Popis Služby Bezpečný internet

Tento Popis služby je platný pro **službu Bezpečný internet** objednané (pro Specifikace služby Bezpečný internet uzavřené) v období od **25. 2. 2015** do odvolání.

1 Obsah Služby

Služba Bezpečný Internet je komplexní doplňkovou službou k internetovým službám, převážně pro nižší segment (DSL, případně nižší rychlosti DIA). Jejím hlavním cílem je poskytnutí sdíleného centrálně spravovaného bezpečného připojení. Úkolem Služby je ochrana internetového připojení zákazníka.

1.1 Rizika Internetu

1.1.1 Malware

Existuje nepřeberné množství ohrožení na Internetu, namátkou malware (globální označení pro škodlivý software – MALicious softWARE). Zahrnuje viry, trojské koně, spyware, síťové červy (worms) atd. Jedná se o software, který přímo škodí (maže soubory, krade hesla …). Malware dnes se šíří převážně pomocí Internetu. Je tedy nutné kontrolovat přenášený obsah pomocí aktualizovaného antiviru.

1.1.2 Spam

Další hrozbou je spam alias nevyžádaná pošta. Ačkoli by se mohlo zdát, že spam přímo neškodí, není to úplně pravda. Jednak zahlcuje konektivitu nevyžádaným a tudíž zbytečným provozem, dále mnohdy obsahuje odkazy na webové stránky se škodlivým obsahem (malware). Nejlepší je zbavit se spamu už na vstupu do firmy a k tomu je potřeba kvalitní antispam.

1.1.3 Síťové útoky

Tato kategorie zahrnuje útoky na slabiny operačních systémů a aplikací. Ze zkušeností (a také z Murphyho zákonů :-) vyplývá, že žádný program není bohužel bez chyb. Síťové útoky tyto zranitelnosti využívají a mohou díky nim škodit (buď získají na systému administrátorská práva, případně zapříčiní nefunkčnost programu apod.). Tyto zranitelnosti pro aktuální verze programů odstraňuje zpravidla výrobce pomocí záplat/patchů (např. Microsoft pomocí Windows Update nebo Service Packů), nicméně nikoliv v čase objevení zranitelnosti (zero day zranitelnosti). Proto je nezbytné těmto útokům zamezit. Samotný firewall nestačí, je k tomu potřeba také IPS (Intrusion Prevention System).

1.1.4 Zahlcení šířky pásma

Je většinou důsledkem problémů z předchozích bodů. Viry či napadené systémy se snaží komunikovat s protějšky vně firmy a tím ubírají kapacitu internetové linky.

Kromě těchto příčin zahlcují konektivitu také prohlížení nežádoucích stránek zaměstnanci (různé sociální sítě, internetové hry, …). Zabránění prohlížení těchto stránek, nejen že zvyšuje produktivitu, ale také bezpečnost, jelikož mnoho nedovolených stránek obsahuje škodlivý obsah. Filtraci obsahu provádí webfiltering ve volitelných kategoriích, které jsou pravidelně aktualizovány.

Další příčiny zahlcování linky způsobují síťové aplikace. Jejich kontrola je velmi problematická, protože převážná většina z nich se „maskuje“ jako běžné prohlížení stránek. Mezi tyto aplikace řadíme různé instantní komunikátory (Skype, ICQ …) a také peer-to-peer aplikace pro sdílení/stahování obsahu (Bittorent, …). Jejich řízení či kontrolu provádí modul Application control.

1.1.5 Ostatní

Navíc je nutné zdůraznit, že seznam není zdaleka úplný a konečný (tj. existují další kategorie „škodlivin“ – např. zadní vrátka/backdoors, phishing, pharming …). Podobně jako ve vojenství – kdy na každou zbraň se záhy najde protizbraň, platí i v internetovém světě, že se útoky stávají sofistikovanější. Je nutné tuto oblast neustále sledovat a pružně reagovat na aktuální hrozby. To s sebou nese náklady nejen na technologie, ale také na lidské zdroje, protože sebelepší technologie, která není odborně spravována a aktualizována, nám problémy dlouhodobě nevyřeší. Navíc, jak je z výčtu zranitelností vidět, jedna technologie nestačí, je nutné nasadit komplexní řešení (UTM – Unified Threat Management).

