Metody zabezpečení webového provozu

Jakub Truschka
Konference Security
Praha, 17.2.2010

Obsah přednášky

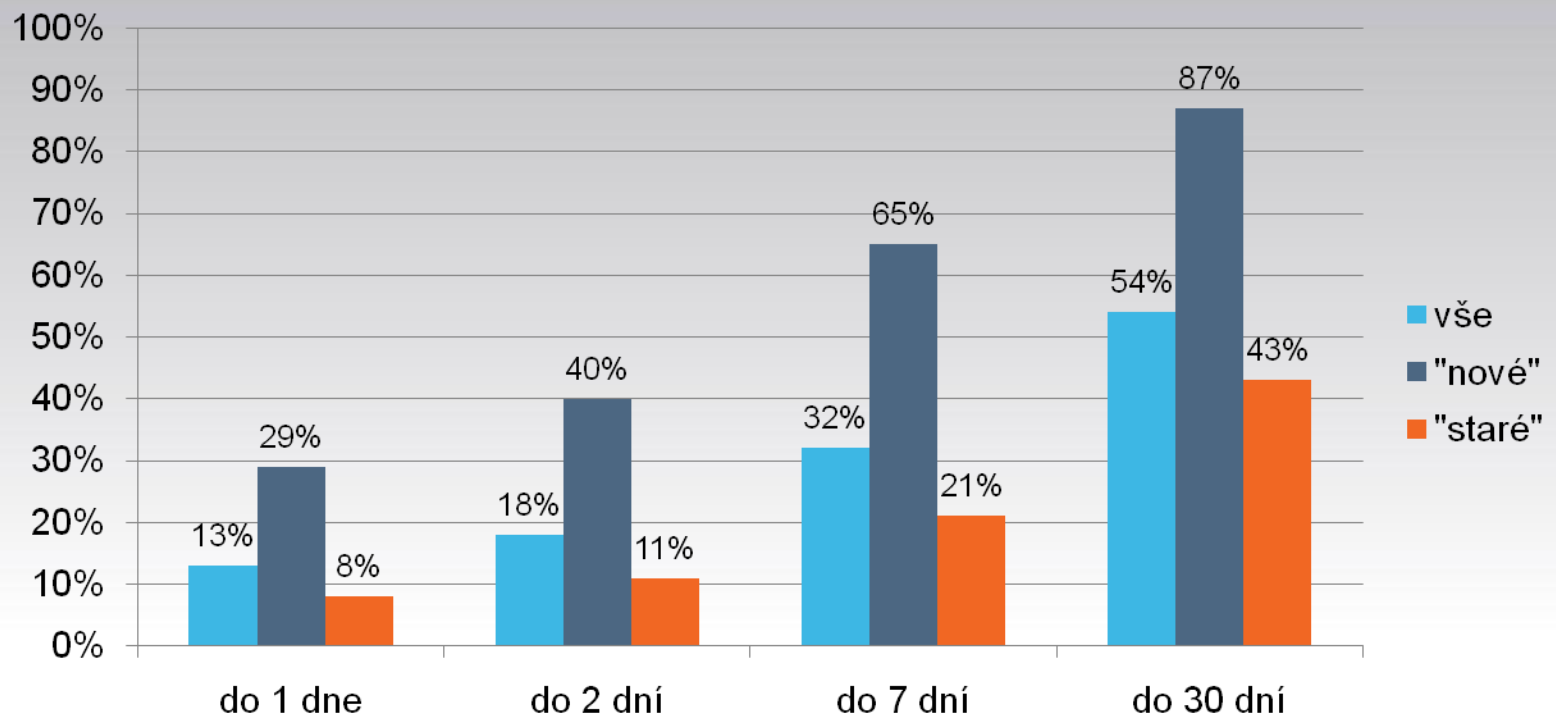
- Aktuální bezpečnostní hrozby
  v oblasti spamu a malwaru
- Výhody obrany na vstupním bodu sítě
  z hlediska bezpečnosti a efektivity
- Fungování webové bezpečnostní brány
  na příkladu řešení TrustPort Net Gateway

