Zkvalitnění procesu řešení bezpečnostních incidentů v síti WEBnet

FR Cesnet 369/2010

Radoslav Bodó <bodik@civ.zcu.cz> <bodik@cesnet.cz>

Michal Kostěnec <kostenec@civ.zcu.cz>

Úvod

- Proces řešení bezpečnostních incidentů ve WEBnetu je standardizován a dokumentován – Provozní řády LPS
- Administrátoři sítě však nemají plnou kontrolu nad všemi koncovými zařízeními
    - Pro vyřešení incidentu je potřeba kontaktovat lokálního správce a zjistit od něj identitu uživatele (campus)
    - Manipulaci s agendami (RT, WHOIS, Eduroam, …) bylo nutné provádět ručně
    - Blokování zařízení bylo možné vypnutím příslušného access portu > uživatel nepozná rozdíl od chyby ...

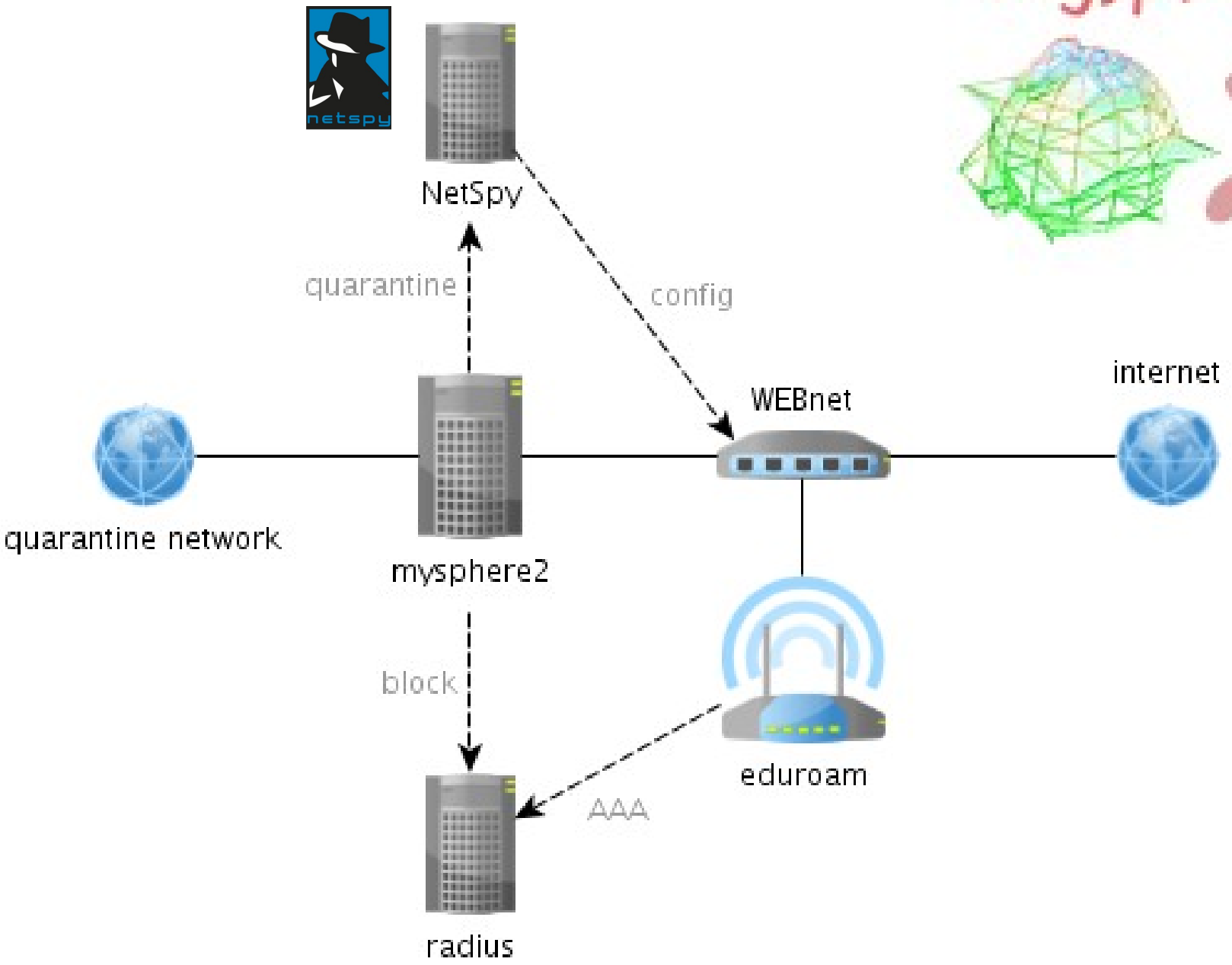
Úvod a cíle

- Cíle projektu
  - Vypracovat nástoj, který by pro pracovníky WIRT automatizoval některé úkony spojené s procesem řešení (emaily, blokování, …)
  - Najít způsob jak informovat uživatele přímo (jakoby obejít lokálního správce)
  - Neodpojovat zařízení úplně, ale raději vhodně omezi provoz
    - Dodat nástroje a informace pro správnou reakci na incident

