

Vulnerabilis
Securis

Aghast

HOMO
Awarensis

Dexterous

OTRS

Evolve řešení incidentů v Cesnetu

Pavel Kácha, 2007
CESNET, z. s. p. o.

Historie

- postmaster@, hostmaster@, abuse@
- Mailbox
 - Problém Reply-To
- Později sdílený mailbox (IMAP)
 - Nutná striktní štábní kultura (1 RW, ostatní RO)
 - Nutné předávání služeb s popisy otevřených kauz
 - Problém vláken - kauzy rozsypané po mailboxu
 - Problém škálování na více osob

Co dál?

- Na většinu incidentů není třeba profesionální erudice
- Dostat incidenty do cíle rychleji
- 1. linie - Pracoviště stálé služby
 - Běžné mohou vyřídit sami, ostatní předat nám
- Musí tedy:
 - Rozeznat typ a závažnost incidentu
 - Identifikovat příslušného správce (tým)
 - Předat incident

Potřeby

- Whois (RIPE)
- Udržení mailů k jedné kauze pohromadě
- Informace o původcích akce
- Metadata (příslušnost k síti)
- Šablony pro předávání a odpovídání
- PGP, S/MIME
- Libre, nebo alespoň rozumně open source
- Ticketovací systém

Alternativy

OTRS, Trac, Mantis, RTIR, RoundUp,
Thunderbird + IMAP + extensions, Bugzilla,
Sirios, Issue Tracker, Issue Tracking Product,
Issue Management Tool, phpticket, batts,
Ticketsmith, whups, Keystone, phpSupport,
DCL, frontdesk, JitterBug, Teacup PRMS, CLC,
OcoMon, Techtables, PHPTasks, Gedeon,
WebCall, WREQ, PEST, oTasks, EdenCRM,
urqm, PHPHelpdesk, openTicket, BugIn,
PHPSAT, GNATS, IssueDealer...

Viz <http://www.cesnet.cz/doc/techzpravy/2006/tickets-review/>



[Odhlásit](#) [Náhled fronty](#) [Phone-Ticket](#) [Email-Ticket](#) [Vyhledat](#) [Nastavení](#) [Klient](#) [Bulk-Action](#) | [Statistiky](#) [Admin](#) [Nová zpráva \(0\)](#) [Locked Tickets \(0\)](#)

[Fronta: Misc]

Zobrazené tikety: 1-4 - Strana: [1](#) - Tiketů k dispozici: 4 - Všechny tikety: [4](#)

Řady: [My Queues \(2\)](#) - [Certs \(2\)](#) - [Certs-Masters \(2\)](#) - [Certs-Scrap \(37\)](#) - [MDS \(397\)](#) - [Misc \(4\)](#) - [Spam \(2533\)](#)

■ [Ticket#: 2006121447000031] Spam complaint from UOL
[1MAoO2sWT2230sj06ml]

[Stáří: 117 dní(dny) 10 hodin]

[Zámek](#) - [Zobrazit](#) - [Historie](#) - [Priorita](#) - [Poznámka](#) - [Zavřít](#)

Vytvořeno:14/12/2006 04:07:43

Od: abuse@support.juno.com
Komu: abuse@cesnet.cz
Předmět: Spam complaint from UOL [1MAoO2sWT2230sj06ml]

Stav: nová
Priorita: 3 normální
Fronta: Misc

ID klienta: [abuse@support\[.\]](#)
Stupňování žádné
v:
NETNAME: ZUOL-TCZ
IP: 195.113.148.186
ADMIN: abuse@zuol.cz

■ [Ticket#: 2006122347000078] [SpamCop (193.84.39.1)
id:2076348072]Delivery failure / chyb[.]

