Integrovaná bezpečnosť / Integral safety 2013
Proceedings of the International Scientific Conference, Trnava, November 15, 2013. Strix: Žilina, Edition ESE-16, First Edition, ISBN 978-80-89281-92-3

BEZPEČNOSŤ BEZDRÔTOVÝCH SIETI AKO GLOGALNY PROBLEM OCHRANY INFORMÁCII

PETER LOŠONCZI

SAFETY OF WIRELESS NETWORK AS THE GLOBAL PROBLEM OF THE INFORMATION PROTECTION

ABSTRAKT
Štúdia sa zaoberá analýzou manažmentu bezpečnosti bezdrôtových sietí a ich ohrození. Úvodná časť je zameraná na teoretické spracovanie sledovanej problematiky. Jadro štúdie identifikuje a analyzuje bezpečnostné trhliny štandardu IEEE 802.11 a popisuje použitie odporúčaných postupov na zabezpečenie. V závere je zhodnotenie výsledkov a všeobecný prístup k bezdrôtovej bezpečnosti.
Kľúčové slová: *bezpečnosť, bezdrôtové siete, bezpečnosť bezdrôtových sietí*

ABSTRACT
The study deals with the analysis of the wireless networks security management and at risk. The introductory part focuses on the theoretical processing of the studied issue. The core of study identifies and analyzes the security cracks in the IEEE 802.11 standard and describes the use of the recommended safety procedures. In conclusion of this study there is the results evaluation and general approach for wireless security.
Key words: *security, wireless networks, wireless networks security*

ÚVOD

„V prítmí zafajčenej miestnosti leží na stole nabitá odistená pištoľ, hneď vedľa blikajúcej obrazovky a klávesnice počítača pripojeného do Internetu... Ale veď tú pištoľ môže hocikto zobrať do ruky a vedome či náhodou na niekoho vystreliť! Ale veď ten počítač, zjavne nechránený, možno použiť na zlomyseľný útok!“
Citácia, uvedená hneď v úvode, veľmi presne vystihuje súčasnú situáciu na Slovensku. V dnešnej dobe predstavujú bezdrôtové siete moderný trend mobilnej aj hlasovej komunikácie. Za rozmachom bezdrôtových sietí je množstvo výhod, ktoré táto technológia ponúka. Výhodami sú mobilita, flexibilita, úspora nákladov...
No bezpečnostné povedomie akoby zostávalo stále iba pri pohľade na položenú pištoľ. Poniektorí by možno ešte namietli, že aj nechránený počítač je hrozba, ale málokto sa pozastaví nad tým, že vďaka bezdrôtovému prístupu tu máme celé potenciálne nechránené počítačové siete s prístupom na internet aj intranet.
Najvýraznejším prvkom bezdrôtovej siete je mobilita, ktorá umožňuje jednotlivé zariadenia voľne pripájať kdekoľvek v oblasti dosahu signálu siete. Flexibilita ponúka možnosť variabilne rozmiestniť zariadenia v zóne, kde je dosah signálu, a čo je najdôležitejšie - bez potreby inštalácie kabeláže. V dnešnej rýchlej dobe spoločnosti požadujú technológie, ktoré im v prípade rozšírenia firmy umožnia pružne modifikovať aj počítačovú sieť. Staršie objekty a domy neboli navrhované s inštalačnými šachtami, potrebnými na vedenie káblov, preto je u nich možnosť bezdrôtového pokrytia využívaná veľmi často. Výrazný ekonomický faktor, akým je úspora nákladov, má svoje kľúčové postavenie pri výbere technológie požívanej na prenos dát práve pre malé a stredné podniky, kde by inštalácia metalickej sieťovej kabeláže pre koncové zariadenia bola ekonomicky nerentabilnejšia než vybudovanie bezdrôtovej siete.
Ak sa ale pozrieme na bezpečnostné povedomie, u väčšiny sietí bezpečnosť končí prvotným zabezpečením pri vytvorení počítačovej siete.

Medzi základné otázky, ktoré by mali predchádzať rozhodnutiu o budovaní či nebudovaní bezdrôtového IS, patria tieto [11]:
1. Je nový IS skutočne potrebný?
2. Poznáme a berieme do úvahy riziká spojené s vybudovaním nového IS?
3. Vieme vytvoriť primerané podmienky na realizáciu projektu zameraného na vybudovanie nového IS?
4. Budeme IS budovať sami alebo si ho necháme vybudovať externou firmou?

Pri odpovediach na tieto otázky, by sme mali vedieť, čo sa skrýva pod pojmami informačná bezpečnosť, bezdrôtová sieť a Wi-Fi, mali by sme poznať štandardy, ktoré sú vydané pre nami požadovaný bezdrôtový IS, spôsob komplexnej prevádzky zvoleného bezdrôtového IS a samozrejme aj metódy jeho zabezpečenia, druhy možných útokov a spôsob ochrany pred nimi. To zahŕňa aj navrhnutie riešenia bezpečnosti pre IS.

BEZPEČNOSŤ

Pojem bezpečnosť. Vysvetliť pojem informačná bezpečnosť nie je jednoduché. Každý si totiž pod týmto pojmom predstavuje niečo iné, či už je to vojak, lekár alebo informatik. Objasnime si najskôr pojmy bezpečnosť a informácia.
Vo všeobecnosti by sa mohla samotná bezpečnosť definovať „ako stav, v ktorom sa daný objekt necíti byť ohrozený z hľadiska svojich oprávnených záujmov“. [7]

Proceedings of the International Scientific Conference, Trnava, November 15, 2013. Strix: Žilina, Edition ESE-16, First Edition, ISBN 978-80-89281-92-3

Informácia je správa, oznámenie, zistenie, ktoré znižuje alebo úplne odstraňuje neznalosť, neistotu. Aby táto informácia mala pre nás nejakú výpovednú hodnotu, musí byť zabezpečená jej úplnosť, dostupnosť, jednoznačnosť, časovosť, primeranosť.
Informácie majú určité vlastnosti. Podľa normy ISO/IEC TR 13335-1 tam môžeme zaradiť vlastnosti ako sú integrita (neporušiteľnosť informácie zásahom technickej časti systému alebo ľudského faktora), dôvernosť (informácia nemôže byť odhalená, zneužitá neoprávneným subjektom), dostupnosť (informácia je schopná bezprostredného použitia), nepopierateľnosť, autenticita (stav v ktorom informácia zodpovedá skutočnosti a je nespochybniteľného dôvodu). [12]

Informačný systém - súbor technických (hardvér) a programových (softvér) prostriedkov, záznamových médií, dát a personálu, ktoré spoločnosť používa na spracúvanie informácií v určitej oblasti pôsobenia. Medzinárodný štandard ISO/IEC 12207 - Information Technology - Life Cycle Process, vydaný v roku 1995 definuje informačný systém ako integrované zloženie ľudí, produktov a procesov, ktorí poskytujú schopnosti zabezpečiť určené potreby alebo ciele. [11]
Snahou je teda dosiahnuť stav, kedy sa za pomoci hardvérových, softvérových či personálnych opatrení zaistí primerané zabezpečenie informačného systému. Primeranosť spočíva práve v prispôsobení tohto stavu dôležitosti toho, čo zabezpečujeme.

