

# Závěrečná zpráva projektu 369/2010 Zkvalitnění procesu řešení bezpečnostních incidentů v síti WEBnet

Radoslav Bodó, Michal Kostěnek  
Západočeská univerzita v Plzni  
Centrum informatizace a výpočetní techniky  
email: {bodik,kostenec}@civ.zcu.cz

12. prosince 2011

## Abstrakt

Cílem projektu bylo zkvalitnění a zrychlení procesu řešení bezpečnostních incidentů v síti WEBnet, která je součástí sítě CESNET.

Při dnešních rozměrech Internetu je udržení sítě bez jediného napadeného počítače nemožné. Proces řešení bezpečnostních incidentů zahrnuje v prvních fázích akce potřebné k lokalizaci zdroje incidentu, jeho dočasného odpojení od sítě a notifikaci správce systému či jeho uživatele. Vzhledem k povaze sítě WEBnet byl k informování uživatele nutný předchozí kontakt pracovníků CIV s lokálním správcem. V této době byly stanice odpojeny od sítě a uživatel tak byl bez přímé možnosti získání informací a to do doby, než jej kontaktuje lokální správce.

V rámci tohoto projektu jsme vytvořili systém, který zablokuje připojení uživatele tak, aby mu byly odepřeny služby sítě WEBnet a pomocí unášení HTTP přenosů byl vytvořen informační kanál, který dopraví potřebné informace uživateli pracujícím u stanice a zpřístupní mu nástroje vhodné pro řešení incidentu.

# Obsah

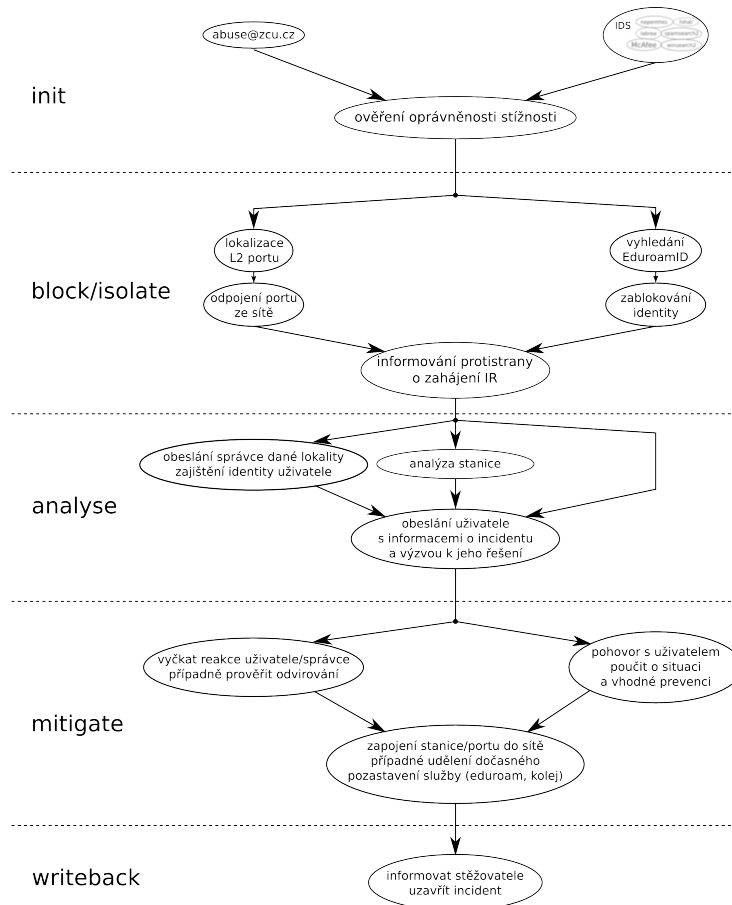
<b>1 Úvod a cíle projektu</b>	<b>4</b>
<b>2 Způsob řešení</b>	<b>5</b>
2.1 Analýza dostupných prostředků . . . . .	5
2.1.1 Manipulace s DHCP . . . . .	5
2.1.2 Manipulace s DNS . . . . .	5
2.1.3 Manipulace s provozem na hranici sítě . . . . .	6
2.1.4 Manipulace s provozem na páteřních uzlech v síti . . . . .	6
2.1.5 802.1x . . . . .	7
2.1.6 Dedikované VLAN a orchestrace access portů . . . . .	8
2.1.7 Výsledky analýzy . . . . .	9
2.2 Implementace vybraného řešení . . . . .	9
2.2.1 WEBnet a NetSpy . . . . .	10
2.2.2 WEBnet a Mysphere2 . . . . .	11
2.2.3 Mysphere2 a WEBnet . . . . .	13
2.2.4 Poznámky k nasazení . . . . .	15
2.2.5 Provozní instalace . . . . .	15
<b>3 Shrnutí výsledků</b>	<b>15</b>
<b>4 Vzdělávání a publikace v rámci grantu</b>	<b>18</b>
<b>5 Dosažené cíle</b>	<b>18</b>
<b>6 Zdůvodnění změn v projektu</b>	<b>19</b>
<b>7 Výstupy a využitelnost</b>	<b>19</b>
<b>8 Přínosy projektu</b>	<b>19</b>
<b>9 Tisková zpráva</b>	<b>19</b>
<b>10 Výkaz hospodaření s prostředky</b>	<b>20</b>
<b>A Přílohy</b>	<b>22</b>
A.1 Ukázka časování zpracování incidentů . . . . .	22
A.2 Množiny incidentů pro vyhodnocení změny procesu . . . . .	23
A.3 Nastavení karanténního firewallu . . . . .	24
A.4 Ukázky obrazovek pro získání zpětné vazby od uživatele . . . . .	26
A.5 support.zcu.cz :: Jak postupovat v případě zavirování počítače . . . . .	28
A.6 Podrobný vývojový diagram . . . . .	30
A.7 Ukázky administrátorské části aplikace Mysphere2 . . . . .	33
A.8 Ukázky generovaných informačních emailů . . . . .	34

## Seznam obrázků

1	Pohled na proces řešení bezpečnostních incidentů. . . . .	4
2	Ukázka zónového souboru bind9 – DNS sinkhole. . . . .	6
3	Ukázka přesměrování požadavků pro vybrané klienty. . . . .	6
4	WEBnet WCCP testbed . . . . .	7
5	Řešení pomocí karanténní sítě . . . . .	8
6	Návrh karanténního systému . . . . .	9
7	Schéma karanténního systému . . . . .	10
8	Informační stránka <b>redirects/spam</b> . . . . .	12
9	Informační stránka <b>redirects/p2pshare</b> . . . . .	12
10	Matice vyžadovaných reakcí . . . . .	12
11	Zjednodušený stavový diagram Mysphere2 . . . . .	13
12	Komponentový diagram aplikace Mysphere2 . . . . .	14
13	Provozní instalace Mysphere2 . . . . .	16
14	Typy řešených incidentů . . . . .	16
15	Stavy řešených incidentů ke dni 19.11.2011 . . . . .	17
16	Přehled založených incidentů v čase . . . . .	17
17	Ukázka načasování zpracování incidentů . . . . .	22
18	Informační stránka <b>responses/virus</b> . . . . .	26
19	Informační stránka <b>responses/p2pshare</b> . . . . .	27
20	Vývojový diagram: Založení incidentu. . . . .	30
21	Vývojový diagram: Informování uživatele. . . . .	30
22	Vývojový diagram: Zablokování uživatele. . . . .	31
23	Vývojový diagram: Získání zpětné vazby. . . . .	31
24	Vývojový diagram: Odblokování uživatele. . . . .	32
25	Vývojový diagram: zavření incidentu. . . . .	32
26	View incidents/view . . . . .	33
27	View incidents/notice . . . . .	33
28	View incidents/index . . . . .	34

# 1 Úvod a cíle projektu

Proces řešení bezpečnostních incidentů v síti WEBnet byl vytvořen na základě veřejných best practices<sup>1</sup>, doporučení bezpečnostní skupiny CESNET-CERTS<sup>2</sup> a dále byl optimalizován a formalizován na základě grantů FR CESNET 155/2005[3], 218R1/2007[5] a 230R1/2007[6]. Na obrázku 1 je zobrazen jeden z pohledů na tento bezpečnostní proces.



