T-Mobile

Zásady zabezpečení pro uživatele GPRS

Obsah

1. Úvod

Cílem dokumentu je popsat zásady zabezpečení, které by měl aplikovat uživatel T-Mobile GPRS. Zásady zabezpečení jsou rozděleny následujícím způsobem:

- obecné zásady – základní bezpečnostní opatření související s provozem klientského počítače,
- zásady ochrany proti škodlivému kódu a virům,
- zásady používání elektronické pošty – opatření pro nastavení a práci s elektronickou poštou,
- zásady fyzické bezpečnosti,
- opatření pro zabezpečení komunikace – doporučení a návody pro zabezpečení důvěrnosti spojení.

V každém bodu je uvedena sada doporučení z dané oblasti (tzv. best practices), která jsou doplněna o odkazy na informační zdroje. U opatření, jejichž implementace vyžaduje komplikovaný postup, jsou uvedeny ukázky postupů nastavení.

2. Zásady zabezpečení

Uživatelé služeb T-Mobile GPRS by měli zvážit implementaci následujících bezpečnostních opatření:

2.1 Obecné zásady

1. Pravidelná aktualizace systému Windows prostřednictvím systému Active Update (http://windowsupdate.microsoft.com).
2. Instalovat software pouze z důvěryhodných zdrojů, vyvarovat se instalace nedůvěryhodného software z Internetu.
3. Pro přístup k počítači používat alespoň 8 znaků dlouhé heslo, obsahující velká i malá písmena a číslice.
4. Zablokování odchozích mezinárodních hovorů z mobilního telefonu na úrovni GSM: http://t-mobile.cz/cms/default.asp?menu=136. Nejprve si změnte svůj blokovací kód (čtyřmístné číslo) na něco jiného než 0000 pomocí:

****03*330*starý kód*nový kód*nový kód# Odeslat**

Pak pomoci

***331* blokovací kód # Odeslat (OK)**

nastavit blokování mezinárodních hovorů.

2.2 Zásady ochrany proti škodlivému kódu a virům

5. Instalace antivirového software a jeho pravidelná aktualizace. Doporučený AV software:
   AVG: http://www.grisoft.cz/cz/cz_index.php
   Avast!: http://www.avast.com/index_cze.html
   F-Secure AV Client security: http://www.aec.cz
6. Pravidelná kontrola souborů na disku antivirem.
7. Nastavení antiviru tak, aby kontroloval příchozí poštu, internet, případně další komunikační kanály.
8. Nastavení rezidentní ochrany antiviru a automatického antivirového testování pro dokumenty a software přidávané do systému.
9. Instalace personálního firewallu a jeho pravidelná aktualizace. Doporučujeme jeden y následujících:
   Kerio PF: http://www.kerio.cz/kpf_home.html
   Norton PF: http://www.symantec.com/region/cz/product/npf_index.html
   F-Secure AV Client security http://www.aec.cz

Ve verzi Windows XP je k dispozici také vestavěný Internet Connection Firewall (ICF). ICF ve výchozí konfiguraci blokuje všechna příchozí spojení k počítači uživatele. Nastavení ICF pro GPRS připojení můžete provést takto: Ovládací panely > Síťová připojení. Zde vyberete připojení přes T-Mobile GPRS, dále Vlastnosti > Upřesnit. Zde zaškrtněte „Chránit počítač a síť...“ viz. obrázek č. 3.1.

10. Personálním firewallem povolit pouze odchozí spojení z počítače, a to pouze důvěryhodným aplikacím.
    Poznámka: ICF neumožňuje omezit, které programy mohou navázat odchozí spojení.
11. Pravidelná kontrola systému na přítomnost trojských koní, spyware a červů speciálním software. Doporučujeme:
    AdAware: http://www.lavasoftusa.com/software/adaware
    Spybot: http://www.safer-networking.org

2.3 Zabezpečení elektronické pošty

Poznámka: opatření v této kapitole jsou zaměřena zejména na uživatele poštovních klientů MS Outlook a Outlook Express.