2 Charakteristika Služby

Efektivní ochrana internetového připojení musí síť chránit před veškerými vyjmenovanými zranitelnostmi. T-Mobile Czech Republic toto zabezpečuje pomocí komplexní platformy postavené nad produkty přední bezpečnostní firmy Fortinet. Jedná se o vysoce dostupný cluster UTM zařízení v datovém centru dle Tier III. UTM je zkratkou pro Unified Threat Management a obsahuje následující ochrany:

- Ochranu před síťovými útoky (firewall + IPS)
- Ochranu před nevyžádanými maily (antispam)
- Ochranu viry (antivir)
- Obsahovou filtraci webu (webfiltering/content filtering)
- Řízení aplikací (application control)

Všechny tyto ochrany jsou pravidelně aktualizovány pomocí celosvětové sítě firmy Fortinet – **FortiGuard** (www.fortiguard.com), tak aby služba byla schopna čelit nejnovějším hrozbám.

Služba přináší tyto výhody pro zákazníka:

- Bezpečný přístup k internetu
- Efektivní využití přístupové linky
- Komplexní spravované řešení certifikovanými odborníky
- Nulové investice na pořízení

Popis Služby Bezpečný internet

Tento Popis služby je platný pro **službu Bezpečný internet** objednané (pro Specifikace služby Bezpečný internet uzavřené) v období od **25. 2. 2015** do odvolání.

- Kompletní outsourcing bezpečnosti umožňuje IT týmu uživatele věnovat se plně problematice vlastní práce, nikoliv se zatěžovat problematikou hrozeb Internetu
- Nízká cena
- Standardizovaný produkt (rychlé a jednoduché nasazení)
- Řešení s vysokou dostupností umístěné v datacentru pod nepřetržitým dohledem

3 Varianty Služby

Služba Bezpečný Internet nabízí předpřipravené balíčky, které kombinují jednotlivé ochrany do bezpečnostních profilů. Můžete si zvolit Vám vyhovující kombinaci ze třech hlavních profilů plus nabízíme dále dva doplňkové, které jsou určeny ke snadnému nastavení.

Tři hlavní profily jsou:

- **Bronze**
- **Silver**
- **Gold**

A dva doplňkové profily:

- Off
- Lite

Nastavení ochran v jednotlivých profilech shrnuje přehledně následující tabulka

Profil		Firewall + IPS	Antispam	Antivir	Webfilter				Application Control			
					Adult Mature Content	Security Risk	Potentially Liable	Bandwidth Consuming	P2P	Game	Malware	Proxy
Doplňkové	Off											
	Lite	•										
Hlavní	Bronze	•		•								
	Silver	•		•		•	•		•		•	
	Gold	•	•	•	•	•	•	•	•	•	•	•

3.1 Bronze

Profil Bronze kombinuje následující ochrany:

- Firewall + IPS
- Antivir

Jednotlivé bezpečnostní ochrany jsou popsány v samostatné sekci Ochrany.

Tento Profil je základní variantou, která nabízí ochranu před nejčastějšími hrozbami (převážně viry, trojské koně, apod. – obecně malware a dále před síťovými útoky – firewall, IPS).

3.2 Silver

Profil Silver kombinuje následující ochrany:

- Firewall + IPS
- Antivir
- *Webfilter*
  - *kategorie Security Risk*
  - *kategorie Potentially Liable*
- *Application Control*
  - *kategorie Malware*
  - *kategorie P2P (Peer-to-Peer)*

Kurzívou jsou odlišeny ochrany, které nejsou obsaženy v profilu Bronze. Jednotlivé bezpečnostní ochrany jsou popsány v samostatné sekci Ochrany.