Obzvlášť pre malé a stredné podniky nie je rentabilné vybudovať sieť s maximálnym zabezpečením, vysokými nákladmi a pritom malým rizikom zneužitia prenášaných, zabezpečovaných informácií. Opačným prípadom je malé zabezpečenie z dôvodu šetrenia nákladov alebo podceňovania, zľahčovania rizika tam, kde ide o dáta dôverného charakteru, ako je napr. ochrana osobných údajov a pod. Platí to všeobecne, ale práve pri bezdrôtovom prenose by sa malo zvlášť prihliadať na riziko zneužitia informácií, IS či samotnej siete a nepodceňovať ho.

Informačná bezpečnosť' je teda zachovanie dôvernosti, integrity a dostupnosti informácií, okrem toho aj iné požiadavky, ktoré môžu byť tiež zahrnuté, ako sú autenticita, sledovateľnosť, nemožnosti poprieť zodpovednosť a spoľahlivosť. [11]

Informačná bezpečnosť' by sa následne mohla rozdeliť ešte na tieto druhy:
- *fyzická bezpečnosť (PHYSEC) - ochrana IS proti neoprávnenému vniknutiu osôb, spôsoby zničenia nepotrebných informácií na záznamových médiách, ochrana proti prírodným živlom,*
- *počítačová bezpečnosť (COMPUSEC) - výber a spoľahlivosť IS, servis a kontrola prístupu k týmto prostriedkom,*
- *personálna bezpečnosť (PERSEC) - eliminácia hrozieb zapríčinená zlyhaním ľudského faktora, vyčlenenie právomocí a zodpovednosti pracovníkov,*
- *komunikačná bezpečnosť (COMSEC) - ochrana dát proti odpočúvaniu, pri prenose, spracovávaní, proti modifikovaniu a taktiež ochrana pred neoprávneným vniknutím do vnútornej siete,*
- *logická bezpečnosť (LOGISEC) - zabezpečuje filter prístupu k informáciám ako je kontrola prístupu, autentizácia používateľov, rozdelenie právomocí používateľom.*

Informačnú bezpečnosť, zloženú z viacerých druhov ochranných zabezpečení založených na rôznych technológiách a princípoch môžeme nazývať aj vrstevná informačná bezpečnosť

BEZDRÔTOVE SIETE A ICH BEZPEČNOSŤ

Princíp bezdrôtovej siete

Bezdrôtový prístup WA *Wireless Access* predstavuje z pohľadu rádiových služieb v zmysle „Rádiokomunikačného poriadku"*Radio Regulations"* bezdrôtové pripojenie pre pevnú službu, mobilnú službu, pevnú družicovú službu a pre mobilnú družicovú službu. Bezdrôtová sieť sa teda dá charakterizovať ako akýkoľvek typ počítačovej siete, ktorý nepotrebuje pre svoju komunikáciu fyzický kábel. Môžeme sem zaradiť všetky bezdrôtové siete, medzi ktoré patria všetky systémy založené na báze prenosu dát vzduchom z jedného bodu do druhého. Ako prenosové prostriedky je v podstate možné použiť rádiové, optické alebo infračervené vysielanie. Siete založené na infračervenom žiarení alebo optické siete ale vyžadujú priamu viditeľnosť medzi vysielačom a prijímačom s dosahom rádovo v metroch, majú malú prenosovú rýchlosť, pričom nezanedbateľné sú aj vyššie náklady na takéto riešenie. Pre vytvorenie bezdrôtovej siete LAN potrebujeme dva základné komponenty, ktorými sú prístupový bod (Access Point) a adaptér na pripojenie počítača do siete. Adaptéry môžu byť rôzne. Pre stolné počítače sa môžu použiť adaptéry pre port PCI, ale aj v poslednej dobe najčastejšie používané adaptéry pre port USB. Prístupový bod je zariadenie, ktoré je do siete pripojené pomocou ethernetového kábla a ďalej potom mení sieťovú prevádzku na rádiové signály, ktoré zachytávajú pomocou adaptéra stolné počítače alebo notebooky. V nezastavanom priestore sa dá dosiahnuť dobré spojenie na dĺžku od 30 m po niekoľko stoviek metrov. V zastavanom priestore s chodbami a priečkami je táto vzdialenosť redukovaná o použité materiály, ktorými signál prechádza. Prepojením počítačov bez alebo s príslušenstvom tak, že dokážu navzájom komunikovať bezdrôtovým spôsobom, vznikne bezdrôtová počítačová sieť.

RM OSI model v rámci štandardu IEEE 802.11

IEEE 802.11 je štandard prijatý v roku 1997, pochádzajúci z rodiny štandardov 802.xx pre lokálne a metropolitné siete, ktoré vypracovala medzinárodná nezisková organizácia IEEE so sídlom v New Yorku. Všetky štandardy 802.xx sú vo svojej podstate postavené na referenčnom modeli prepojenia otvorených systémov RM OSI. V praxi sa zvykne označovať skratkou RM OSI alebo len ISO/OSI, ktorý vytvorila medzinárodná štandardizačná organizácia ISO. Ide o model siedmich vrstiev,

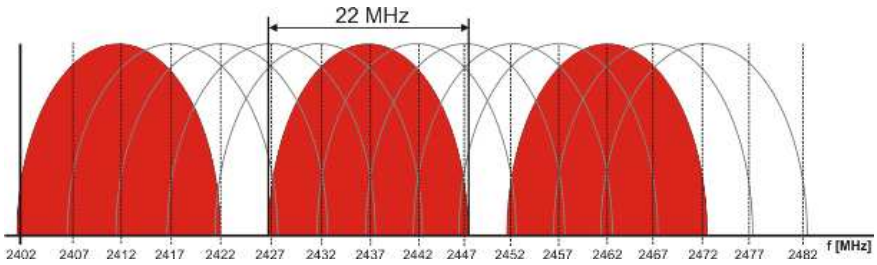
ktoré popisujú štruktúru a priebeh komunikácie od najnižšej fyzickej vrstvy, až po aplikačnú vrstvu. Typické pre tento model je hierarchické usporiadanie.
Pre štandardy 802.11 sú podstatné spodné dve vrstvy a to fyzická vrstva a spojová vrstva.
Fyzická vrstva (v rámci potrieb štandardu 802.11) poskytuje pre vyššiu (spojovú) vrstvu službu - prenos bitov cez daný komunikačný kanál.
Spojová vrstva mení tok bitov z fyzickej vrstvy na rámce a tým vytvára cestu pre prenos dátových blokov medzi dvomi bodmi v sieti. Táto vrstva sa využíva hlavne vtedy, ak je komunikačné spojenie náchylné na chyby, čo pri bezdrôtovom prenose je častým problémom.