Řešení – Mysphere2

- Nechceme uživatele odpojovat, ale omezovat, aby mohl pomocí počítače stále získat informace a měl k dispozici nástroje pro řešení incidentu
  - KDC/AD, AFS, LDAP – login
  - support.zcu.cz, phone.zcu.cz, webmail.zcu.cz – info
  - FAI, ftp.zcu cz, downaload.zcu.cz, EPO – reinstall
  - Všechno ostatní je zahozeno
  - **Všechen ostatní web je přesměrován ...**

Analýza – Navržené řešení



Mysphere2 - virus

Mysphere2: Automat pro správu bezpečnostních incidentů [studentx]

Tento počítač byl odpojen od sítě WEBnet

Přístup na požadovanou stránku http://www.ubal.to/... Vám byl z bezpečnostních důvodů odepřen.

Bylo detekováno nevhodné chování tohoto počítače (ui505p02-lps.civ.zcu.cz :: 147.228.53.147), které indikuje jeho napadení virem nebo jiné zneužití. Konkrétně rozesílá vysoké množství nevyžádaných zpráv. Pro opětovné odblokování, prosím, postupujte jednou z následujících možností:

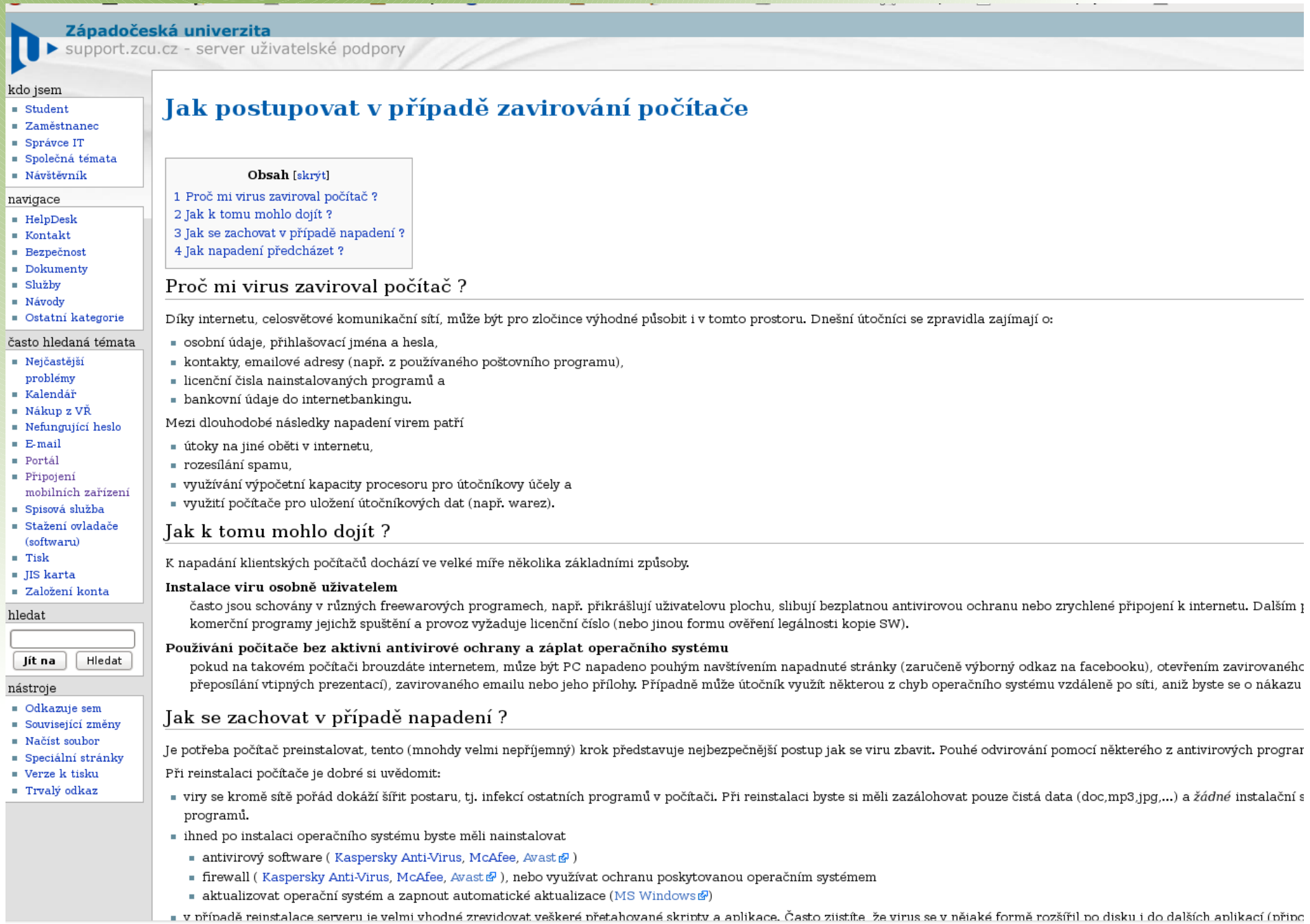
A. Kontaktujte, prosím, svého lokální správce (support.zcu.cz - Seznam lokálních správců), který zařídí nápravu.