Tento Profil rozšiřuje základní Profil Bronze o další ochrany Webfilter a řízení aplikací (Application control). Přináší tedy vyšší úroveň zabezpečení oproti základní variantě (Bronze) hlavně z hlediska zabezpečení vyšší produktivity práce na internetu (zamezuje navštěvování vybraných neproduktivních stránek) a z hlediska lepšího využití propustnosti linky (zamezuje používání aplikací pro sdílení „peer-to-peer“, které kromě toho, že zahlcují konektivitu, jsou také často zdrojem zranitelností).

3.3 Gold

Profil Gold kombinuje následující ochrany:

Popis Služby Bezpečný internet

Tento Popis služby je platný pro **službu Bezpečný internet** objednané (pro Specifikace služby Bezpečný internet uzavřené) v období od **25. 2. 2015** do odvolání.

- Firewall + IPS
- Antispam
- Antivir
- Webfilter
    - kategorie Security Risk
    - kategorie Potentially Liable
    - *kategorie Adult/Mature Content*
    - *kategorie Bandwidth Consuming*
- Application Control
    - kategorie Malware
    - kategorie P2P (Peer-to-Peer)
    - *kategorie Game*
    - *kategorie Proxy*

Kurzívou jsou odlišeny ochrany, které se nenachází v Profilu Silver. Jednotlivé bezpečnostní ochrany jsou popsány v samostatné sekci Ochrany.

Tento Profil je nejvyšší variantou Služby. Dále rozšiřuje Profil Silver o další kategorie webfilteringu (Webfilter) a řízení aplikací (Application control). Přináší tedy nejvyšší úroveň zabezpečení oproti ostatním variantám (Bronze, Silver) hlavně z hlediska zabezpečení vyšší produktivity práce na internetu (rozšiřuje okruh blokovaných neproduktivních stránek) a z hlediska lepšího využití propustnosti linky (zamezuje používání aplikací pro sdílení „peer-to-peer“, nedovoluje obcházení nastavených pravidel pomocí proxy služeb a také zakazuje používání síťových her). Jako jediný Profil obsahuje také ochranu před nevyžádanými zprávami (antispam).

3.4 Lite

Doplňkový profil, který vypíná ochrany antivir, Webfilter a Application control. Ostatní (firewall + IPS) zůstávají aktivní a filtrují provoz. Účelem tohoto Profilu je ponechat základní ochranu sítě a dovolit používání i neproduktivních stránek a aplikací včetně potenciálně nebezpečných kategorií (malware, security risk). Při volbě tohoto Profilu je možné snadno poznat, zda Vaše aplikace či stránka v některém z hlavních profilů (Bronze, Silver, Gold) nefunguje díky zařazení do některé z blokovaných kategorií.

3.5 Off

Doplňkový profil sloužící k vypnutí veškerých ochran. Při volbě tohoto Profilu je služba Bezpečný internet stále aktivní, veškerý provoz prochází přes bezpečnostní platformu T-Mobile (UTM), ale neuplatňují se na něj **žádné restrikce**. Pokud je tento Profil aktivní déle než 72h, dojde k automatickému odstranění záznamů o konfiguraci Služby (pro automaticky zřizované služby DSL) a aktivace jiného profilu tedy probíhá v souladu s článkem 5.2

4 Ochrany

Seznamte se s principy fungování Bezpečného internetu. Nemusíte být specialisty na bezpečnost, abyste pochopili jednoduchost a efektivnost nabízeného řešení.

Bezpečný internet kombinuje rozličné ochrany v jedné službě. Cílem je nabídnout zákazníkům komplexní zabezpečení sítě před zranitelnostmi na Internetu a také lépe řídit využití internetové linky (blokování neproduktivního provozu).

Všechny ochrany jsou udržovány v aktuálním stavu pomocí pravidelných update (několikrát denně) skrz celosvětovou síť FortiGuard, tak aby mohli čelit i nejnovějším zranitelnostem.

4.1 Antivir

Antivirová ochrana ve zkratce chrání před viry :-) Neustále aktualizovaný antivir je nedílnou součástí UTM zařízení a v reálném čase kontroluje internetový provoz na přítomnost virů a ostatních forem malware (trojské koně, spyware apod.). Prověřuje veškeré formy komunikace, přes které škodlivý kód může do vaší sítě přijít.