[Stáří: 107 dní(dny) 15 hodin]

[Zámek](#) - [Zobrazit](#) - [Historie](#) - [Priorita](#) - [Poznámka](#) - [Zavřít](#)

Vytvořeno:23/12/2006 23:47:51

Od: "Grant Ross" <2076348072@reports.spamcop.net>
Komu: abuse@cesnet.cz
Předmět: [SpamCop (193.84.39.1) id:2076348072]Delivery failure / chyba doručení

Stav: nová
Priorita: 3 normální
Fronta: Misc

ID klienta: [2076348072@rep\[.\]](#)
Stupňování žádné
v:
NETNAME: CZU-T34CZ
CZU-T34CZ
IP: 193.84.39.1
193.84.32.166[.]
ADMIN: abuse@czu.cz

■ [Ticket#: 2006122647000349] Reported spam originating
from 195.113.185.22

[Stáří: 104 dní(dny) 19 hodin]

[Zámek](#) - [Zobrazit](#) - [Historie](#) - [Priorita](#) - [Poznámka](#) - [Zavřít](#)

Vytvořeno:26/12/2006 19:43:23

Od: do-not-reply@abuso.cantv.net
Komu: abuse@cesnet.cz, abuse@hknet.cz, postmaster@hknet.cz
Předmět: Reported spam originating from 195.113.185.22

Stav: nová
Priorita: 3 normální
Fronta: Misc

ID klienta: [do-not-reply@a\[.\]](#)
Stupňování žádné
v:
NETNAME: HKNET-TCZ

OTRS - Výhody

- Pracuje přímo s poštou (ukládá MIME originál)
- Autentizace proti LDAP
- Metadata
- Dynamické šablony
- Stabilní identifikátory příslušnosti mailů
- Detailní log všech akcí
- PGP, S/MIME
- Perl

OTRS - Nevýhody

- Šablony pouze na Reply, ne na Forward
- Pouze Forward v těle zprávy
- Subject: Re/Fwd
- Ne právě oslňující výkon
- Živý projekt, ale málo vývojářů
- Fóra projektu obvykle pomohou jen se základními dotazy
- **Perl**

Stavy/Fronty

- Nový, Otevřený, Update
- Vyřešeno, Nevyřešeno
- Upozornění, IDS, Info
- Odpad, Organizační

- Certs - hlavní fronta
- Certs-Masters - my
- Certs-IDS - LaBrea
www.cesnet.cz/doc/techzpravy/2006/ids/
- Certs-Scrap - unusable complaint
- Spam, MDS

Pavel Kácha, CSIRT master of the day
CESNET Computer Security Incident Response Team
Zikova 4
160 00 Prague 6
The Czech Republic

Vážení kolegové,

CESNET Computer Security Incident Response Team obc
zprávu o nedoručitelnosti elektronické pošty ze str
147.33.15.5, který je ve Vaší správě.

Autorům stížnosti se nelíbí, že tyto zprávy neodmít
server už v průběhu SMTP konverzace: RCPT TO -> odp

Příloha: Browse... Připojit

Následující stav tiketu: 5 : 10

Doba čekání na vyřízení (pro stavy čekání na vyřízení*):

Jednotky času(jednotky práce):

- otevřít
- uzavřeno - vyřešeno
- uzavřeno - nevyřešeno
- otevřít
- uzavřeno - automat
- uzavřeno - hlášení IDS
- uzavřeno - jsme informováni
- uzavřeno - odpad
- uzavřeno - organizační
- uzavřeno - upozornění

IP harvesting

- Jak integrovat *whois*?
 - Webový? Speciální interface?
- OTRS je předřazen modul, který
 - Najde v mailu vše, co vypadá jako IP adresa
 - Zjistí, zda patří do rozsahů Cesnetu
 - Pokud ano, dotáže se RIPE na detaily
 - IP adresu, jméno sítě, adresu správce připojí jako metadata

IP harvesting II

- Při předání se příjemce doplní z metadat
- Více nebo žádná IP adresa - ruční zásah
 - Ale stává se minimálně
- PSS má tedy pro většinu incidentů potřebné informace připravené, pokud ne, předá nám

Od: Netvigator Postmaster <postmaster@netvigator.com>
Komu: abuse@cesnet.cz
Předmět: Spamming IP: 195.113.79.75
Vytvořeno: 06/04/2007 19:47:44

Dear Sir/Madam,

The spammer below is either using your resources to send out bulk unsolicited commercial e-mail ("spam") or is deceptively trying to make it look like he is. In either case, a legitimate company like yours probably would not approve. The information below should be all you need.