Dáta, ktoré sa prenášajú, vznikajú v zdroji a sú prenášané k cieľu. Každá vrstva je závislá od služby nižšej vrstvy. Výmena informácií medzi vrstvami je uskutočňovaná pomocou protokolu každej vrstvy cez bloky, označované ako protokolárne dátové jednotky (PDU), ktoré potom nižšia vrstva zapuzdruje - vloží PDU z vyššej vrstvy do svojho dátového poľa. Potom pripojí potrebné záhlavia a zapätia, ktoré táto vrstva potrebuje na poskytovanie svojej funkcie. Ďalej sú dáta prenášané dolu vrstvami OSI modelu a v každej vrstve sú pridávané ďalšie záhlavia a zapätia. Zapuzdrenie vrstvy 7, 6, 5 a 4 sa označuje ako segment. Sieťová vrstva zapuzdruje dáta zo štvrtej vrstvy a označuje sa ako paket**.** Linková vrstva zapuzdruje informáciu od sieťovej vrstvy do rámca**.** Fyzická vrstva zakóduje linkový rámec do postupnosti bitov pre prenos po prenosovom médiu na prvej vrstve. [12]

Práve spôsob prenosu na fyzickej vrstve je podstatný pre štandard 802.11. Od spôsobu prenosu dát sa v podstate odvíja aj rýchlosť danej siete. Medzi tri základné spôsoby prenosu dát patria:

- DSSS (*Direct Sequence Spread Spectrum* - technika priameho rozprestretého spektra)
- OFDM (*Orthogonal Frequency Division Multiplexing* - ortogonálny frekvenčný multiplex)
- FHSS (*Frequency-hopping spread spectrum* - rozprestreté spektrum s preskakovaním medzi frekvenciami)

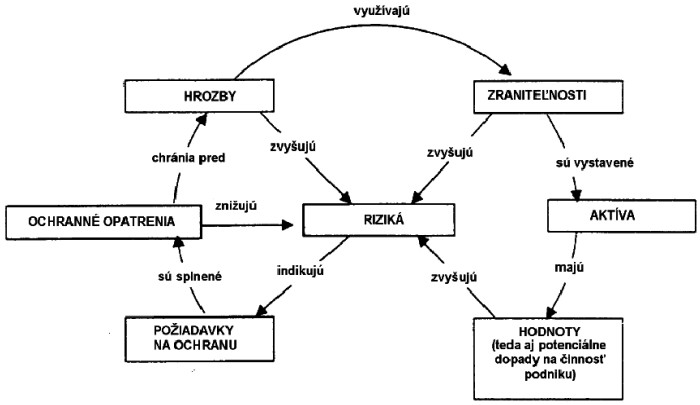
DSSS - systém rozprestrie na 22 Mhz frekvenčnom pásme vysielané pakety pri použití matematického kódovania. Prijímač potom inverzným spôsobom signál dekóduje. V danom bezlicenčnom pásme takto môžu vedľa seba bez rušenia existovať iba tri rozdielne AP. (obr. 1)



Obr. 1 Rozprestretie kanálov v pásme 2,4 GHz [25]

OFDM - systém rozdelí prenosové pásmo na veľké množstvo úzkych kanálov. Dáta sa v každom kanáli prenášajú relatívne pomaly, signál je o to robustnejší, ale vo výsledku je rýchlosť prenosu daná súčtom všetkých kanálov, a to až 54 Mbit/s.

FHSS - systém rozdelí pásmo na 82 podkanálov (každý je široký 1 Mhz) a na každom z nich vyšle pakety, potom preskočí na inú frekvenciu a vysiela ďalej. Spôsob preskakovania je periodický a je známy vysielaču aj prijímaču.