Obrázek 1: Pohled na proces řešení bezpečnostních incidentů.

V síti WEBnet neznají kmenoví zaměstnanci provozovatele sítě konkrétní identity uživatelů všech uzlů sítě, její větší část je využívána ostatními subjekty univerzity, které mají na správu lokální počítačové techniky vlastní pracovníky, kteří obhospodařují tyto části sítě.

Při řešení bezpečnostního incidentu, tak bylo vždy nutné vyhledat koncového uživatele prostřednictvím tohoto správce (emailem) a posléze informovat samotného uživatele. Většinu kroků bylo potřeba provádět ručně (vyhledat správce, zablokovat stroj nebo eduroam identitu, manipulovat s tickety systému RT, ...). Navíc v čase vyhledávání identity uživatele byl stroj odpojen od páteří sítě a uživatel neměl žádnou možnost dozvědět se, proč bylo jeho připojení zablokováno nebo tento stav odlišit od případné poruchy na jeho zařízení nebo síti.

Cílem tohoto projektu bylo zlepšit tento proces tak:

- aby byl uživatel informován přímo, nikoliv pouze prostřednictvím lokálního správce,

<sup>1</sup>[http://www.sans.org/reading\\_room/whitepapers/incident/](http://www.sans.org/reading_room/whitepapers/incident/)

<sup>2</sup>Kropáčová, Vachek, Kácha: Výklad pro Incident Response Policy a Incident Handling Policy sítě CESNET2 (AS2852)

- aby měl uživatel při řešení dostupné vhodné nástroje pro získání informací a následné řešení bezpečnostního incidentu,
- aby bezpečnostní pracovníci nemuseli vše zpracovávat ručně, tudíž aby došlo k zautomatizování některých akcí.

## 2 Způsob řešení

V rámci řešení tohoto projektu jsme chtěli nalézt takové technologické prostředky, aby byly důležité informace o nastalém incidentu uživateli prezentovány přímo a v první fázi nebyla nutná spolupráce s lokálním správcem (což přináší časové prodlevy). Toho jsme chtěli dosáhnout využitím hlavního komunikačního kanálu současnosti – služby World Wide Web.

Úkolem bylo automaticky vytvářet řízené síťové prostředí pro vybrané uzly tak, aby byl jejich provoz cíleně omezen (ne však odepřen), aby bylo možné doručit uživateli informaci o tom, proč bylo jeho připojení omezeno a jaké kroky má podniknout pro opětovné připojení stanice do sítě WEBnet. Současně mu odepřít ostatní IP konektivitu tak, aby bylo zamezeno závadné aktivitě.

### 2.1 Analýza dostupných prostředků

Vzhledem k charakteru sítě WEBnet existuje několik způsobů, jak vytyčených cílů dosáhnout. Hlavním kritériem pro výběr daného způsobu byla složitost implementace v síti WEBnet, zejména s ohledem na výkon sítě a jejích páteřních prvků a možnosti obcházení pravidel karanténní sítě.

#### 2.1.1 Manipulace s DHCP

V síti WEBnet je vyžadováno, aby všechny uzly využívaly k získávání parametrů pro připojení k síti službu DHCP. Izolace problematického uzlu by mohla být dosažena vhodnými úpravami konfigurace dané stanice (např. změna DNS serveru).

V síti však není plošně (na 100%) nasazen *DHCP snooping*, *Dynamic ARP inspection* a *IP Source Guard*. Navíc přidělené adresy mají dlouhou dobu platnosti (cca délku pracovní doby), kterou nemusí klient respektovat. Například linuxový dhcp klient z balíku *dhcp3-client* (verze 3.1.1-6+lenny4) nežádá o novou adresu po vypojení linky.

```
3.7 When clients should use DHCP
A client SHOULD use DHCP to reacquire or verify its IP address and
network parameters whenever the local network parameters may have
changed; e.g., at system boot time or after a disconnection from the
local network, as the local network configuration may change without
the client's or user's knowledge.
```

Změna síťových parametrů by při použití tohoto způsobu byla příliš dlouhá a navíc nepredikovatelná.

#### 2.1.2 Manipulace s DNS

V síti WEBnet je doporučeno, aby všechny uzly používaly DNS servery provozovatele sítě. Manipulací s odpověďmi těchto služebních serverů problematickým klientům by bylo možné dosáhnout potřebného efektu.

V praxi by to znamenalo na DNS serverech spustit druhou instanci forwarderu/rekurzivního resolveru s konfigurační zónou dle obrázku 2 a nechat jí selektivně zpracovávat požadavky pouze pro vybrané klienty (viz obr. 3).

Řešení by bylo vhodné pouze pro malé nebo silně uzavřené sítě, kde je zaručeno, že nejsou používány jiné než schválené DNS resolvers. V síti WEBnet by to nebyl vhodný způsob řešení.

```

$TTL 3600
. IN SOA pf. pf.pf.isolation.zcu.cz (
    2009020901 ; serial
    10800       ; refresh
    3600        ; retry
    604800      ; expire
    400         ; default_ttl
)
    IN      NS      pf.

support.zcu.cz. IN A 147.228....
webmail.zcu.cz. IN A 147.228....
webkdc.zcu.cz.  IN A 147.228....

*.zcu.cz.       IN      A 10.1.1.1
*.cz.           IN      A 10.1.1.1
*.              IN      A 10.1.1.1
                IN      MX      5      pf.
1.1.1.10.in-addr.arpa. IN PTR      pf

```

Obrázek 2: Ukázka zónového souboru bind9 – DNS sinkhole.

```

iptables -t nat -A PREROUTING -s $IP -m udp -p udp --dport 53 -j REDIRECT --to-port 1053
iptables -t nat -A PREROUTING -m $MAC --mac-source $2 -p udp --dport 53 -j REDIRECT --to-port 1053

```

Obrázek 3: Ukázka přesměrování požadavků pro vybrané klienty.

### 2.1.3 Manipulace s provozem na hranici sítě

V malých a středně velkých sítích se často využívá způsob odepření služeb internetu problematickým uzlům pomocí hraničních prvků sítě. Tam, kde jsou hlavními branami softwarové routery na bázi operačních systémů Linux, se dá potřebného efektu dosáhnout pomocí manipulace s průchozím provozem pomocí komponenty jádra OS – Netfilteru.

Tento způsob je však nevhodný pro vysokorychlostní sítě typu WEBnet. Problematickým uzlům by nezabránil v komunikaci uvnitř sítě a potenciálnímu využití některé z proxy služeb pro komunikaci s veřejným internetem.

### 2.1.4 Manipulace s provozem na páteřních uzlech v síti

V rozlehlých vysokorychlostních sítích, konkrétně v jejich páteřních oblastech, je kladen důraz na rychlost zpracování paketů. Z tohoto důvodu je nutné používat taková zařízení, která využívají speciální hardwarové obvody pro rychlé operace s pakety. Jednou z nejdůležitějších vlastností aktivních síťových prvků je schopnost filtrování komunikace pomocí definovaných pravidel, tzv. ACL<sup>3</sup>. U páteřních směrovačů, tedy zařízeních pracujících na třetí vrstvě ISO/OSI modelu, se využívá dalších speciálních modulů pro manipulaci s pakety, tzv. PFC<sup>4</sup> karet. Tyto karty umožňují díky hardwarové akceleraci manipulovat s velkým objemem dat bez výraznějšího zvýšení odezvy. Zmiňované akcelerované obvody využívají např. prvky Cisco řady Catalyst 6500 a 7200.

Jednou z možností páteřních boxů je manipulace webovým provozem díky protokolu WCCP<sup>5</sup>. Implementace tohoto protokolu umožňuje přesměrovat vybrané pakety (vyhodnocené ACL) do transparentní HTTP proxy (např. Squid) a zbytek provozu buď omezit, nebo nechat beze změny. WCCP protokol může pracovat ve dvou režimech, tunelovacím pomocí GRE<sup>6</sup> protokolu nebo na principu přepisování hlaviček rámců na druhé vrstvě ISO/OSI. Režim přepisování L2 hlaviček je možné využít pouze v případě, kdy je omezená VLAN zakončena na stejném zařízení jako HTTP proxy.

