EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja
OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE
it akadémia

Modul 12: Bezpečnosť pri využívaní IKT

Bezpečnosť počítačových sietí

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY
www.itakademia.sk
ITMS2014+: 312011F057

3 Bezpečnosť počítačových sietí

3.1 Počítačové siete a pripojenia

3.1.1 Čo je počítačová sieť, typy počítačových sietí - lokálne siete (LAN), bezdrôtové lokálne siete (WLAN), rozľahlé siete (WAN), virtuálne privátne siete (VPN)

Počítačová sieť je systém vzájomne prepojených a spolupracujúcich počítačov, medzi ktorými môžeme pohodlne a rýchlo prenášať údaje, zdieľať prostriedky a komunikovať medzi používateľmi. Podľa rozsahu môžeme počítačové siete rozdeliť na tri kategórie.

LAN (Local Area Network) je typicky sieť v rozsahu jednej budovy, resp. inštitúcie. Väčšinou sú dobre chránené pred prístupom z vonku. V súčasnosti využíva v podstate dve technológie, a to Ethernet pre káblové (drôtové) prepojenie a WiFi pre bezdrôtové prepojenie - takáto sieť sa tiež nazýva pojmom WLAN (Wireless Local Area Network).

MAN (Metropolitan Area Network) je typicky sieť v rozsahu mesta, ktorá prepája jednotlivé LAN, napríklad siete poskytovateľov pripojenia do Internetu. V súčasnosti využíva najmä optické prepojenia, prípadne špeciálne bezdrôtové prepojenia na väčšie vzdialenosti.

WAN (Wide Area Network) sú rozľahlé siete v rozsahu regiónu, štátu, kontinentu či celého sveta, napr. armádne siete, Internet a podobne.

VPN (Virtual Private Network) - je technológia prepojenia viacerých počítačov pomocou verejnej (nedôveryhodnej) siete tak, akoby boli pripojené na jednu spoločnú súkromnú sieť (dôveryhodnú). Využívajú sa napr. na bezpečný prenos medzi vzdialeným používateľom a vnútornou sieťou organizácie (prístup z domu, počas služobnej cesty), prípadne spojenie medzi pobočkami firmy a podobne.

3.1.2 Vplyv pripojenia sa do siete na bezpečnosť, napríklad na šírenie škodlivého softvéru, na neoprávnený prístup k údajom, na narušenie súkromia

Ak nemáme počítač pripojený do počítačovej siete, útok naň môže byť zrealizovaný len fyzickým kontaktom, teda buď sa útočník dostane k počítaču, alebo používateľ donesie malware na pamäťovom médiu. Únik informácií z takého počítača bez spolupráce používateľa je prakticky nemožný.

Ak počítač pripojíme do počítačovej siete, vystavujeme ho tým možným útokom po sieti (najmä po pripojení do neznámej alebo verejnej siete), ktoré sa väčšinou snažia zneužiť zraniteľnosť nejakej sieťovej služby, prípadne využiť zle nastavenú sieťovú službu, a tak získať neoprávnený prístup k informáciám uloženým v počítači, nainštalovať malware, alebo ovládnuť celý počítač. Rapídne sa zvyšuje možnosť úniku informácií z počítača, či už činnosťou malware alebo chybou používateľa pri využívaní sieťových služieb.

3.1.3 Úloha správcu počítačovej siete v procese riadenia autentifikácie, autorizácie, pri správe používateľských účtov, pri monitorovaní a inštalovaní relevantných bezpečnostných záplat a aktualizácií, pri monitorovaní sieťovej komunikácie, pri riešení nájdeného škodlivého softvéru v rámci spravovanej siete