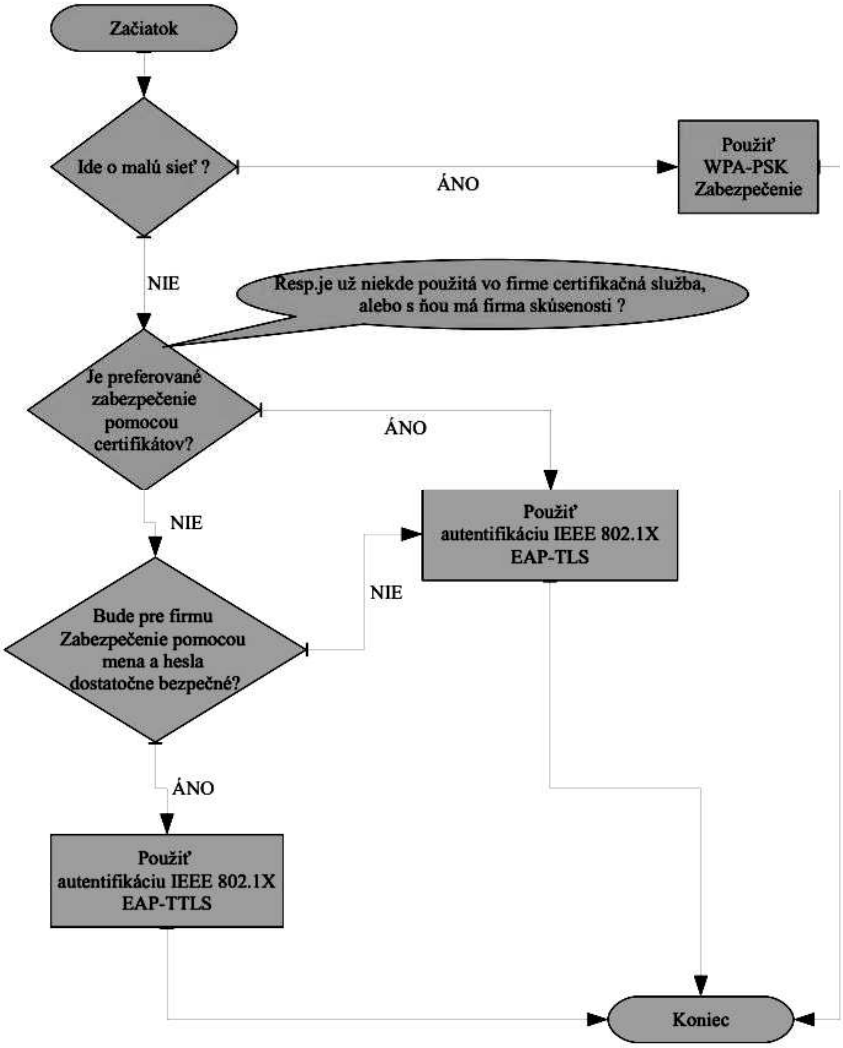


Obr. 2 Vzťahy medzi bezpečnostnými prvkami [11]

Proceedings of the International Scientific Conference, Trnava, November 15, 2013. Strix: Žilina, Edition ESE-16, First Edition, ISBN 978-80-89281-92-3

Majúc na zreteli tieto názory, každá firma, ktorá chce chrániť svoje záujmy, a to nie iba pri vytváraní WLAN siete alebo LAN siete, by mala ako prvý krok vykonať analýzu rizík. Preto práve analýza rizík musí zahŕňať analýzu hodnôt aktív, hrozieb, zraniteľností a potenciálnych rizík, ktoré by mohli spôsobiť narušenie dôvernosti, integrity, dostupnosti a spoľahlivosti chránených hodnôt.

Pri zavádzaní týchto balíčkov, ale aj ako prvotné základné nastavenie je vhodné pri zostavovaní WLAN siete hneď špecifikovať rozsah siete, kde sa určí, či danú sieť bude potrebné v budúcnosti rozširovať. V konkrétnom prípade modelovej firmy pôjde o stálu veľkosť bezdrôtovej siete. Ale napríklad škola ako malý/stredný podnik môže začať s malou sieťou a pri neskoršom rozširovaní priestorov by sa malo počítať aj s rozširovaním bezdrôtovej siete. Preto je vhodné dopredu špecifikovať, či pôjde o väčšiu sieť so zapojením študentov do intranetu, prípadne do siete Eduroam, čo je medzinárodný projekt zaoberajúci sa podporou mobility a roamingu v sieťach národného výskumu a vzdelávania, alebo pôjde o súkromnú sieť slúžiacu pre potreby zamestnancov školy. Veľmi užitočný preto môže byť aj vývojový diagram pre štandardné nastavenie zabezpečenia WLAN (Obr. 3)



Obr. 3 Vývojový diagram základného zabezpečenia WLAN

Identifikácia aktív

Vývojový diagram zobrazený vyššie patrí samozrejme medzi základné nastavenie zabezpečenia siete, v ktorom sa nezohľadňujú už skôr spomínané prvky, ako sú rôzne hrozby, riziká a ohrozenia konkrétne pôsobiace na firmu. Na to, aby sme mohli tieto jednotlivé prvky zahrnúť do analýzy rizík, potrebuje každá firma identifikovať aktíva, ktoré chce ochraňovať.

Medzi aktíva firmy zvyčajne patria [11]:

- *fyzické aktíva, ako napr. hardvér, budovy a pod.,*
- *informácie,*

- *softvér,*
- *schopnosť vytvárať určité produkty, služby,*
- *ľudia,*
- *nehmotné hodnoty, ako napr. dobré meno firmy, imidž...*

Pre každú firmu sú aktíva špeciálne, resp. závisia od predmetu činnosti danej firmy. V prípade modelovej firmy pri stavbe WLAN by sa medzi aktíva mohli zaradiť:

- *vybavenie - bezdrôtová sieť, zariadenia v sieti (prepínače, smerovače, AP), pracovné stanice,*
- *dáta - projekty, elektronické dokumenty,*
- *softvér - operačný systém, licencované programy, aplikačné programy,*
- *služby - VPN, e-mail, DHCP služba, zdieľanie dát, manažment siete, komunikačná služba so zariadením, tlač, DNS,.*

Webová služba.
Aktíva môžeme ďalej rozdeliť podľa úrovne dôvernosti na aktíva prístupné iba riadiacim pracovníkom, aktíva prístupné všetkým zamestnancom a pod.

Identifikácia hrozieb
Na základe vyhodnotenia identifikácie aktív môže firma pristúpiť k identifikácii hrozieb. Hrozba pre aktíva je spôsob, ktorým môže byť spôsobená strata dôvernosti, integrity alebo dostupnosti aktíva. Pri identifikácii hrozieb ide teba o určenie, proti čomu chceme aktíva chrániť. V prípade WLAN siete môže ísť hlavne o útok na informácie, ktoré prúdia v sieti. Aj keď sa hrozby dajú rozdeliť na úmyselné, náhodné a hrozby prostredia, hlavné je zamerať sa na úmyselné hrozby. Detailnejším delením v tomto prípade môže byť rozdelenie na pasívne a aktívne hrozby. Príkladom hrozby môže byť napr. nefunkčný server.

Možné typy úmyselných hrozieb/útokov na WLAN sieť:

- *DoS (Denial of Service) - útočník zabráni normálnemu používaniu alebo správe siete, prípadne sieťového zariadenia.*
- *Deuatentizačný útok - útočník sa snaží prinútiť klienta k opätovnej autentizácii.*
- *Odpočúvanie - útočník pasívne načúva v sieti (odchytáva sieťovú komunikáciu) a hľadá dáta, ktoré obsahujú citlivé informácie.*
- *Modifikácia správ - útočník upraví, vymaže správu, prípadne preusporiada správy.*
- *Reprodukcia správ - útočník monitoruje prenos a preposiela správy, tváriac sa ako legitímny komunikujúci.*
- *Analýza prenosu - útočník monitoruje prenos s cieľom zistiť komunikačné vzory a účastníkov komunikácie.*
- *MITM (Man In The Midle) - útočník aktívne prerušuje komunikáciu medzi dvoma zariadeniami s cieľom zachytiť autentizačné údaje. Vydáva sa pritom za legitímneho komunikujúceho. Pre WLAN je to napr. falošné AP tváriace sa ako autorizovaný AP.*