Manipulace provozu protokolem WCCP byla v rámci projektu vyzkoušena v režimu GRE a to jak v testovacím prostředí v zapojení dle obrázku 4, tak i na produkční síti, ale tento způsob

<sup>3</sup>Access Control List

<sup>4</sup>Policy Feature Card

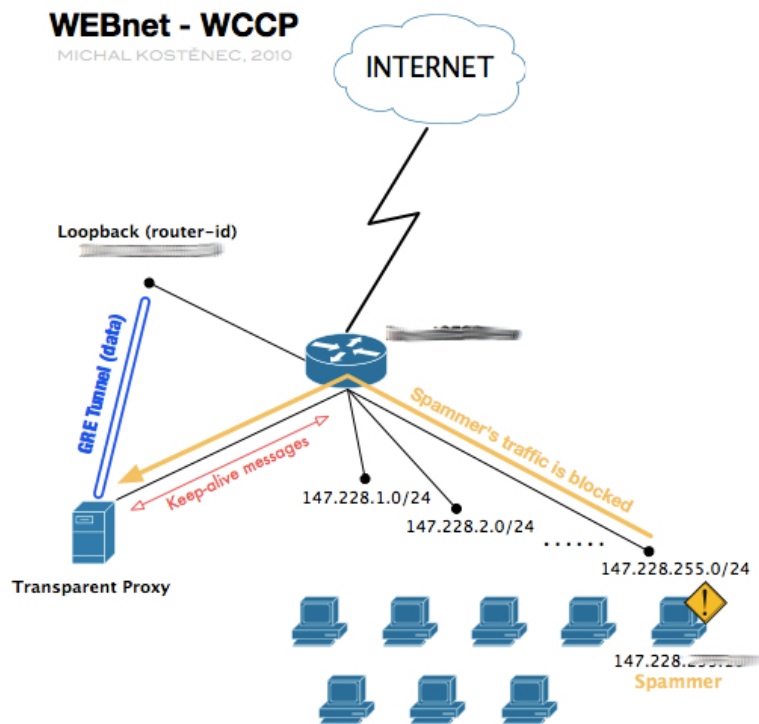
<sup>5</sup>Web Cache Control Protocol – <http://www.cisco.com/en/US/docs/ios/11.2/feature/guide/wccp.html>

<sup>6</sup>Generic Routing Encapsulation Protocol

má několik omezujících vlastností, kvůli nimž nebylo možné tuto techniku pro vytyčené cíle dále využívat.

V testované páteřní síti se nachází směrovače řady Catalyst 6500 a směrovače Catalyst 4900M. U těchto aktivních prvků je v současné době možné využívat protokol WCCP, avšak u řady 4900M je možná konfigurace pouze v režimu manipulace s L2 hlavičkami. Proto bylo možné omezovat komunikaci pouze v některých částech sítě. Další nevýhodou této metody je častá změna konfigurace páteřních směrovačů, konkrétně dynamická změna definicí ACL.

Pokud by měla implementace tohoto způsobu pokračovat, bylo by nutné odzkoušet konfiguraci jednoho cílového cache serveru pro více WCCP zdrojů a možnost aplikování protokolu do vzdálených lokalit. Tyto možnosti nebyly zkoumány, ale podle dostupných informací lze tyto požadavky na funkčnost realizovat použitím multicast režimu implementovaného ve WCCP verze 2.

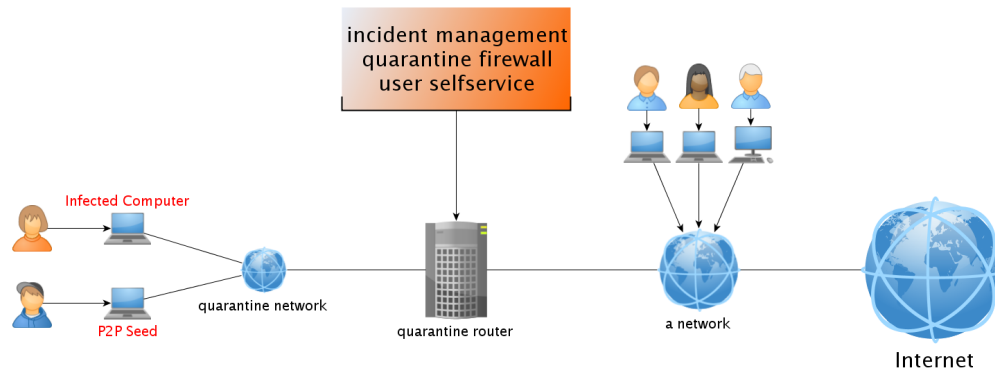


Obrázek 4: WEBnet WCCP testbed

### 2.1.5 802.1x

Jedním z možných řešení je plošné používání plného NAC<sup>7</sup> nebo alespoň řízení přístupu protokolem 802.1x (viz Eduroam). Připojení daného zařízení do sítě by bylo řízeno na základě identifikace subjektu/uživatele a v rámci autorizačních rozhodnutí by bylo možné jej připojovat do speciální (karanténny) části sítě.

Vzhledem k různorodosti zařízení (počítače, telefony, kopírky, tiskárny, ...) připojovaných do sítě WEBnet nelze nasadit tento přístup na všechny přístupové porty. Použití v takovém režimu (pouze na vybrané porty) by přineslo neakceptovatelné množství konfiguračních změn na aktivních prvcích v síti.



Obrázek 5: Řešení pomocí karanténní sítě

### 2.1.6 Dedikované VLAN a orchestrace access portů

Další možností je zavedení speciální dedikované podsítě (VLAN<sup>8</sup>) a orchestrace aktivních prvků vhodným nástrojem k dynamickému řízení příslušnosti koncového portu do podsítě (access vlan). Jejich zakončením na linuxovém routeru a filtrováním provozu je možné kontrolovat konektivitu zařízení, která jsou do něj připojena. Vzhledem k očekávanému zatížení (maximálně desítky napadených počítačů) je toto softwarové řešení vhodné i pro vysokorychlostní sítě typu WEBnet/CESNET.

Pro automatizovanou konfiguraci síťových prvků je možné využít několik dostupných nástrojů.

**Packetfence** V průběhu projektu bylo zapojeno laboratorní prostředí pro systém PacketFence[7] – Open Source NAC. Po konfiguraci umožňuje:

- dohled a řízení aktivních prvků většiny výrobců síťového hardware (přes SNMP),
- podporu 802.1x,
- webovou samoobsluhu pro registraci uživatelů a zařízení,
- několik druhů autentizačních mechanismů (ldap, radius, local),
- karanténování zařízení (např. ve spolupráci s IDS Snort) s webovou aplikací pro řešení incidentů,
- webovou a CLI administraci.

Software je tvořen komponentami v PHP (management), Perlu (registrace, orchestrace). Ty se starají o generování konfiguračních souborů pro standardní linuxové demony (httpd, bind, dhcpd. . .). Vlastní instalace není triviální, ale s výhodou je možné využít virtuálního stroje, který je od výrobců připraven.

Systém je však navržen s předpokladem, že je hlavním autoritativním zdrojem konfigurace pro síťové prvky a jeho úprava pro potřeby nasazení v síti WEBnet by byla neproveditelná. O jeho nasazení však dále uvažujeme v kolejni části sítě WEBnet, kde jsou požadavky i možnosti správy sítě odlišné.

**NAV** Podobnou funkcionalitu poskytuje i software NAV – Network Administration Visualized [8, 9]. Na rozdíl od předchozího řešení umí automaticky detekovat a vyhledávat aktivní prvky v síti (autodiscovery) a jeho části jsou napsány v Pythonu a Javě. V průběhu projektu nebyl tento systém zkoušen.