B. Uveďte počítač do vhodného stavu svépomocí dle návodu support.zcu.cz - Jak postupovat v případě zavirování počítače.
Po reinstalaci nebo odvirování připojte nezávadný stroj do sítě a vyplňtě žádost o odblokování.
Odblokování je možno provést ihned po odpojení závadného stroje od sítě, není tedy třeba čekat na přeinstalaci (bude se hodit např. je-li do zásuvky připojen switch, který je využíván více stroji).

I přes blokování jsou pro vyřešení problému stále dostupné vybrané informační systémy:

- https://webmail.zcu.cz
- http://support.zcu.cz

Support.zcu.cz – virus



Západočeská univerzita
support.zcu.cz - server uživatelské podpory

kdo jsem
- Student
- Zaměstnanec
- Správce IT
- Společná témata
- Návštěvník

navigace
- HelpDesk
- Kontakt
- Bezpečnost
- Dokumenty
- Služby
- Návody
- Ostatní kategorie

často hledaná témata
- Nejčastější problémy
- Kalendář
- Nákup z VŘ
- Nefungující heslo
- E-mail
- Portál
- Připojení mobilních zařízení
- Spisová služba
- Stažení ovladače (softwaru)
- Tisk
- JIS karta
- Založení konta

hledat
Jít na | Hledat

nástroje
- Odkazuje sem
- Související změny
- Načíst soubor
- Speciální stránky
- Verze k tisku
- Trvalý odkaz

Jak postupovat v případě zavirování počítače

Obsah [skrýt]
1 Proč mi virus zaviroval počítač ?
2 Jak k tomu mohlo dojít ?
3 Jak se zachovat v případě napadení ?
4 Jak napadení předcházet ?

Proč mi virus zaviroval počítač ?

Díky internetu, celosvětové komunikační síti, může být pro zločince výhodné působit i v tomto prostoru. Dnešní útočníci se zpravidla zajímají o:

- osobní údaje, přihlašovací jména a hesla,
- kontakty, emailové adresy (např. z používaného poštovního programu),
- licenční čísla nainstalovaných programů a
- bankovní údaje do internetbankingu.

Mezi dlouhodobé následky napadení virem patří

- útoky na jiné oběti v internetu,
- rozesílání spamu,
- využívání výpočetní kapacity procesoru pro útočníkovy účely a
- využití počítače pro uložení útočníkových dat (např. warez).

Jak k tomu mohlo dojít ?