Neúmyselná hrozba pre WLAN môže byť napr. rušenie siete. To môže byť spôsobené použitím nevhodných materiálov pre vedenie, atmosférickými vplyvmi alebo zvolením nevhodného kanálu, na ktorom vysiela Wi-Fi v mieste, kde už na danom kanáli vysiela iná Wi-Fi sieť. Ako príklad pre ochranu pred hrozbami prostredia môže slúžiť ochrana pred požiarom alebo prepätiu elektrickej siete. Pri identifikácii hrozieb netreba samozrejme zabúdať ani na hrozby pochádzajúce od vlastných zamestnancov (napr. správcov siete) alebo bývalých zamestnancov. Niektoré hrozby môžu pôsobiť na viaceré aktíva. V takom prípade môžu mať za následok rôzne dopady v závislosti na tom, aké aktíva sú ovplyvnené. Účinok softvérového vírusu v jednom osobnom počítači môže mať obmedzený alebo miestny dopad. Ale rovnaký softvérový vírus na sieťovom súborovom serveri môže mať rozsiahly dopad.

Zraniteľnosti
Samotná zraniteľnosť nemusí byť príčinou nejakej škody. Je to ale slabé miesto, ktoré umožní hrozbe ovplyvňovať aktíva firmy. Prednostná pozornosť musí byť preto stále venovaná miestam, kde bola identifikovaná nejaká hrozba. Z toho vyplýva, že prvotná identifikácia zraniteľných miest nepostačuje na dlhodobú prevádzku samotnej siete, nakoľko ide o dynamický systém, v ktorom sa neustále objavujú nové postupy útočníkov, odhaľujú nové slabiny a pod. Ide teda o nepretržitý proces zlepšovania a kontroly - Demingov PDCA cyklus. Do toho môžeme zahrnúť aj prostredie, v ktorom firma pôsobí. Za príklad je možné uviesť pridanie novej siete inou firmou s následným zarušením pásma, v ktorom dovtedy firma bez problémov fungovala. Analýzou zraniteľností sa preskúmavajú slabé miesta využiteľné hrozbami, ktoré sa zistili pri identifikácii hrozieb v predchádzajúcom kroku.

Práve bezdrôtové Wi-Fi siete sú z pohľadu infraštruktúry najzraniteľnejším bodom, keďže šírenie signálu sa ťažko kontroluje, z dlhšieho časového horizontu trpia šifrovacími zraniteľnosťami a samotné bezdrôtové zariadenia často obsahujú známe a neopravené zraniteľnosti v použitom firmware. Podľa prieskumov prevažná väčšina Wi-Fi sieti trpí niektorou zo závažných bezpečnostných zraniteľností. Preto je vhodné sa zameriavať hlavne na zraniteľnosti, ako sú: použité kryptografické algoritmy, presah signálu, odchytávanie dát a ich následné dešifrovanie, konfigurácia AP ekvivalentná s pevnou (káblovou) infraštruktúrou, čo v prípade narušenia vedie k tomu, že útočník má prístup do vnútornej siete.

Príklady možných zraniteľností a útokov:
Chyba WPS - Veľké množstvo používaných Wi-Fi routerov už dnes ponúka funkciu WPS, ktorá umožňuje stisnutím tlačidla priamo na routeri jednoducho pripojiť podporované zariadenia bez komplikovaného nastavovania. Táto technológia je zameraná na zjednodušenie konfigurácie bezdrôtovej siete bežným používateľom**.** V tomto prípade ale WPS predstavuje aj bezpečnostnú hrozbu.

Pre zjednodušenie je na routeri od výroby napísaný osemmiestny PIN kód, ktorý používateľ zadá v zariadení. PIN obsahuje 8 číslic, preto sa zdá, že uhádnuť správnu kombináciu nie je v dostupnom čase možné. Ak ale útočník zvolí zlú kombináciu, vracia sa mu okrem iného aj informácia o tom, či bolo niektoré štvorčíslie zadané správne. Tým sa funkcia zabezpečenia WPS cez PIN redukuje z 80 miliónov možných kombinácií na zhruba 11 000. Útočníkovi teda stačí hádať prvú polovicu PIN kódu. Potom už potrebuje iba nájsť číslice z druhej polovice. Pre pripojenie útočníka teda stačí, aby sa pri stisnutí tlačidla zdržiaval v okolí niekto, kto práve zisťuje, či niektorý z routerov v okolí nemá zapnutú službu WPS a bol pripravený to zneužiť. Po zverejnení chyby bol zverejnený aj softvér (wpscrack) využívajúci túto chybu**.**

Chopchop útok - Útok na protokol WEP dovoľuje útočníkovi dešifrovať paket bez znalosti kľúča. Tento útok využíva slabinu, kde sa skráti šifrovaná správa o posledný bajt a signál nebude platný. To napraví hradlo XOR s určitou hodnotou. Bezpečnostným nedostatkom je, že táto hodnota závisí presne na odtrhnutom bajte. Preto sa odhadom vyberie jeden z 256 bajtov a XORuje sa so správou. Na zistenie správnosti odhadu sa odošle takto zmenená správa AP. Ak bol odhad správny AP odošle správu naspäť do siete. Opakovaním tohto postupu sa získa otvorený text.

Útok hrubou silou (Brute force attack) - Útok funguje proti sieťam typu WPA a WPA2 využívajúcim predzdieľaný kľúč (PSK). Na tento útok je potrebné získať handshake. Handshake sa používa na získanie dočasného kľúča používaného na ochranu prevádzky siete. Na získanie handshaku sa použije deuatentizačný útok alebo sa jednoducho počká, kým sa nejaký klient nepripojí. Po získaní handshaku útočník získa štyri hodnoty z piatich, ktoré potrebuje. Postupným dosadzovaním kľúča (zo slovníka vygenerovaného „hrubou silou“) sa snaží získať rovnaký výsledok, aký zachytil v handshaku. Preto slabé heslo, resp. normálne slovo alebo slovné spojenie napomáha rýchlemu prelomeniu hesla. Tu záleží aj na výkone stroja, na ktorom útok prebieha. Výkonný hardvér dokáže otestovať až 20000 kľúčov za sekundu.