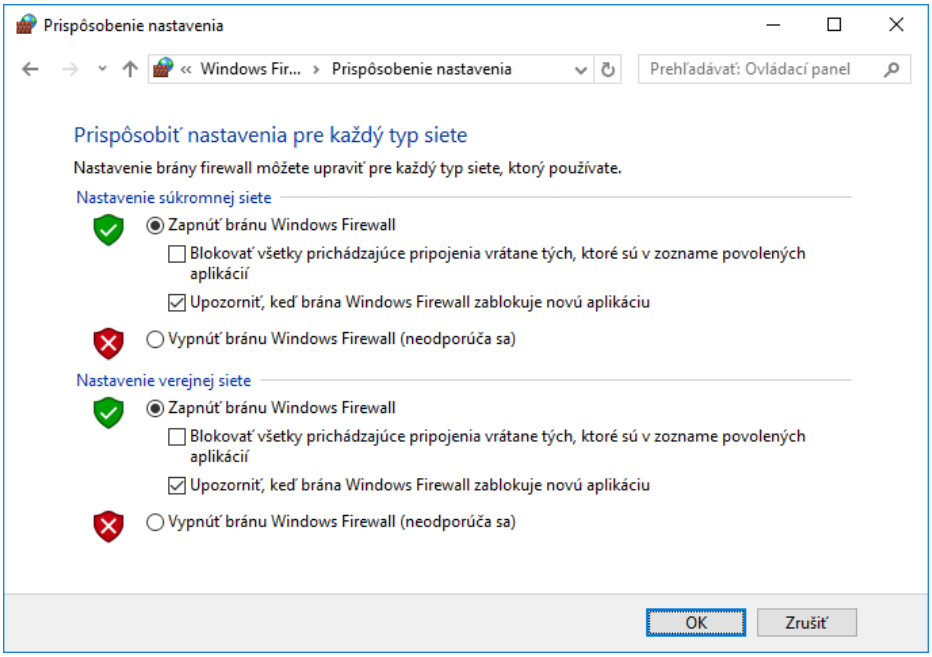
Správca počítačovej siete (administrátor) nastavuje spôsob autentifikácie používateľov v sieti, spravuje používateľské kontá (vytvára a maže), nastavuje pre používateľov oprávnenia (autorizuje ich) pre prístup do lokálnej siete aj do internetu, konfiguruje firewall a sieťové služby, monitoruje sieť, stará sa o inštaláciu softvéru a bezpečnostných záplat a rieši malwarové incidenty.

3.1.4 Funkcia brány firewall, jeho obmedzenia v súkromnom i pracovnom prostredí

Firewall je zariadenie (hardvérové alebo softvérové) pre riadenie sieťovej prevádzky. Zjednodušene sa dá povedať, že slúži ako kontrolný bod, ktorý definuje pravidlá pre komunikáciu medzi sieťami (alebo počítačom a sieťou) a tým povoľuje (resp. zakazuje) komunikáciu podľa vopred definovaných pravidiel.

3.1.5 Aktivácia firewallu, konfigurácia jednoduchých pravidiel

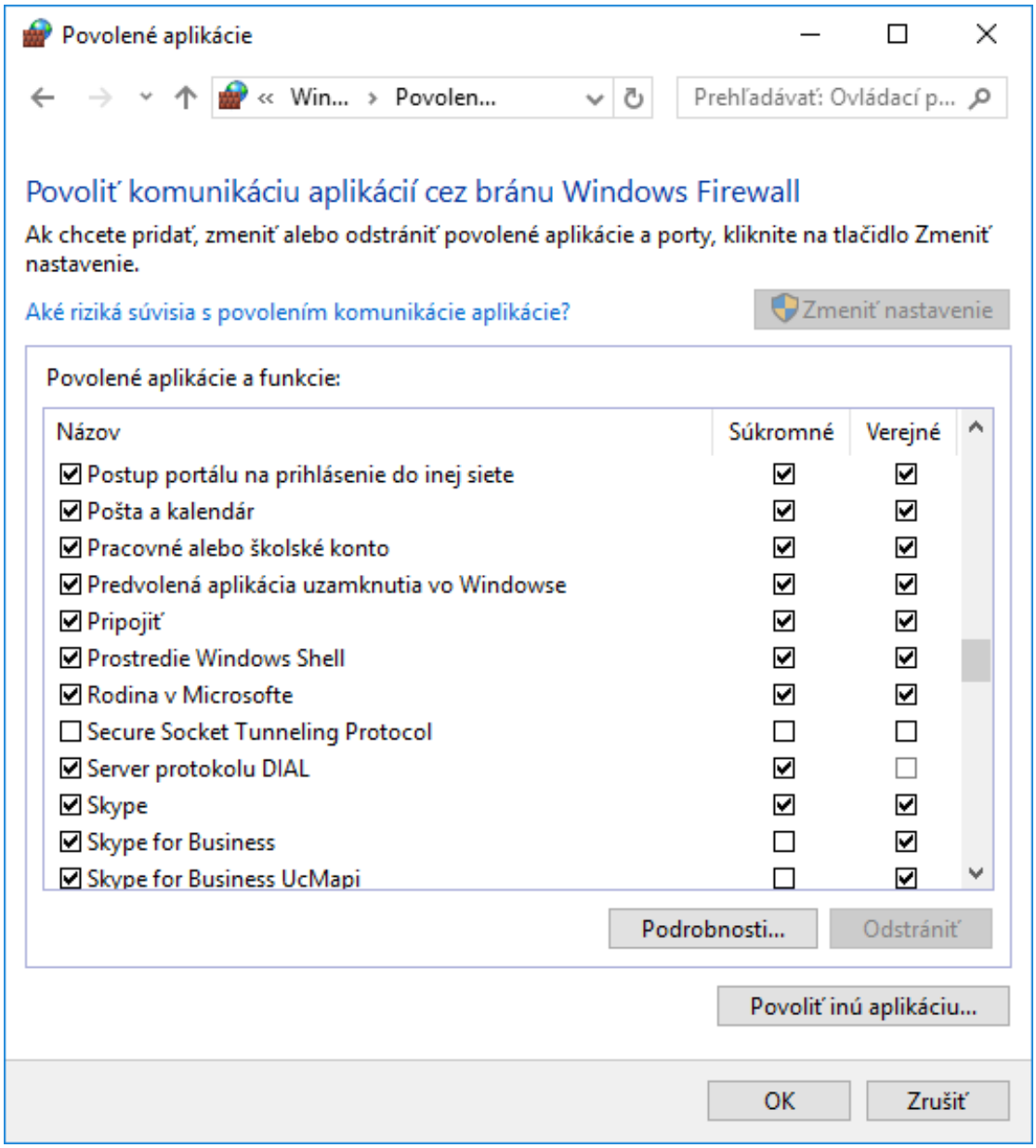
Firewall v systéme Windows môžeme ľahko vypnúť alebo zapnúť. Stačí vojsť do Ovládacieho panela a zvoliť "Systém a zabezpečenie" a ďalej "Windows Firewall". V ľavom menu zvolíme položku "Zapnúť alebo vypnúť bránu Windows Firewall" (Obrázok 1).