Please take the necessary actions to stop the spam.

Thanks for your cooperation !

Stupňování -
v:
Vlastník: andrea (Andrea Kropáčová)

Linked (Normální):
Linked (Parent):
Linked (Child):

NETNAME: UZSI-TCZ
IP: 195.113.79.75
ADMIN: abuse@uzsi.cz

Šablony pro předávání

- Vlastní úpravy, Forward přepsán
(snažíme se protlačit upstream)
- Nyní používá stejné šablony, jako Reply
- Doplnění příjemce z metadat
(abuse kontakt sítě)

Zvolený incident:

[OTRS] Pavel Kácha (ph@rook.cz) Thu May 03 11:43:04 2007

 [Logout](#)  [QueueView](#)  [Phone-Ticket](#)  [Email-Ticket](#)  [Search](#)  [Preferences](#)  [Customer](#)  [Bulk-Action](#) |  [Stats](#)  [Admin](#)  [New message](#) (0)  [Locked Tickets](#) (0)

[Queue: Certs]

Tickets shown: 1-3 - Page: [1](#) - Tickets available: 3 - All tickets: [3](#)

Queues: [My Queues \(7\)](#) - [Certs \(3\)](#) - [Certs-IDS \(4\)](#) - [Certs-Masters \(7\)](#) - [Certs-Scrap \(39\)](#) - [MDS \(410\)](#) - [Spam \(3147\)](#)

[Ticket#: 2007050247000101] [SpamCop (http://repeatmusic.hk/) id:2270535498]SPAM-LOW: D[...] [Age: 1 day 1 hour]

[Lock](#) - [Zoom](#) - [History](#) - [Priority](#) - [Note](#) - [Close](#)

Created:05/03/2007 08:18:34

From: "Jacob Chiong" <jacob@farexmarketing.com>
To: "Cesnet Certs" <certs@cesnet.cz>
Subject: Re: [Ticket#2007050247000101] [SpamCop (http://repeatmusic.hk/) id:2270535498]SP[.]

State: aktualizace
Priority: 3 normal
Queue: Certs

CustomerID: 2270535498@rep[...]
Escalation none
in:
NETNAME: UPOL-TCZ
IP: 158.194.183.102
ADMIN: abuse@upol.cz

[Ticket#: 2007050347000153] [SpamCop (http://puusn.payhold.hk/?804331472279) id:22717048[...] [Age: 1 hour 0 minute]

[Lock](#) - [Zoom](#) - [History](#) - [Priority](#) - [Note](#) - [Close](#)

Created:05/03/2007 10:42:57

From: 2271704881@reports.spamcop.net
To: abuse@cesnet.cz
Subject: [SpamCop (http://puusn.payhold.hk/?804331472279) id:2271704881]\$1.59 a pill is t[.]

State: new
Priority: 3 normal
Queue: Certs

CustomerID: 2271704881@rep[...]
Escalation none
in:
NETNAME: UPOL-TCZ
IP: 158.194.183.102
ADMIN: abuse@upol.cz

Posouzení a výběr šablony:

[Zoom Ticket#: 2007050347000153] [SpamCop (<http://puusn.payhold.hk/?804331472279>) id:22717048[.]