K napadání klientských počítačů dochází ve velké míře několika základními způsoby.

Instalace viru osobně uživatelem
často jsou schovány v různých freewarových programech, např. přikrášlují uživatelovu plochu, slibují bezplatnou antivirovou ochranu nebo zrychlené připojení k internetu. Dalším p
komerční programy jejichž spuštění a provoz vyžaduje licenční číslo (nebo jinou formu ověření legálnosti kopie SW).

Používání počítače bez aktivní antivirové ochrany a záplat operačního systému
pokud na takovém počítači brouzdáte internetem, může být PC napadeno pouhým navštívením napadnuté stránky (zaručeně výborný odkaz na facebooku), otevřením zavirovaného
přeposílání vtipných prezentací), zavirovaného emailu nebo jeho přílohy. Případně může útočník využít některou z chyb operačního systému vzdáleně po síti, aniž byste se o nákazu

Jak se zachovat v případě napadení ?

Je potřeba počítač preinstalovat, tento (mnohdy velmi nepříjemný) krok představuje nejbezpečnější postup jak se viru zbavit. Pouhé odvirování pomocí některého z antivirových prograr

Při reinstalaci počítače je dobré si uvědomit:

- viry se kromě sítě pořád dokáží šířit postaru, tj. infekcí ostatních programů v počítači. Při reinstalaci byste si měli zazálohovat pouze čistá data (doc,mp3,jpg,...) a *žádné* instalační s programů.
- ihned po instalaci operačního systému byste měli nainstalovat
  - antivirový software (Kaspersky Anti-Virus, McAfee, Avast)
  - firewall (Kaspersky Anti-Virus, McAfee, Avast), nebo využívat ochranu poskytovanou operačním systémem
  - aktualizovat operační systém a zapnout automatické aktualizace (MS Windows)
- v případě reinstalace serveru je velmi vhodné zrevidovat veškeré přetahované skripty a aplikace. Často zjistíte, že virus se v nějaké formě rozšířil po disku i do dalších aplikací (přípc

Mysphere2 - virus

Mysphere2: Automat pro správu bezpečnostních incidentů [studentx]

INFO: Přihlášení bylo úspěšné

Reagovat na incident (sphr2 I#119)

Bylo detekováno nevhodné chování tohoto počítače (ui505p02-lps.civ.zcu.cz :: 147.228.53.147), které indikuje jeho napadení virem nebo jiné zneužití. Konkrétně rozesílá vysoké množství nevyžádaných zpráv. Po odvirování stroje můžete použít níže uvedený formulář nebo https://webmail.zcu.cz a dát nám vědět, že byl incident vyřešen a jakým způsobem.

1. Kontaktním formulářem

Vyberte prosím provedenou akci:

- Stroj byl zbaven virové nákazy
- Stroj byl přeinstalován
- Stroj byl odpojen od sítě, jedná se o sdílenou zásuvku
- Jiná akce, prosím uveďte jaká

Odeslat

2. Kontaktovat lokálního správce

V případě problémů, můžete kontaktovat lokálního správce. Jejich seznam naleznete na adrese support.zcu.cz - Seznam lokálních správců.

- https://webmail.zcu.cz
- http://phone.zcu.cz

3. Ručně emailem

Přihlaste k systému https://webmail.zcu.cz a zašlete nám zprávu na **abuse@zcu.cz** ručně. Zprávu formulujte podle vzoru:

```
Subject: [ZCU RT3 #131555] [sphr2#119] ui505p02-lps.civ.zcu.cz - napadený stroj
AddRequestor: studentx@civ.zcu.cz

Text nad tímto řádkem ignorujte, následuje sdělení pro uživatele...
Please ignore lines above, message for user follows ...
---------------------

Dobry den, chtel bych pozadat o odblokovani pripojeni pro stroj
ui505p02-lps.civ.zcu.cz (147.228.53.147).

    A) Stroj byl zbaven virové nákazy. (cleaned)
    B) Stroj byl přeinstalován. (reinstalled)
    C) Stroj byl odpojen od sítě, jedná se o sdílenou zásuvku. (shareduplink)
    D) Jiná akce, prosíme uveďte jaká. (other)

S pozdravem
Jmeno Prijmeni
Orion login
```

4. HelpDesk CIV

V případě problémů, můžete kontaktovat HelpDesk CIV .