12. Pravidelná aktualizace poštovního klienta za použití oprav od výrobce software je nejúčinnějším prostředkem zabezpečení.
    Aktualizace pro sadu kancelářského software MS Office jsou k dispozici zde:
    http://office.microsoft.com/productupdates
    Aktualizace Outlook Express: http://www.microsoft.com/windows/ie/
13. Celá řada virů a škodlivého kódu využívá vlastnosti systému Windows, umožňující automatického spuštění příloh obsahujících virus. Poslední verze produktů Outlook 2000, Outlook 2002, Outlook 2003 a Outlook Express poskytují uživateli ochranu proti těmto útokům, jelikož automaticky znemožňují uživateli přístup k příloze s příponou nebezpečného typu.
    Pro uživatele starších verzí MS Office je možné zvýšit zabezpečení odstraněním tzv. asociace pro soubory s nebezpečnými příponami:

    Postup pro Windows 98: Tento počítač > Nástroje > Možnost složky > Typy Souborů. Zde najít typy souborů WSC, WSH, WSF, SCT, VBE a VBS a pro ně kliknout na „Odebrat“ (viz. obrázek č. 3.2).
    Anglická verze Windows: MyComputer > Tools > Folder Options > File Types.

    Poznámka: odstraněním asociace pro výše uvedené typy souborů mohou přestat fungovat některé aplikace. V takovém případě je nutné vrátit nastavení zpět pomocí volby „Přidat“.
14. Některé verze poštovního klienta MS Outlook ve výchozím nastavení otevírají další nepřečtenou zprávu, pokud je aktuální zpráva smazána nebo přesunuta do jiné složky. Z bezpečnostního hlediska je výhodnější, pokud uživatel může o otevření nové pošty rozhodnout sám.

    Nastavení pro MS Outlook: Nástroje > Možnosti > Předvolby > Možnosti e-mailu, zde nastavit „zpět do Doručené pošty“, viz. obrázek č. 3.3.
    Anglická verze Windows: Tools > Options > Preferences > E-mail options, After moving or deleting an open item > return to the Inbox.
15. Pro určité typy příloh elektronické pošty MS Outlook automaticky vytváří jejich náhled a zobrazuje jej uživateli. Vytvořením náhledu však může dojít ke spuštění nebezpečného kódu obsaženého v příloze. Proto může být výhodné automatický náhled zakázat.

    Nastavení MS Outlook: Zobrazit > Automatický náhled
    Anglická verze MS Outlook: View > Auto Preview

    Poznámka: Tato úprava může vést ke snížení komfortu při čtení pošty.
16. Ve výchozím nastavení systém Windows skrývá přípony některých typů souborů. Soubor obsahující virus s názvem ILOVEYOU.TXT.VBS je pak prezentován uživateli jako ILOVEYOU.TXT. Následující nastavení systému Windows umožní zobrazovat skutečná jména pro většinu typů souborů (některé přípony souborů budou i po této úpravě systémem záměrně skrývány, pro tyto typy souborů by byla nutná editace registrů).

    Nastavení Windows: Tento počítač > Nástroje > Možnosti složky > Zobrazit, Skrýt příponu souborů známých typů, viz.obrázek č. 3.4,
    Ve verzi Windows XP je menu Nástroje dostupné přes panel Průzkumníka (Windows Explorer).
    Anglická verze Windows: Folder > View > Hide file extensions for known file types

17. Viry a škodlivý kód se často šíří také prostřednictvím VBA maker v souborech kancelářského balíku MS Office. Microsoft vyvinul řešení, které zabrání spuštění těchto maker, pokud nepochází z důvěryhodného zdroje.

    Nastavení zabezpečení makra v MS Outlook na vysoké:
    Nástroje > Makro > Zabezpečení > Úroveň zabezpečení > Vysoké (viz. obrázek č. 3.5)
    Anglická verze MS Outlook: Tools > Macro > Security > Security Level > High

    V posledních verzích kancelářského balíku MS Office doplněných o dostupné aktualizace je nastavení zabezpečení na „vysoké“ výchozím. Toto nastavení umožňuje spouštět pouze makra, pocházející z důvěryhodných zdrojů.