Konkrétně se jedná o:

- Elektronická pošta (e-mail) a její přílohy (protokoly POP3, IMAP, SMTP)
- Běžné surfování a stahování souborů (protokol HTTP)
- Stahování souborů specializovaným protokolem (protokol FTP)
- Sdílení souborů přes instant messaging (ICQ apod.)

Antivirová kontrola je prováděna na základě obsahu souboru nikoliv na základě jeho přípony a inspekce probíhá také v komprimovaných souborech (ZIP, ARJ, RAR atd.) včetně několikanásobně vnořených archivů (ZIP v ZIPu v ZIPu atd.)

Popis Služby Bezpečný internet

Tento Popis služby je platný pro **službu Bezpečný internet** objednané (pro Specifikace služby Bezpečný internet uzavřené) v období od **25. 2. 2015** do odvolání.

V současné době drtivá většina malware pochází z Internetu. Je tedy velmi výhodné odfiltrovat tyto škodliviny už v centrálním bodě u Poskytovatele (T-Mobile Czech Republic) a svoji linku používat už na čistý provoz.

4.2 Antispam

Ochrana Antispam má za cíl odstranit z poštovní komunikace (protokoly POP3, IMAP, SMTP) nevyžádané zprávy. Kvůli zamezení ztráty e-mailu, který není spam, nejsou zprávy mazány, ale zařízení přidává před začátek předmětu zprávy slovo „SPAM“ pro snadné zařazení do složky Nevyžádaná pošta pomocí automatických pravidel (buď na poštovním serveru, nebo na poštovním klientu). Detekce nevyžádané pošty probíhá na několika úrovních:

- Dle zdrojové IP adresy (seznam spam serverů)
- Dle přítomnosti phishingové URL ve zprávě
- Dle kontrolního součtu (slouží k detekci obrázkových a PDF spamů)

4.3 Firewall + IPS

Jedná se o základní síťovou ochranu. Slovo firewall v češtině znamená protipožární zeď a její funkce je přesně taková, zabránit průniku požáru z jedné strany na druhou. A to je také hlavním principem i v internetovém světě. Bránit průniku z Internetu do vnitřní sítě zákazníka.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System) je systém na detekci (Detection) a zabránění/prevenci (Prevention) narušení.

Na základě předdefinovaných signatur, které jsou nepřetržitě doručovány do zařízení (skrz FortiGuard), je příchozí provoz kontrolován na přítomnost těchto signatur a je-li nalezena shoda, je tento provoz zablokován. Seznam posledních rizik je dostupný na stránkách http://www.fortiguard.com/library.html včetně podrobného popisu těchto rizik. Rizika jsou dělena do několika kategorií podle závažnosti a nastavení IPS u Služby Bezpečný internet blokuje všechny zranitelnosti v následujících úrovních:

- medium
- high
- critical

Je-li nějaká komunikace zablokována díky IPS, zdroj této komunikace je preventivně zařazen do karantény na 30 minut. Zdrojem je myšlena IP adresa útočníka.

4.4 Webfiltering

Ochrana Webfiltering slouží k filtraci webových stránek na základě jejich obsahu. V rámci jednotlivých profilů jsou přednastaveny kategorie, které zabraňují navštěvování webových stránek v daných kategoriích.

Popis Služby Bezpečný internet

Tento Popis služby je platný pro **službu Bezpečný internet** objednané (pro Specifikace služby Bezpečný internet uzavřené) v období od **25. 2. 2015** do odvolání.

