum W-LAN bewilligt zu bekommen?

44. Wer wird über die Bewilligung entscheiden – also ob es für diese Personen wirklich notwendig ist, via W-LAN sich mit dem Netz zu verbinden?

45. Wie sollen diese drahtlosen Netzwerke gesichert werden?

46. Welche zusätzlichen Sicherheitsvorkehrungen (zu denen eines „Standard"-Netzwerks) sollen getroffen werden?

47. Welche Kosten werden dadurch entstehen?

48. Werden W-LAN fähige Geräte an zugangsberechtigte Personen zur Verfügung gestellt?

49. Sind regelmäßige Sicherheitskontrollen dieses W-LAN´s geplant? Wenn ja, durch welches Unternehmen bzw. welche Behörde? Welche Kosten fallen dadurch an?