Beck-Tews útok na TKIP - Útok sa dá vykonať na sieť, ktorá podporuje a využíva QoS (Quality of Service). Útok umožňuje útočníkovi dešifrovať ARP žiadosť (ARP - Address Resolution Protocol - je protokol, ktorý zabezpečuje preklad lokálnych IP adries na MAC adresy sieťových uzlov) v smere od AP k stanici, a tak získať prúdový kľúč a MIC kľúč pre daný paket. Následne môže vytvoriť vlastné pakety v smere od AP k stanici a preniknúť do siete. K tomu potrebuje zhruba 12 až 15 minút. Zabrániť takémuto útoku sa dá napr. znížením intervalu platnosti PTK (prechodného párového kľúča) na hodnotu menšiu ako 10 minút, odporúča sa až na 2 minúty.

Útok Ohigashi-Morii - Do MITM (Man in the middle) útoku sa aplikuje útok Beck-Tews, a teda nie je potrebná služba QoS, preto je použiteľný na WPA všeobecne. Výsledný čas na prelomenie sa pohybuje okolo minúty.

V súhrne sa pre zabezpečenie pomocou WEP dajú definovať nasledujúce typy útokov [16]:
- *Pasívne útoky zamerané na dešifrovanie prenosov na základe štatistickej analýzy.*
- *Aktívne útoky zamerané na vkladanie nových prenosov z neautorizovaných klientov na základe znalostí jednoduchého textu, ktoré mohli byť získané použitím techniky pasívneho útoku.*
- *Aktívne útoky zamerané na dešifrovanie správ na základe oklamania prístupového bodu.*
- *Útoky založené na analýze zhruba jednodennej prevádzky. Zhromaždené dáta boli potom použité k automatizovanému dešifrovaniu prevádzky v reálnom čase. Tento typ útoku sa niekedy nazýva zostavenie slovníka.*

Tab. 1 Hrozby a zraniteľností pre modelovú firmu

Hrozby	**Zraniteľnosti**
Porucha zariadenia	Zariadenia, služby
Krádež	Zariadenia, služby, informácie
Únik informácií	Informácie
Útoky DoS	Zariadenia, služby
Man in middle útok	Informácie, služby
Strata kontroly zariadenia	Informácie, služby
Neschopnosť, neznalosť pracovníka riešiť problém	Zariadenia, služby, informácie
Zanedbanie povinností	Zariadenia, služby, informácie
Chyba používateľa	Zariadenia, služby, informácie

Závery z analýzy rizík pre modelovú firmu
Pre modelovú firmu je z pohľadu jej umiestnenia napr. v centre mesta možné hneď definovať niektoré hrozby a zraniteľnosti, ktoré musí pri prijímaní bezpečnostných opatrení a bezpečnostnej politiky brať do úvahy.

- *Rušenie - v centre mesta a v susedstve iných firiem je pravdepodobnosť vzájomného rušenia sa rôznych sietí dosť vysoká.*
- *Odpočúvanie - pokiaľ ide o dnes už základný štandard zabezpečenia dát šírených vzduchom, musí prenos dát prebiehať v šifrovanej podobe.*
- *Man in the middle - zabezpečiť sieť proti prieniku tretej osoby do siete, napr. pomocou ďalšieho AP tváriaceho sa ako legálne AP.*
- *WPS autentizácia zariadení - je určená primárne obyčajnému používateľovi, malo by teda ísť v prevažnej miere o WLAN siete v domácnostiach.*
- *Slabé heslá pri používaní WPA-PSK autentizácie - rôzne typy útokov na WEP, WPA a WPA2 sa spoliehajú na nedostatočnú silu hesla, zvoleného pre autentizáciu pomocou PSK.*
- *Nepriradenie zodpovednosti za vytvorenú bezpečnostnú politiku a neurčenie povinností konkrétnym pracovníkom.*

Tieto hrozby patria samozrejme medzi základné hrozby, kvôli ktorým nie je potrebné prevádzať hĺbkovú analýzu, postačí analýza základná. Cieľom tejto práce nie je navrhnúť konkrétne zabezpečenie modelovej firmy, ale skôr ukázať v jednoduchej postupnosti krokov, na čo by mala každá firma myslieť pri budovaní hoci iba obyčajnej a v dnešnej dobe tak rozšírenej WLAN siete. Preukázanie sily bezpečnostných opatrení na obmedzenie možných hrozieb je totiž aj dobrým signálom pre potenciálnych partnerov a zákazníkov, čo je práve pre malé a stredné podniky nezanedbateľnou konkurenčnou výhodou.

Riadenie rizík
Po vykonaní analýzy rizík by mala firma prijať náležité bezpečnostné opatrenia, vychádzajúce z výsledkov analýzy. Tieto bezpečnostné opatrenia sú jednou z činností riadenia rizík**.**

Bezpečnostné opatrenia
Bezpečnostné opatrenia slúžia na zabezpečenie ochrany pred hrozbami, na zníženie využitia zraniteľností, eliminujú dopady bezpečnostného incidentu. Ochranné opatrenia vykonávajú viacero funkcií, ako sú napr. prevencia, monitorovanie, detekovanie a pod. Každá firma budujúca nejaký IS, nielen WLAN sieť, by mala zvážiť, aké bezpečnostné opatrenia vybrať, aby to bolo pre ňu z hľadiska nákladov ešte efektívne a samozrejme, aby to spĺňalo podmienky požadovanej bezpečnosti, resp. aby zostatkové riziko bolo eliminované na akceptovateľnú úroveň. Preto je podstatné aj priradenie závažnosti jednotlivým hrozbám a zraniteľnostiam v prebiehajúcej analýze a určenie spôsobu ich zníženia na prijateľnú úroveň. Príkladom bezpečnostných opatrení pre WLAN je napríklad monitorovanie a analýza siete, šifrovanie dát, certifikačné nástroje, riadenie prístupu do siete a pod.

Podľa vzťahu opatrenia k priebehu bezpečnostného incidentu môžeme bezpečnostné opatrenia rozdeliť na:
- preventívne - minimalizácia príčiny možného vzniku,
- dynamické - minimalizácia možných dopadov aktuálne prebiehajúceho incidentu,
- následné - minimalizácia možných dopadov prebehnutého incidentu.

Z iného hľadiska je možné bezpečnostné opatrenia rozdeliť na [1]:
- technické opatrenia fyzickej a objektovej ochrany,
- softvérové opatrenia,
- hardvérové opatrenia,
- režimové a organizačné opatrenia.