Obrázok 1: Zapnutie/vypnutie brány Windows Firewall

Ak v ľavom menu zvolíme možnosť "Povoliť komunikáciu aplikácií cez bránu Windows Firewall" (Obrázok 2) dostaneme sa k dialógu, kde môžeme ručne povoľovať/zakazovať

funkcie a aplikácie firewallu. Tento dialóg obsahuje len veľmi zjednodušené nastavenia firewallu, pre komplexnejšie nastavenia sú potrebné hlbšie znalosti o počítačových sieťach.



Obrázok 2: Povolenie komunikácie aplikácií cez bránu Windows Firewall

Všimnite si, že v oboch spomínaných dialógoch je firewall oddelený do profilov - pre súkromné siete (doma, v práci - na miestach, kde je prehľad o pripojených klientoch) a na verejné siete (hlavne rôzne verejné wifi siete). Dá sa takto nakonfigurovať odlišné správanie firewallu vzhľadom k nastaveniu pripojenej siete.

3.2 Bezpečnosť bezdrôtovej siete

3.2.1 Typy zabezpečenia bezdrôtovej siete - Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) / Wi-Fi Protected Access 2 (WPA2), Media Access Control (MAC) filtrovanie, Service Set Identifier (SSID) skrývanie

Komunikáciu realizovanú pomocou bezdrôtovej (WiFi) siete je ľahké odpočúvať. Na rozdiel od (drôtovej) siete sa totiž netreba nikam pripájať, stačí byť v dosahu signálu. Preto je vhodné chrániť prístup k tejto sieti heslo a zároveň takúto komunikáciu šifrovať. Na ochranu bezdrôtovej siete sa využívajú viaceré typy zabezpečenia.

Prístup k sieti sa dá obmedziť **filtrovaním MAC adries**. Využíva filtrovanie pripojených zariadení na základe MAC adresy (Media Access Control), ktorá slúži na identifikáciu sieťového rozhrania v lokálnych počítačových sieťach, ale je ľahko prekonateľná a je to iba ochrana prístupu, nechráni proti samotnému odpočúvaniu.

WEP (Wired Equivalent Privacy) je zastaralé zabezpečenie bezdrôtových sietí. V minulosti bolo prelomené, preto je v súčasnosti toto zabezpečenie považované za nedostatočné.

WPA (Wi-Fi Protected Access) bolo vyvinuté za účelom náhrady WEP. Využíva rovnakú šifrovaciu metódu ako WEP, ale pre správu šifrovacích kľúčov používa protokol TKIP (Temporal Key Integrity Protocol), ktorý mení dočasný kľúč každých 10000 paketov. Pre pripojenie sa využívajú dva spôsoby autentifikácie:

- PSK (Pre-Shared Key) - využíva heslo, ktoré je spoločné pre všetkých používateľov siete,
- Enterprise - využíva autentizačný server a vyžaduje autentifikáciu konkrétneho používateľa (meno a heslo).

WPA a jeho nasledovníka WPA2 je dnes možné prelomiť a preto sa odporúča využiť ich nasledovníka **WPA3**, ktorý je považovaný za bezpečný.