[Age: 1 hour 2 minutes]

[Back](#) - [Lock](#) - [History](#) - [Print](#) - [Priority](#) - [Free Fields](#) - [Link](#) - [Owner](#) - [Customer](#) - [Note](#) - [Merge](#) - [Pending](#) - [Close](#)

Created:05/03/2007 10:42:57

|-->>> **1. customer (email-external) (plain) 2271704881@repor[.]: [SpamCop ([http://puu\[.\]](http://puu[.]))-05/03/2007 10:42:57**

From: 2271704881@reports.spamcop.net
To: abuse@cesnet.cz
Subject: [SpamCop (<http://puusn.payhold.hk/?804331472279>) id:2271704881]\$1.59 a pill is the best price for V1agr@ ever pro..
Created: 05/03/2007 10:42:57

[SpamCop V630]

This message is brief for your comfort. Please use links below for details.

Spamvertised web site:

<http://puusn.payhold.hk/?804331472279> [#####
#####2]<http://puusn.payhold.hk/?804331472279> is
158.194.183.102; Thu, 03 May 2007 08:42:40 GMT

[Offending message]

Return-Path: <Melinda@vc.netyou.jp>

X-Spam-Flag: YES

X-Spam-Checker-Version: SpamAssassin 3.1.5 (2006-08-29) on
bpa09de.bpaserver.net

X-Spam-Level: *****

X-Spam-Status: Yes, score=31.6 required=5.0 tests=DRUGS_ERECTILE,
DRUGS_ERECTILE_OBFU,FUZZY_VPILL,HELO_DYNAMIC_HCC,HTML_IMAGE_ONLY_16,
HTML_MESSAGE,HTML_SHORT_LINK_IMG_2,MIME_HTML_MAIN,MIME_HTML_MAIN,
PART_CID_STOCK,PART_CID_STOCK_LESS,RAZOR2_CF_RANGE_51_100,
RAZOR2_CF_RANGE_E4_51_100,RAZOR2_CF_RANGE_E8_51_100,RAZOR2_CHECK,
STOCK_IMG_HDR_FROM,STOCK_IMG_HTML,SUBJ_DOLLARS,TVD_FW_GRAPHIC_ID1,
URIBL_BLACK,URIBL_JP_SURBL,URIBL_OB_SURBL,URIBL_SC_SURBL
autolearn=disabled version=3.1.5

X-Spam-Report:

* 3.3 HELO_DYNAMIC_HCC Relay HELO'd using suspicious hostname (HCC)
* 0.4 SUBJ_DOLLARS Subject starts with dollar amount

State: new
Priority: 3 normal
Queue: Certs
Locked: unlock
CustomerID: 2271704881@reports[.]
Accounted 0
time:
Escalation -
in:
Owner: root@localhost (Admin OTRS)

Linked
(Normal):
Linked
(Parent):
Linked
(Child):

NETNAME: UPOL-TCZ
IP: 158.194.183.102
ADMIN: abuse@upol.cz

Customer Info:

Compose Answer (email):

- ◆ [Empty](#)
- ◆ [FWD upozornění - Abuse](#)
- ◆ [FWD upozornění - Bounce](#)
- ◆ [FWD upozornění - Spam](#)

Volba stavu a předání incidentu:

From: Cesnet Certs <certs@cesnet.cz>
To: 2271704881@reports.spamcop.net
Cc:
Bcc:
Subject: Re: [Ticket#2007050347000153] [SpamCop (http://puusn.payhold.hk/?804331472279) id
Options: [[Address Book](#)] [[Attachments](#)]
Text:
Dear Administrator,

the CESNET Computer Security Incident Response Team has received attached e-mail notice regarding spam abuse originating at computer 158.194.183.102 which belongs to your network/domain.

Would you please check the integrity of this computer and solve the problem (if any) as soon as possible?

With best regards

Attachment:

Next ticket state:
closed successful
closed unsuccessful
open
uzavřeno - automat
uzavřeno - hlášení IDS
uzavřeno - jsme informováni
uzavřeno - odpad
uzavřeno - organizační
uzavřeno - upozornění

Pending Date (for pending* states):

Time units (work units):

https://rt.cesnet.cz/otrs-2.1.2...&ResponseID=4&TicketID=9758&ArticleID=11...

