Nemzetközi Távközlési Adatvédelmi Munkacsoport

International Working Group on Data Protection in Telecommunications

Munkadokumentum a vezeték nélküli hálózatok potenciális kockázatairól. Általános ajánlások.*

35. Ülés, Buenos Aires, 2004. április

A vezeték nélküli kommunikáció számos olyan előnyt kínál, mint a hordozhatóság és a flexibilitás, fokozott hatékonyság és alacsonyabb üzembe helyezési költségek, és ezért mind népszerűbbé válnak. A vezeték nélküli technológiák számos különféle tulajdonsággal rendelkeznek, amelyek különféle alkalmazásokhoz és szükségletekhez igazodnak. A vezeték nélküli hálózati (Wireless Local Area Network – WLAN) eszközök például lehetővé teszik, hogy felhasználóik személyi számítógépeikkel irodáik vagy otthonuk egyik helyiségéből egy másikba települjenek át anélkül, hogy ehhez vezetékes csatlakozásra lenne szükség vagy a hálózathoz való csatlakozást elveszítenék.

Alkalmi hálózatok, melyeket például a bluetooth tesz lehetővé, megengedik az adatoknak a hálózati rendszerekkel való szinkronizálását, az alkalmazás megosztását a különféle eszközök között, és szükségtelenné teszik a nyomtató vagy egyéb perifériális eszközök kábeles összekötését. A mobilis végfelhasználói készülékek, például a kéziszámítógép (PDA) és a mobiltelefon lehetővé teszik a távolban dolgozó munkatársaknak, hogy a személyes adatbázisokat szinkronizálják és hozzáférést biztosítsanak a vállalati szolgáltatásokhoz, például az e-mail-ekhez és az Internethez. A vezeték nélküli technológiák a jövő távlatában nagyobb funkcionalitást kínálnak.

A vezeték nélküli technológia alkalmazása azonban kockázatokkal jár, különösen azért, mert a vezeték nélküli technológia használatának alapját képező összeköttetési eszköz, a rádióhullám, gyakran nyitott a beavatkozásokra, hacsak nem teszik meg a megfelelő óvintézkedéseket.

Ezek a kockázatok az alábbiak:

- A hálózati felhasználó helymeghatározási adatainak és egyéb személyes adatainak rögzítése;
- Külső felhasználók felhatalmazást nélkülöző és észrevétlen hozzáférése a vállalat hálózataihoz;
- A vállalati tűzfalak megkerülése és az e-mail-ek szűrése a vezeték nélküli hálózatok azon felhasználói által, akik hozzáféréssel rendelkeznek a vállalati vagy hatósági hálózatokhoz, ami vírus támadásokhoz és spam-ekhez vezethet;
- A személyes kommunikáció lehallgatása, továbbá észrevétlen kapcsolat létesítése a vezeték nélküli hálózatok felhasználói között, különösen a nyilvános helyeken.

A Munkacsoport felszólítja az IEEE munkacsoportot[1] és a WI-FI Szövetséget[2], valamint a hálózati termékek értékesítőit, hogy magas prioritást tulajdonítsanak az adatok és a

* A Munkacsoport „Working Paper on potential privacy risks associated with wireless networks. Main Recommendations" című munkadokumentumának fordítása (Dr. Könyves-Tóth Pál munkája) figyelemmel német nyelvű változatára is. Letölthető: **http://www.datenschutz-berlin.de/content/europa-**

magánszféra védelmének a vezeték nélküli technológia folyamatban lévő és jövőbeli fejlesztése során[3].

Javaslatok

A) Kockázatelemzés és a kívánt biztonsági szint

A vezeték nélküli hálózatok üzemeltetőinek[4] ismerniük kell a hálózat nélküli és a mobil technológiák technikai és biztonságtechnikai következményeit.

A vezeték nélküli hálózatok üzemeltetőinek – a vezeték nélküli technológia alkalmazásba vételét megelőzően – kockázatelemzést kell végezniük annak biztosítása céljából, hogy információikat, rendszerműveleteiket és a műveletek folyamatos voltát felülvizsgálták, és ezeket kezelni képesek.

Saját érdekében minden felhasználónak személyes kockázatelemzést kell végeznie mielőtt vezeték nélküli technológiát vagy szolgáltatást vásárolnak, használnak vagy üzemeltetnek, mert saját személyes biztonsági követelményeik határozzák meg, mely termékek vagy szolgáltatások jöhetnek számításba.