SSID je identifikátor (názov) bezdrôtovej siete. Prístupový bod bezdrôtovej siete pravidelne vysiela tento identifikátor - je však možné nakonfigurovať ho tak, aby tento identifikátor nevysielal, čo môže prispieť k zvýšeniu bezpečnosti bezdrôtovej siete. Pokiaľ je však bezpečnosť siete postavená výlučne len na skrývaní SSID, jedná sa o bezpečnostnú slabinu.

3.2.2 Riziká používania počítačovej siete (odpočúvanie komunikácie, prevzatie sieťového spojenia, odpočúvanie a pozmeňovanie komunikácie)

V nezabezpečenej WiFi sieti sú všetky zariadenia pripojené bez ochrany ich komunikácie, takže nie sú chránené voči útočníkom.

Komunikáciu cez takéto pripojenie môže odpočúvať ktokoľvek v dosahu signálu. Útočník sa môže vydávať za niekoho iného a tak získať prístup k počítačovým systémom. Hroziacim útokom je aj tzv. "Man in the middle" (MITM, človek uprostred), kedy útočník odpočúva sieťovú komunikáciu medzi účastníkmi tak, že sa stane aktívnym

prostredníkom. Na takúto sieť sa môže pripojiť v podstate ktokoľvek a potom hrozia ďalšie útoky súvisiace s prienikom do systému obete.

Ak sa už rozhodnete pripojiť na verejne prístupnú Wi-Fi sieť, skúste sa držať nasledujúcich zásad, ktoré zvýšia pravdepodobnosť, že vaše údaje nezneužije tretia strana. Stránky, kde zadávate chúlostivé informácie (prakticky všade, kde sa prihlasujete menom a heslom) navštevujte iba ak sú zabezpečené dodatočným šifrovaním (URL stránky začína na "https://"). Veľmi dobre môže poslúžiť aj firewall s nastavenými striktnými pravidlami filtrovania prichádzajúcich spojení. Ak je to možné, použite šifrované VPN.

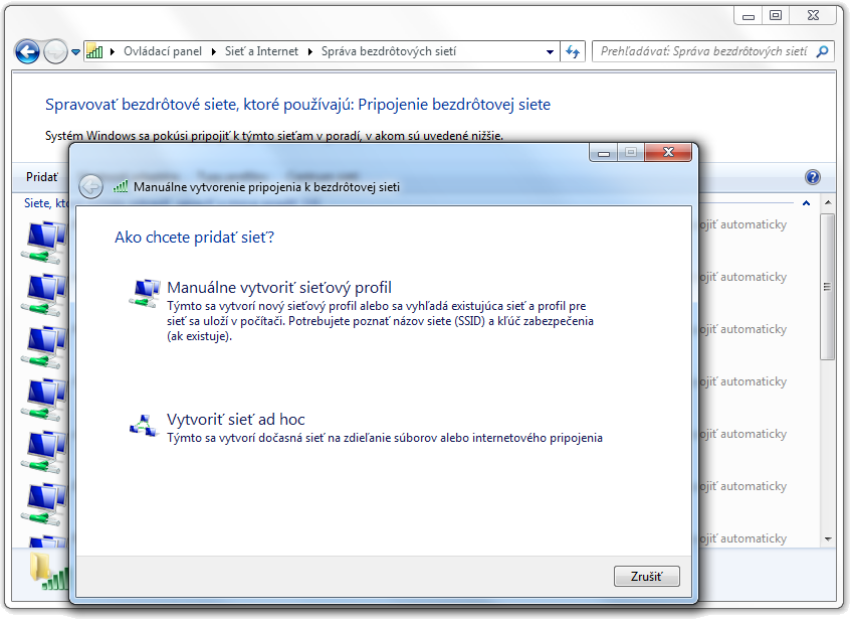
3.2.3 Vytvorenie prípojného bodu (hotspot)

Z bežného počítača vybaveného bezdrôtovým sieťovým rozhraním možno konfiguráciou vytvoriť prípojný bod a takým spôsobom umožniť, aby sa iné počítače pripojili za účelom zdieľania sieťovej konektivity, výmeny dát, využitia nejakých sieťových služieb a podobne.