<sup>7</sup>Network Access Control

<sup>8</sup>A virtual local area network

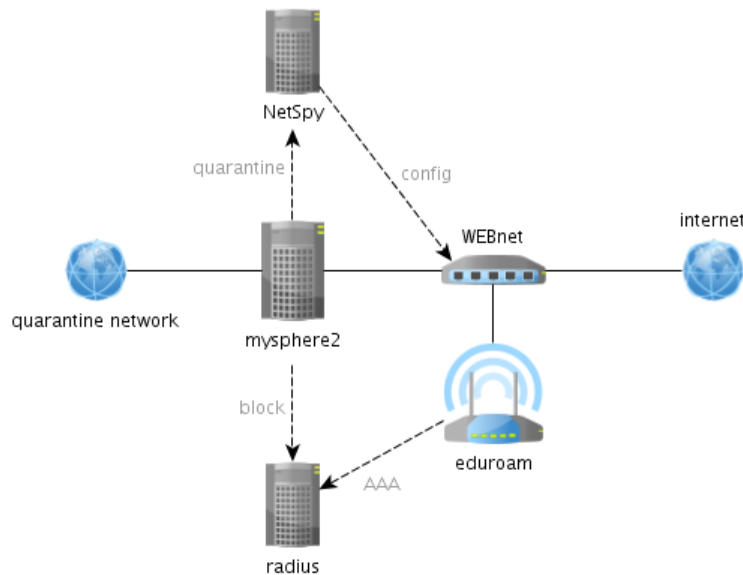


**NetSpy** V síti WEBnet je pro potřeby automatizace konfigurace přístupových prvků provozován vlastní software NetSpy[16], který je vyvíjen pracovníky CIV.

### 2.1.7 Výsledky analýzy

Analýzou byl navržen následující postup:

- navržení a implementace karanténní sítě v síti WEBnet s ohledem na její metropolitní charakter,
- rozšíření sw NetSpy tak, aby podporoval konfiguraci karantény na vybraný port,
- doplnění sw NetSpy o rozhraní HTTP REST pro možnost automatického řízení externím procesem,
- implementace vlastního nástroje pro správu incidentů
  - vyhledávání informací o přípojném bodu nebo identitě uživatele sítě,
  - rozesílání notifikací přes systém Request Tracker,
  - řízení karantény v campusu (propojením se systémem NetSpy),
  - blokování identit sítě Eduroam,
  - automatizaci úkonů v ostatních interních agendách sítě WEBnet,
  - webové rozhraní pro informování uživatelů a přijímání zpětné vazby,
  - vytvoření a implementace vhodné politiky omezování provozu v karanténní síti.



Obrázek 6: Návrh karanténního systému

## 2.2 Implementace vybraného řešení

Pro síť typu WEBnet bylo vybráno řešení navržené v kapitole 2.1.7 – možnost karanténní VLAN a orchestrace portů. Z pohledu síťového administrátora není toto řešení zcela „čisté“, ale lze ho považovat za přijatelné řešení v sítích, kde není možné plošně implementovat protokol 802.1x.

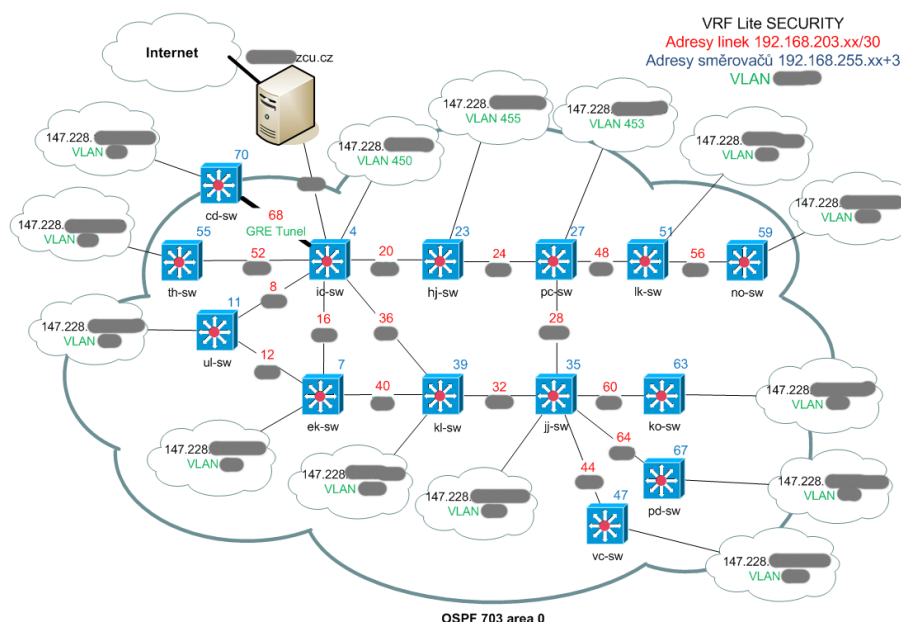
Dle obecných doporučení není vhodné použít pro celou síť pouze jednu VLAN, proto bylo třeba pro každou páteřní lokalitu vytvořit samostatnou karanténní VLAN, v tomto případě 13 nových VLAN. Tyto VLAN je třeba zakončit na vhodných směrovačích, tzn. nastavit IP adresu, kterou

budou využívat blokována zařízení při své komunikaci jako bránu. Dalším krokem je povolení karanténí VLAN na všech spojovacích (trunk) portech v konkrétních páteřních lokalitách. Při použití většího počtu karanténí sítí je vhodné použít směrovací protokol, konfigurace tedy dále obnášela konfiguraci OSPF<sup>9</sup> procesů v každé páteřní lokalitě.

Pro „fyzické“ oddělení síťového provozu celé soustavy karanténí sítí byla použita technologie VRF-lite<sup>10</sup>. Protokol VRF-lite poskytuje možnost vytvoření několika oddělených směrovacích tabulek na jednom směrovači. V tomto případě bylo VRF-lite využito také proto, aby bylo možné použít na páteřní síti privátní rozsahy adres, které by byly v běžném případě zahozeny.

Při následné implementaci se vyskytl požadavek na připojení vzdálené lokality (Cheb) do systému karanténí VLAN. Při použití zvoleného přístupu, byl tento krok poměrně jednoduchý. Pro připojení byl využit tunelovací protokol GRE, který dovoluje tunelovat i směrovací protokoly. V lokalitě Cheb byla vytvořena další karanténí VLAN, nakonfigurován OSPF proces a GRE tunelem jej „připojili“ do stávající soustavy.

Každé karanténí podsíti je přidělen adresní prostor pro 14 blokováných zařízení (sítě s CIDR<sup>11</sup> maskou /28), což je dle našich zkušeností v současné době dostačující, protože počty incidentů se pohybují v jednotkách. Aktuální konfigurace obsahuje 14 karanténí VLAN zapojených dle obrázku 7.



Obrázek 7: Schéma karanténího systému

### 2.2.1 WEBnet a NetSpy

NetSpy je monitorovací nástroj vytvořený speciálně pro prostředí sítě WEBnet. NetSpy periodicky stahuje obsah ARP tabulek (`mac-address-table`) a informace o MAC adresách připojených na konkrétních portech monitorovaných zařízení (SNMP OID:1.3.6.1.2.1.4.22 – `ipNetToMediaTable`). Následně hledá v nalezených datech párové hodnoty, tj. MAC adresu a odpovídající IP adresu. Nalezené hodnoty jsou uloženy do databáze spolu s časovým razítkem a informacemi o portu, do kterého je nalezené zařízení (MAC adresa) připojeno. V nalezených datech je možné nejen vyhledávat, ale je možné i blokovat zařízení nalezená na koncových portech.

<sup>9</sup>Open Shortest Path First

<sup>10</sup>Virtual Routing and Forwarding

<sup>11</sup>Classless Inter-Domain Routing

Pro potřeby projektu byla doprogramována funkčnost vložení zařízení do karanténní VLAN. Systém NetSpy nejprve port vypne, přístupová VLAN je změněna na karanténní a po uplynutí definovaného intervalu je port opět zapnut. Původní VLAN je uložena do databáze pro pozdější obnovení funkčnosti. Původní verzi systému NetSpy lze ovládat pouze přes webové rozhraní, pro potřeby automatizovaného blokování zařízení bylo tedy nutné vytvořit jednoduché REST API pro zaslání požadavků přes protokol HTTP.