Stav současných bezpečnostních hrozeb

- Spam
  - Podíl spamu meziročně vzrostl na 87,7 % z 81,2 %
  - Podíl botnetů na spamu klesl na 83,4 % z 90 %
  - Spící botnety jako záloha aktivních botnetů
  - Spam obsahující maskované odkazy
  - Neanglický spam vzrostl na 5 % veškerého spamu
- Malware
  - Podíl pošty s malwarem v příloze klesl na 0,35 % z 0,70 %
  - Nárůst cílených útoků na vládní, bankovní, mediální organizace
  - Zneužívání zranitelností sociálních sítí
  - Nárůst falešného bezpečnostního softwaru
  - Posun od manuální k automatické instalaci webového malwaru
  - Používání stále se měnící posloupnosti přesměrování

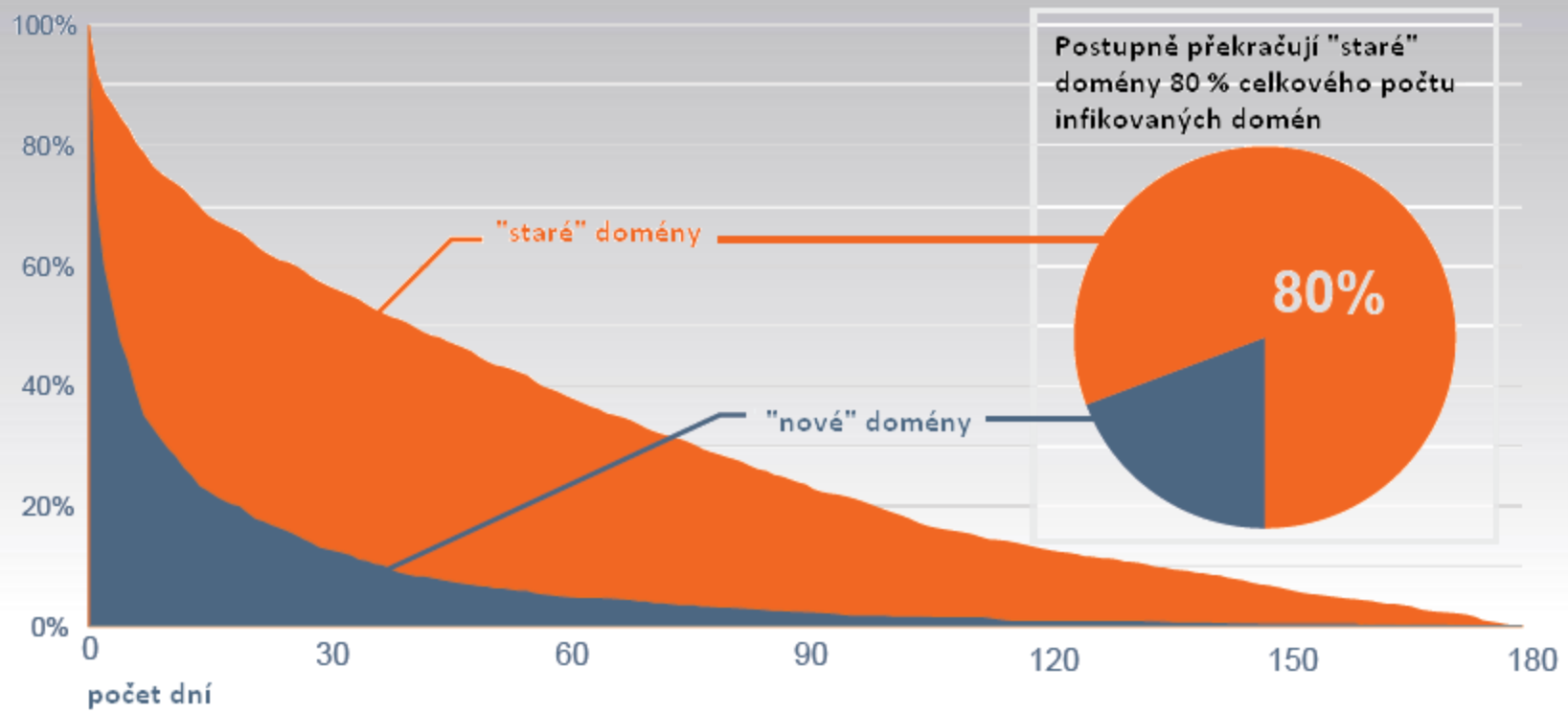
Statistické údaje: MessageLabs Intelligence, prosinec 2009