Mysphere2 - p2p

Mysphere2: Automat pro správu bezpečnostních incidentů [nikdo]

Tento počítač byl odpojen od sítě WEBnet

Přístup na požadovanou stránku http://www.ubal.to/...
Vám byl z bezpečnostních důvodů odepřen.

Z tohoto počítače (ui505p02-lps.civ.zcu.cz :: 147.228.53.147) byla sdílena autorská díla pomocí P2P sítě, což vedlo ke stížnosti od společnosti bodik. Pro obnovení připojení je nutná Vaše návštěva CIV.

A. Domluvte si schůzku s pracovníky CIV prostřednictvím webového formuláře a vyčkejte na potvrzení vybraného termínu.

I přes blokování jsou pro vyřešení problému stále dostupné vybrané informační systémy:

- https://webmail.zcu.cz

Mysphere2 - p2p

Mysphere2: Automat pro správu bezpečnostních incidentů [studentx]

INFO: Přihlášení bylo úspěšné

Reagovat na incident (sphr2 I#119)

Z tohoto počítače (ui505p02-lps.civ.zcu.cz :: 147.228.53.147) byla sdílena autorská díla pomocí P2P sítě, což vedlo ke stížnosti od společnosti bodik. Pro obnovení připojení je nutná Vaše návštěva CIV.

1. Kontaktním formulářem

Po odeslání formuláře vyčkejte na potvrzení vybraného termínu, které Vám zašleme emailem https://webmail.zcu.cz

Dobrý den, rád bych si s Vámi smluvil schůzku ohledně incidentu [sphr2#119]
K pohovoru se mohu dostavit kterýkoli den, nejlépe vsak

DD.MM.YYYY v HH:II.

Upřesněte, prosím tedy termín, kdy se mám dostavit.

S pozdravem
Jmeno Prijmeni

Odeslat

2. Kontaktovat lokálního správce

V případě problémů, můžete kontaktovat lokálního správce. Jejich seznam naleznete na adrese support.zcu.cz - Seznam lokálních správců.

- https://webmail.zcu.cz
- http://phone.zcu.cz

3. Ručně emailem

Přihlaste k systému https://webmail.zcu.cz a zašlete nám zprávu na **abuse@zcu.cz** ručně. Zprávu formulujte podle vzoru:

Subject: [ZCU RT3 #131555] [sphr2#119] Pohovor s pracovniky CIV - Test Konto NENI_PRACOVISTE
AddRequestor: studentx@civ.zcu.cz

Text nad timto řádkem ignorujte, následuje sdělení pro uživatele...
Please ignore lines above, message for user follows ...

Dobrý den, rád bych si s Vámi smluvil schůzku ohledně incidentu [sphr2#119]
K pohovoru se mohu dostavit kterýkoli den, nejlépe vsak

DD.MM.YYYY v HH:II.

Upřesněte, prosím tedy termín, kdy se mám dostavit.

S pozdravem
Jmeno Prijmeni
Orion login

4. HelpDesk CIV

V případě problémů, můžete kontaktovat HelpDesk CIV .

I přes blokování jsou pro vyřešení problému stále dostupné vybrané informační systémy:

Mysphere2 – notfound

Mysphere2: Automat pro správu bezpečnostních incidentů [nikdo]

Tento počítač byl odpojen od sítě WEBnet

Přístup na požadovanou stránku ... Vám byl z bezpečnostních důvodů odepřen.