### 2.2.2 WEBnet a Mysphere2

Kromě karanténních sítí je nezbytnou komponentou implementovaného řešení brána, která je schopna omezovat a manipulovat s provozem karanténovaných zařízení.

V tomto případě byla brána vytvořena serverem s OS/Linux, který byl připojen do sítě WEBnet a nakonfigurován jako výchozí brána ze všech karantén. Brána poskytuje zařízením v síti routování provozu směrem k veřejnému internetu, službu DHCP a obsahuje catch-all http server (Apache2).

Vzhledem k charakteru sítě WEBnet (používání SSO Kerberos a WebAuth, adresářové služby, doménové služby OS Windows, distribuovaný souborový systém AFS ...), nemůže být provoz karanténovaných zařízení omezen úplně. Cílem implementovaného řešení bylo ponechání dostupnosti některých služeb tak, aby mohl uživatel reagovat na bezpečnostní incident. Zejména pak, aby byl schopen:

- přihlásit se na stanici – za použití služeb DNS, KDC/AD, AFS, LDAP,
- použít server uživatelské podpory `support.zcu.cz` – k získání dodatečných informací,
- používat webový telefonní seznam ZČU – k vyhledání kontaktů po ZČU a zachování produktivity pracovníka,
- používat FAI<sup>12</sup>, `ftp.zcu.cz` a `download.zcu.cz` – k možnosti získání SW pro reinstalaci zařízení,
- používat systém pro centrální ochranu antivirovým SW,
- použít webmailový systém ZČU `webmail.zcu.cz` – ke komunikaci s bezpečnostní skupinou,
- použít aplikaci pro řešení bezpečnostních incidentů – ke komunikaci s bezpečnostní skupinou.

K řízení provozu byl použit subsystém netfilter, komponenta linuxového jádra. Konkrétní nastavení je možné nalézt v příloze A.3 (str. 24).

Přesměrování je provedeno na lokální webový server, na kterém běží aplikace, která umožňuje uživateli získat informace o bezpečnostním incidentu a odeslat zpětnou vazbu nebo požádat o další pomoc či informace. Ukázkové screenshoty jsou na obrázcích 8 a 9.

Konkrétní informace jsou zobrazovány na základě IP adresy (resp. MAC adresy<sup>13</sup>) klienta s ohledem na typ incidentu a na to, zda se jedná o původce incidentu nebo zda požadavek přichází ze zařízení, které se pouze nachází v karanténní podsíti díky tomu, že přípojný bod (access port) sdílí s počítačem který byl odpojen.

Současná implementace aplikace reflektuje zavedené postupy pro řešení bezpečnostních incidentů v síti WEBnet (viz obrázek 10).

Pro typ incidentu `p2pshare` aplikace vyžaduje sjednání osobní schůzky s pracovníky bezpečnostní skupiny, na které uživateli pracovník vysvětlí možné dopady jeho aktivit v souladu s doporučeními CESNET-CERTS (`response/p2pshare`). Pro ostatní typy incidentů `spam`, `botnet`, `scan` ... zobrazí doporučení o vhodném dalším postupu (`responses/virus`). Vhodný postup pro vyčištění zařízení od virové nákazy byl v rámci projektu vypracován na serveru uživatelské podpory<sup>14</sup> a je k nalezení v příloze A.5 (str. 28).

Ve všech případech tedy systém umožňuje uživateli komunikovat s bezpečnostní skupinou přes interní webové formuláře nebo doporučuje ostatní standardní prostředky pro komunikaci. Ukázkové screenshoty jsou v příloze A.4 (str. 26).

<sup>12</sup>systém pro hromadné instalace ZČU

<sup>13</sup>párováním původní MAC adresy se záznamy z karanténního DHCPD

<sup>14</sup><http://support.zcu.cz/napadeny-stroj>

**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](mailto:support.zcu.cz) - [Seznam lokálních správců](#)), který zařídí nápravu.

B. Uveďte počítač do vhodného stavu svépomoci dle návodu [support.zcu.cz - Jak postupovat v případě zavirování počítače](#). Po reinstalaci nebo odvírování připojte nezávadný stroj do sítě a vyplňte [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>

Obrázek 8: Informační stránka `redirects/spam`

**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. Domluvit 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>

Obrázek 9: Informační stránka `redirects/p2pshare`

Typ	Vyžadovaná reakce
spam	odvírování a zpětná vazba
botnet	odvírování a zpětná vazba
scan	odvírování a zpětná vazba
p2pshare	pohovor správců WIRT
other	kontaktovat lokální správce nebo <a href="mailto:abuse@zcu.cz">abuse@zcu.cz</a>

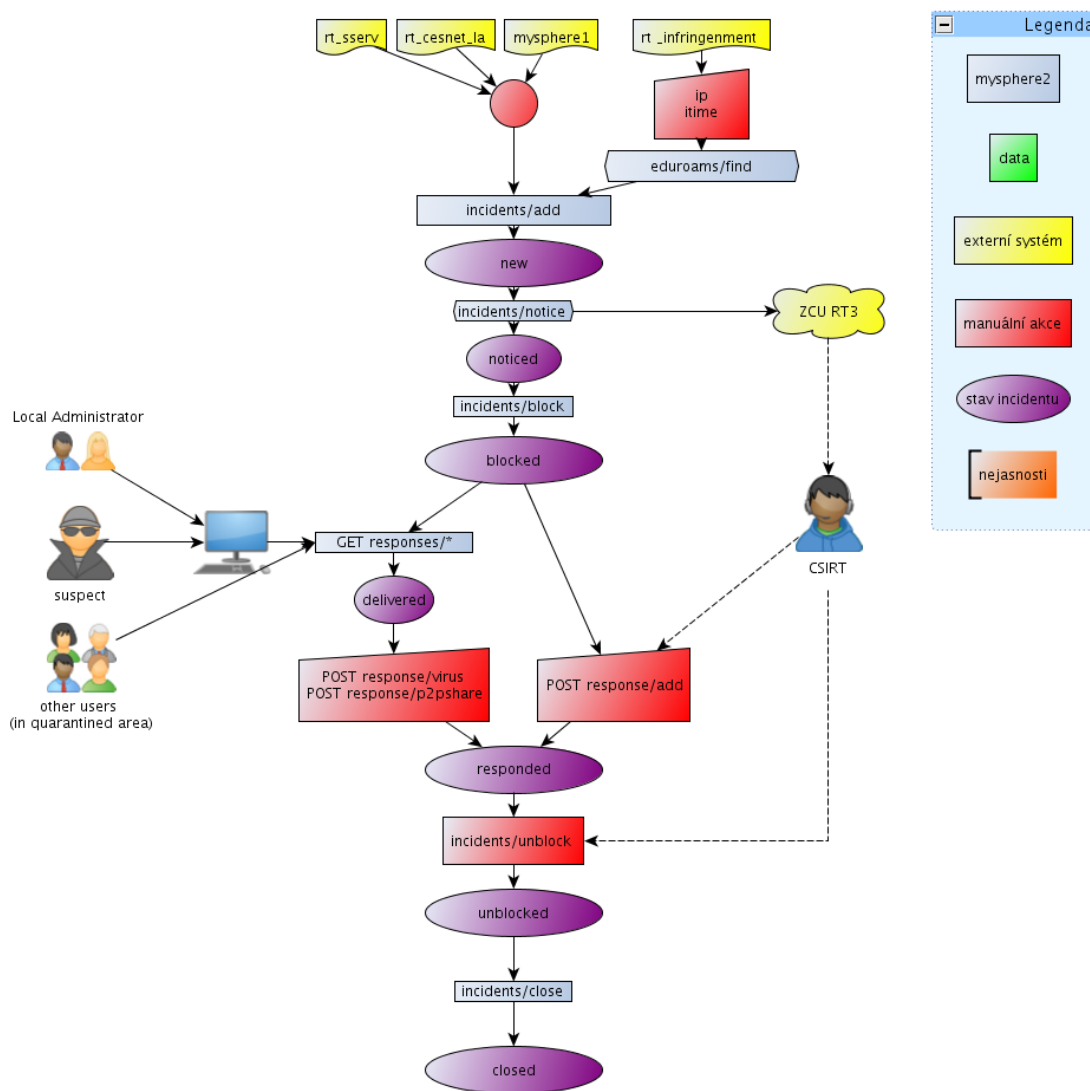
Obrázek 10: Matice vyžadovaných reakcí

Interakce aplikace s uživatelem je zaznamenávána do systémového protokolu a zrcadlena do systému Request Tracker ZČU. Grafický vzhled aplikace byl vypracován v souladu s manuálem jednotného vizuálního stylu ZČU.