ZÁVERY K RIADENIU RIZÍK PRE MODELOVÚ FIRMU

Na základe analýzy je možné pre modelovú firmu navrhnúť tieto bezpečnostné opatrenia:
- Znížiť vyžarovaný výkon jednotlivých antén, a pokiaľ je to možné, vymeniť použité všesmerové antény za smerové.
- V zarušenom prostredí, akým je napr. centrum mesta, je vhodné zriadiť Wi-Fi sieť v pásme 5 GHz, a nie v pásme 2,4 Ghz.
- Zamedziť jednoduchému pripojeniu falošného AP (napr. nahradením za iné zariadenie pripojené do siete).
- Zakázať použitie protokolu WEP pre šifrovaný prenos dát a namiesto neho použiť šifrovanie pomocou WPA-PSK
- Zabezpečiť politiku vytvárania hesiel zložených z kombinácie normálnych a špeciálnych znakov a číslic na eliminovanie možnosti prelomenia hesla slovníkovým útokom.
- Priradiť zodpovednosť za vypracovanie a pravidelnú aktualizáciu bezpečnostnej politiky konkrétnemu zamestnancovi.

Informačná bezpečnostná politika
Informačná bezpečnostná politika je základným dokumentom v oblasti informačnej bezpečnosti podniku, ktorý by mal obsahovať predstavu vrcholového manažmentu o riešení bezpečnosti a zároveň základné požiadavky na jednotlivé bezpečnostné oblasti.

Pri spracovaní bezpečnostnej politiky existuje päť základných krokov:

- identifikácia toho, čo chceme chrániť - inventarizácia aktív,
- určenie, proti čomu chceme aktíva chrániť - identifikácia hrozieb,
- určenie pravdepodobnosti hrozieb,
- zavedenie opatrení, ktoré chránia aktíva pred identifikovanými hrozbami a cena opatrení musí byť nižšia, ako škoda spôsobená ohrozením konkrétneho aktíva,
- kontinuálne opakovanie procesu a implementácia opatrení v prípade odhalenia slabých miest v zabezpečení.

Pri posudzovaní a rozhodovaní, či je potrebné pre malý podnik vytvárať tento dokument, je užitočná citácia: Veľkosť organizácie nemá vplyv na rozsah riešenia bezpečnosti. Teda, v prípade malej organizácie vlastne nie je možné vynechať niektoré oblasti a okruhy riadenia, je však možné budovať jednoduchší systém riadenia, ale súčasne komplexne pokrývajúci problematiku bezpečnosti IT.
Informačná bezpečnostná politika je časťou všeobecnej bezpečnostnej politiky v kategórii komunikačná bezpečnosť. Z hľadiska rozsahu sa bezpečnostná politika dá rozdeliť na stručnú a rozsiahlu. Pri zohľadnení, že sa jedná o malý alebo stredný podnik s menšou veľkosťou WLAN siete, je postačujúce vypracovanie stručnej parciálnej bezpečnostnej politiky, kde ako príklad môže poslúžiť vzor na vypracovanie bezpečnostnej politiky uvedenom na obr. 24. Výhodou je rýchla a nenáročná príprava takého dokumentu. Taktiež sa s ňou môžu bez problémov oboznámiť dotknuté osoby, nie je potrebné ju príliš často aktualizovať a keď sa aktualizuje, ide opäť o pomerne rýchly proces. Samozrejme takto definovaná bezpečnostná politika je iba časťou komplexnej informačnej bezpečnostnej politiky, no pre potreby zabezpečenia WLAN siete je postačujúca a slúži aj ako fyzicky preukázateľný dokument o úrovni zabezpečenia pre obchodných partnerov, pokiaľ je to potrebné. [7]
Zaisťovanie bezpečnosti bezdrôtových sietí v kontexte ochrany informácií, je jedným z čiastkových cieľov bezpečnostného vzdelávania. Úlohou bezpečnostného vzdelávania je umožniť bezpečnostným pracovníkom získať a osvojiť si poznatky a znalosti metód, na základe ktorých budú schopní analyzovať bezpečnostné prostredie a jeho činitele vo vzťahu k rôznym objektom, identifikovať a hodnotiť bezpečnostné riziká a ohrozenia a prognózovať ich vývoj, určovať postupy a opatrenia na riadenie, bezpečnostných rizík a ohrození, plánovať a organizovať opatrenia riadenia rizík, bezpečnostného a krízového manažmentu v súlade s dostupnými zdrojmi a kapacitami, projektovať a riadiť komplexné bezpečnostné systémy [24]

RESUME

V tomto bode je popísaný rýchly všeobecný návod na zabezpečenie siete a vypracovanie bezpečnostnej politiky. Po vytvorení WLAN siete prichádza na rad jej zabezpečenie, pri ktorom je odporúčané dodržať minimálne nasledujúce kroky:

- Analýza rizík: Pri vytvorení malej siete firma zváži svoje aktíva, ktoré je potrebné chrániť, ich hodnotu, prípadne im priradí stupne dôležitosti. Na základe toho sa rozhodne, aký prístup analýzy rizík (základný, neformálny, formálny, kombinovaný) je vhodný na dosiahnutie požadovanej úrovne bezpečnosti. Po identifikácii aktív môže firma pristúpiť k identifikácii hrozieb, kde zohľadní úmyselné aj neúmyselné možné hrozby podľa vyššie uvedených príkladov a z toho vyplývajúcich zraniteľností.
- Riadenie rizík: V tomto kroku sú prijaté bezpečnostné opatrenia, ktoré znížia mieru ohrozenia na úroveň akceptovateľného rizika. To znamená, že v prípade bezpečnostného incidentu nedôjde k majetkovým či nemajetkovým škodám firmy. Netreba ale zabúdať na skutočnosť, že cena bezpečnostných opatrení musí byť nižšia, ako škoda spôsobená ohrozením konkrétneho aktíva.
- Bezpečnostná politika pre danú WLAN: Je vhodné vytvoriť rámcové bezpečnostné politiky ako súčasť celkovej bezpečnostnej politiky. Spracovaním dokumentu sa stanovia pravidlá a úlohy, ktoré so potom budú aplikovať v praxi. Pri vypracovaní je potrebné splniť všetky požiadavky dané vybraným štandardom zvoleným v prvom kroku pri analýze rizík.