    Poznámka: starší verze balíku MS Office (Ofice 97, 98) touto volbou nedisponují.
18. Celá řada virů a škodlivého kódu se šířila nikoliv v příloze, ale přímo v těle zpráv. Nastavení omezení spouštění škodlivého kódu v těle zpráv je definováno na úrovni MS Internet Explorer (MSIE), který definuje čtyři bezpečnostní zóny (viz. Nástroje > Možnosti > Zabezpečení v MSIE).

    Prvním krokem k zabezpečení je nastavení zóny v MS Outlook:
    Nástroje > Možnosti > Zabezpečení, zde nastavit Zóny zabezpečení na „Servery s omezeným přístupem“, viz. obrázek č. 3.6.
    Anglická verze MS Outlook:
    Tools > Options > Security, Restricted zones.

    Nastavení pro Outlook Express je podobné (Nástroje > Možnosti > Zabezpečení, viz. obrázek č. 3.7)

    Dalším krokem je pak nastavení vlastností této zóny v MS Internet Explorer:
    Nástroje > Možnosti > Zabezpečení, zde vybrat „Servery s omezeným přístupem“, Úroveň zabezpečení zóny by měla být nastavena na „Vysoká“. Nastavení „Vysoká“ je výchozí, lze jej tedy nastavit kliknutím na „Výchozí úroveň“ (viz. obrázek č. 3.8)

    Poznámka: Výše uvedené nastavení způsobí, že pošta s interaktivním obsahem (ActiveX, Java script apod.) nebude interpretována a nemusí se zobrazovat korektně. Většina elektronické pošty však interaktivní obsah neobsahuje.

2.4 Zásady fyzické bezpečnosti

19. Šifrování citlivých dat, uložených na přenosných počítačích. Doporučujeme:
    PGP Disk http://www.pgpi.org/products/pgpdisk
    CompuSec http://www.ce-infosys.com.sg/CeiNews_FreeCompuSec.asp
20. Přenosný počítač neponechávat bez dozoru v dopravních prostředcích, restauracích a dalších veřejných místech.
21. V případě ztráty mobilního zařízení zablokujte svoji SIM kartu na Infolince T-Mobile.

2.5 Opatření pro zabezpečení komunikace

Ačkoliv spojení prostřednictvím sítě GSM je šifrováno, spojení vytvořené do Internetu již není po opuštění sítě T-Mobile nijak chráněno.

Uživatelé připojující se do Internetu (např. na platební či bankovní portály) by měli použít šifrovaný přenos dat, kdykoliv je to ze strany internetového serveru možné (tj. použít protokol https namísto http).

Pokud uživatel používá GPRS pro přístup do vnitřní sítě své organizace, měl by použít šifrování na bázi VPN, případně použít produkt určený pro firemní zákazníky – Corporate APN.

V současnosti existuje několik možností, jak provést zabezpečení komunikace na bázi VPN, všechny jsou založeny na standardu zabezpečení IPSec. Klientský VPN software, který byl úspěšně otestován spolu s T-Mobile GPRS infrastrukturou zahrnuje:

- Cisco VPN klient,
- CheckPoint SecuRemote/SecureClient,
- L2TP klient ve WindowsXP.

Ve zbývající části jsou pro jednotlivé VPN klienty diskutovány požadavky na jejich nastavení.

2.5.1 Cisco VPN klient

Klient musí být nastaven tak, aby použil IPSec tunneling nad UDP protokolem. Nastavení této možnost v Cisco VPN klientovi je znázorněno na obr. č. 3.9. Žádné další speciální nastavení není zapotřebí. URL pro Cisco VPN klienta:
http://www.cisco.com/univercd/cc/td/doc/product/vpn/client/
V aktuální verzi VPN klienta je IPSec tunneling nastavením výchozím.
Pro funkčnost VPN spojení je zapotřebí, aby IPSec tunneling podporoval i VPN koncentrátor na druhé straně spojení.