Zneškodnění nebo vyčištění infikovaných webových domén



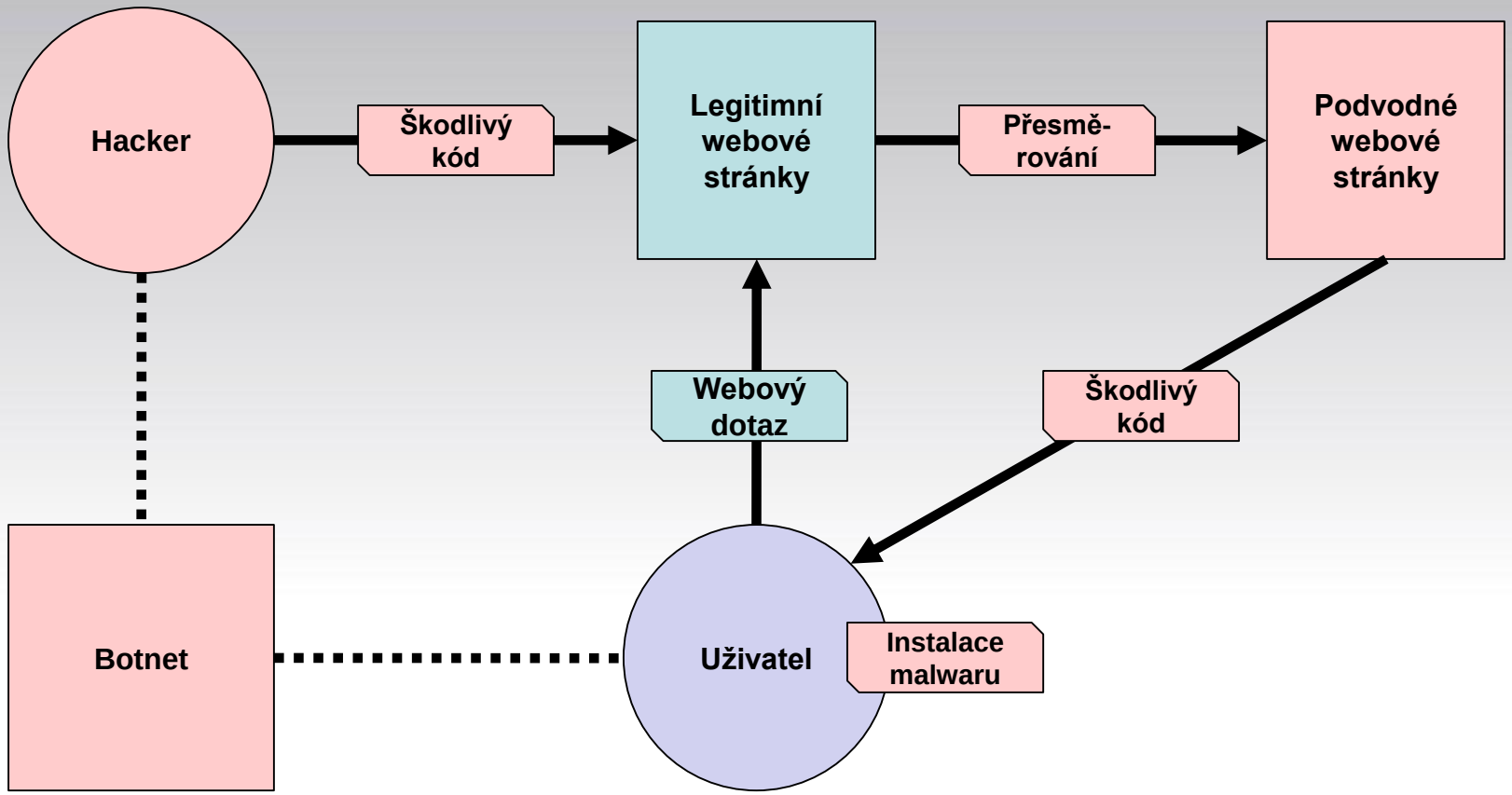
Zdroj: MessageLabs Intelligence, prosinec 2009