Archivace

- Maily v databázi v původní podobě
- Veškerá komunikace může být součástí ticketu
 - Komunikace - vnější i vnitřní
 - Poznámky k řešení
 - Přílohy (výpisy z logů, forenzní data)
- Fulltextové prohledávání
- Dělení i slučování ticketů

Spam

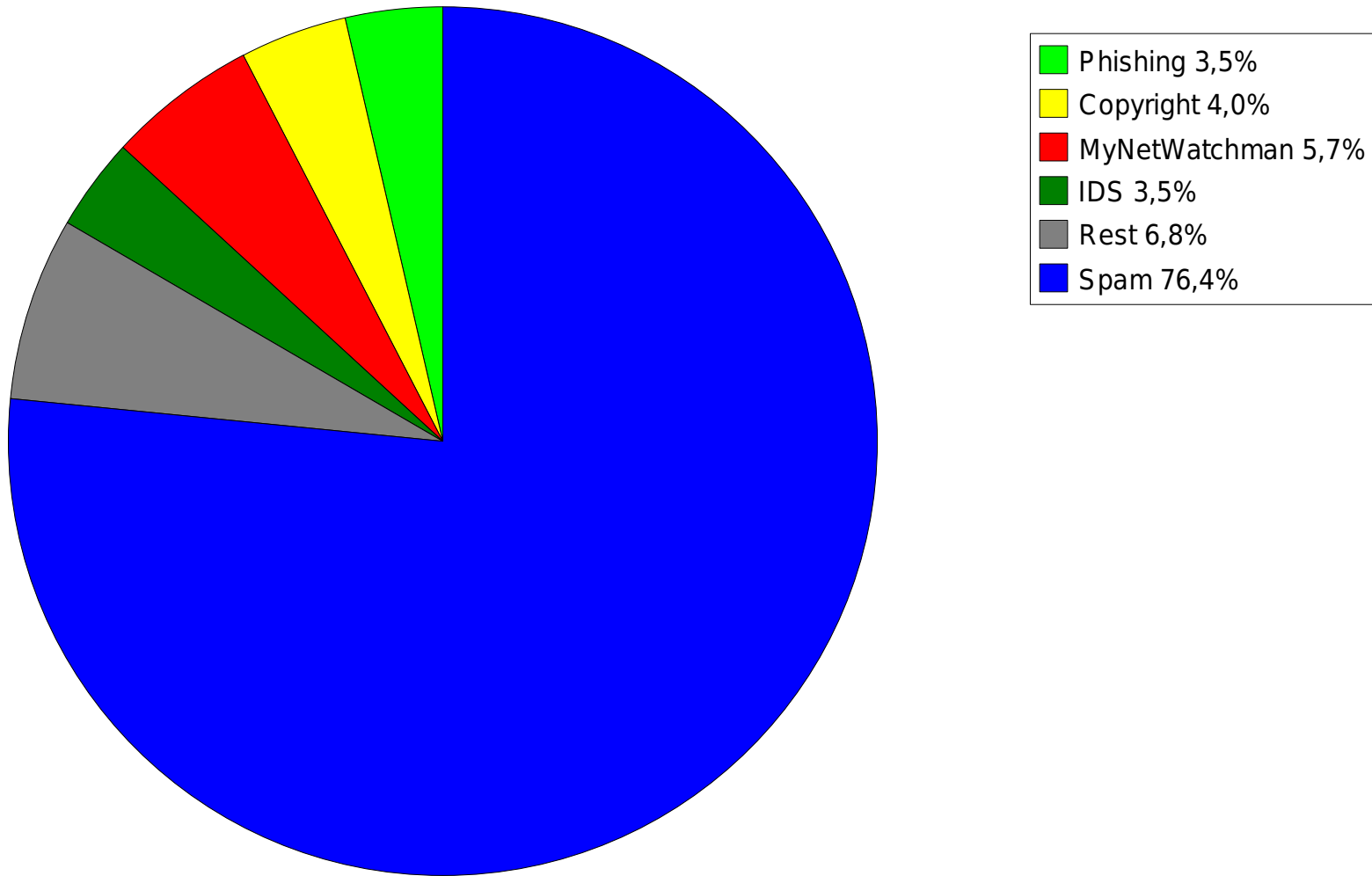
- SpamAssassin...
 - ... ale hlášení o incidentu může vzorek spamu obsahovat a tedy být jako spam označeno!
- Whitelist na klíčová slova

```
/abuse mail|abuse-mail|abuse of|abuse report|abuse spam|  
e-mail spam|multiple spam|received spam|report abuse|  
reported spam|reporting spam|returned spam|spam:|spam  
abuse|spam complaint|spamcop|spam from|spam mail|  
spammails|spam mails|spammer|spamming|spam-rbl|stop the  
spam|ube:|ube-uce|ube\/uce|uce:|uce-ube|uce\/ube|ube  
from|uce from|\[uce\]|\[spam\]|spam received|uce  
complaint|ube complaint|phish|fraud/
```