ZÁVER

Bezpečnosť informačných systémov sa dostáva na predné miesta riešených problémov. Táto skutočnosť platí všeobecne, nielen pre prudko sa rozširujúce WLAN siete. Malé a stredné organizácie ale stále podceňujú význam informačnej bezpečnosti, práve preto bolo cieľom štúdie objasniť dôvody vhodného zabezpečenia WLAN siete a možné druhy hrozieb, útokov a zraniteľností, ktoré takejto nezabezpečenej sieti hrozia (eliminácia známych problémov, ako je prechod medzi nadväzujúcimi AP, vzájomné rušenie frekvencií, nutnosť napájania AP pomocou adaptéra). Zároveň materiál upozorňuje na dôležitosť spracovania bezpečnostnej dokumentácie, aby si práve malé a stredné organizácie uvedomili a nepodceňovali jej význam. Zameranie je skôr na všeobecnejší, a teda univerzálnejší postup pri vypracovávaní bezpečnostnej dokumentácie vo forme dokumentu bezpečnostnej politiky a jeho zavádzaní do praxe v týchto organizáciách, keďže každý jeden informačný systém je svojím spôsobom jedinečný, a aj keď je možné v ňom aplikovať všeobecne odporúčané štandardy a postupy zabezpečenia, môže obsahovať určité špecifiká charakterizujúce práve tú jednu konkrétnu firmu, pri ktorých bude potrebné zabezpečiť daný informačný systém alebo sieť dodatočným spôsobom a ošetriť špecifické hrozby a zraniteľnosti. Súčasnosť poukazuje na potrebu kvalitného zabezpečenia všetkých sietí, v ktorých sa prenášajú informácie, pretože tieto v sebe nesú čoraz väčšie hodnoty a tie je potrebné chrániť. Vývoj v posledných 10 rokoch priniesol kvalitné techniky šifrovania zvyšujúce bezpečnosť dát, ale napriek tomu stále veľký počet firiem, hlavne stredných a menších, chráni svoje bezdrôtové siete neadekvátnym spôsobom a neuvedomuje si dôsledky prípadných únikov dát.

ZOZNAM POUŽITEJ LITERATÚRY

[1] BLIŠŤANOVÁ, M. - SEDLÁK V. 2012, Manažérske informačné systémy, Košice 2012, vydanie prvé, Košice 2012, ISBN 978 -80-89282-78-4. s. 81,
[2] HOLES, M. 2007, Vytvorenie domácej bezdrôtovej siete, PC REVUE, 1/2007, str. 50 - 55
[3] KLEGA, V. 2011, Opravdovým šéfem sítě, CHIP 10/2011, str. 74 - 77
[4] KLEGA, V. 2011, Wi-Fi Direct: Přímé spojení, CHIP 10/2011, str. 78 - 79
[5] KÖHRE, T. 2004, Stavíme si bezdrátovou síť Wi-Fi, Computer Press, Brno 2004, 95 str., ISBN 80-251-0391-9
[6] LOVEČEK, T. 2007, Bezpečnosť informačných systémov, Žilina 2007, 247 str., ISBN 978-80-8070-767-5
[7] MESÁROŠ, M. - REITŠPÍS, J. - KRIŽOVSKÝ, S. 2010, Bezpečnostný manažment, Košice 2010, 150 str., ISBN 978-80-89282-48-7
[8] MFSR 2011, Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike v roku 2011, - [on-line] Available on - URL: www.informatizacia.sk/ext_dok-prieskum_ib_2009/12773c
[9] OUELLET, E. 2002, Building A Cisco Wireless LAN, Syngress 2002, 501 str. ISBN: 1-928994-58-X
[10] POŽÁR, J. 2005, Informační bezpečnost, Plzeň 2005, 309 str., ISBN 80-86898-38-5
[11] STRNÁD, O. 2008, Systémový prístup k riadeniu informačnej bezpečnosti, Synergie, Trnava 2008, 233 str., ISBN 978-80-89291-20-5
[12] TOPeL, 2008, OSI model - princípy fyzickej vrstvy, Žilina 2008, Tvorba obsahov pre e-Learning, 54 str. - [on-line] Available on - URL: http://www.kis.fri.uniza.sk/~ludo/top_el/OSI/OSI.pdf
[13] TŘÍSKA, J. 2008, Technológie počítačových sietí. - [on-line] Available on - URL: http://www.spsepn.edu.sk/skola/pk_info/studium/ucebtext/ele/ siete/bezdrotove_siete.pdf
[14] UVSR_OPIS3_SU_F1 Vychodiska.doc. 2008, Zvýšenie prístupnosti k širokopásmovému internetu. - [on-line] Available on - URL: http://www.opis.gov.sk/data/files/5452.pdf
[15] V.802.11 Wireless LAN 2007, 142 str. Dostupné na: www.apl.jhu.edu/~hhsu/cs771/cs771-II.pdf
[16] ZEMAN, J. - TANUŠKA, P. 2006, Niektoré problémy bezpečnosti počítačových sietí založených na technológií wifi, 7 str. Dostupné na: www.mtf.stuba.sk/docs//internetovy_casopis/2006/2/tanuska.pdf
[17] Zákon č. 275/2006 Zb. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov
[18] Zákon č 312/2010 Zb. o štandardoch pre informačné systémy verejnej správy
[19] LAN/MAN Standards Committee of the IEEE Computer Society, 2009, IEEE Std 802.11n - 2009, IEEE [1] Standard for Information Technology, Part 11: WLAN MAC and PHY Specifications-Amendment
[20] [on-line] Available on - URL: http://www.informatizacia.sk/
[21] [on-line] Available on - URL: http://wiki.airdump.cz/Hlavní_strana
[22] [on-line] Available on - URL: http://www.hack4fun.eu/
[23] [on-line] Available on - URL: http://www.security-portal.cz/
[24] Kováčová, L. - Klimo, V.: Fundamentals of security education in the process of globalization, In.Odes´kyi Politechnichnyi Universytet PRATSI, Iss.2 (41), 2013 Odesa, s.217-222, ISSN 2076-2429
[25] [on-line] Available on - URL: http://pc.poradna.net/q/view/580236-pomoc-s-routrem-slaby-signal-v-dome

Poďakovanie
Štúdia bola spracovaná v rámci riešenia inštitucionálneho projektu: IP/29/VSBM/2012 AV, Názov projektu: Vplyv bezpečnosti a prevádzky wifi sieti na infraštruktúru vysokej školy

ADRESA AUTORA

Ing. Peter LOŠONCZI, PhD., Vysoká škola bezpečnostného manažérstva v Košiciach, Kukučínova 17, Košice, e-mail: peter.losonczi@vsbm.sk

RECENZIA TEXTOV V ZBORNÍKU
Recenzované dvomi recenzentmi, členmi vedeckej rady konferencie. Za textovú a jazykovú úpravu príspevku zodpovedajú autori.

REVIEW TEXT IN THE CONFERENCE PROCEEDINGS
Contributions published in proceedings were reviewed by two members of scientific committee of the conference. For text editing and linguistic contribution corresponding authors.