### 2.2.3 Mysphere2 a WEBnet

Mysphere2 je webovou aplikací, která se nestará pouze o komunikaci s uživatelem. Jejím hlavním úkolem je administrace a automatizace procesu řešení bezpečnostních incidentů a to i v částech sítě, kde je nutné uplatnit jiný postup (např. Eduroam – blokovat uživatele dle identity na základě accountingu v Radius serveru).

Aplikace udržuje interní databázi o založených incidentech a umožňuje administrátorovi řídit životní cyklus incidentu dle obrázku 11. Mezi hlavní komponenty patří kontroléry **incidents**, **redirects**, **responses** a **eduroams**. Jejich metody implementují potřebné akce.

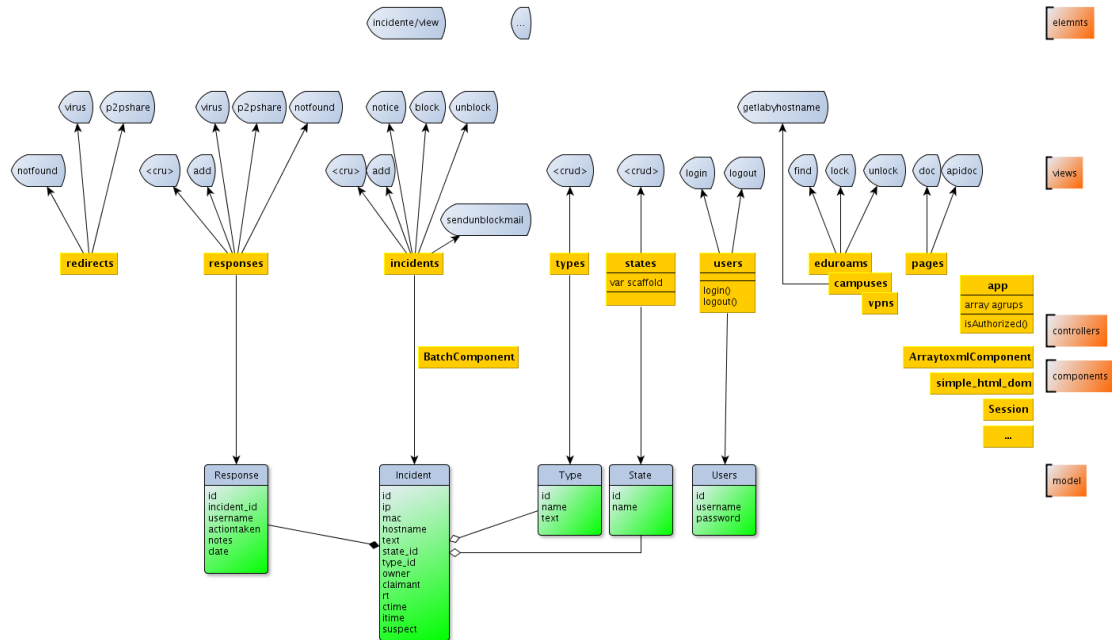


Obrázek 11: Zjednodušený stavový diagram Mysphere2

Pro implementaci byl zvolen webový framework CakePHP<sup>15</sup>, který umožňuje psaní aplikací objektově orientovaným přístupem a návrhovým vzorem MVC<sup>16</sup>. Výhodami tohoto frameworku jsou:

<sup>15</sup><http://www.cakephp.org>

<sup>16</sup>Model-View-Controller



Obrázek 12: Komponentový diagram aplikace Mysphere2

- obsáhlá dokumentace, zásuvné moduly, sbírka zdrojových kódů, podpora komunity,
- podpora MVC (by desing) a ORM (deklarativně),
- automatické generování kódu defaultních view a kontrolérů pro operace nad daty modelů (CRUD),
- snadnost rozšíření frameworku na všech jeho úrovních (autorizace k metodám kontrolérů na bázi skupin, napojení na externí autentizaci ...),
- možnost implementace ACL až na úroveň datových položek modelu (vhodné k implementaci delegované správy).

Obecný charakter modelovaného procesu a jeho promítnutí do implementace za použití standardního frameworku pro vytvoření aplikace umožňuje jeho snadnou rozšiřitelnost a případné využití i v ostatních částech sítě CESNET i přesto, že aktuální kontroléry provádějí akce specifické pro síť WEBnet. Zdrojové kódy mohou být zpřístupněny bezpečnostní skupinou CESNET-CERTS.

V současné verzi umožňuje aplikace administrátorům zejména:

- vyhledávat identity uživatelů Euroamu na základě informací [ip:time] (find),
- spravovat jednotlivé incidenty a jejich metadata (crud),
- obeslat uživatele nebo lokální správce emailem podle definovaných předloh (notice),
- (od)blokovat stroje v kampusu (block/unblock) a identity v Eduroamu (block/unblock) (spoluprací s externími systémy – NetSpy, eduroam-admin),
- získávat potřebná doplňková data ze servisních služeb WEBnetu (LDAP, STAG-XML<sup>17</sup>, DHCPD),
- vkládat záznamy do servisních agend WEBnetu (RT, WHOIS<sup>18</sup>).

Projekt je dokumentován pomocí systému Doxygene a podrobným vývojovým diagramem, viz

<sup>17</sup>informace o metadatech uživatelů

<sup>18</sup>Aplikace pro pracoviště Helpdesk CIV

příloha A.6 (str. 30). Ukázky administrátorské části aplikace jsou v příloze A.7 (str. 33), ukázky generovaných notifikačních emailů v příloze A.8 (str. 34)

#### 2.2.4 Poznámky k nasazení

V původně zamýšleném nasazení bylo pro karanténní síť vybráno adresování z privátních rozsahů RFC1918, při testovacím provozu se však ukázalo, že vzhledem k silnému napojení mnoha stanic v síti WEBnet na autentizační systém Kerberos, není možné toto adresování používat (defaultně se využívají lístky s adresou – address tickets). Pro pilotní provoz bylo provedeno přeadresování všech karanténních podsítí na veřejné IP rozsahy z volného adresního prostoru sítě WEBnet.

Při implementaci nebylo provedeno penetrační testování implementovaného software a v průběhu testovacího provozu byly odhaleny 2 chyby v systému NetSpy.

NetSpy nemá *detention pursuit*, pokud je zařízení přepojeno do jiného access portu, získá opět plný přístup do sítě. Před nasazením systému to byl častý postup, kterým uživatel řešil nefunkčnost síťové konektivity a neměl k dispozici žádné informace o tom, proč byl odpojen a zda se nejedná o chybu zařízení. Po nasazení systému Mysphere2 do pilotního provozu nebyl žádný takový případ zaznamenán.

Veškerý provoz jdoucí přes karanténní bránu je zaznamenáván pro potřeby případné forenzní analýzy incidentu. Z karanténní sítě je možné pašovat data do veřejného internetu pomocí strančního DNS kanálu. Analýzou provozu karanténovaných stanic nebyl žádný takový pokus potvrzen. Další analýzou provozu by bylo možné získat doplňkový zdroj dat pro systém MENTAT[10].

#### 2.2.5 Provozní instalace

Popisovaný systém provozujeme v síti WEBnet v zapojení podle obrázku 13.