2.5.2 CheckPoint Secure Client

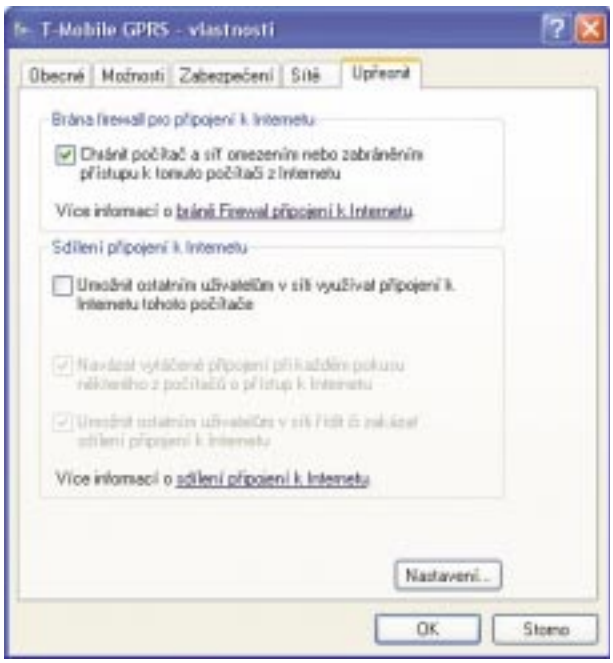
Klient musí být nastaven tak, aby zabaloval IPSec pakety do UDP, viz. obrázek č. 3.10. Poslední verze Secure Clienta tuto vlastnost implicitně testují a používají, pokud to umožňuje vzdálené zařízení. Odkazy:
http://ww.checkpoint.com/techsupport/downloads_sr.html

2.5.3 Microsoft L2TP/IPSec klient

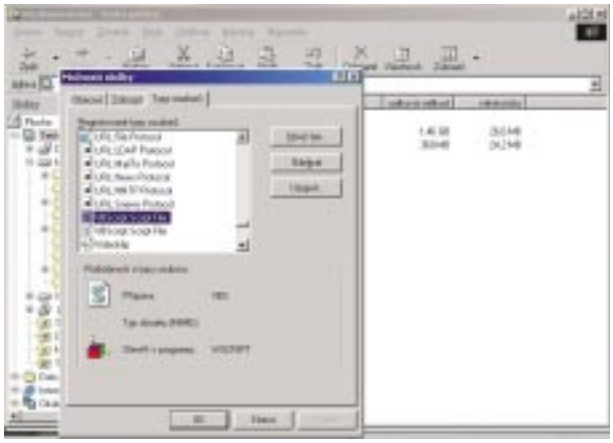
Od verze MS Windows 2000/XP, standardní instalace obsahuje VPN klienta, používající protokol L2TP/IPSec. Nastavení L2TP/IPSec pro Windows XP je zobrazeno na obr. č. 3.11.
Pro verzi Win98/NT/ME je k dispozici zdarma ke stažení speciální verze L2TP klienta, URL:
http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp
Oba klienti použijí UDP enkapsulaci pro IPSec automaticky, pokud to vzdálený server nabídne.