Hlavní kategorie	Podkategorie	Popis
Adult Mature Content	Alternative Beliefs	Websites that provide information about or promote religions not specified in Traditional Religions or other unconventional, cultic, or folkloric beliefs and practices. Sites that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers, satanic or supernatural beings.
	Abortion	Websites pertaining to abortion data, information, legal issues, and organizations.
	Other Adult Materials	Mature content websites (18+ years and over) that feature or promote sexuality, strip clubs, sex shops, etc. excluding sex education, without the intent to sexually arouse.
	Advocacy Organizations	This category caters to organizations that campaign or lobby for a cause by building public awareness, raising support, influencing public policy, etc.
	Gambling	Sites that cater to gambling activities such as betting, lotteries, casinos, including gaming information, instruction, and statistics.
	Nudity and Risque	Mature content websites (18+ years and over) that depict the human body in full or partial nudity without the intent to sexually arouse.
	Pornography	Mature content websites (18+ years and over) which present or display sexual acts with the intent to sexually arouse and excite.
	Dating	Websites that host or promote dating, interpersonal relationship related material.
	Weapons (sales)	Websites that feature the legal promotion or sale of weapons such as hand guns, knives, rifles, explosives, etc.
	Marijuana	Sites that provide information about or promote the cultivation, preparation, or use of marijuana.
	Sex Education	Educational websites that provide information or discuss sex and sexuality, without utilizing pornographic materials.
	Alcohol	Websites which legally promote or sell alcohol products and accessories.
	Tobacco	Websites which legally promote or sell tobacco products and accessories.
	Lingerie and Swimsuit	Websites that utilizes images of semi-nude models in lingerie, undergarments and swimwear for the purpose of selling or promoting such items.
	Sport Hunting and War Games	Web pages that feature sport hunting, war games, paintball facilities, etc. Includes all related clubs, organizations and groups.
Security Risk	Malicious Websites	infected with destructive or malicious software, specifically designed to damage, disrupt, attack or manipulate computer systems without the user's consent, such as virus or trojan horse.
	Phishing	Counterfeit web pages that duplicate legitimate business web pages for the purpose of eliciting financial, personal or other private information from the users.
	Spam URLs	Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.
Potentially Liable	Drug Abuse	Websites that feature information on illegal drug activities including: drug promotion, preparation, cultivation, trafficking, distribution, solicitation, etc.
	Hacking	Websites that depict illicit activities surrounding the unauthorized modification or access to programs, computers, equipment and websites.
	Illegal or Unethical	Websites that feature information, methods, or instructions on fraudulent actions or unlawful conduct (non-violent) such as scams, counterfeiting, tax evasion, petty theft, blackmail, etc.
	Discrimination	Sites that promote the identification of racial groups, the denigration or subjection of groups, or the superiority of any group.
	Explicit Violence	This category includes sites that depict offensive material on brutality, death, cruelty, acts of abuse, mutilation, etc.
	Extremist Groups	Sites that feature radical militia groups or movements with aggressive anti-government convictions or beliefs.
	Proxy Avoidance	Websites that provide information or tools on how to bypass Internet access controls and browse the Web anonymously, includes anonymous proxy servers.
	Plagiarism	Websites that provide, distribute or sell school essays, projects, or diplomas.
	Child Abuse	Websites that have been verified by the Internet Watch Foundation to contain or distribute images of non-adult children that are depicted in a state of abuse. Information on the Internet Watch Foundation is available at http://www.iwf.org.uk/.
Bandwidth Consuming	Freeware and Software Downloads	Sites whose primary function is to provide freeware and software downloads. Cell phone ringtones/images/games, computer software updates for free downloads are all included in this category.
	File Sharing and Storage	Websites that permit users to utilize Internet servers to store personal files or for sharing, such as with photos.
	Streaming Media	Websites that allow the downloading of MP3 or other multimedia files.
	Peer-to-peer File Sharing	Websites that allow users to share files and data storage between each other.
	Internet Radio and TV	Websites that broadcast radio or TV communications over the Internet.
	Internet Telephony	Websites that enable telephone communications over the Internet.

Aktuální seznam konkrétních oblastí s popisem co je jejich obsahem naleznete opět na stránkách FortiGuard –

http://www.fortiguard.com/webfiltering/webfiltering.html

V případě, že si nejste jisti, zda daná stránka není filtrována na základě nastavení, je možné si její zařazení do konkrétní kategorie na výše uvedené stránce ověřit také (http://www.fortiguard.com/ip_rep.php).

Pokud je stránka blokována Službou Bezpečný internet, zobrazí se v internetovém prohlížeči srozumitelná stránka s informací, že požadovaná stránka je blokována nastavením Služby Bezpečný internet.