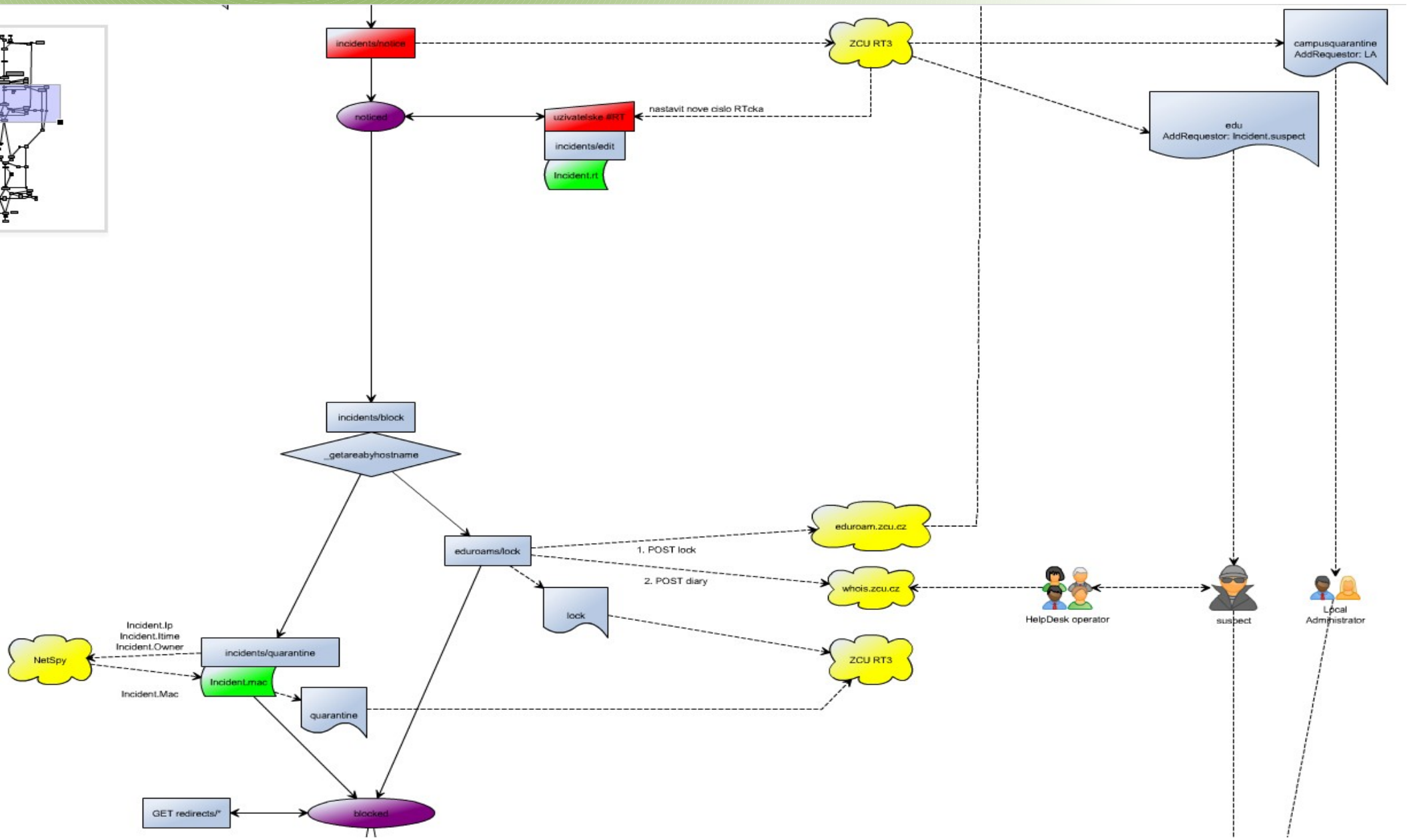
Pro tento počítač nebyl nalezen incident, pravděpodobně je vaše připojení sdílené s počítačem, který je napaden virem nebo generuje nevhodnou síťovou komunikaci a vaše připojení bylo proto omezeno.

A. Pro opětovnou aktivaci se obraťtě se na Vašeho lokálního správce, jejich seznam naleznete na adrese **support.zcu.cz - Seznam lokálních správců**.

I přes blokování jsou pro vyřešení problému stále dostupné vybrané informační systémy:

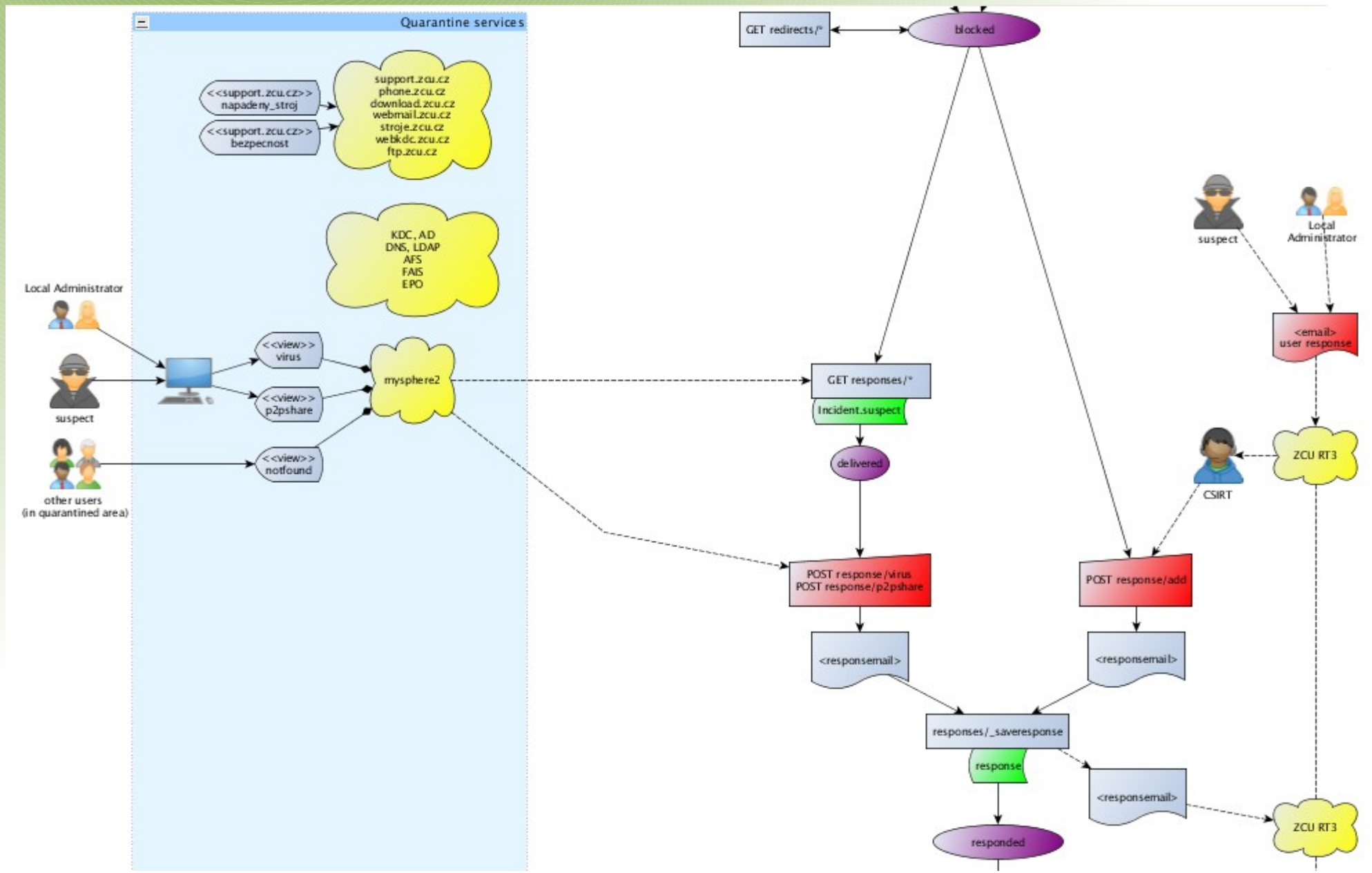
Řešení – Mysphere2 a administrátor

- Po založení a obeslání následuje umístění do karantény, ale WEBnet není jenom campus, ale také Eduroam. Mysphere2 zvládá i eduroam (blokovat konto, IP jsou sdílená)