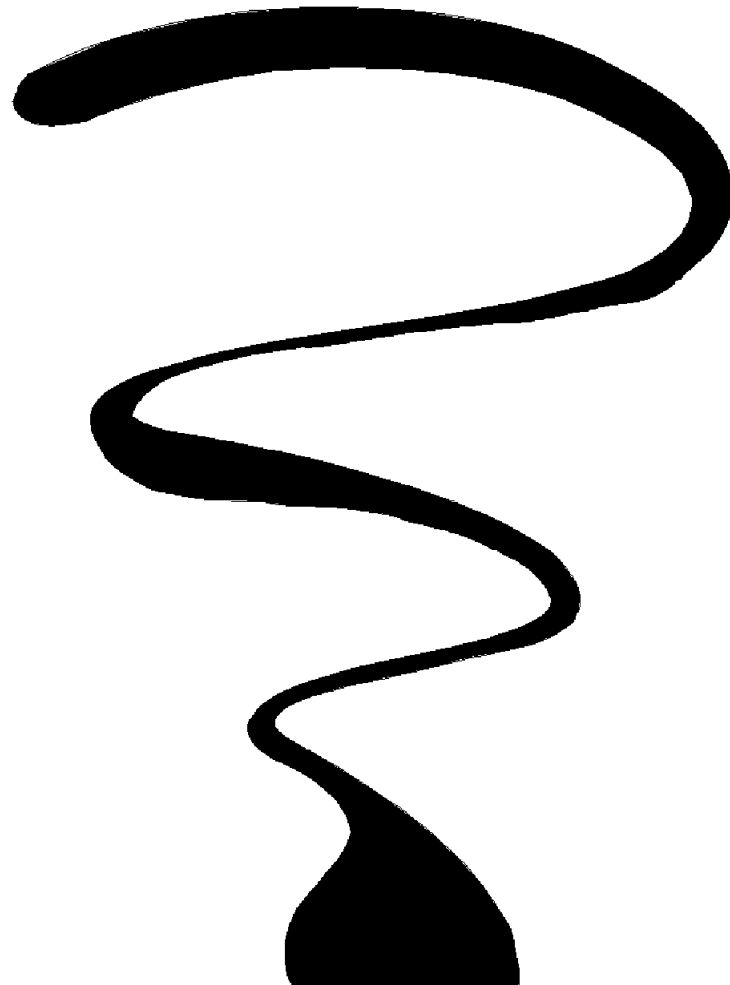
Užitečné

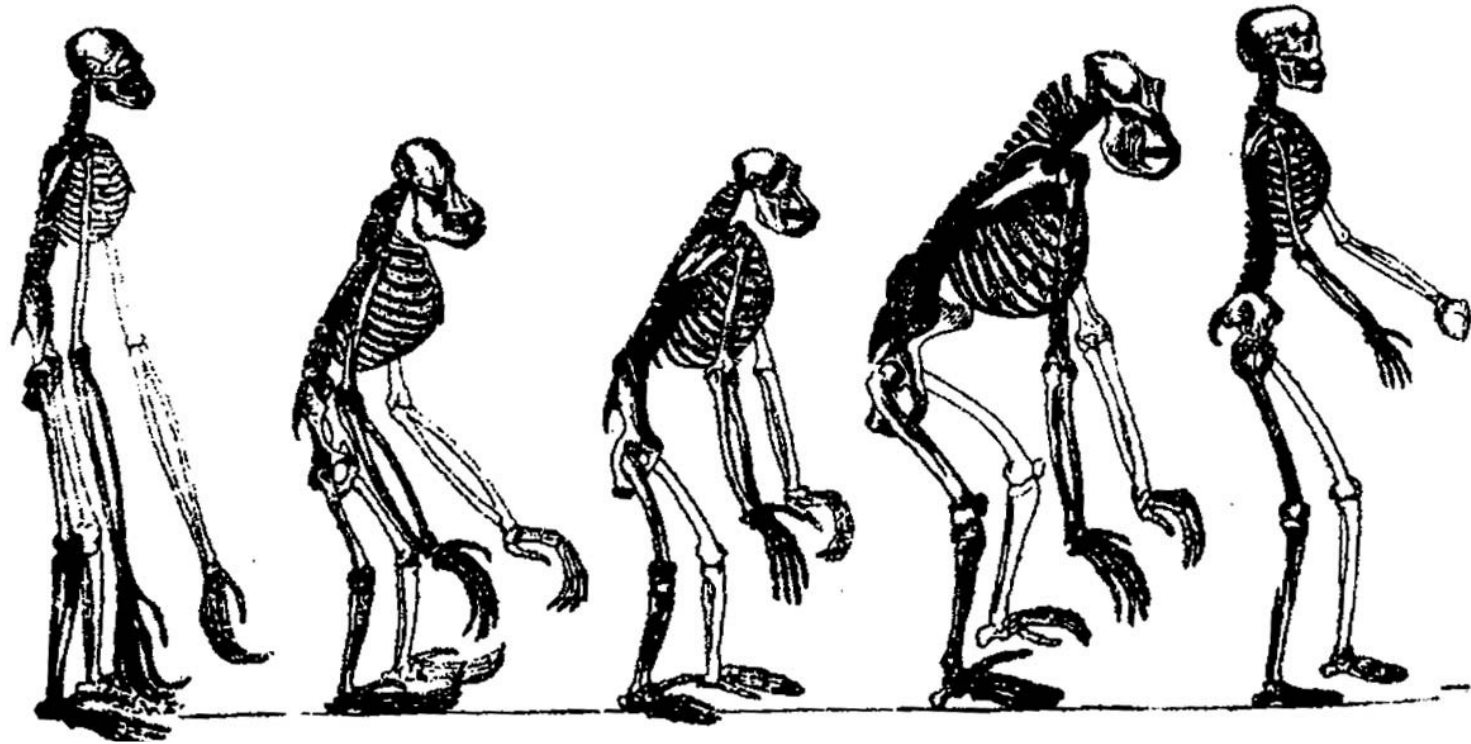
- Podepisujeme PGP
- Jsme schopni ověřit a dešifrovat PGP i S/MIME
- FollowUpSearchIn*
(páruje i návratovky)
- Komplexní, ale průhledný databázový model
 - Např. statistika je otázkou několika šikovních SQL dotazů
 - Plánujeme detekci opakovaných stížností
 - Plánujeme automatickou eskalaci neřešených

Typy incidentů v roce 2007



Dotazy





Big Bang

Pine

My a OTRS

Stálá služba
a OTRS

My na
Havaji

Děkuji za pozornost