3. Obrázky

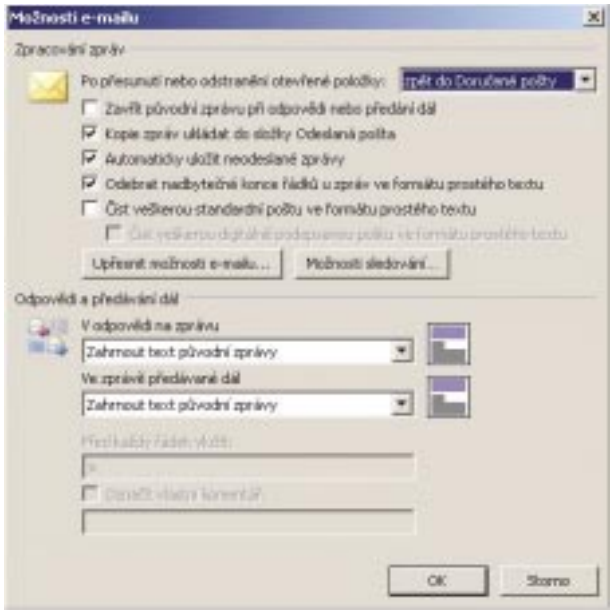
3.1 Nastavení ICF



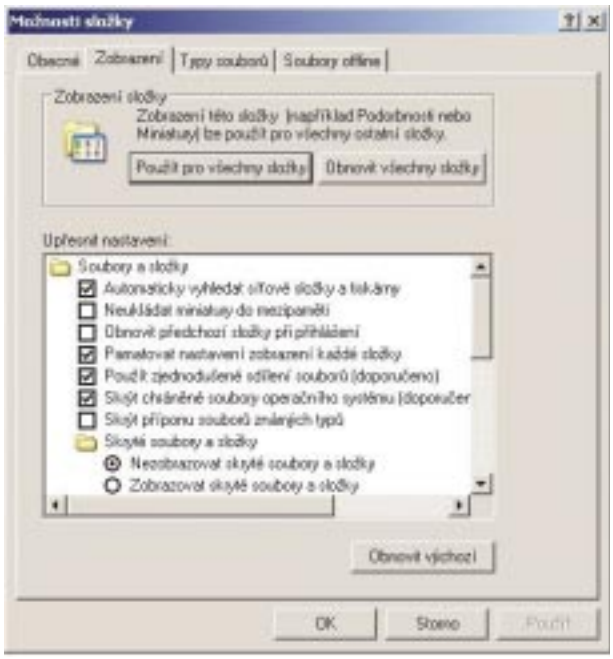
3.2 Zrušení asociace pro VBS a VBE skripty