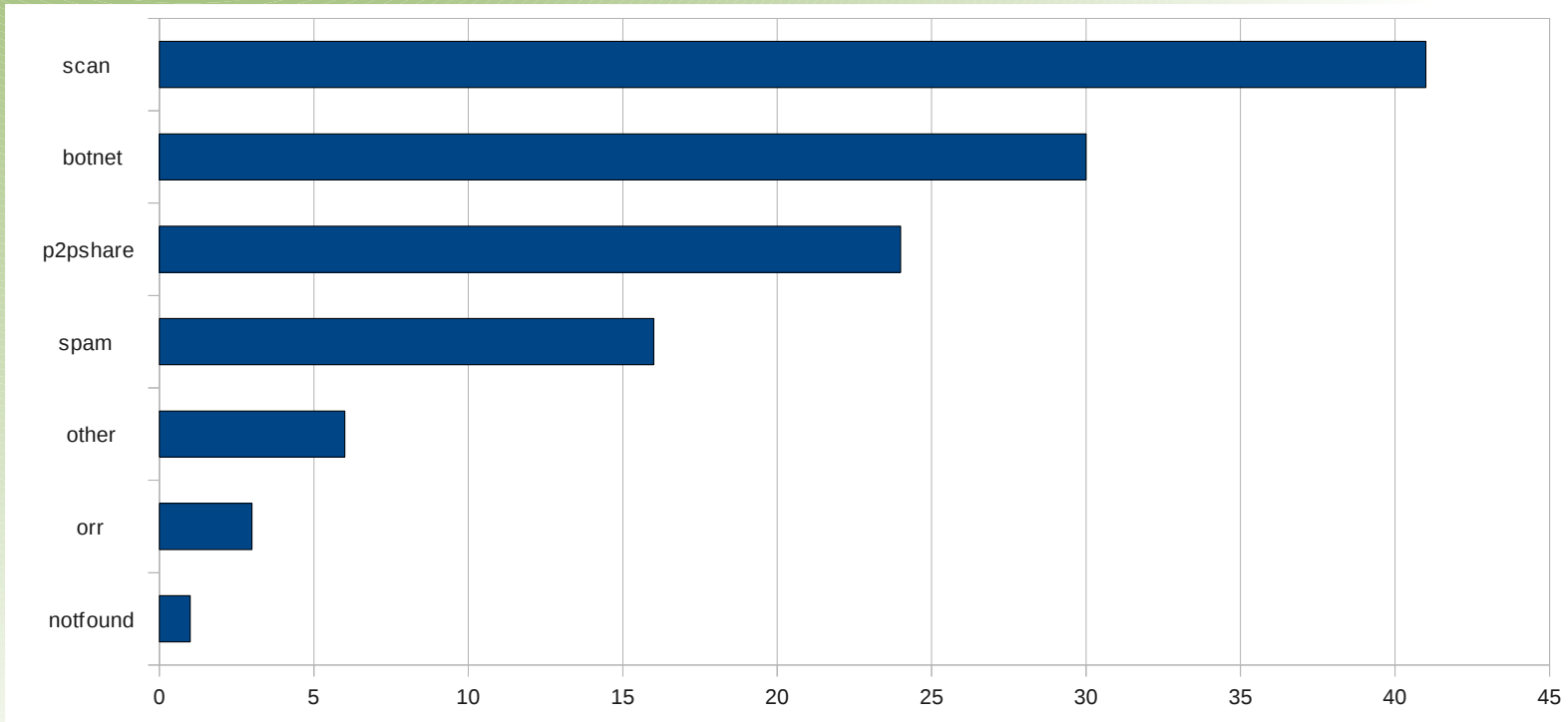
Řešení – Mysphere2 a administrátor

- … a zbývá čekat …



Shrnutí výsledků

- Řešili jsme 70 incidentů



Shrnutí výsledků

- Řešili jsme 70 incidentů
  - TTUI – Time to user informated
  - TTFR – Time to (user) first reaction
  - TTR – Time to incident resolution

	TTIU [m]	TTFR [m]	TTR [m]
Bez `mysphere2`			
Průměr	564	12562	26126
Medián	143	2834	7668
S `mysphere2`			
Průměr	1114	5682	10154
Medián	392	1583	6013

I přesto, že se zvýšil čas do informování uživatele (TTUI) (z důvodů vývoje SW) **zkrátil se** po zavedení systému čas do první reakce uživatele (TTFR) a **celková doba** do vyřešení incidentu (TTR) **na polovinu**.

Dosažené cíle, výstupy a využitelnost

- Proces byl optimalizován
- Máme funkční infrastrukturu, která automatizuje části procesu řešení bezpečnostních incidentů >> prijimame napady ;]
- Síťová karanténa poskytuje uživatelům informace a prostředky pro správnou reakci na incident

Co vy na to ?

- Setkali jste se uz s mysphere2 ?
- Pomohl Vám správcům ?
- Co říkají uživatelé v campusu ?
- Už byl odpojen Jan Tleskač ?

CIV!
www.civ.zcu.cz

Otázky ?

CESNET

netspy

mysphere 2