4.5 Application Control

Řízení aplikací (Application Control) chrání počítače za pomoci zakazování definovaných síťových aplikací. Aplikace jsou řazeny do kategorií a na základě této kategorizace je možné konkrétní kategorii zakázat. Všechny aplikace z této kategorie jsou potom blokovány.

Kategorie	Popis	Typické aplikace
P2P	The p2p category consists of P2P (Peer to Peer) applications and associated P2P protocols, which can establish a P2P network to provide fast data sharing	BitTorrent, Direct.Connect, Edonkey.Handshake, FlashGet, Gnutella, KaZaa, Skype, Donkey, iTunes.File.Sharing, ...
Proxy	The proxy category consists of proxy software and websites, which can make indirect network connections to other networks and bypass the firewall policy.	Adobe.Flash.Proxy.Auto.Discovery, GNU.HTTPTunnel, GTunnel, HTTP.Tunnel, Hamachi, Kproxy, Proxy.HTTP, SOCKS4, SOCKS5, Socks2HTTP, TCP.Over.DNS, TinyProxy, Tor, ...
Game	The game category consists of network games including internet games.	AIM.Game, All.Slots.Casino, Battle.Net, CounterStrike, Dark.Age.Of.Camelot, FarmVille, Games.For.Windows.Live, Guildwars, Minecraft, Playstation.Network, Quake, Ragnarok.Online, Second.Life, Valve.Games, Warcraft, Wolfenstein, WorldofWarcraft, Yahoo.Games, Zynga.Games, ...
Malware	The malware category consists of botnet detection in the network.	Bredolab, Gbot.Botnet, Gootkit.Bot, Gumblar, Hiloti.Botnet, Imrabot, Katusha, Koobface, Koobface.Botnet, LOIC.Botnet, Yahoo.Messenger.Worm.IRC, Zeus, ...

Aktuální popis kategorií je možné vidět zde: http://www.fortiguard.com/applicationcontrol/appcontrol.html

Vyhledání konkrétní aplikace a její zařazení je možné zde: http://www.fortiguard.com/applicationcontrol/app_pop_risk.html

Popis Služby Bezpečný internet

Tento Popis služby je platný pro **službu Bezpečný internet** objednané (pro Specifikace služby Bezpečný internet uzavřené) v období od **25. 2. 2015** do odvolání.

5 Pro které služby

Služba je dostupná pro tyto hlavní služby poskytující internetové připojení:

5.1 IP Kompet premium

Jedná se o projektově zřizovanou Službu standardním procesem T-Mobile Czech Republic.

V rámci zřízení Služby je možné si vybrat IP adresy/rozsahy na které bude následně uplatněna Služba Bezpečný internet. Těchto rozsahů může být v rámci Služby maximálně 8.

Tato varianta je shora omezena na služby do 30Mbps. Pro vyšší rychlosti doporučujeme individuální řešení bezpečnosti pomocí standardní služby **Managed Firewall**.

5.2 DSL (Digital Subscriber Line)

- IP komplet DSL

K výše vyjmenovaným službám se Služba zřizuje automatickým zřizovacím procesem (automatický provisioning) pomocí samoobslužného portálu WebCare. Zřízení Služby proběhne následující pracovní den po zadání požadavku ve WebCare.

6 Samoobslužný portál

6.1 WebCare

Na tomto portále (http://webcare.gts.cz) je možné Službu objednat (pro IP komlet DSL služby) a také je možné provádět základní nastavení (pro obě varianty DIA i DSL u aktivních služeb). V rámci nastavení je možné měnit profil zabezpečení (odezva na změnu je v reálném čase).

6.2 Produktový web

www.gtsbezpecnyinternet.cz

Tento web populární formou popisuje detaily nejen o Službě, ale také o jednotlivých hrozbách, které se na Internetu vyskytují. Dále je zde sekce vysvětlivek, kde formou slovníku vysvětlujeme jednotlivé pojmy z bezpečnostní oblasti, stejně tak sekce často kladených dotazů, kde odpovídáme na opakované dotazy.