3.2.4 Vytvorenie osobného hotspotu

Vytvoriť prípojný bod v systéme Windows 7 je jednoduché:

- **`Štart ▶ Ovládací panel ▶ Sieť a Internet`**
- v ľavej časti zvolíme **`Správa bezdrôtových sietí`**
- **`Pridať ▶ Vytvoriť sieť ad hoc`** (Obrázok 3)

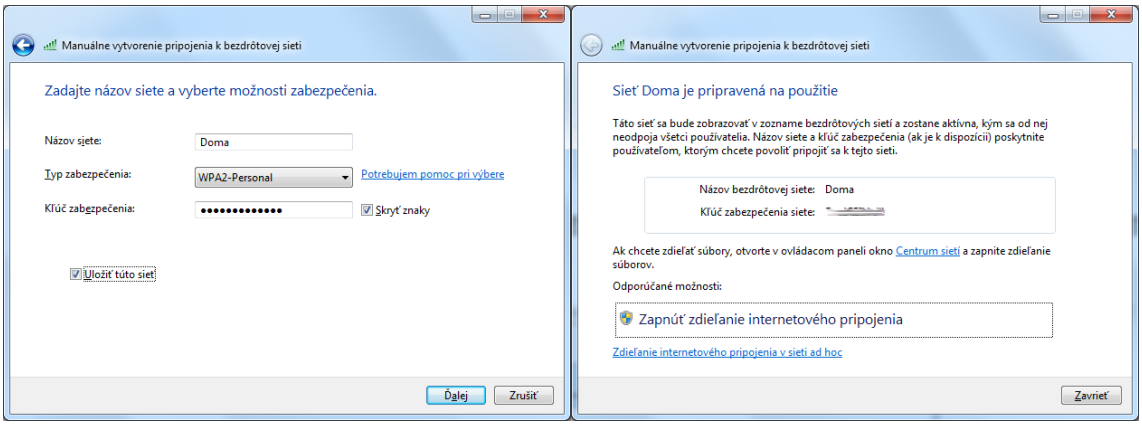


Obrázok 3: Vytvorenie hotspotu vo Windows 7

V nasledujúcej časti nastavíme (Obrázok 4):

- názov siete SSID,
- typ zabezpečenia,
- kľúč zabezpečenia KEY.

Zapnutím zdieľania internetového pripojenia je možné využiť osobný hotspot. Niektoré úkony môžu požadovať administrátorský prístup.



Obrázok 4: Nastavenie siete

Pre Windows 10 vytvoríme nasledovným spôsobom. Otvoríme si príkazový riadok pod administrátorským účtom a nasledovným príkazom vytvoríme ad-hoc sieť:

```
netsh wlan set hostednetwork mode=allow ssid=SSID key=PASSWORD
```

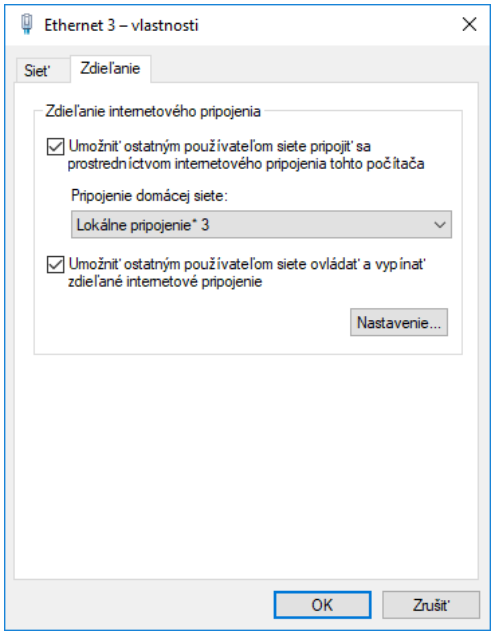
Reťazec SSID nahradíme názvom siete podľa vlastného výberu a reťazec PASSWORD nahradíme heslom. Nasledovným príkazom aktivujeme novovytvorenú sieť:

```
netsh wlan start hostednetwork
```

Tretím krokom povolíme zdieľanie Internetového pripojenia. Otvoríme ovládací panel a zvolíme položku "Sieť a internet" a "Centrum sietí". V ľavom menu klikneme na "Zmeniť nastavenia adaptéra" - otvoríme okno so zoznamom sieťových pripojení.

Klikneme pravým tlačidlom na to pripojenie, ktorým sa počítač pripája na Internet a zvolíme "Vlastnosti" a prejdeme na záložku "Zdieľanie" (Obrázok 5). zaškrtneme možnosť "Umožniť ostatným používateľom siete pripojiť sa prostredníctvom internetového pripojenia tohto počítača" a vo výberovom menu "Pripojenie domácej siete" vyberieme novovytvorenú ad-hoc sieť.

Teraz je možné sa iným zariadením pripojiť k vytvorenej ad-hoc sieti a prostredníctvom nej sa pripojiť na Internet.



Obrázok 5: Zdieľanie sieťového pripojenia