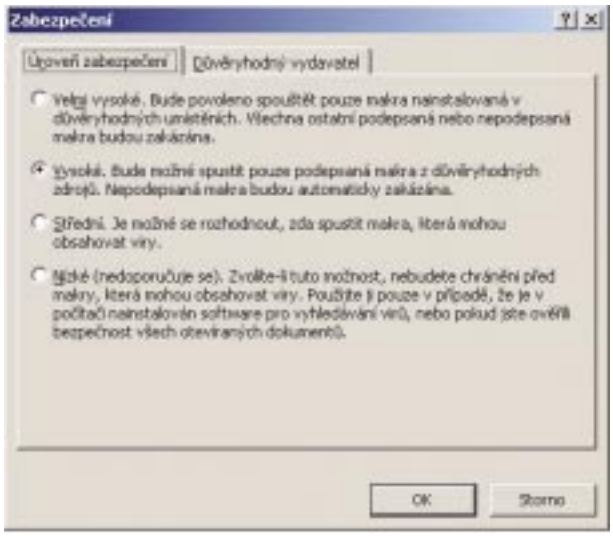
3.3 MS Outlook: Skok zpět do Inboxu



3.4 Skutečné názvy příloh

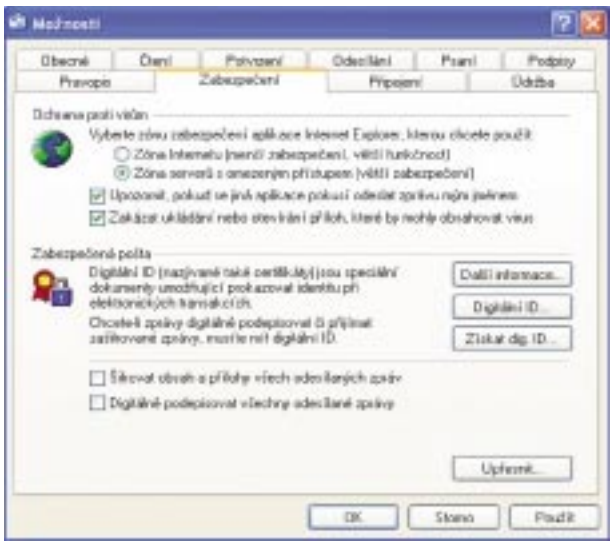


3.5 Zabezpečení maker

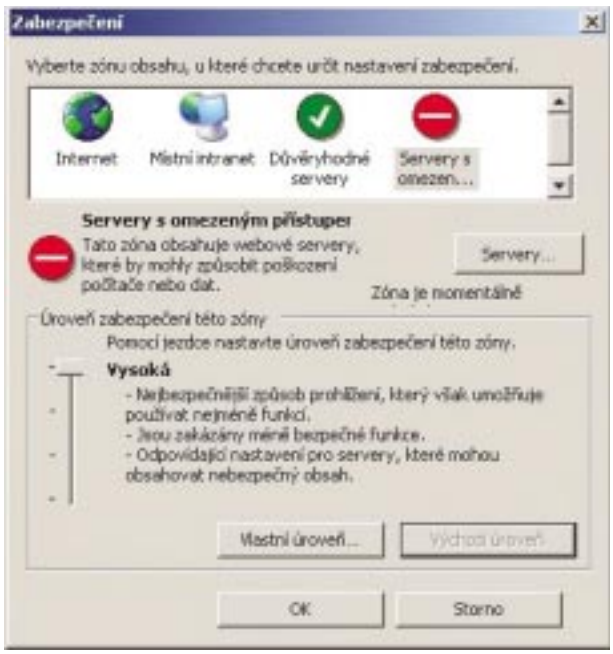


3.6 Nastavení zóny v MS Outlook

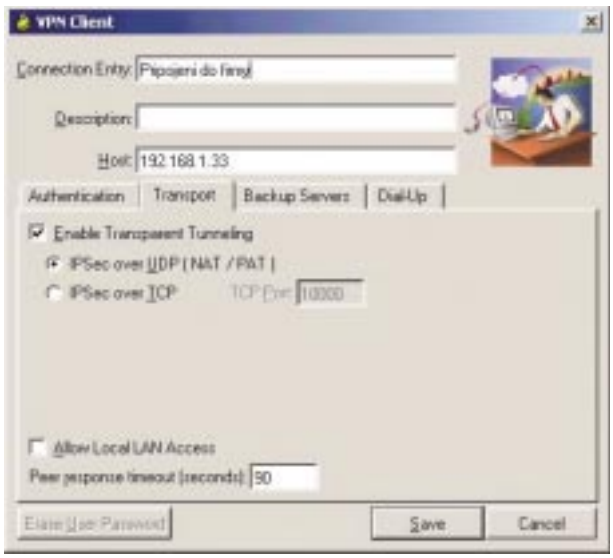
3.7 Nastavení zóny v Outlook Express



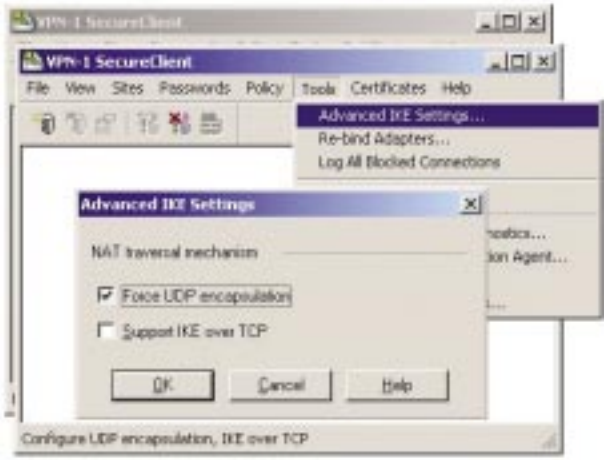
3.8 Nastavení zóny v MSIE



3.9 Nastavení Cisco VPN klienta



3.10 Nastavení CheckPoint SecureClient



3.11 Nastavení L2TP IPSec