Struktura webových domén šířících malware

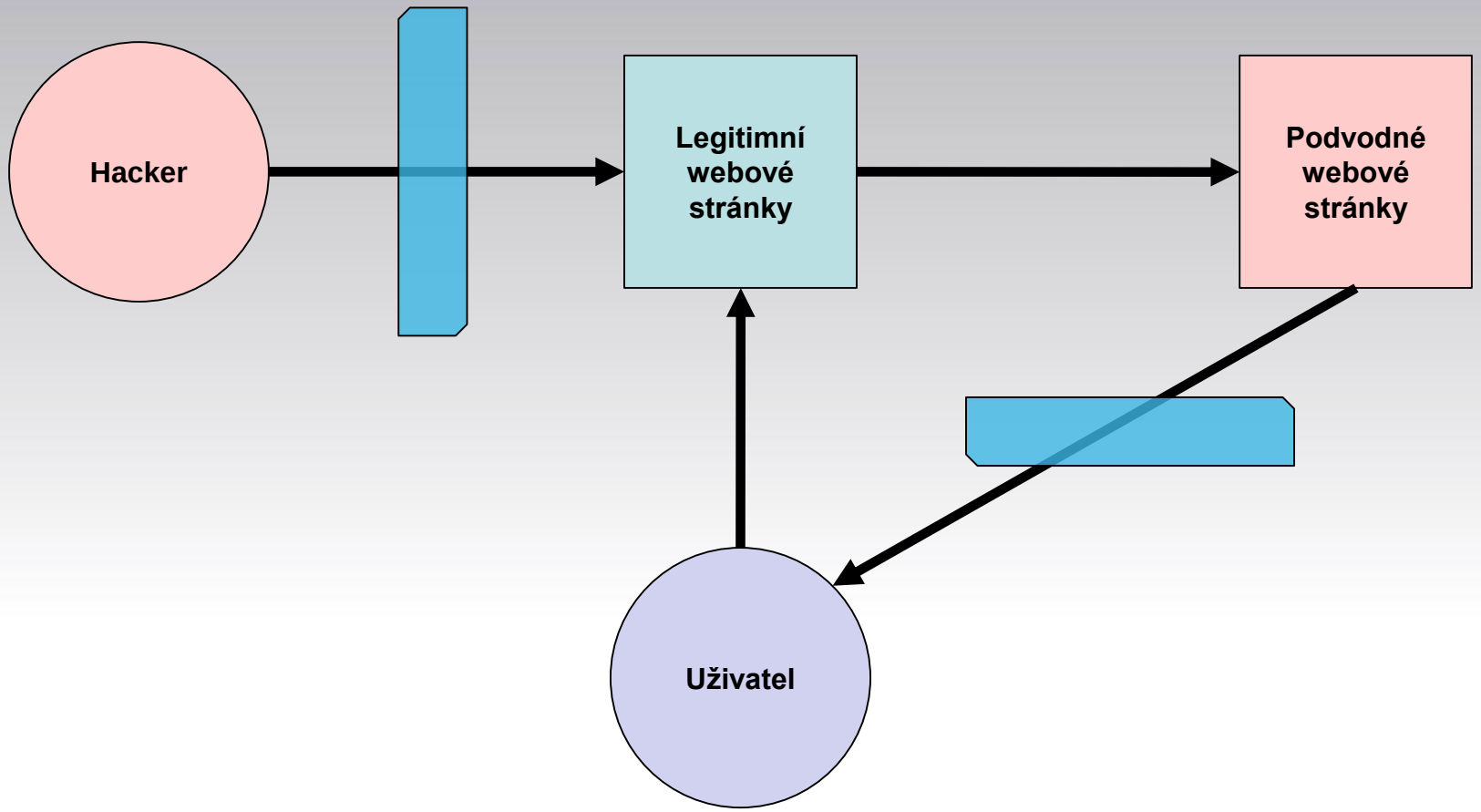


Zdroj: MessageLabs Intelligence, prosinec 2009

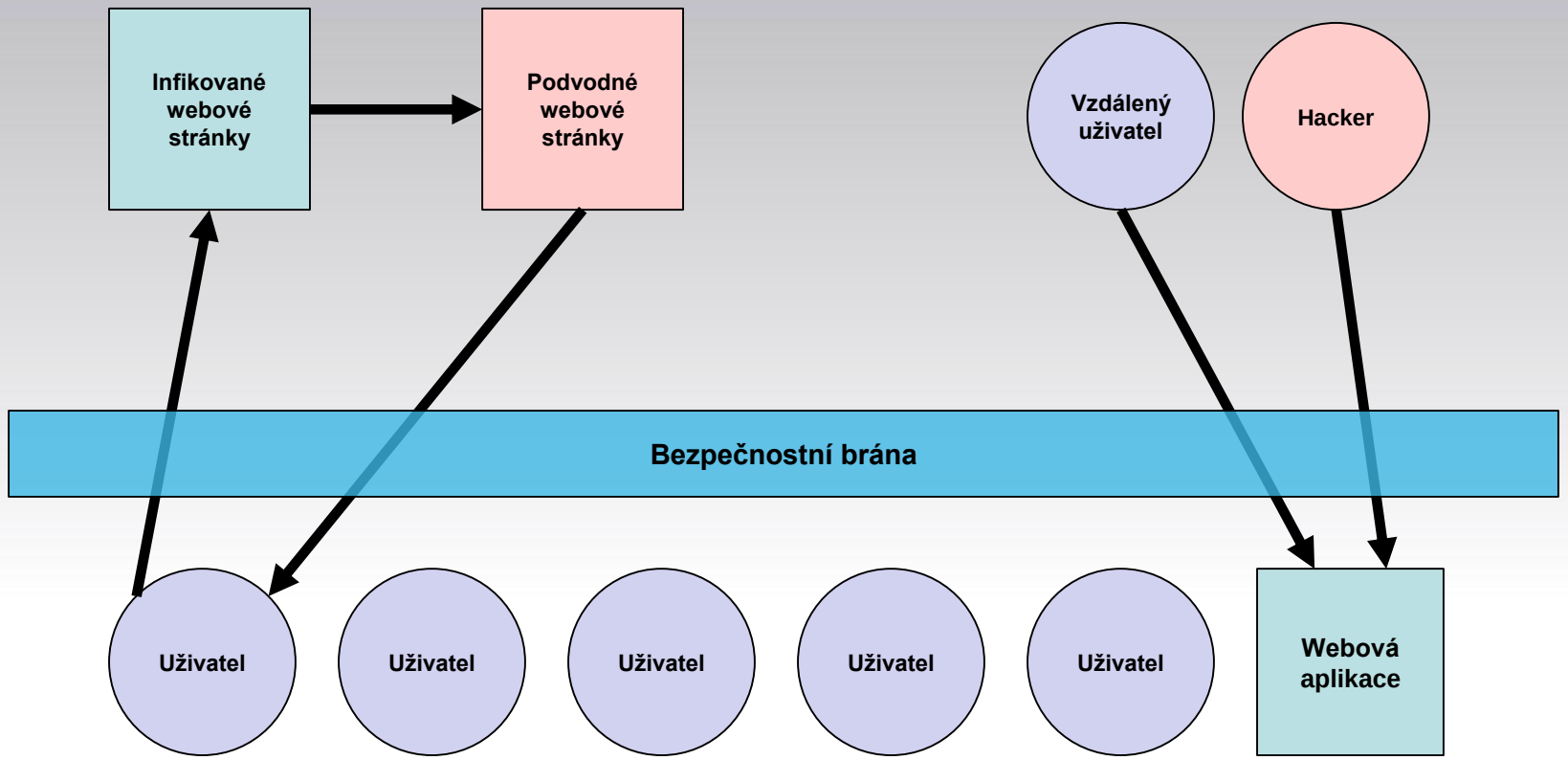
Typický současný webový útok



Možnosti obrany proti webovým útokům



Obrana webového provozu na vstupním bodu sítě

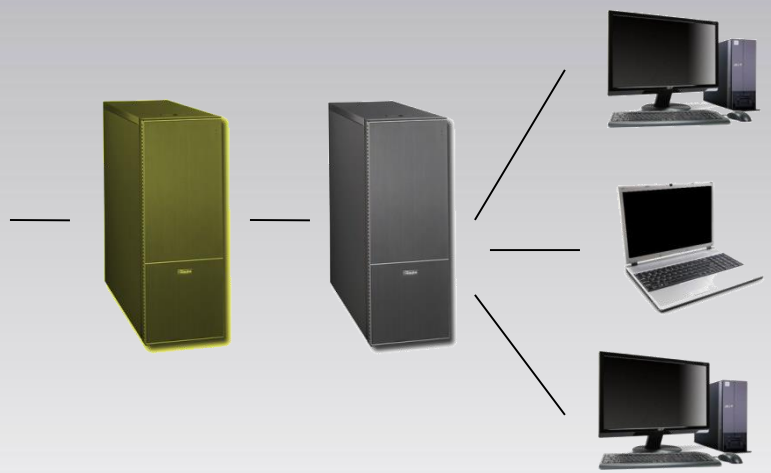


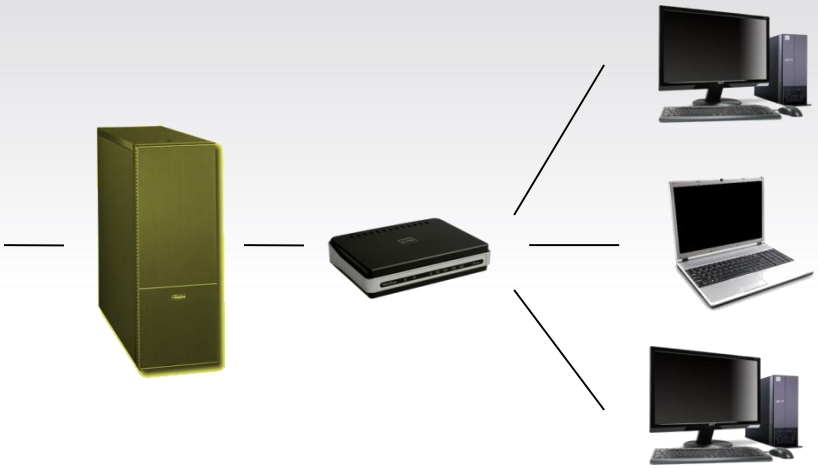
Výhody bezpečnostní brány na vstupním bodu sítě

- Jednoznačně oddělí internet a vnitřní síť
- Kontroluje veškerá data pouze jednou
- Nepustí malware a spam ke koncovým uživatelům

- Umožňuje jednotnou správu bezpečnosti
- Poskytuje data pro analýzu provozu
- Umožňuje vzdálenou správu řešení