B) A hálózati paraméterek beállítása

A vezeték nélküli hálózatok üzemeltetőinek gondosan meg kell tervezniük a vezeték nélküli technológia alkalmazásba vételét, és megfelelő paramétereinek az eszközeiken való beállítását, hogy mind a hálózat funkcionalitását, mind a szolgáltatás biztonságát garantálják. Különösen a hálózathoz való hozzáférést kel magas biztonsági szabványok szerint védeniük.

A felhasználóknak követniük kell és tudatában kell lenniük a vezeték nélküli eszközök konfigurálási módjának annak érdekében, hogy magas szintű biztonságot és védelmet garantáljanak.

C) A biztonság kezelése

---

international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group .

[1] Az IEEE 802.11 Working Group for Wireless Area Networks, WLANs (vezeték nélküli hálózati munkacsoport). Bővebben: **http://grouper.ieee.org/groups/802/11/**. Az IEEE (Eye-triple-E) egy nem profitorientált professzionális technikai társaság, melynek mintegy 175 országban 360 ezer egyéni tagja van. Teljes neve: Institute of Electrical and Electronics Engineers, Inc., jóllehet a szervezetet általában IEEE-nek hívják, s rá így is hivatkoznak.

[2] Wi-Fi: Wireless Fidelity. Bővebben: **http://www.wi-fi.org/**. A Wi-Fi Alliance szervezet, egy nem profitorientált ipari csoport, amely a 802.11 vezeték nélküli technológia elfogadását világszerte támogatja, és biztosítja, hogy valamennyi Wi-Fi CERTIFIED 802.11 alapú vezeték nélküli hálózat együttműködik minden, azonos hullámhosszon működő és tulajdonságokkal rendelkező Wi-Fi CERTIFIED készülékkel.

[3] Lásd: NIST közlemény 800-48: vezeték nélküli hálózat biztonsága 802.11, bővebben: **http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf**. A NIST (National Institute of Standards and Technology, Nemzeti Szabványosítási és Technológiai Intézet) az Amerikai Egyesült Államok Kereskedelmi Részlegének szövetségi, nem szabályozó ügynöksége. Küldetése: fejleszteni és támogatni a méréstechnikát, a szabványokat és a termelékenységet növelő technológiát, elősegíteni a kereskedelmet és fokozni az életminőséget. Küldetését a NIST négy kooperatív programban teljesíti.

[4] Angolul: " bárki, aki vezeték nélküli hálózatokat kíván telepíteni és használni.

A vezeték nélküli hálózatok üzemeltetőinek biztonsági intézkedésekről kell gondoskodniuk, ezeket ellenőrizniük kell annak érdekében, hogy a vezeték nélküli hálózat biztonságát fenntartsák.

A vezeték nélküli hálózat üzemeltetőinek rendszeresen felül kell vizsgálniuk az ebben rejlő biztonsági jellemzőket, pl. a hitelesítést és titkosítást, amelyek a vezeték nélküli hálózatban léteznek. A vezeték nélküli hálózatokban létező hitelesítés különösen fontos, és egy szigorúbb hozzáférési ellenőrzésen, a jelszavak rendszeres módosításán alapulhat.

A vezeték nélküli hálózat üzemeltetőinek tájékoztatniuk kell a felhasználókat a hálózat biztonsági szintjéről és a kommunikáció bizalmas voltának biztosítására szolgáló intézkedésekről.

D) Egyéb megfontolások

A vezeték nélküli hálózatok szolgáltatóinak meg kell felelniük a jogszabályi kötelezettségeknek[5], amely a különféle jogrendszerekben eltérő lehet.

A Munkacsoport hangsúlyozza továbbá, hogy a biztonsági koncepciók a felhasználóknak nehezen érthetőek. A gyakorlati alkalmazás még a tapasztalt IT-szakértők számára is problematikus lehet. Az ipar egészének kezelnie kell a problémát mind technikai, mind informális szinten annak érdekében, hogy fokozzák a technológiába vette bizalmat. Az alapértelmezett beállításoknak magas adatvédelmi szintet kell biztosítaniuk.

Mindazoknak, akik az Interneten kínálnak szolgáltatásokat, különösen a WEB-mailer-eknek, az alkalmazási felületen fel kell ajánlaniuk a titkosítás lehetőségét. A különleges adatoknak a vezeték nélküli hálózaton való továbbítása esetén az erős titkosítás elengedhetetlen.

A felhasználókat nem lehet megakadályozni abban, hogy álnéven vagy névtelenül férjenek hozzá a nagyközönség számára hozzáférhető szolgáltatásokhoz.

[5] Lásd: Az Európai Parlament és a Tanács 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv).