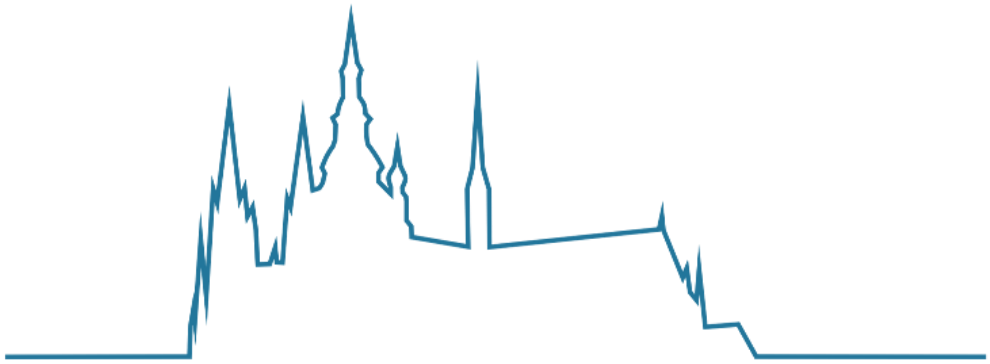
Lynt SERVICES



WordCamp Praha 2015

Bezpečnost Wordpressu, tipy pro každého

Vláďa Smitka

vladimir.smitka@lynt.cz

@smitka (ale skoro nic nepíšu)

Lynt services s.r.o.

http://lynt.cz

Lynt SERVICES

Obsah

- Fakta a zamyšlení
- Běžné útoky
- Obnova po útoku
- Bezpečnostní řetězec
- Bezpečnostní pluginy

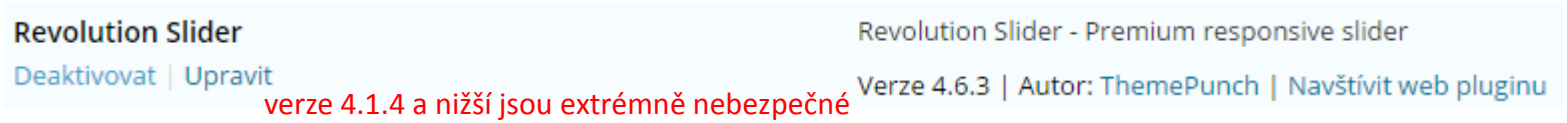
„Wordpress je o pluginech“

Největší hrozba

Otázka: „Jaká je podle tebe aktuálně největší bezpečnostní hrozba Wordpressových webů?“

Odpověď: „Neaktualizovaný Slider Revolution.“

- Pravděpodobně nejčastěji kradený plugin
- Součást mnoha šablon, kde je však bez podpory a updatů
- Stará verze neobsahuje autoupdate – nutno aktualizovat ručně!
- Prvek, který se velmi snadno pozná



verze 4.1.4 a nižší jsou extrémně nebezpečné

http://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html

5 + 2 nejlepších bezpečnostních tipů

Aktualizujte

Zálohujte

Používejte bezpečnostní plugin

Buďte opatrní

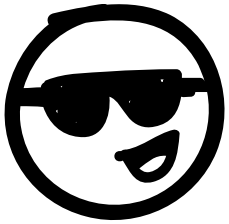
Smažte, co nepotřebujete a nedávejte světu moc informací

Aktualizujte!

AKTUALIZUJTE!!!

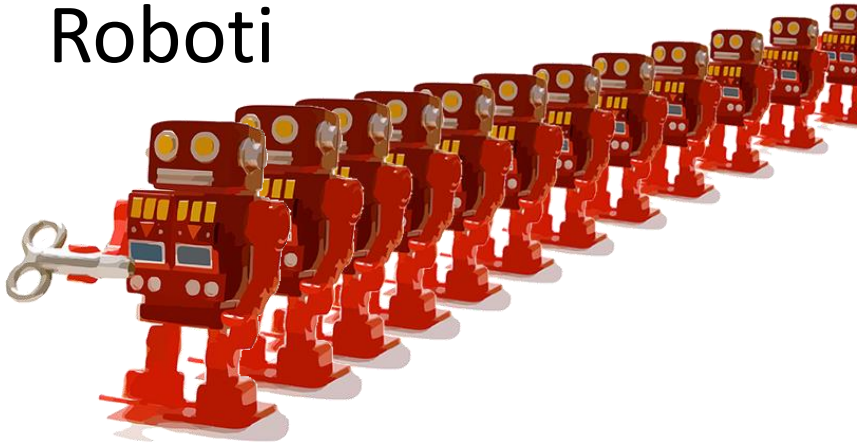
WordCamp HACK kampaň

- Během hodiny jsem nalezl 400 českých zranitelných Wordpress webů
- Hledal jsem známé a již opravené chyby ve 3 populárních pluginech
- Tvůrce/majitele jsem mailem informoval a pozval na WordCamp



Kdo mě chce napadnout?

Roboti



Anonymní hackeři

Motivovaní hackeři

Děti - script kiddies

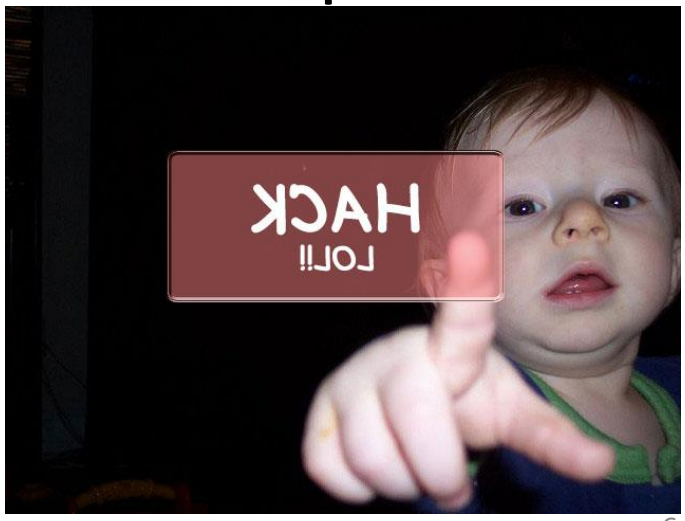


Photo by Lisa, CC BY-SA 2.0

Jak to udělá?

Bezpečnostní chyba v pluginech a šablonách

Odchytnutí hesla a cookie

Brutal force útok na Admin

Z jiných webů na hostingu

Spam z komentářů (+pingbacky)

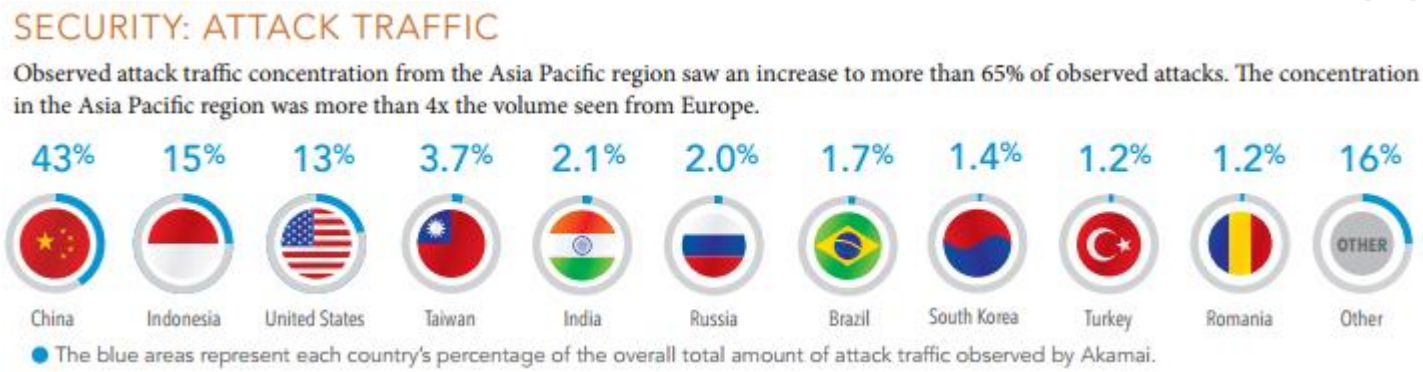
Útok oklikou – phishing, malware (keylogger, uložené heslo FTP)

Bezpečnostní chyba v jádru WP

Co mi udělá a proč to dělá?

- **Cizí kód**
  - Vloží spamové odkazy, reklamu, přesměrování
  - Nechají návštěvníky stahovat malware
  - Použijí web na DDOS a jiné útoky
- **Krádež informací**
  - Získají osobní informace uživatelů webu
- **Omezení provozu**
  - Odstaví web/server (DOS)

Fakta



http://www.akamai.com/stateoftheinternet/

43% útoků přichází z Číny
Potřebuji čínský traffic?
Nemělo by smysl celou Čínu zablokovat?

Zablokovat USA?
Spíše ne, můžu zablokovat vyhledávače, CDN…

Zablokovat vše mimo ČR?
Určitě ne. IP geolokace není 100% přesná.
Firemní uživatelé se mohou připojovat přes centrálu v jiné zemi.
Čeští uživatelé mohou přistupovat např. z dovolené (dovolená v Číně?).


NO, THANKS!

Jak zablokovat Čínu? – *na doma*

Seznam IP adres: http://www.ip2location.com/blockvisitorsbycountry.aspx

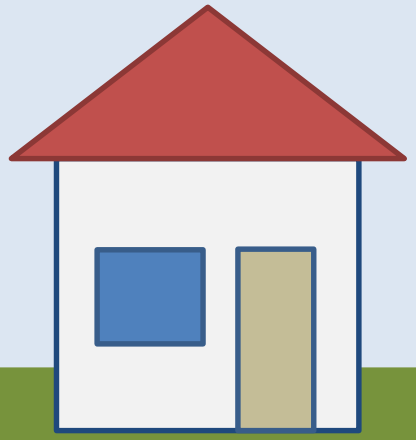
- Iptables
  - Nepoužívat vygenerovanou konfiguraci – tisíce pravidel, skrze které musí projít každý packet
  - iptables -A INPUT -m tcp -m state --state NEW -j CHINA_WALL
  - Pokročilé: optimalizace – více chainů podle části IP
- .htaccess/konfigurace nginx
- mod_geoIP
- Pluginy (např. placený Wordfence)
- HW krabička

```
//mod_geoIP v konfiguraci Apache
GeoIPEnable On
GeoIPDBFile /path/to/GeoIP.dat
SetEnvIf GEOIP_COUNTRY_CODE CN BlockCountry
SetEnvIf GEOIP_COUNTRY_CODE RU BlockCountry
Deny from env=BlockCountry

//mod_geoIP v .htaccess
RewriteCond %{ENV:GEOIP_COUNTRY_CODE}
^(CN|RU)$
RewriteRule ^(.*)$ - [F,L]
```

- Další varianta – přístupy z blokovaných zemí přesměrovat na stránku s CAPTCHA

Dělám nový web



Aktuality:
1.4.2003 spustili jsme nový web!

Lynt SERVICES

Priority při tvorbě webu

Krása

kolem toho se většinou točí celý vývoj webu

Rychlost

toho si všímáme, až když web běží

Bezpečnost

řešíme, až když se něco stane

Lynt SERVICES

Co se stane když…

- nám nabourají web?
- přijdu o důvěrná data, ztratím důvěryhodnost, web nebude fungovat a bude penalizovaný

- je web hrozivě pomalý?
- návštěvníci jsou otrávení a mohou jít jinam, vyhledávače nebudou chtít indexovat

- nemám na hlavní stránce slider se super efekty?
- nic?

Opravdové priority

z hlediska dopadu na business

Bezpečnost

Rychlost

Krása

Lynt SERVICES

Čas na praktické ukázky!

Slider Revolution - LFI

- Verze 4.1.4 a nižší
- Stažení libovolného zdrojového souboru z hostingu
- Registrace všech Ajaxových volání pro privilegované i nepriveligované uživatele
- **/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php**

- Detaily: http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-slider-revolution-4-1-4

FancyBox for Wordpress - XSS

- Verze 3.0.2 a nižší
- Vložení libovolného javascriptu na všechny stránky
- Použití hooku admin_init bez dodatečné kontroly oprávnění (aktivuje se při každém dotazu do administrace – admin-ajax.php, admin-post.php)
- **/wp-admin/admin-ajax.php?page=fancybox-for-wordpress +**
  proměnná mfbfw[padding]=</script><script>zlý kód</script>

- Detaily: http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-fancybox-for-wordpress-3-0-2

Mail Poet – Upload PHP

- Verze 2.6.8 a nižší
- Nahrání PHP souboru na web a jeho spuštění
- Opět použití admin_init bez dodatečné kontroly skutečného oprávnění + chybné použití $_REQUEST v první opravě
- **/wp-admin/admin-post.php?page=wysija_campaigns&action=themeupload + proměnná my-theme = zlý zip**

- Detaily: http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-mail-poet-2-6-8

Wordpress Video Gallery - SQLi

- Verze 2.7
- SQL injection – získání libovolných dat z databáze
- Špatně ošetřené uživatelské vstupy, dlouho bez opravy
- **/wp-admin/admin-ajax.php?action=rss&type=video&vid=-1 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39 FROM wp_users ;--**

- Detaily: http://lynt.cz/blog/zranitelnost-ve-wordpress-pluginu-wordpress-video-gallery-2-7

Wordpress 3.9.2 - XSS

„Wordpress verze 3.9.2 je v pohodě.“

Vladimír Smitka, 4. WP konference, listopad 2014

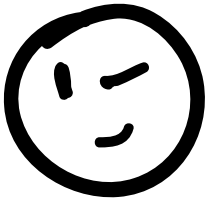
- Obejití kontroly povolených tagů v komentářích
- [<blockquote cite="]">[" onmouseover="alert('ojojoj!');
  " style="background-color:red;position:absolute;top:0;
  left:0;height:100%;width:100%;"][<a href="]>ahojky

„Co je bezpečné dnes, nemusí být bezpečné zítra.“

Vladimír Smitka, 4. WP konference, listopad 2014

Co mohlo snížit dopady?

- Aktualizace



- Zabránění spouštění PHP ve složce /wp-content/uploads

  .htaccess v této složce:

  ```
  php_flag engine off
  ```

Jiná možnost:

```
<FilesMatch \.php$>
   Order allow,deny
   Deny from all
</FilesMatch>
```

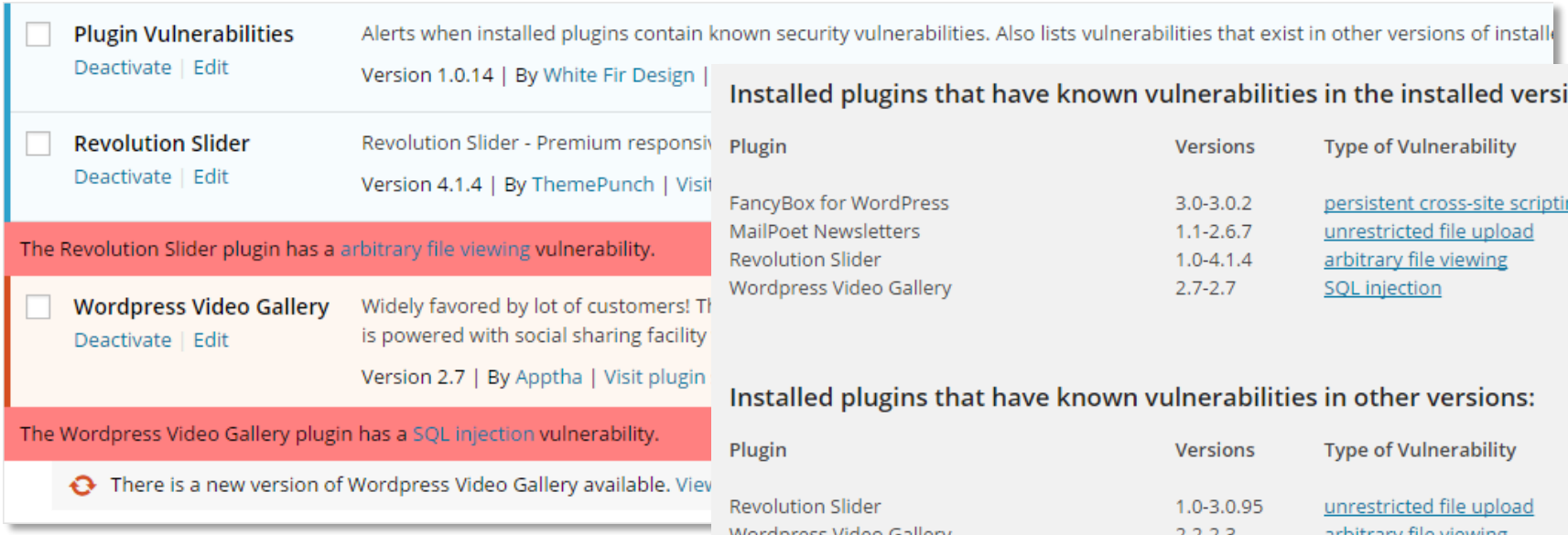
- Blokace dotazů obsahujících wp-config.php

  Globální .htaccess:

  ```
  RewriteCond %{QUERY_STRING} wp-config.php
  RewriteRule ^(.*)$ - [F,L]
  ```

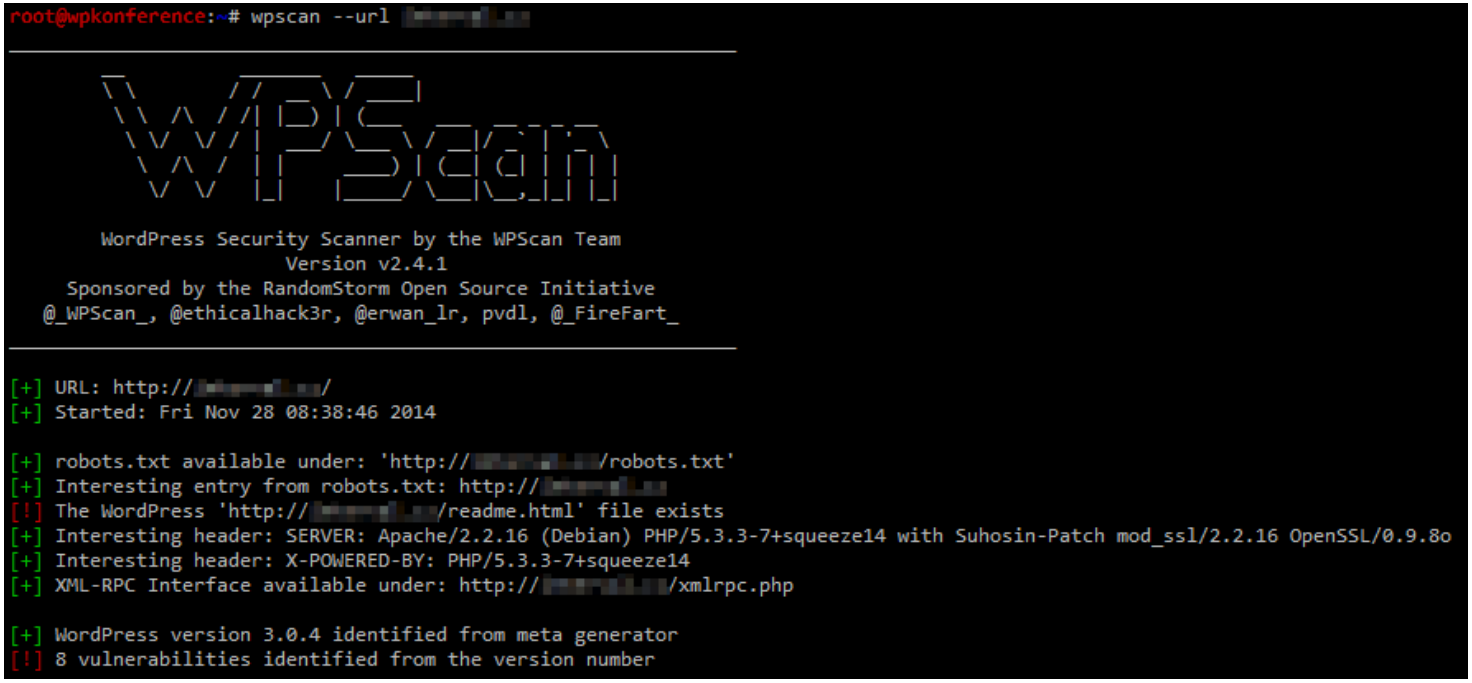
Jak poznám, že mám i já zranitelný plugin?

- Sleduji dění a vím
- **Plugin Vulnerabilities**
- https://wordpress.org/plugins/plugin-vulnerabilities/



Jak to pozná útočník?

- První, nejdelší a nejdůležitější část útoku, je průzkum (Reconnaissance)
- WPScan – nejpoužívanější nástroj



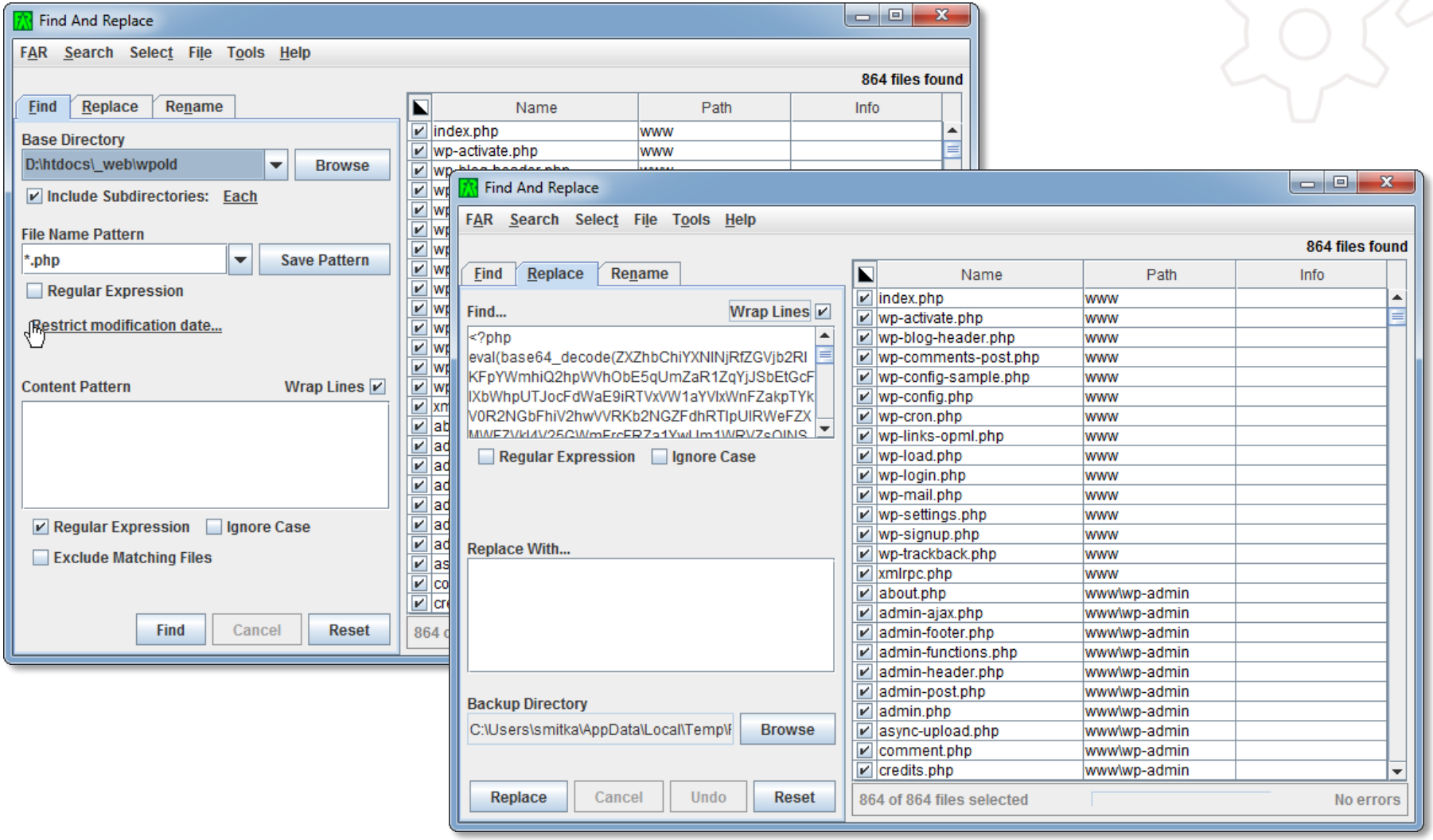
Stalo se, byl jsem napaden!

Obnova po útoku

- Obnova z čisté zálohy
  - Smazat starý web nahrát čistý
- Přeinstalování + ruční dezinfekce
  - FAR
    - nejčastěji malware přidá kód do všech php souborů na webu
    - editor pro hromadné odstranění/nahrazení škodlivého kódu
    - v souborech však mohou být i další škodlivé kódy
  - Prohlédnutí SQL dumpu
    - Pokusit se nalézt <iframe, <script, x-shockwave-flash, eval, base64_decode, gzip_, preg_replace
    - Pokusit se identifikovat, zda jsou nálezy regulérní
- Odstranění malware neřeší příčinu!

Lynt SERVICES

FAR



Checklist

- Dezinfekce, odstranění příčiny (často aktualizace)
- Změna hesla na FTP
- Změna hesla do DB
- Změna hesel uživatelů
- Nové šifrovací klíče: https://api.wordpress.org/secret-key/1.1/salt/
  - Od WP 3.1. se generují při instalaci
    define('AUTH_SALT', 'put your unique phrase here');
- Kontrola souborů pluginem (Wordfence, Sucuri Scanner)

Zálohování

„Zálohování je alfou a omegou práce na počítači“

Ruční
občas všechno někam stáhnu, není to ideální ale alespoň něco

Zálohování řeší server
ideální stav (zeptejte se svého webhostera jakým způsobem to má vyřešené)

Zálohovací plugin
kompromisní řešení, může však přinášet různé další benefity

Zálohovací pluginy

- BackWPup
  - pouze záloha - nemá obnovu, tu lze ale jednoduše udělat ručně
  - umí zálohu na více úložišť
  - lze spouštět externím voláním speciální URL
- UpdraftPlus
  - záloha i obnova
  - záloha na jedno zvolené úložiště (Pro verze více)
- BackupBuddy
  - pouze placená verze
  - kompletní řešení (migrace webů na jiné domény, obnova zálohy speciálním skriptem na novém hostingu, široká podpora externích úložišť, obnova jednotlivých souborů, zvládá serializovaná data)

Jak na zálohování pluginem?

- Preferovat zálohu na externím úložišti
- Pokud je na lokálním
  - zjistit kde a zkusit, zda se soubory záloh opravdu nedají otevřít z prohlížeče
  - ověřit zda se nezálohují zálohy samotné (vyjmout složku se zálohou ze zálohování)
- Plánování záloh
  - WP-Cron – umí většina pluginů, spouští se pouze, když je na webu návštěvnost (lze ověřit pomocí Crontrol)
  - Externí spouštení – preferovaná cesta, je jistota, že se spustí (cron na serveru, minicron, online cron např. http://www.webcron.org/, https://www.setcronjob.com, https://www.easycron.com)
- Nastavení upozornění mailem o proběhnuté záloze

Lynt SERVICES

Pojďme se bránit!

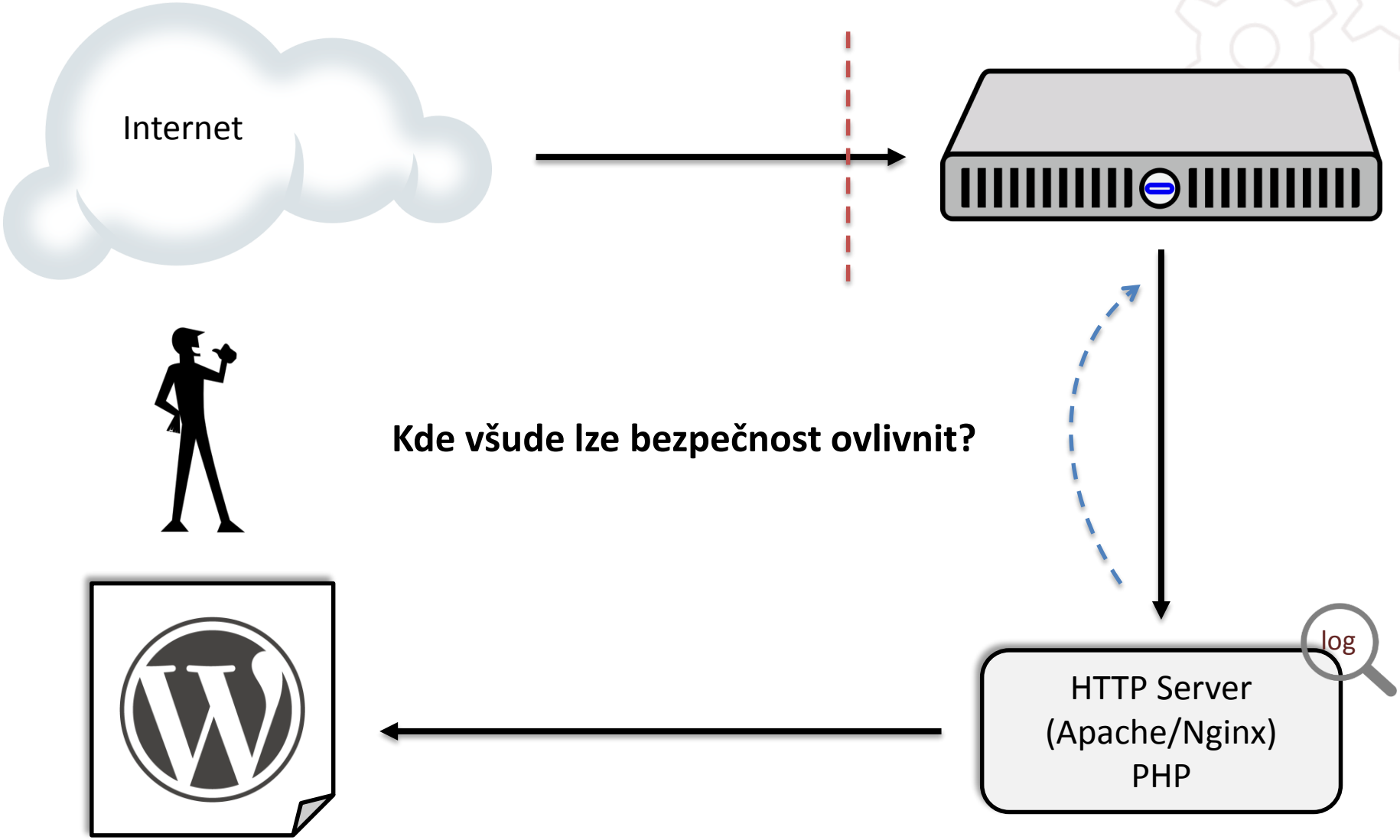
Power!

Jak pomoci výkonu zvýšit bezpečnost?

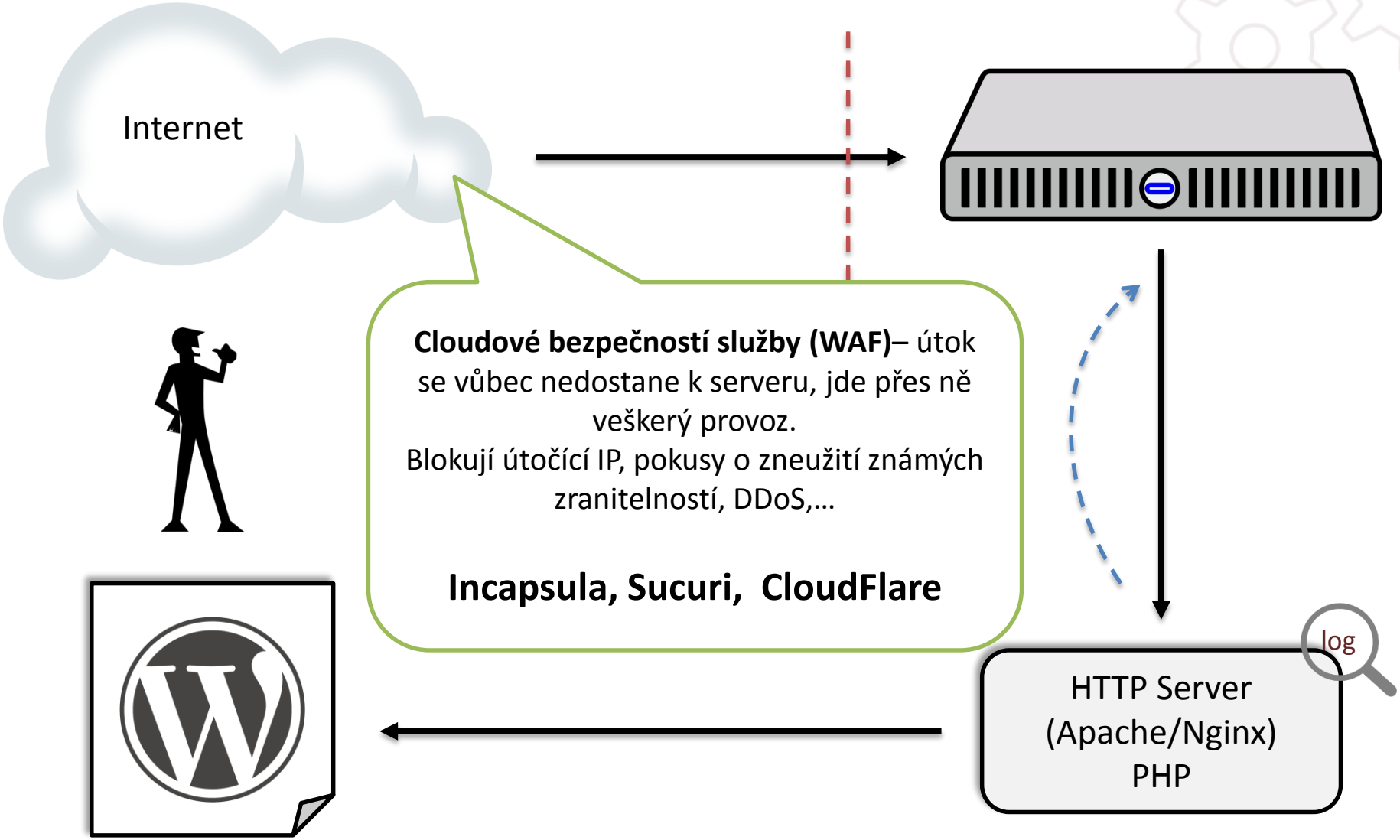
- WP Super Cache
  - Mnoho útoků je typu (D)DoS – vyčerpají dostupné prostředky
  - Pokud použiji stránkovou Cache, budou vracet statické soubory a nebudu spotřebovávat výkon
- Autoptimize
  - Skryji „prozrazující“ javascripty a css do jednoho souboru
  - Snížím počet požadavků na server
  - Pro některé skripty je třeba vytvořit výjimky (Google Maps)

- Vedlejší účinky: rychlejší web, spokojenější návštěvníci, chutnější SEO

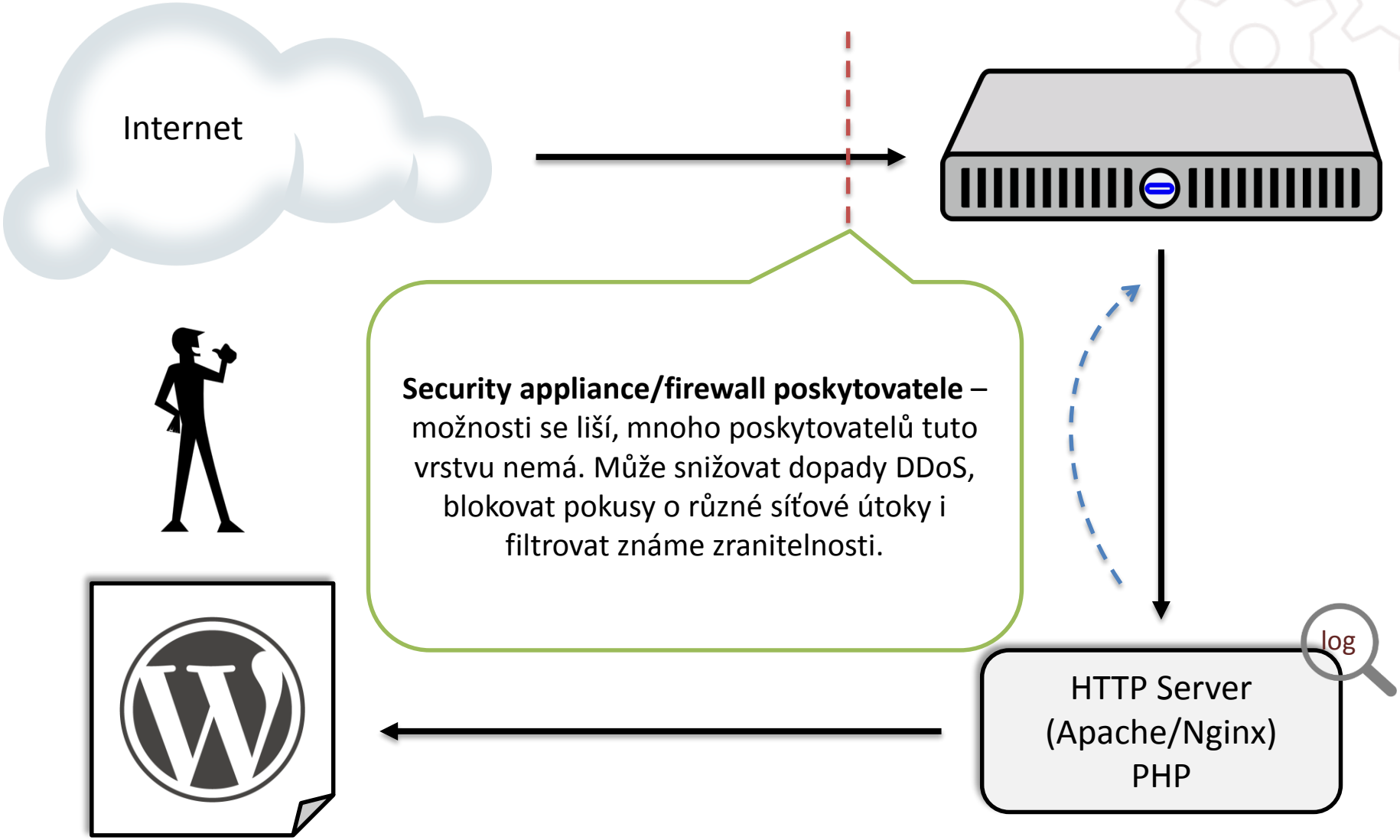
Bezpečnostní řetězec



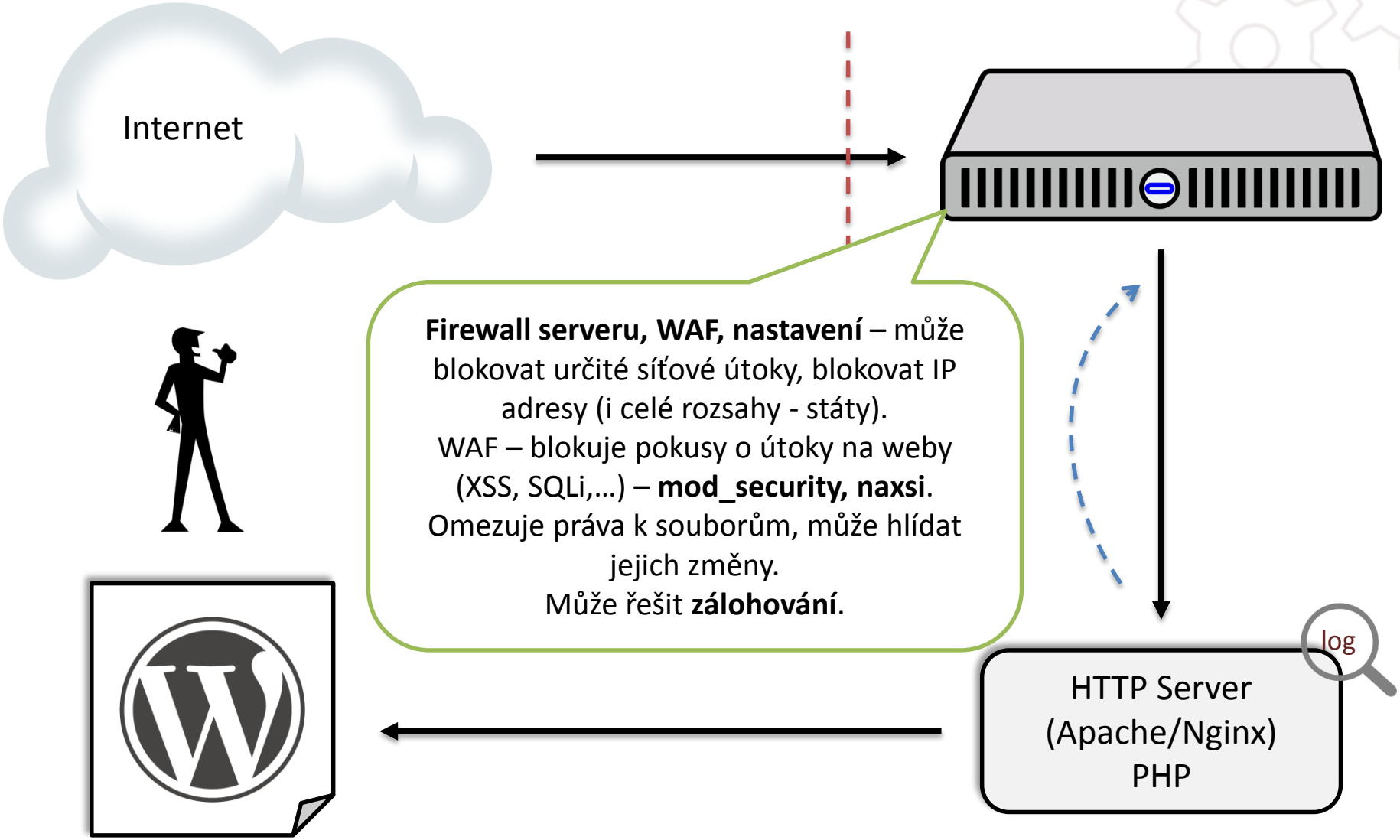
Cloud


Internet
Cloudové bezpečností služby (WAF)– útok se vůbec nedostane k serveru, jde přes ně veškerý provoz.
Blokují útočící IP, pokusy o zneužití známých zranitelností, DDoS,…
Incapsula, Sucuri, CloudFlare
log
HTTP Server
(Apache/Nginx)
PHP

Poskytovatel



Server


Internet
Firewall serveru, WAF, nastavení – může blokovat určité síťové útoky, blokovat IP adresy (i celé rozsahy - státy).
WAF – blokuje pokusy o útoky na weby (XSS, SQLi,…) – **mod_security, naxsi**.
Omezuje práva k souborům, může hlídat jejich změny.
Může řešit **zálohování**.
log
HTTP Server
(Apache/Nginx)
PHP

Server – *na doma*

- Detekce změn v PHP souborech za posledních 24 hodin:
  find /srv/htdocs/muj_web/ -name '*.php' -type f -mtime -1 > output ; mail -s "Zmeny za poslednich 24hod" "vladimir.smitka@lynt.cz" < output

Další seznam IP adres zemí:
http://www.iwik.org/ipcountry/

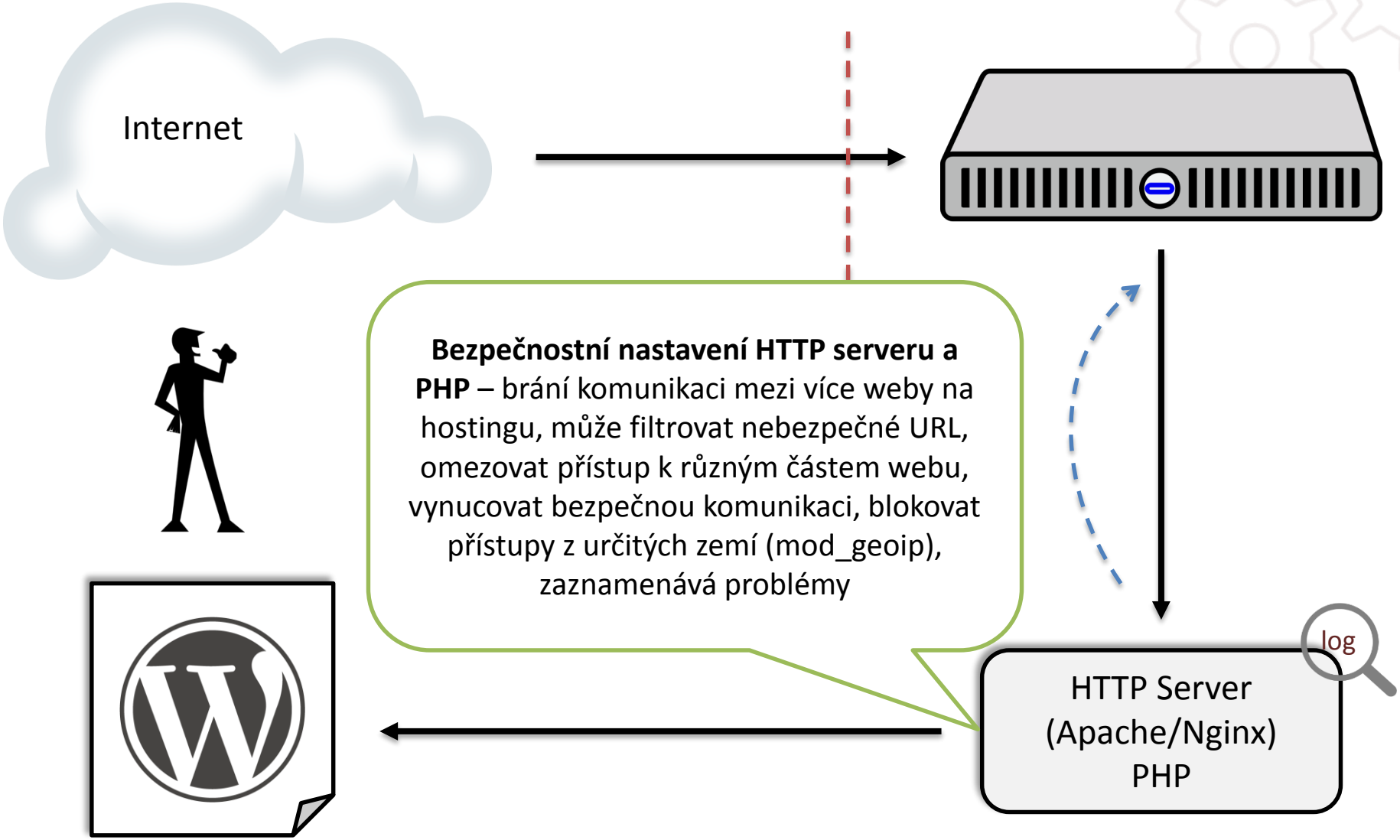
Viz Blokace Číny

Základ mod_security pro WP:
http://blog.erben.sk/2015/02/11/protecting-wordpress-with-mod-security/

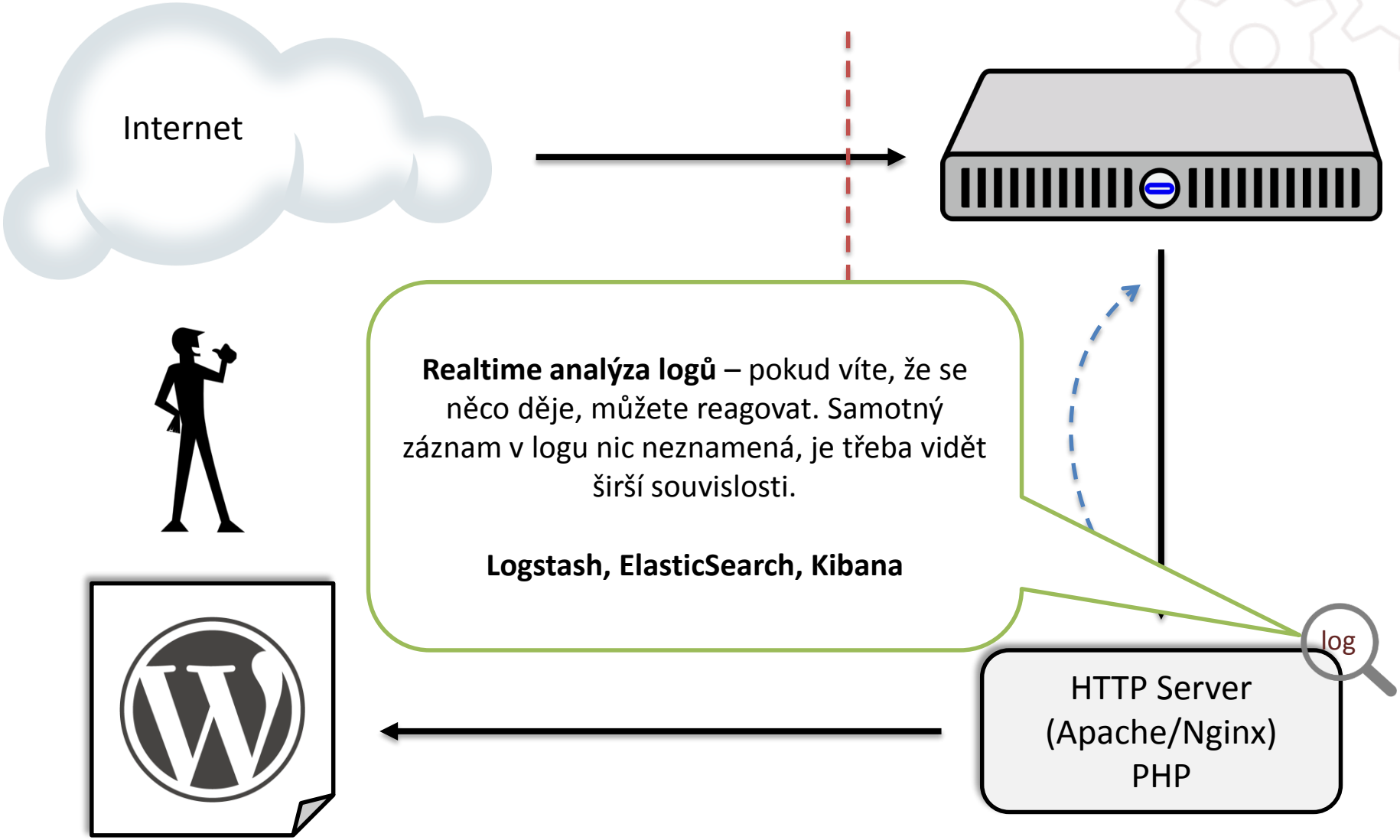
Práva souborů a složek dle All In One WP Security:

root directory	755
wp-includes/	755
.htaccess	644
wp-admin/index.php	644
wp-admin/js/	755
wp-content/themes/	755
wp-content/plugins/	755
wp-admin/	755
wp-content/	755
wp-config.php	644

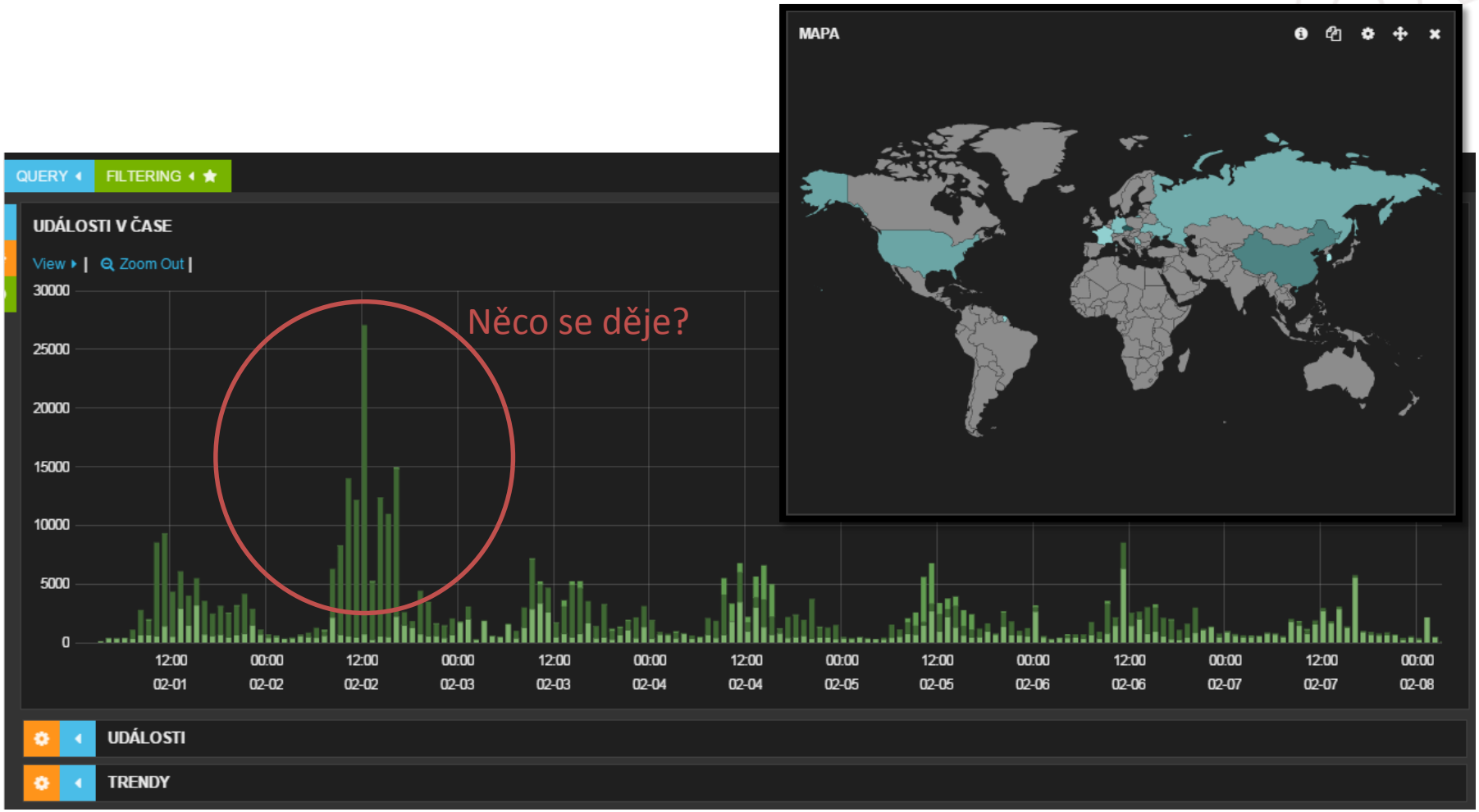
HTTP Server a PHP



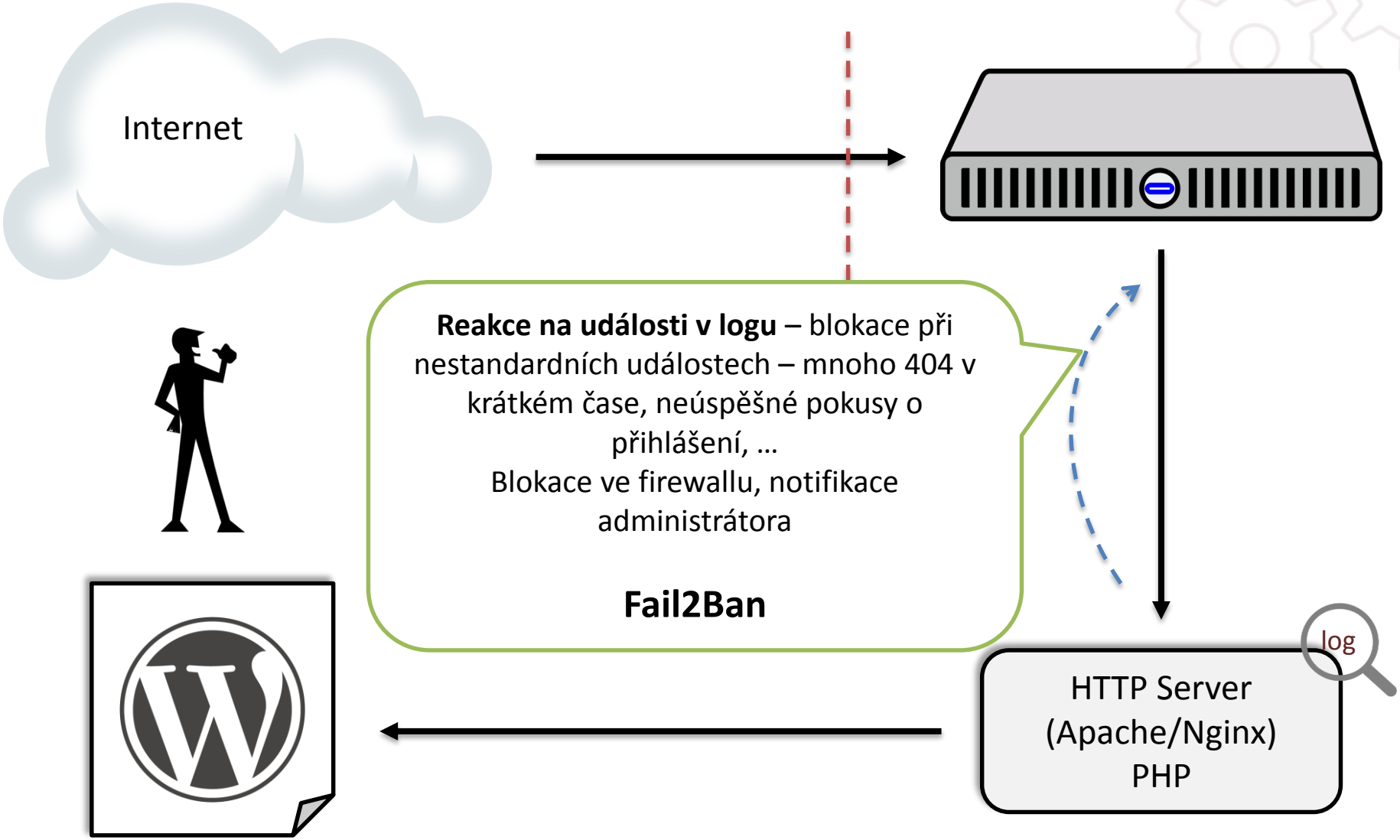
Analýza logů



Ukázka z analýzy logů



Reakce na události



Fail2Ban – *na doma*

- Některé funkce bezpečnostního pluginu můžeme posunout o úroveň níže
- Např. detekci brutal force analýzou logů nebo 404 (může být dobré nelogovat statické soubory):

- **filter.d/wp-auth.conf**

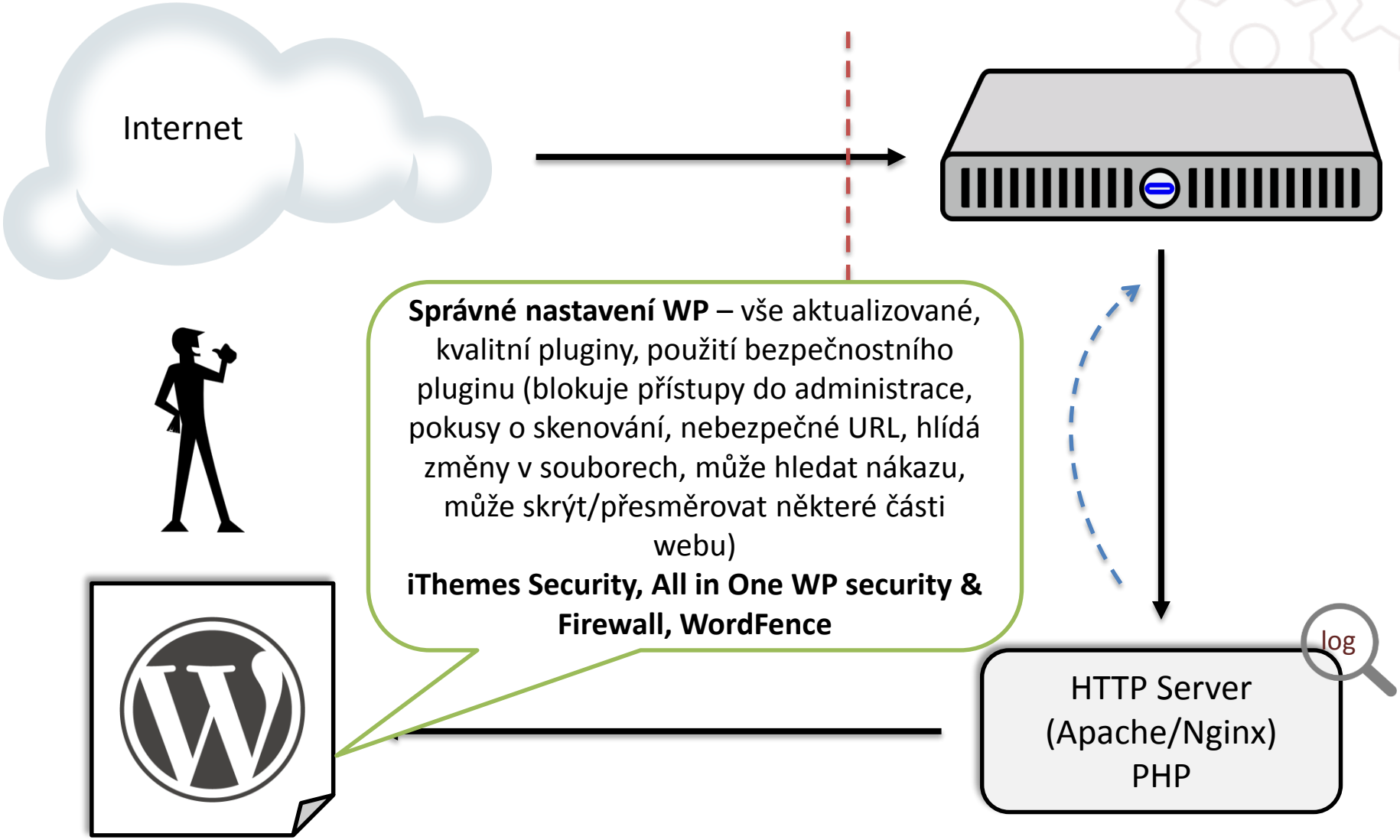
```
# WordPress brute force auth filter: /etc/fail2ban/filter.d/wp-auth.conf:
#
# Block IPs trying to auth wp wordpress
#
# Matches e.g.
# 178.63.72.184 - - [16/Oct/2014:11:40:50 +0200] "POST /wp-login.php HTTP/1.0" 200 1531 "-" "-"
[Definition]
failregex = ^<HOST> .* "POST /wp-login.php
```

- **jail.conf**

```
[wp-auth]
enabled = true
filter = wp-auth
action = iptables-multiport[name=wp-auth, port="http,https", protocol=tcp]
         sendmail-whois[name=WPauth, dest=vladimir.smitka@lynt.cz, sendername="Fail2Ban"]
logpath = /var/log/wordpress/access.*.log
```

- Pozor na logrotate - /usr/bin/fail2ban-client reload wp-auth
- Do WP exituje doplněk, který hlásí do logu neúspěšná přihlášení: https://wordpress.org/plugins/wp-fail2ban/

Nastavení Wordpress



Bezpečnostní plugin

Wordfence

Securing your WordPress website

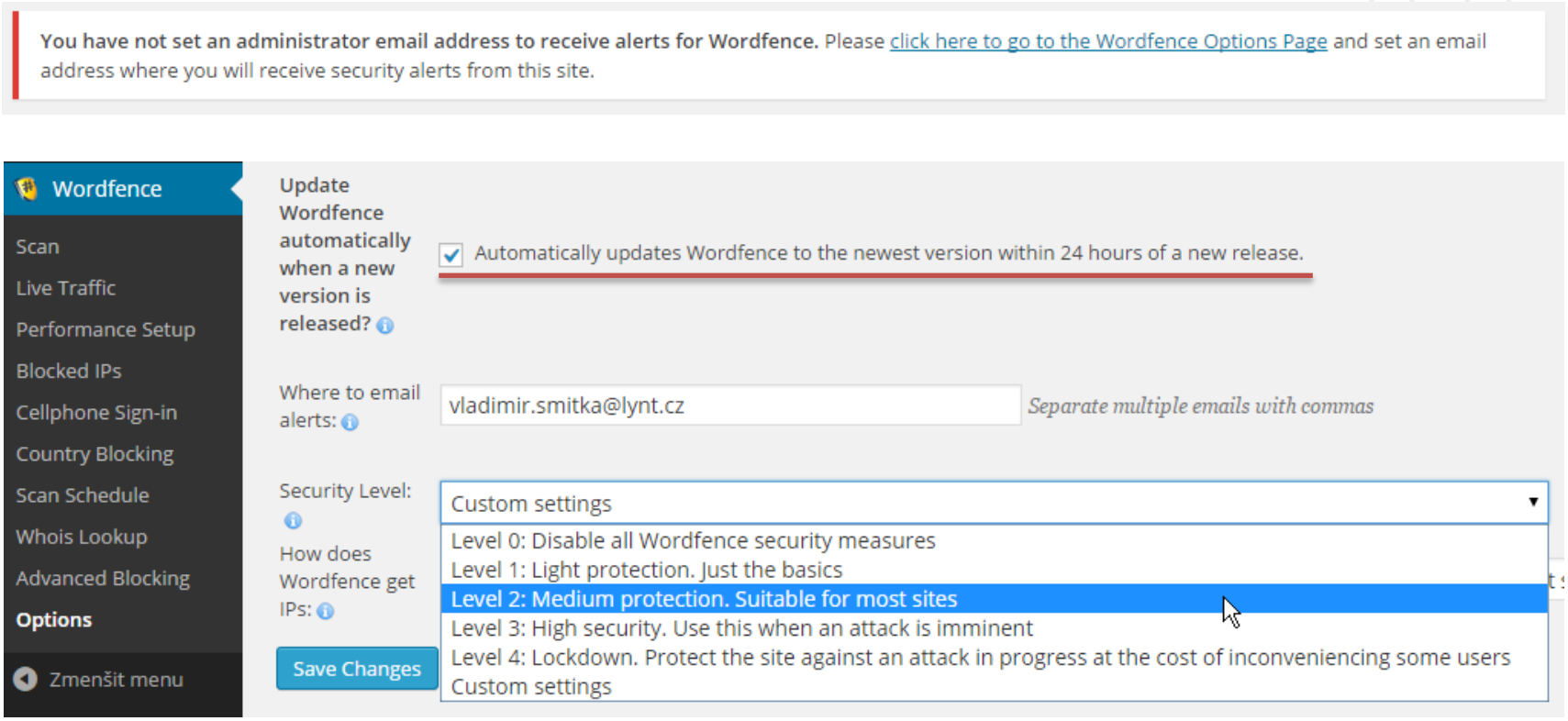
www.wordfence.com

WordFence

- **Aktivní ochrana**
- Detekce botů, omezování provozu (HTTP 503)
- Live traffic
- Sken - kontrola souborů, známých infekcí, test zda je web na blacklistech
- Cache

- A samozřejmě:
  - Hlídání změn v souborech
  - Omezování chybných přihlášení
  - Omezování 404
  - Blokace komentářového spamu

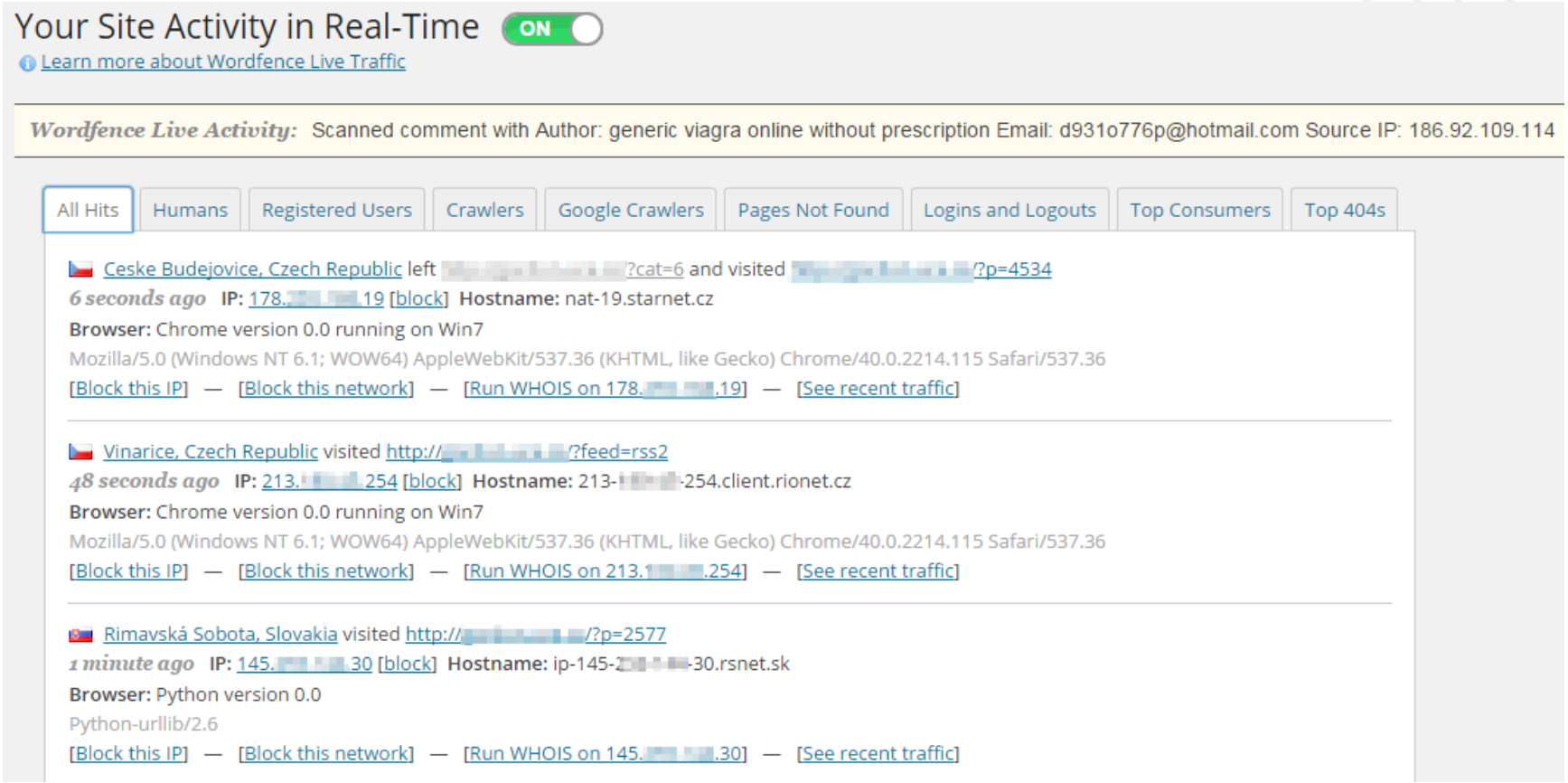
WordFence – po instalaci



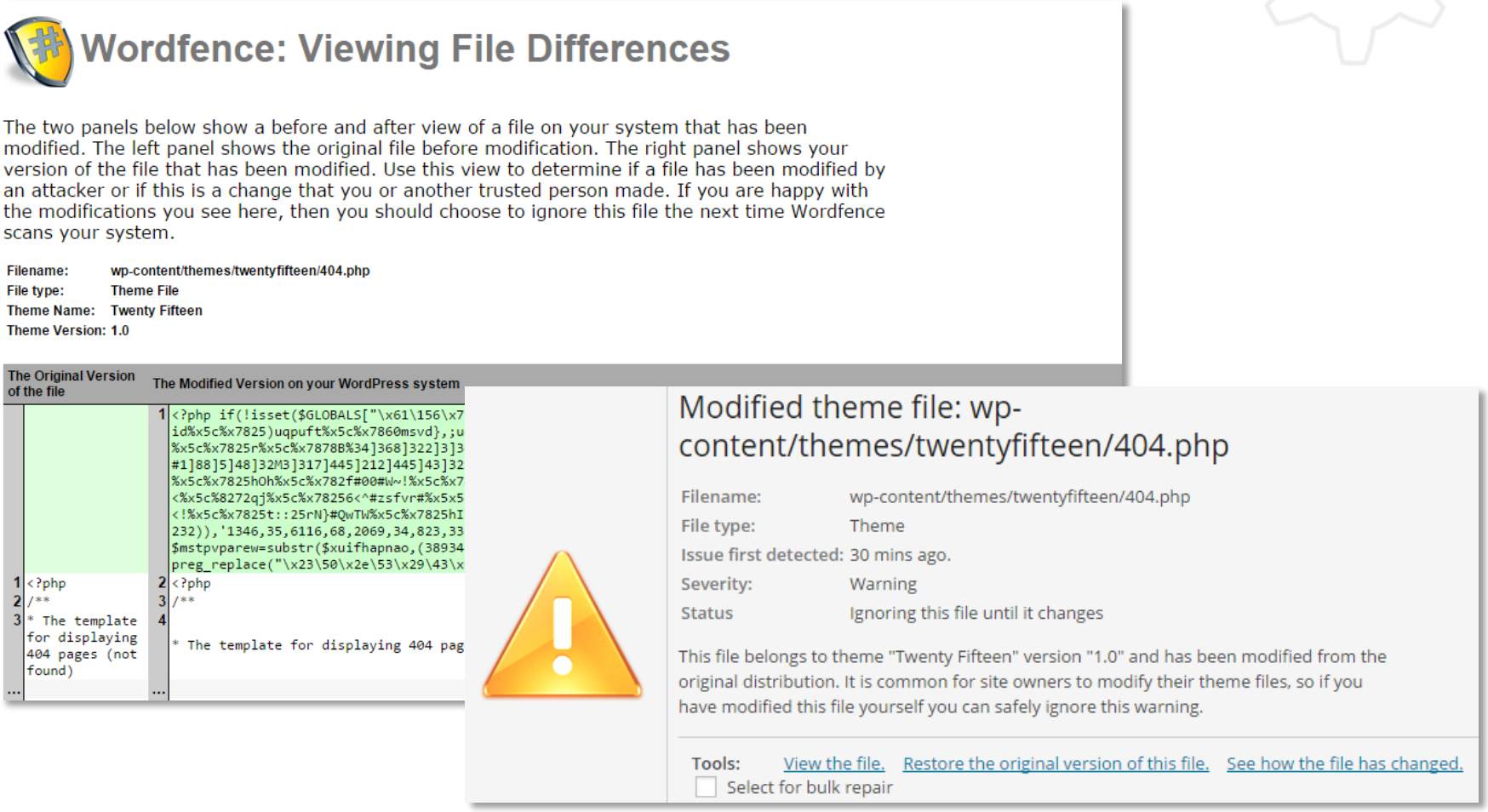
Level 2: začne posílat více upozornění, snižují se limity chybných přihlášení
Level 3: se začínají uplatňovat omezování provozu
Level 4: okamžitě blokuje neplatná jména

Lynt SERVICES

WordFence – Live Traffic



WordFence – detekce změn



Wordfence: Viewing File Differences

The two panels below show a before and after view of a file on your system that has been modified. The left panel shows the original file before modification. The right panel shows your version of the file that has been modified. Use this view to determine if a file has been modified by an attacker or if this is a change that you or another trusted person made. If you are happy with the modifications you see here, then you should choose to ignore this file the next time Wordfence scans your system.

Filename: wp-content/themes/twentyfifteen/404.php
File type: Theme File
Theme Name: Twenty Fifteen
Theme Version: 1.0

The Original Version of the file	The Modified Version on your WordPress system
	1 <?php if(!isset($GLOBALS["\x61\156\x7
	id%x5c%x7825)uqpuft%x5c%x7860msvd},;u
	%x5c%x7825r%x5c%x7878B%34]368]322]3]3
	#1]88]5]48]32M3]317]445]212]445]43]32
	%x5c%x7825hOh%x5c%x782f#00#W~!%x5c%x7
	<%x5c%8272qj%x5c%x78256<^#zsfvr#%x5x5
	<!%x5c%x7825t::25rN}#QwTW%x5c%x7825hI
	232)),'1346,35,6116,68,2069,34,823,33
	$mstpvparew=substr($xuifhapnao,(38934
	preg_replace("\x23\50\x2e\53\x29\43\x
1 <?php	2 <?php
2 /**	3 /**
3 * The template for displaying 404 pages (not found)	4 * The template for displaying 404 pag
...	...

Modified theme file: wp-content/themes/twentyfifteen/404.php

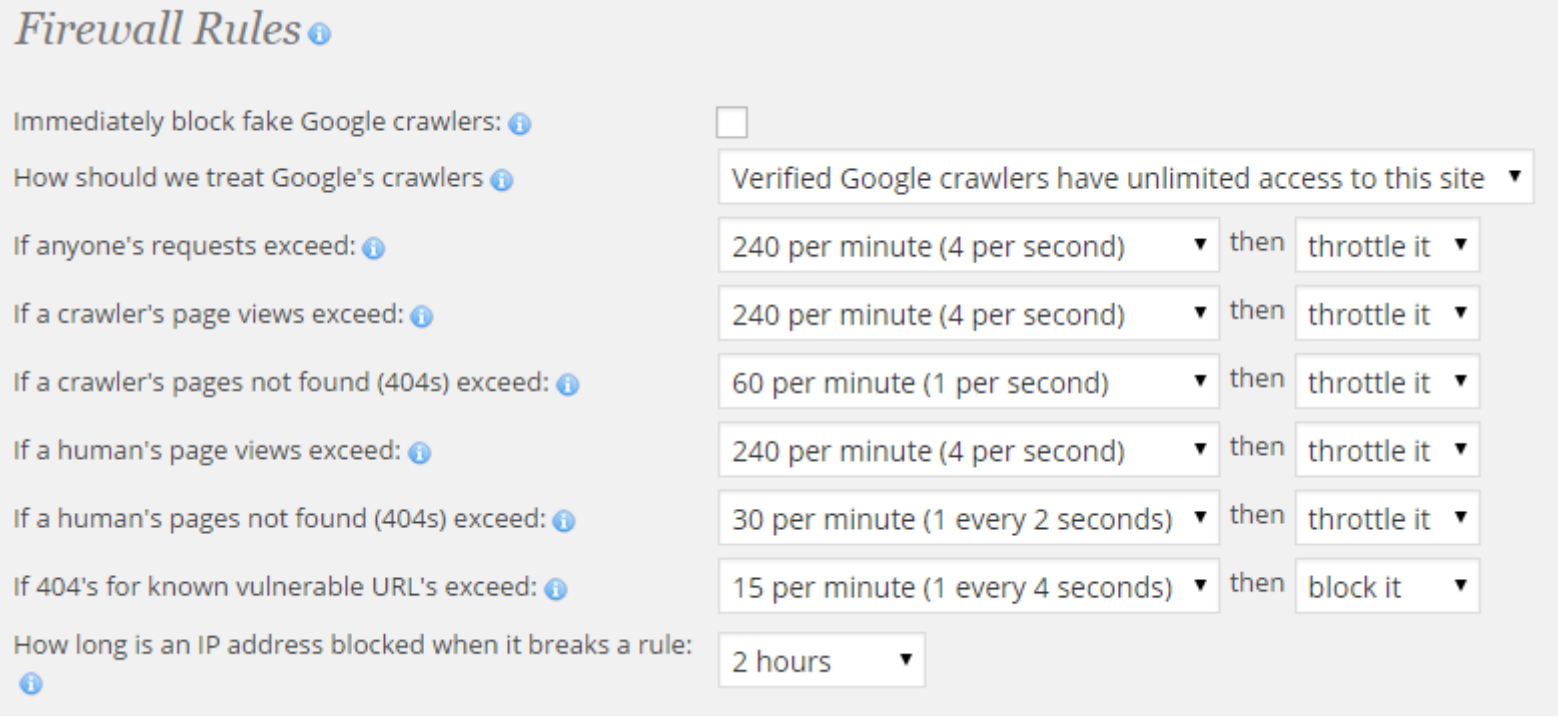
Filename:	wp-content/themes/twentyfifteen/404.php
File type:	Theme
Issue first detected:	30 mins ago.
Severity:	Warning
Status	Ignoring this file until it changes

This file belongs to theme "Twenty Fifteen" version "1.0" and has been modified from the original distribution. It is common for site owners to modify their theme files, so if you have modified this file yourself you can safely ignore this warning.

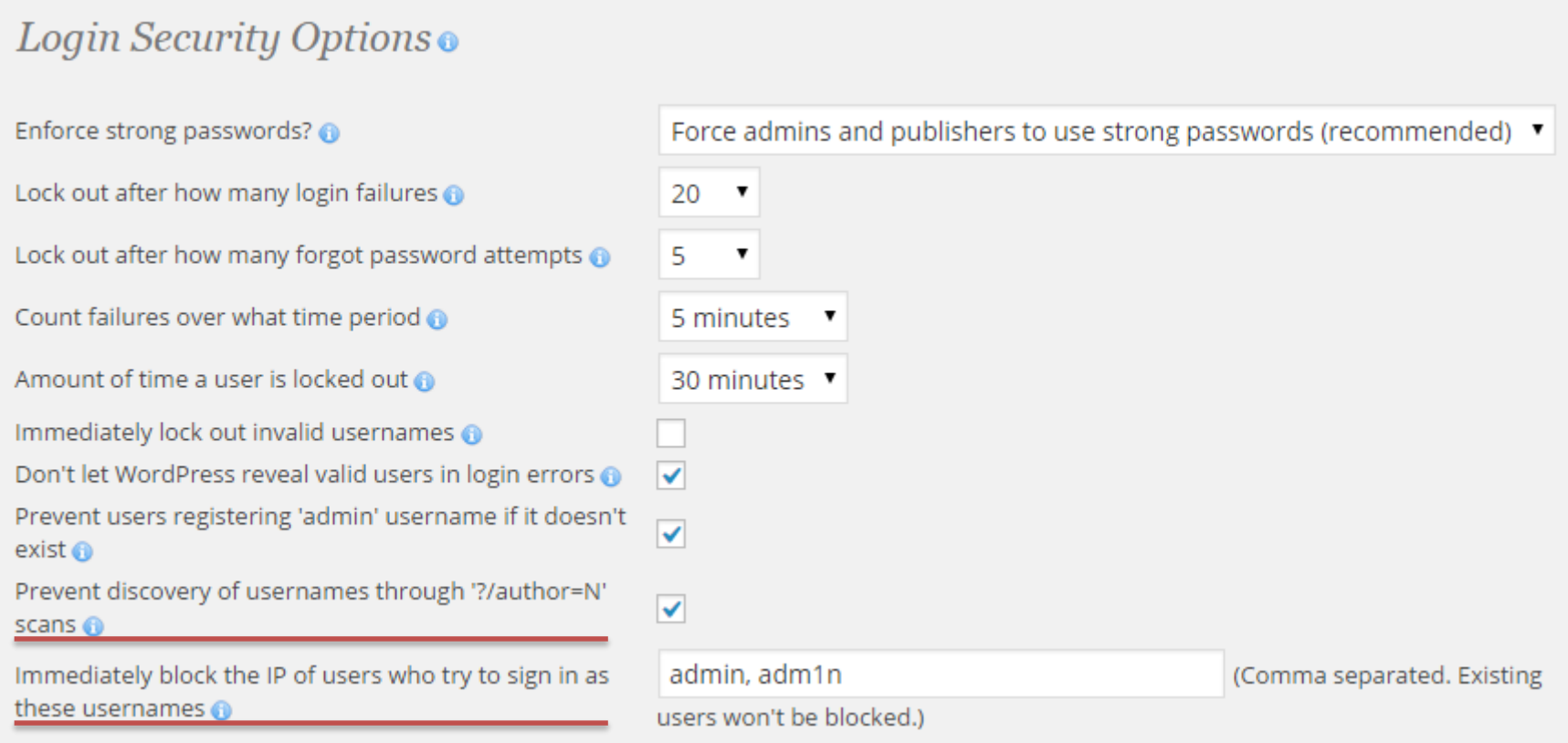
Tools: View the file. Restore the original version of this file. See how the file has changed.
Select for bulk repair

Lynt SERVICES

WordFence – omezování provozu



WordFence – bezpečnost přihlášení



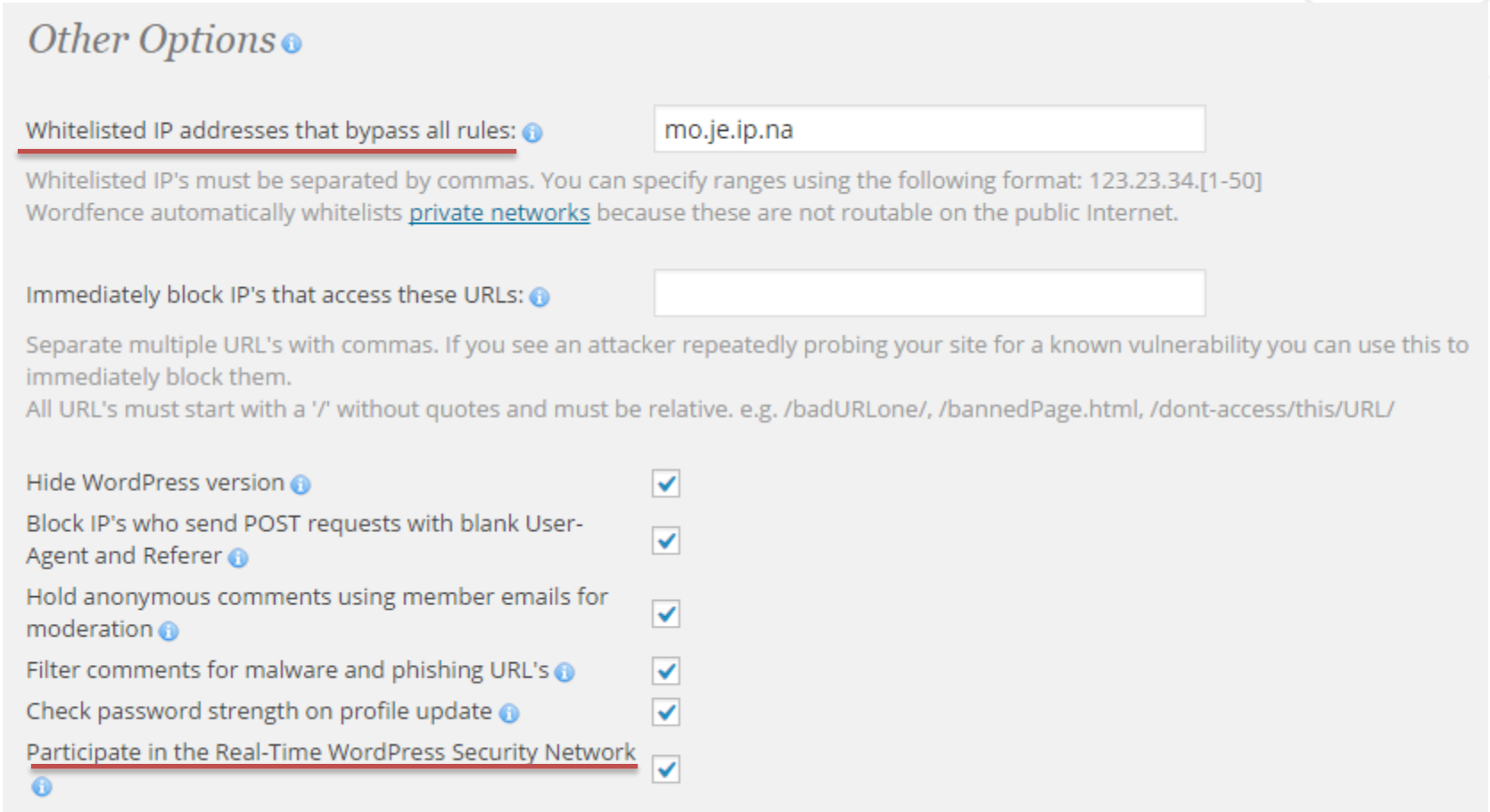
Tip: omezení získávání uživatelských jmen v .htaccess:

RewriteCond %{QUERY_STRING} author=

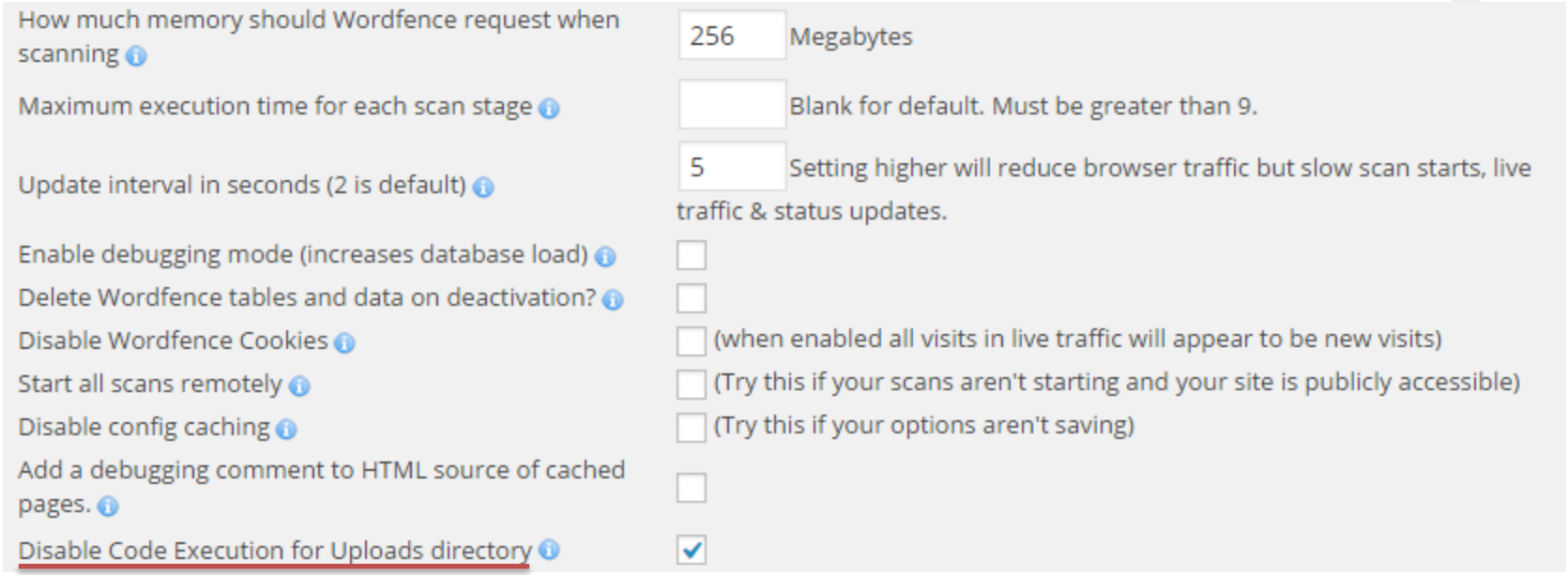
RewriteRule ^(.*)$ http://beznekam.cz? [L,R=301]

Lynt SERVICES

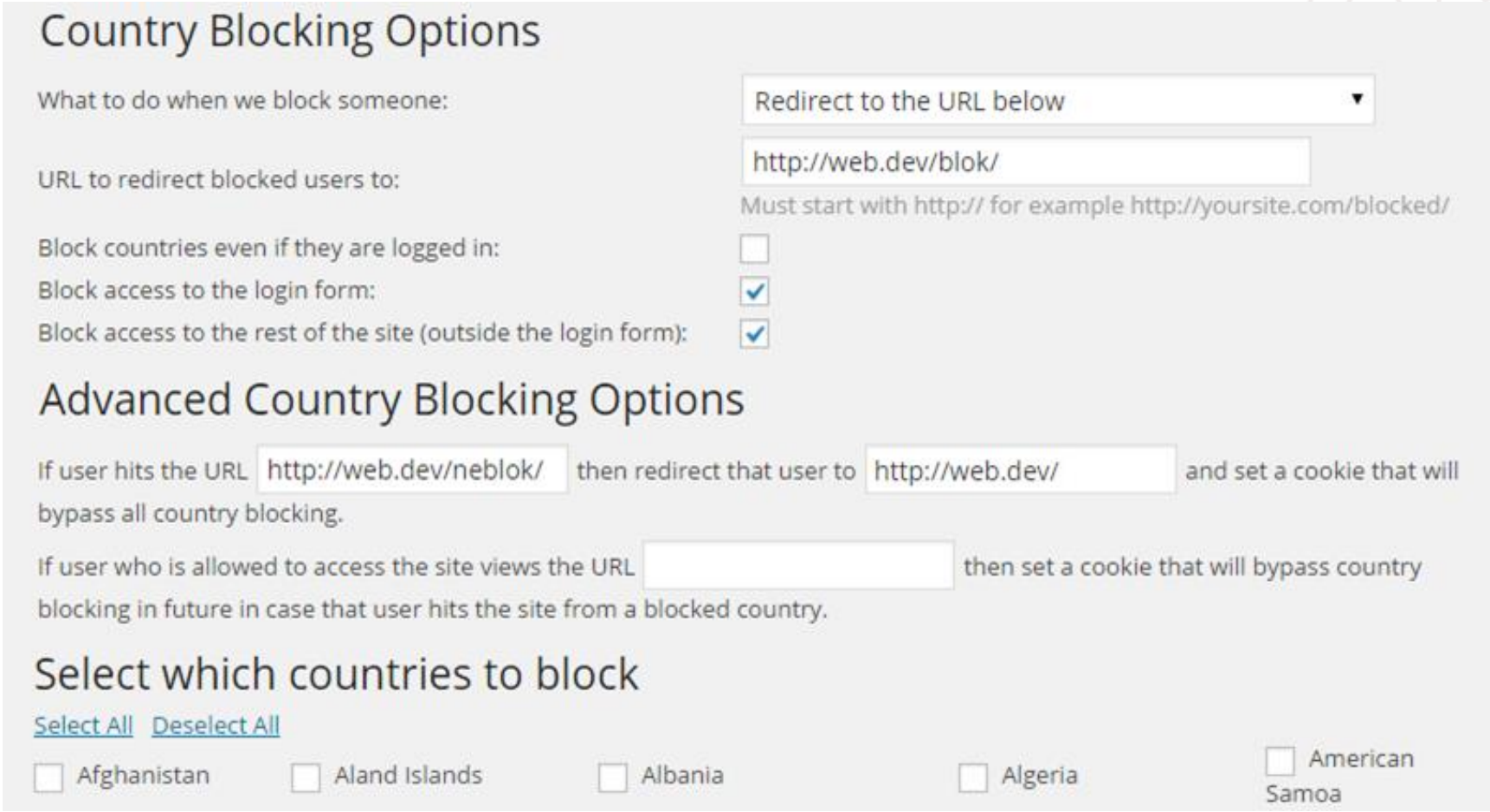
WordFence – další nastavení



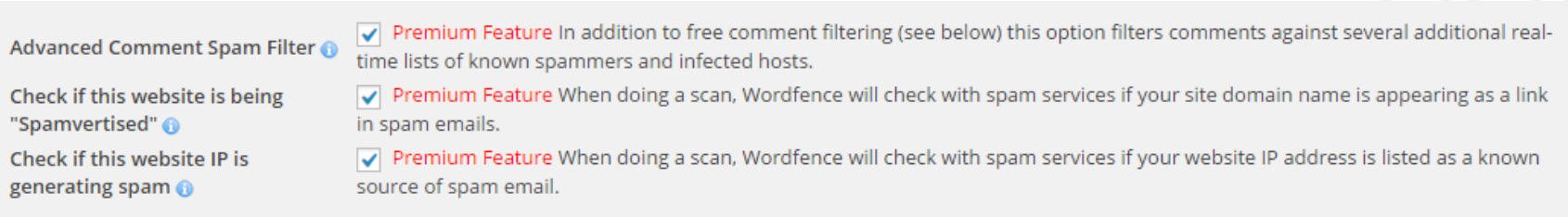
WordFence – další nastavení



WordFence Premium – Country blocking



WordFence Premium – další



- Lepší ochrana proti spamu – používá aktuální databázi spamerů udržovanou Wordfence
- Při scanu zjišťuje, zda se URL webu nevyskytuje ve spamových mailech – brzké varování
- Při scanu ověřuje, zda není IP na blacklistech pro maily

2 fázová autentifikace pomocí SMS:
Your Wordfence code is ABCDEF. – kód se vkládá za mezeru do hesla
Lepší přes [WP Google Authenticator]

Plánování scanu – lze nastavit častější kontroly (dobré, pokud mám více uživatelů s vyššími oprávněními)

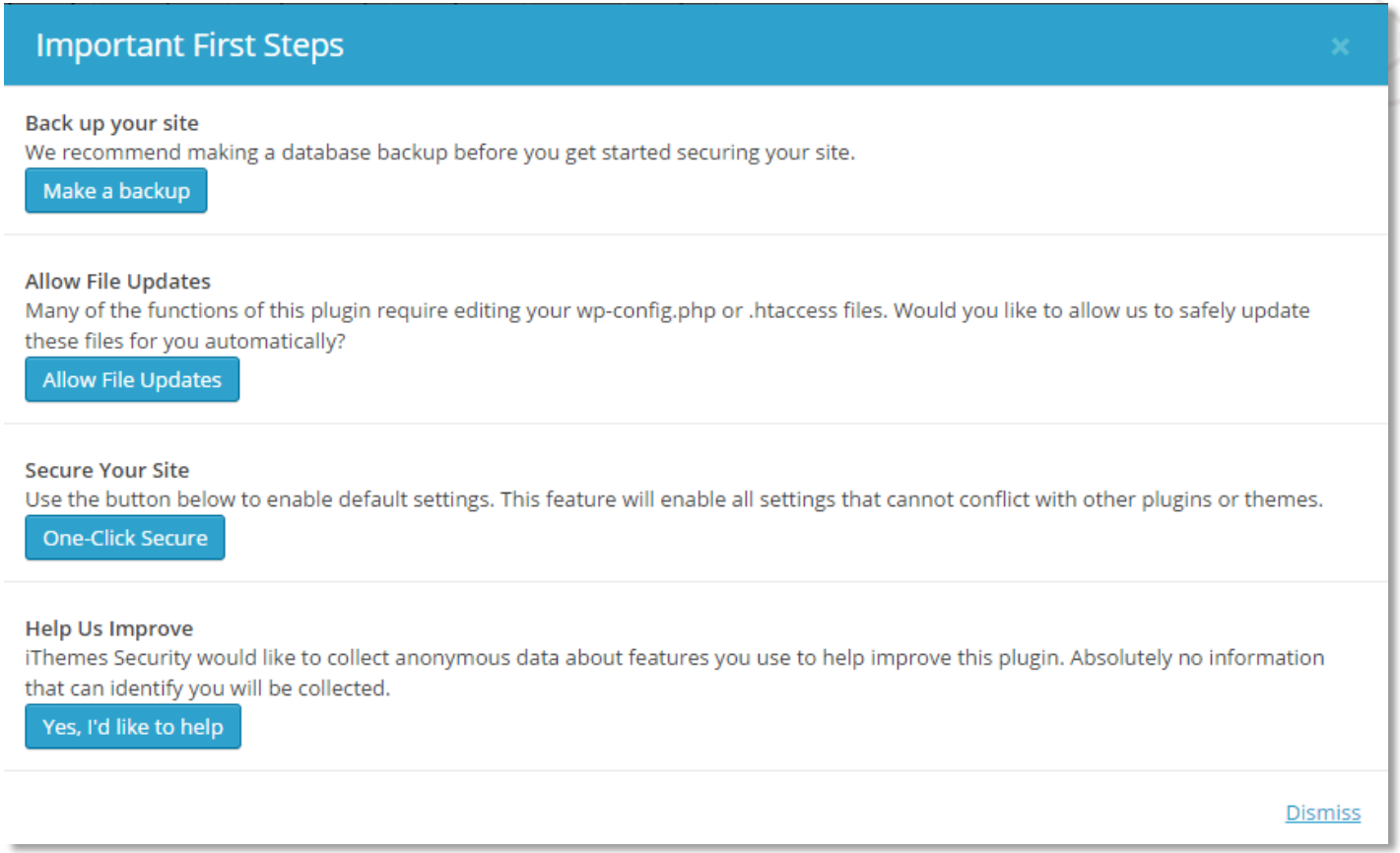
Bezpečnostní plugin

iThemes security

- **Prevence**
- Skrytí administrace, změna prefixu db
- Filtrace zlých URL dotazů

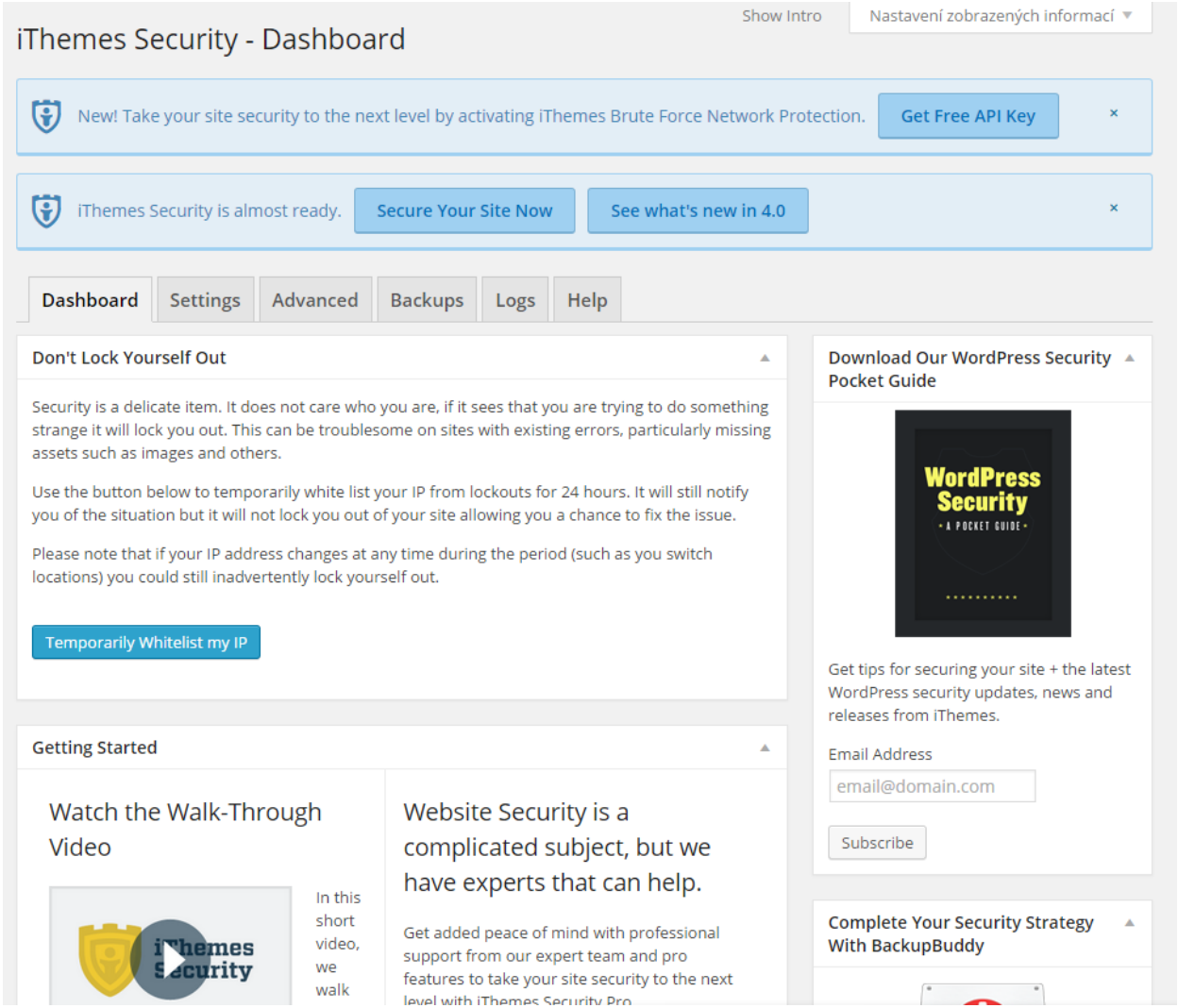
- Samozřejmě:
  - Blokace chybných pokusů o přihlášení a 404
  - Hlídání změn v souborech
  - Blokace komentářového spamu

iThemes Security – po instalaci



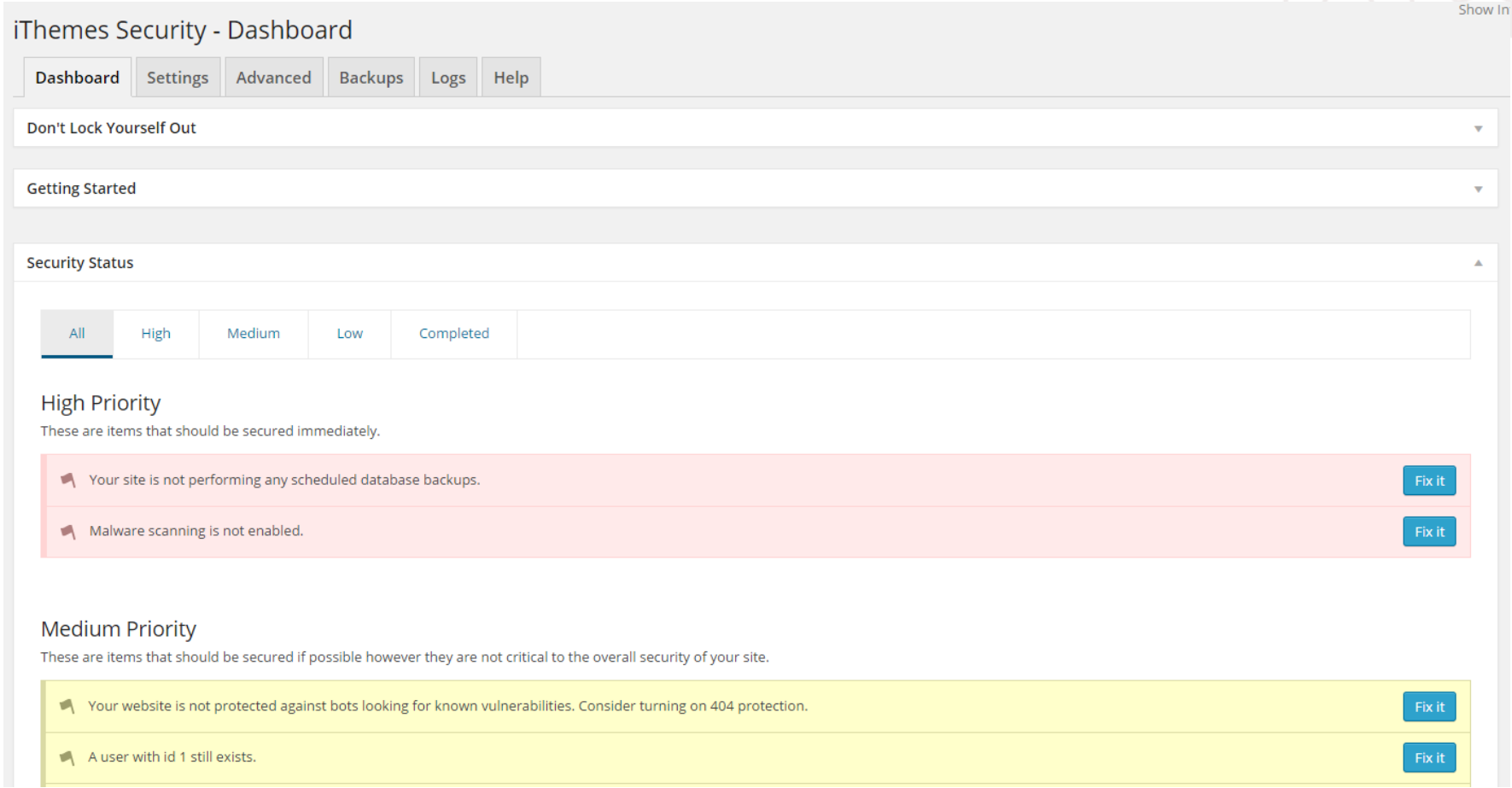
One-Click – nastaví omezení počtu přihlášení, vynutí silná hesla, skryje některé info

iThemes Security – API Key



Lynt SERVICES

iThemes Security - přehled



iThemes security - nastavení

- Global Settings
  - **Write to Files** - Allow iThemes Security to write to wp-config.php and .htaccess – pokud nepovolím, mohu příslušné sekce nakopírovat z dashboardu pluginu
  - **Lockout White List** – vhodné zadat svou IP
  - **Log Type** - Database Only (malé weby, log je pak dostupný na záložce Logs), File Only (velké weby, vhodné také pro zpracování fail2ban)
  - **Path to Log Files** - cesta k logům při File Only, pokud je možnost přístupu mimo složku webu, tak je umístit mimo, pokud ne, lze nechat výchozí (lépe ale jméno složky změnit)
- 404 detection
  - **Enable 404 detection** – zablokuje násilné skenování

Červené = dle mého názoru nejdůležitější nastavení

iThemes security - nastavení

- Away Mode - možno nastavit dostupnost administrace např. jen na pracovní dobu...
- Banned Users
  - **Default Blacklist** - Enable HackRepair.com's blacklist feature - možno povolit - přidá známé útočící useragenty do .htaccess
  - **Enable ban Users** - můžeme si dodefinovat vlastní blokované useragenty a IP (spolupracuje s Enable Blacklist Repeat Offender v Global settings)

iThemes security - nastavení

- Brute Force Protection
  - **Get your iThemes Brute Force Protection API Key** - iThemes získá přístup k globálnímu blacklistu útočících IP adres na iThemes.com
  - **Enable iThemes Brute Force Network Protection** – povolí ochranu dle globálního blacklistu
  - **Enable local brute force protection** - blokuje hádání hesel do administrace – tvoří vlastní blacklist (blokace jsou uloženy v tabulce _itsec_lockouts)
  - **Automatically ban "admin" user** - Immediately ban a host that attempts to login using the "admin" username - pokud mám přejmenovaného admina, tak to může být dobrá nástraha ☺ - jakmile se někdo pokusí přihlásit jako uživatel admin, je okamžitě zablokován

iThemes security - nastavení

- Database Backups
  - **Backup Method** - Email Only (bude posílat zálohu mailem), Save local only - pouze pokud mohu uložit zálohu mimo složku webu (Backup Location)
  - **Schedule Database Backups** - Enable Scheduled Database Backups – automatické vytváření záloh/jinak pouze ručně na záložce Backups
  - Zálohuje pouze DB. Raději bych použil jiné zálohovací řešení mimo WP i se soubory.

- File Change Detection
  - **File Change Detection** - Enable File Change detection
  - **Split File Scanning** - Split file checking into chunks – vhodné pokud mám méně RAM - generuje ale více emailů
  - **Files and Folders List** - pokud používáme cachovací plugin, tak je vhodné zde jeho složku vyjmout

- Hide Login Area
  - **Hide Backend**- Enable the hide backend feature – přesměruje /wp-admin na jinou adresu
  - **Login Slug** – nová adresa administrace - např. admin5547, nebo česky administrace
  - **Enable Theme Compatibility** - Enable theme compatibility – zapnout, pokud přesměrování administrace způsobí nefunkčnost některých šablon a pluginů
  - Přesměrování administrace je dobré dělat až v druhé vlně ladění - neprovádět více změn naráz

iThemes security - nastavení

- Malware Scanning
  - **Enable Malware scanning** - po vložení API klíče z VirusTotal.com může nechat jednorázově otestovat homepage, zda se nenachází na cca 60 blacklistech (Sucuri SiteCheck, Google Safebrowsing,...)
- Secure Soceket Layers (SSL)
  - nastavení pro vynucení SSL přístupu do administrace - vhodné nejprve otestovat, zda je administrace přes https správně dostupná
- Strong Passwords
  - **Strong Passwords** - Enable strong password enforcement - Vynutí používání silných hesel (původní slabá hesla zůstávají)
  - **Select Role for Strong Passwords** - pro jaké role vyžadujete silná hesla (minimálně Šéfredaktor – může vkládat JS do komentářů, ale klidně už od Návštěvníka)

iThemes security - nastavení

- System Tweaks
  - **System Files** - protect System Files - zakáže přístup z internetu přímo k důležitým souborům a k souborům, které prozrazují informace
  - **Suspicious Query Strings** - Filter Suspicious Query Strings in the URL - může zabránit jednoduchým SQL injections (pozor, chyba u nginx – viz další slidy)
  - **Long URL Strings** - Filter Long URL Strings - blokuje příliš dlouhé URL (nad 255 znaků), dále také blokuje URL obsahující funkce eval a base64 a union select (podobnou funkci plní samostatný plugin Block Bad Queries (BBQ))
    + **je dobré přidat blokaci query obsahující wp-config.php**
  - ~~**Non-English Characters**~~ - Filter Non-English Characters - v českém prostředí znefunkční vyhledávání s diakritikou
  - **File Writing Permissions** – nastaví práva pro .htaccess a wp-config.php – lepší si to nastavit sám a podrobněji
  - **Uploads** - Disable PHP in Uploads – zakáže PHP ve složce s uploady

iThemes security - nastavení

- System Tweaks
  - **Generator Meta Tag** + **Display Random Version** - pokusí se zamaskovat verzi WP, jde to udělat lépe – viz další slidy
  - **Windows Live Writer Header** & **EditURI Header** – hlavičky pro integraci s dalšími službami a aplikacemi – jsou potřeba jen zřídka
  - **Comment Spam** - kontroluje, zda byl komentář vložen z našeho webu (případně z wordpress.com) + blokuje komentáře od botů, kteří nemají vyplněn user-agent
  - **File Editor** – vypne editor šablon a pluginů ve WP (lze to jednoduše udělat v wp-config)
  - **XML-RPC** - při "Completely Disable XMLRPC" zakáže veškeré XML-RPC požadavky, např. trackbacky (pro bezpečné použití trackbacků mohu použít plugin https://wordpress.org/plugins/simple-trackback-validation-with-topsy-blocker/)
  - **Login Error Messages** - přestane ukazovat hlášky o chybném přihlášení
  - **Force Unique Nickname** - nutí uživatele zvolit jiný nickname než je jeho přihlašovací jméno (není tak přímo vidět uživatelský účet)
  - **Disable Extra User Archives** - skryje uživatele, kteří nepíšou články (admini,...)

iThemes security – další funkce

- „Pokročilé funkce“ – Advanced
  - **Admin user** – umožňuje přejmenovat uživatele admin na jiné, hůře odhadnutelné jméno
    - Lepší je vytvořit nového uživatele s admin právy, přihlásit se na něj a původního admina smazat (WP nabídne převedení jeho příspěvků na jiného uživatele)
  - **Change content directory** – přejmenování složky wp-content, může přinést problémy a brání pouze některým automatizovaným útokům (správnou složku lze jednoduše vyčíst z kódu stránky)
  - **Change database prefix** – pokud se nechal při instalaci default wp_, tak je možné ho zde změnit
    - Automatizovaný nástroj, ručně je to složitější

iThemes security – *poznámky na doma*

Suspicious Query Strings v Nginx:

```
set $susquery 0;
if ($args ~* "wp-config.php") { set $susquery 1; } #navíc blokace při pokusu stažení wp-config.php
if ($args ~* "\.\./") { set $susquery 1; }
if ($args ~* "\.(bash|git|hg|log|svn|swp|cvs)") { set $susquery 1; }
if ($args ~* "etc/passwd") { set $susquery 1; }
if ($args ~* "boot.ini") { set $susquery 1; }
if ($args ~* "ftp:") { set $susquery 1; }
if ($args ~* "http:") { set $susquery 1; }
if ($args ~* "https:") { set $susquery 1; }
if ($args ~* "(<|%3C).*script.*(>|%3E)") { set $susquery 1; }
if ($args ~* "mosConfig_[a-zA-Z_]{1,21}(=|%3D)") { set $susquery 1; }
if ($args ~* "base64_encode") { set $susquery 1; }
if ($args ~* "(%24&x)") { set $susquery 1; }
if ($args ~* "(&#x22;|&#x27;|&#x3C;|&#x3E;|&#x5C;|&#x7B;|&#x7C;|%24&x)"){ set $susquery 1; }
if ($args ~* "(127.0)") { set $susquery 1; }
if ($args ~* "(globals|encode|localhost|loopback)") { set $susquery 1; }
if ($args ~* "(request|insert|concat|union|declare)") { set $susquery 0; }
if ($args !~ "^loggedout=true"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($args !~ "^action=jetpack-sso"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($args !~ "^action=rp"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($http_cookie !~ "^.*wordpress_logged_in_.*$"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($http_referer !~ "^http://maps.googleapis.com(.*)$"){ set $susquery 0; } # <= špatná logika, má zde být ~*
if ($susquery = 1) { return 403; }
```

Přidání blokace wp-config.php do .htaccess:

```
RewriteCond %{QUERY_STRING} wp-config.php [NC,OR]
```

iThemes security – *poznámky na doma*

Lepší odstranění viditelnosti verze WP než v pluginu:

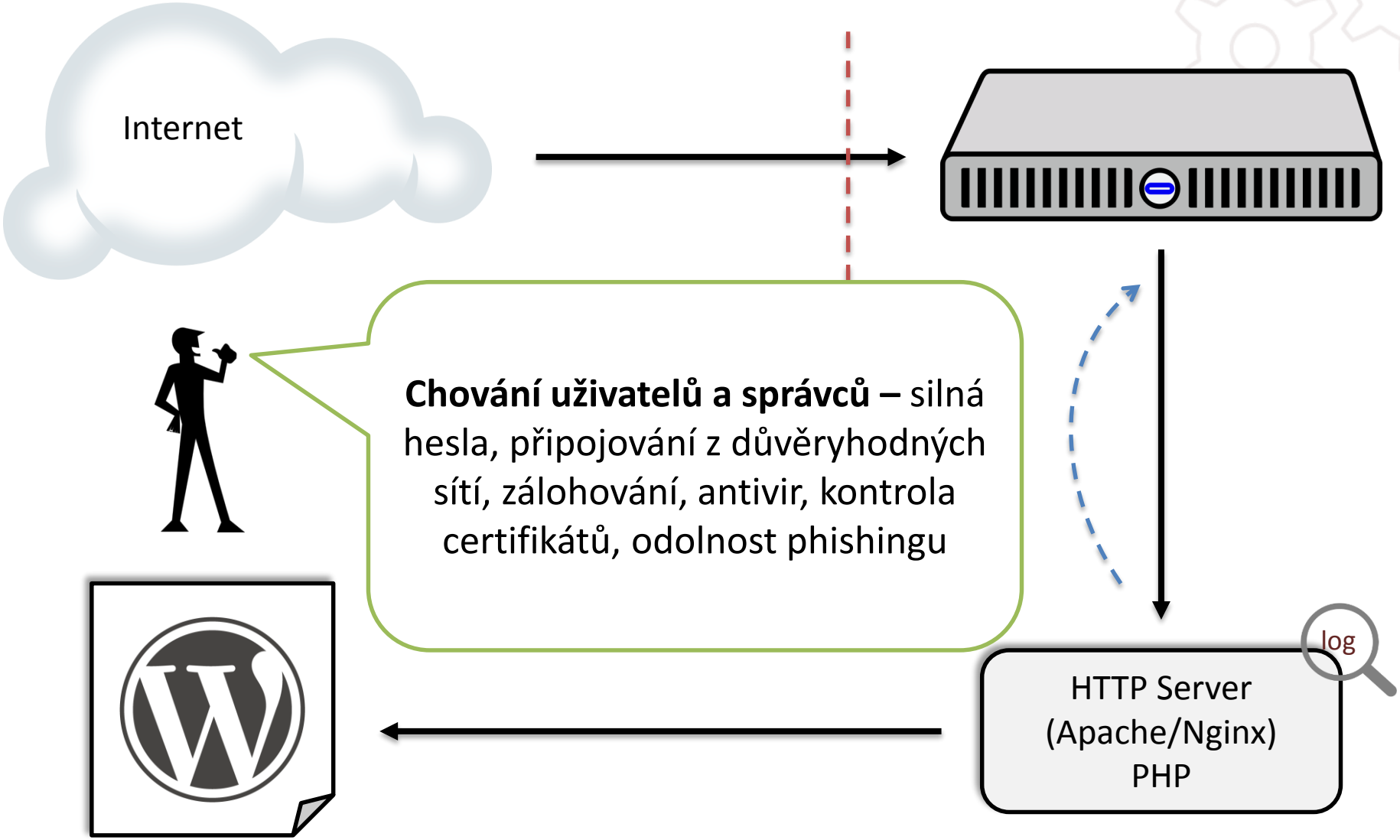
Do functions.php nebo plugin do mu-plugins:

```
function remove_wp_version()
{ return ; }
add_filter('the_generator', remove_wp_version');
```

Odbočka – MU-plugins (Must Use Plugins)
Málo známá funkcionalita WP – jedná se o speciální složku: **/wp-content/mu-plugins**
Skripty/pluginy v této složce jsou automaticky spouštěny a nelze je v administraci deaktivovat.
Hodí se to pro různá bezpečnostní nastavení, např. pokud chceme automatické updaty pluginů a šablon pomocí filtrů – mnoho autorů je dává do wp-config/functions.php – správně mají být zde.

```
add_filter( 'auto_update_plugin', '__return_true' );
add_filter( 'auto_update_theme', '__return_true' );
```

Uživatelé


Internet
Chování uživatelů a správců – silná hesla, připojování z důvěryhodných sítí, zálohování, antivir, kontrola certifikátů, odolnost phishingu
log
HTTP Server
(Apache/Nginx)
PHP

Tipy pro správce WP

- Nastavte přístup do administrace přes HTTPS
  - https://wordpress.org/plugins/wordpress-https/
  - dobrý je i přístup přes VPN, pokud je to možné
- Opravdu pravidelně zálohujte – soubory i databázi
- Netestujte pluginy na produkčním webu
- Smažte co nepotřebujete
- Přidělujte uživatelům oprávnění, která opravdu potřebují
- Pokud máte více webů, používejte systém pro hromadnou správu a aktualizaci (InfiniteWP, ManageWP), pokud méně použijte plugin WP Updates Notifier
- Udržujte si seznam všech použitých pluginů a šablon
- Pokud vám vývojář řekl: *„hlavně neaktualizuje“*, chtějte vědět proč (např. si vyžádejte patch soubory se změnami, co provedl), většinou k tomu není zásadní důvod!

Tipy pro každého

- Používejte silná hesla (používejte password manager např. Keepass)
- Pozor na špatné certifikáty: 

- Používejte kvalitní a aktualizovaný antivir
- Nepřipojujte se z neznámých WiFi
- Smažte z mobilu/tabletu/notebooku všechny uložené sítě, ke kterým se připojuje bez hesla
- Nedůvěřujte všemu, co přijde mailem

Phishing

Předmět: Máňa
Datum: Sat, 28 Feb 2015 14:32:48 +0200
Od: Máňa <mana@sezn.am>
Komu: <ty>

Dobrý den.

Omlouvám se za nežádoucí obtěžování a přeposílám Vám vaše doklady a smlouvu které asi na můj email byly zaslané omylem.

Teda aspoň předpokládám že přesměruji správně jelikož Váš email byl uvedený ve smlouvě.

Veškeré Doklady a smlouvu odesílám přílohou stejně jak jsem to dostala.

Prosím o zjištění důvodu tohoto trapného omylu aby příště na můj email se nedostávali další zprávy obsahující nějakou citlivou informaci.

S pozdravem,

Máňa

Phishing

Předmět: Bezpečnostní problém Hodný Hosting [9314001612]
Datum: Sat, 28 Feb 2015 14:32:48 +0200
Od: Hodný Hosting <hosting@hod.ny>
Komu: <ty>

Vážený zákazníku,

Na Vaší webové prezentaci tvujweb.cz založené na redakčním systému Wordpress byl zjištěna škodlivý kód, který masivně útočí na další weby a infikuje návštěvníky.

Neprodleně nainstalujte náš antivirový plugin Super-WP-Antivir, který naleznete v příloze i s návodem k instalaci. V opačném případě budeme bohužel nuceni Vaši webovou prezentaci pozastavit.

Hodný Hosting, Ltd.

Další zdroje

- Info o zranitelnostech
- https://www.owasp.org/
- https://wpvulndb.com/
- http://blog.sucuri.net/
- http://packetstormsecurity.com/

- Hodnocení pluginů:
- http://www.rankwp.com/

Domácí úkol na zítra

- Zkontrolovat, zda nemám zranitelné pluginy
- Zkontrolovat, zda mám vygenerované unikátní šifrovací klíče ve wp-config.php
- Zazálohovat
- Smazat pluginy, co nepoužívám/byly jen k jednorázové činnosti
- Smazat zbytečné šablony (nechat jen jednu výchozí z instalace a případně rodičovskou)
- Snížit oprávnění uživatelům, kteří jej nepotřebují
- Aktualizovat, co je možné

A to je vše, přátelé.

aktualizujte, zálohujte, používejte bezpečnostní plugin, buďte opatrní