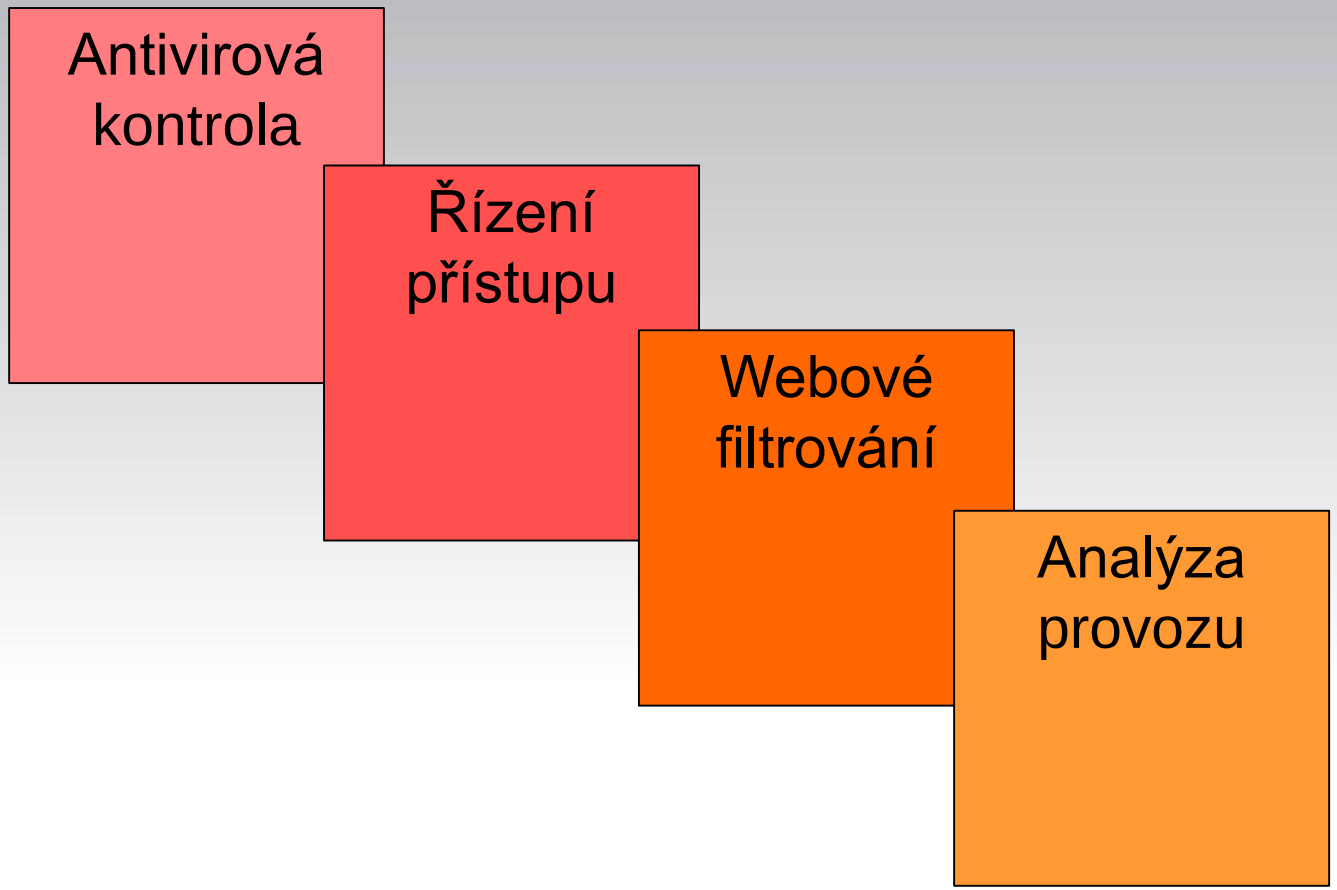
Začlenění webové bezpečnostní brány do sítě





TrustPort Net Gateway

Základní funkce webové bezpečnostní brány



Postup zpracování webového dotazu

- Ověření práv uživatele
  - Porovnání s lokálním seznamem oprávněných uživatelů
  - Autentizace prostřednictvím AD, LDAP
- Ověření serveru a domény
  - Důvěryhodné servery – obsah se stahuje bez kontroly
  - Povolené servery – pouze k těmto serverům se lze připojit
  - Důvěryhodná místa – domény se nekontrolují ani neblokují
  - Zakázaná místa - k doménám se nelze připojit
- Antiphishing – porovnání s databází phishingových serverů
- Webové filtrování – porovnání s databází kategorizovaných serverů

Postup kontroly stahovaného obsahu

- Určení formátu stahovaného souboru – tři režimy
  - Podle přípony stahovaného souboru
  - Podle deklarovaného typu obsahu
  - Analýzou vzorku stahovaných dat
- Seznam zakázaných formátů – soubor nebude povoleno stáhnout
- Seznam důvěryhodných formátů - soubor nebude skenován
- Webové filtrování
  - Heuristická analýza stahované stránky
  - Zařazení stránky do příslušných kategorií
- Antivirové skenování - více skenovacích motorů

Antivirová kontrola

Nastavení skenovacích motorů

- Které motory používat – zvážit poměr zátěže serveru a zabezpečení sítě
- Kolik vláken používat – podle výpočetní kapacity serveru
- Možnost aktivace heuristiky
- Možnost skenování archivů

Antivirová kontrola

Způsob stahování dat

Podmínkou úspěšného skenování je stažení celého souboru. Brána stáhne soubor, oskenuje ho a pošle ho na koncovou stanici. Brána používá dvě metody udržení otevřeného spojení se stanicí:

- Data trickling
  - Brána posílá na stanici periodicky kousky stahovaného a skenovaného souboru
  - Nevýhodou nevědomost uživatele o průběhu
- Indication page
  - Brána zobrazí periodicky aktualizovanou stavovou stránku
  - Stránka nabídne uložení nebo oznámí infekci
  - Nevýhodou omezení metody na prohlížeče

Webové filtrování

Kategorizace webových stránek

Základem webového filtrování je pravidelně aktualizovaná databáze webových adres, roztříděných do definovaných kategorií. Neznámé webové stránky dokáže analyzovat a kategorizovat během stahování.

Příklady kategorií

- Chatování
- Seznamky
- Pornografie
- Hazardní hry
- Obsah násilí
- Nelegální software

Webové filtrování

Smysl webového filtrování

Zájmy podniku jakožto zaměstnavatele:

- Efektivita práce zaměstnanců
- Optimální využití konektivity
- Ochrana pověsti společnosti
- Bezpečnost firemní sítě

TrustPort Net Gateway

TrustPort WebFilter

Jevy pozorované v podnikové praxi:

- Surfování nesouvisející s prací
- Stahování dat nesouvisejících s prací
- Nelegální stahování softwaru a uměleckých děl
- Nebezpečné surfování

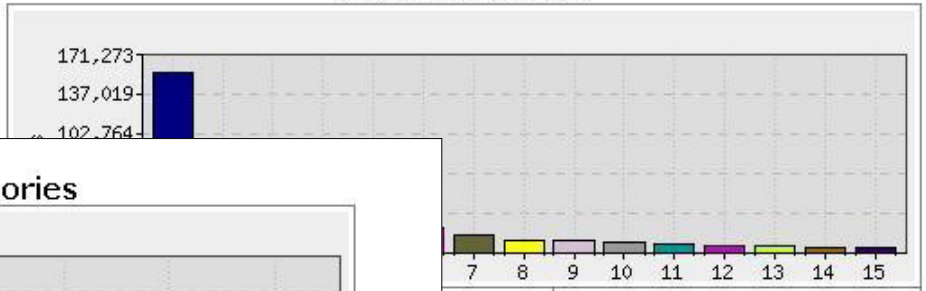
Webové filtrování

Nastavení webového filtrování

- Výběr sledovaných kategorií
  - Podle potřeb podniku
- Režim webového filtrování
  - Povolení všech webových stránek
  - Monitorování vybraných kategorií
  - Blokování vybraných kategorií
  - Blokování všech webových stránek (s výjimkou výslovně povolených)
- Použití heuristické analýzy
  - Žádné stránky
  - Neznámé stránky
  - Všechny stránky

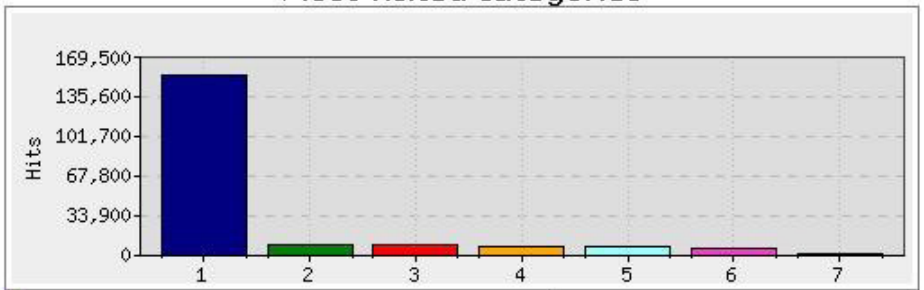
Analýza provozu

Most filtered IPs



	155703
	53938
	50286
	40701
	27493
	20770
	14814
	9805
	9401
	9015

Most visited categories



1 - Porn	154091
2 - Violence	9211
3 - Drugs	8930
4 - Gambling	7578
5 - Warez	6838
6 - Spyware	5813
7 - Hacking	1321

Year
2007
2008
2009

« Back ^Top » Total statistics

Děkuji za pozornost!