### 3 Shrnutí výsledků

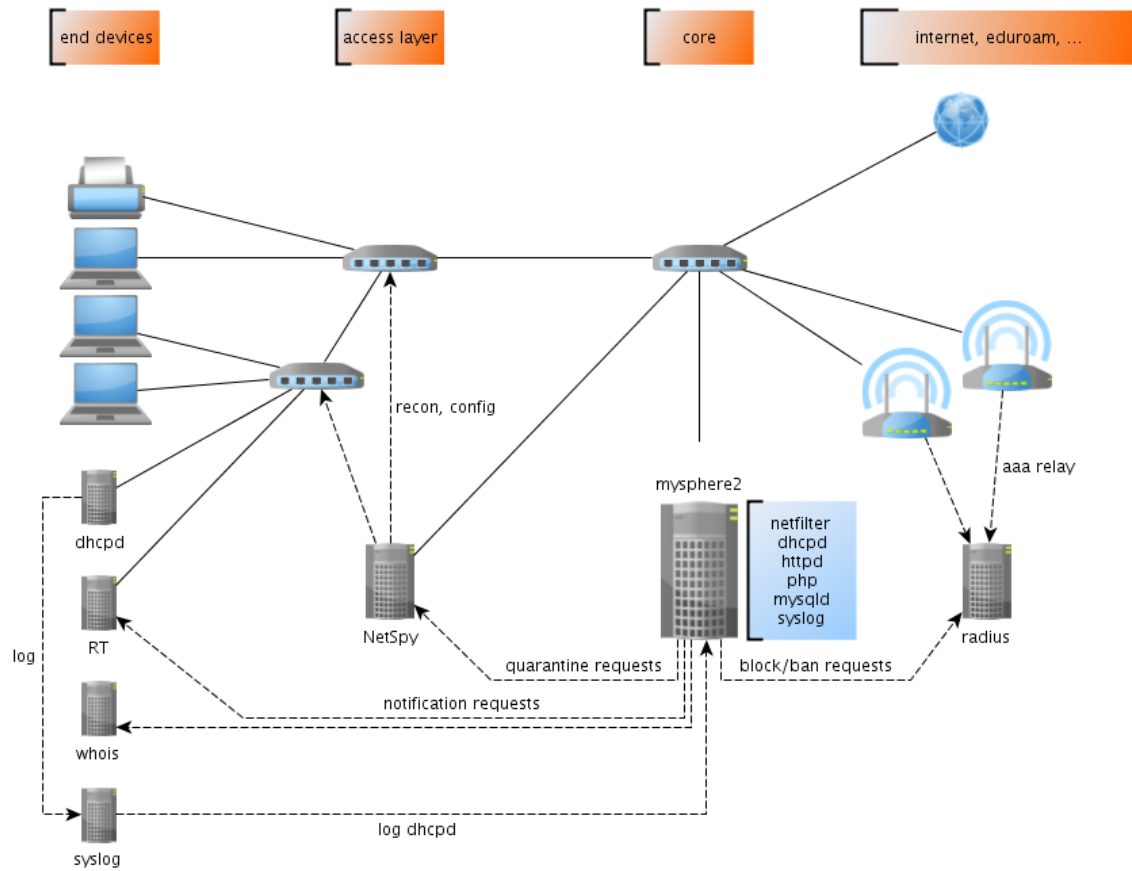
Za dobu pilotního provozu systému Mysphere2 bylo řešeno celkem 70 incidentů (17.5.2011 – 19.11.2011). Na obrázcích 14, 15, 16 je znázorněno rozložení jejich typů, aktuálních stavů a datumů vytvoření.

Pro vyhodnocení míry změny procesu byly ze systému pro správu požadavků (RT) vybrány náhodné vzorky incidentů z doby před a po zavedení systému Mysphere2. Vzorky zahrnovaly 3 incidenty z kategorií **p2pshare**, **botnet**, **spam**, **scan**. Sledované veličiny byly: čas do informování uživatele (TTIU), čas do první reakce uživatele (TTFR), celková doba do vyřešení incidentu (TTR). Následující tabulka ukazuje souhrnné ukazatele, konkrétní informace jsou k nalezení v příloze A.2.

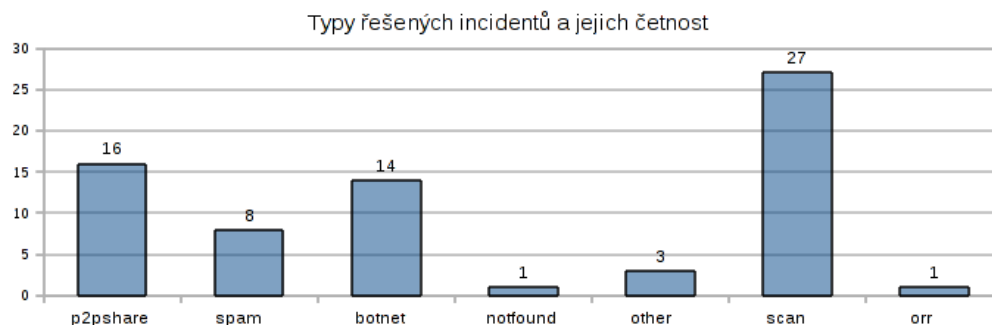
	TTIU [m]	TTFR [m]	TTR [m]
Bez Mysphere2			
Průměr	564	12562	26126
Medián	143	2834	7668
S Mysphere2			
Průměr	1114	5682	10154
Medián	392	1583	6013

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

Z dostupných informací je patrné, že proces řešení bezpečnostních incidentů byl optimalizován a zrychlen. Pro koncové uživatele se tak zvýšila dostupnost, využitelnost i bezpečnost sítě WEBnet a CESNET a jejich služeb.

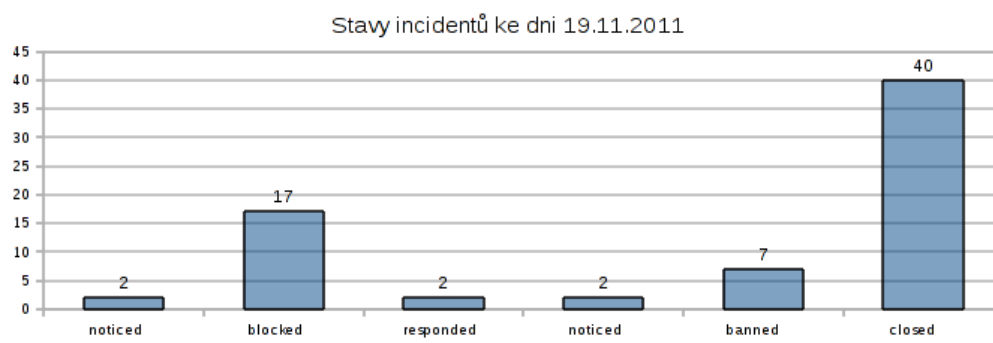


Obrázek 13: Provozní instalace Mysphere2

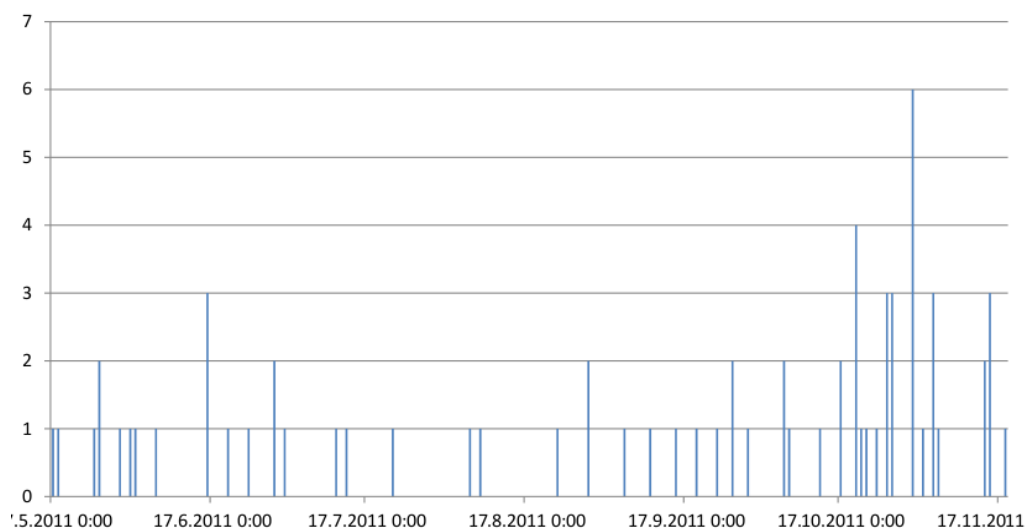


Obrázek 14: Typy řešených incidentů





Obrázek 15: Stavy řešených incidentů ke dni 19.11.2011



Obrázek 16: Přehled založených incidentů v čase

## 4 Vzdělávání a publikace v rámci grantu

V rámci tohoto grantu řešitelé navštívili konferenci IETF.org 88, která se konala v dubnu 2011 a konferenci Chaos Communication Camp 2011, která se konala v srpnu 2011. O poznatcích z této konference informovali na interním semináři CIV a v emailové konferenci `csirt-forum@cesnet.cz`.

Získané znalosti byly využity pro přípravu publikace a prezentace pro konferenci EurOpen.CZ (květen 2011[13]) na téma analýza malware a prezentacemi o systémech IDS [14, 15] na semináři GN3 – Monitoring kampusových sítí, který se konal v říjnu 2011. V listopadu 2011 se řešitelé zúčastnili školení o bezpečnosti webových aplikací.

Z výsledků projektu byla sestavena prezentace pro podzimní seminář řešitelů CESNETu.

### Zakoupené knihy

Z prostředků grantu bylo zakoupeno několik knih, které se týkají řešené problematiky a jsou členům sdružení k dispozici formou MKV<sup>19</sup>.

- *Michał Zalewski*: Silence on the Wire: a Field Guide to Passive Reconnaissance and Indirect  
ISBN: 978-1593270469
- *Himanshu Dwivedi*: Hacking Voip  
ISBN: 978-1593271633
- *Michael Lucas*: Cisco Routers for the Desperate  
ISBN: 978-1593271930
- *Seitz, Justin*: Gray Hat Python  
ISBN: 978-1593271923
- *Eagle, Chris*: Ida Pro Book, 2nd Edition: the unofficial guide to the world's most popular disassembler  
ISBN: 978-1593272890

## 5 Dosažené cíle

Hlavním cílem předkládaného projektu bylo zlepšení procesu řešení bezpečnostních incidentů. V rámci projektu jsme provedli analýzu dostupných technických prostředků, navrhli a implementovali vybrané řešení.

Vytvořili jsme potřebnou síťovou infrastrukturu tak, aby byl v úvodní fázi kontaktován uživatel přímo vhodným komunikačním kanálem a nebyla pro jeho informování potřebná znalost o jeho konkrétní identitě.

Síťové prostředí implementuje vhodný způsob izolace problematického uzlu v síti tak, že není od služeb sítě odpojen úplně, ale jsou mu k dispozici základní služby potřebné k získání uživatelské podpory a ostatní zdroje a nástroje (návod a antivir) nezbytné pro vhodnou reakci na nastalou situaci.

Řešitelé se zúčastnili konference IETF.org 88 a Chaos Communication Camp 2011, které výrazně přispěly ke vzdělání v bezpečnostní oblasti včetně získání zajímavých kontaktů na odborníky v zahraničí. Řešitelé dále absolvovali školení na téma bezpečnost webových aplikací.

Z výsledků projektu byla sestavena prezentace pro podzimní seminář řešitelů CESNETu.

Nově navrženým systémem jsme vyřešili celkem 70 bezpečnostních incidentů a vyhodnocení provozních údajů prokázalo, že se proces řešení bezpečnostních incidentů podařilo zrychlit a optimalizovat.

Domníváme se, že projekt přispěl ke zvýšení zabezpečení sítě WEBnet resp. CESNET. Zamýšlená finanční rozvaha byla dodržena. Cíle projektu byly podle našeho názoru splněny.

<sup>19</sup>Meziknihovní výpůjční služby

## 6 Zdůvodnění změn v projektu

V průběhu projektu nebyly vyčerpány některé plánované prostředky na cestovné a vložné na konferenci.

Nebylo provedeno automatické napojení na systém IDS Mysphere1, implementované řešení je tak odolnější proti útokům typu DoS.

## 7 Výstupy a využitelnost

Výstupem z projektu je implementace karanténních podsíť v síti WEBnet a rozšíření konfiguračního nástroje NetSpy, který dokáže řídit přístupové porty k síti.

Výstupem je také nový systém pro řízení procesu řešení bezpečnostních incidentů s webovým rozhraním, uživatelskou samoobsluhou a napojením na servisní agendy sítě WEBnet. Dalším výstupem jsou informační materiály pro uživatele jak se správně zachovat v případě napadení systému virovou nákazou.

Obecný charakter modelovaného procesu a jeho promítnutí do implementace za použití standardního frameworku pro vytvoření aplikace umožňuje jeho snadnou rozšiřitelnost a případné využití i v ostatních částech sítě CESNET. Zdrojové kódy a informační materiály budou zpřístupněny bezpečnostní skupinou CESNET-CERTS.

Z výsledků projektu byla sestavena prezentace pro podzimní seminář řešitelů CESNETu. Zkušenosti získané v průběhu projektu byly zpracovány formou této závěrečné zprávy.

V některém z příštích projektů bychom se rádi zabývali zlepšením systému Mysphere2 a jeho napojením na další agendy v síti WEBnet (projekt mysphere1) a CESNET (Mentat).

## 8 Přínosy projektu

Cílem a zároveň přínosem projektu je návrh a implementace systému pro optimalizaci a automatizaci procesu řešení bezpečnostních incidentů (Mysphere2 a NetSpy). Proces řešení se zrychlil, díky tomu získala skupina pracovníků řešící tyto incidenty více času na jiné rozvojové činnosti.

Nasazení systému má pozitivní dopad i na koncové uživatele sítě. Ti jsou při používání karanténního systému informováni neprodleně a mají stále dostupné základní prostředky (email, informace, antivir ...), které mohou uživatelé využít pro vyřešení incidentu. Tento přístup zvyšuje jak dostupnost, tak i využitelnost sítě WEBnet a CESNET.

V rámci analýzy dostupných prostředků byl proveden rozbor možností pro dosažení požadovaných cílů a to s ohledem na možnosti sítě WEBnet. Vzhledem k tomu, že podobnou architekturu mají i ostatní sítě členů CESNETu, jsou znalosti a zkušenosti z analýzy k dispozici i ostatním členům sdružení formou této závěrečné zprávy.

V průběhu projektu prošli řešitelé školením bezpečnosti webových aplikací a zúčastnili se několika konferencí. Touto činností byly získány zajímavé kontakty na odborníky z oblasti počítačové bezpečnosti. Získané znalosti a kontakty jsou aktivně využívány k plnění pracovních úkolů v aktivitách CESNETu, zejména pak: CESNET-CSIRT (vývoj IDS), MetaCentrum (penetrační testy) a GN3<sup>20</sup> (prezentace a publikace).

Splněním cílů projektu jsme zakončili sérii projektů [3], [5], [6], inspirovanou činností kolegů z *rwth-aachen.de* (viz [2]), tj. vytvořením prototypu síťového prostředí, které je schopné pružně reagovat na bezpečnostní hrozby v síti.

## 9 Tisková zpráva

Na Západočeské univerzitě v Plzni byl dokončen projekt zkvalitnění procesu řešení bezpečnostních incidentů. V rámci jeho plnění byl v síti WEBnet uveden do provozu systém pro automatizaci

<sup>20</sup>Multi-Gigabit European Academic Network

procesu a samoobsluhu uživatelů, který pomáhá řešit incidenty uvnitř sítí WEBnet a CESNET2 a tím zvyšovat jejich celkovou bezpečnost a dostupnost služeb.

## 10 Výkaz hospodaření s prostředky

Na projektu se podílely 2 subjekty, a to Fond Rozvoje CESNETu a Západočeská univerzita v Plzni. Z prostředků Fondu rozvoje bylo hrazeno cestovné na konferenci Chaos Communication Camp 2011, mzdy a soc. zdrav. pojištění. Z prostředků ZČU byly hrazeny náklady na nákup literatury, cestovné na konferenci IETF.org 88, soc. a zdravotní pojištění, cestovné na konferenci Chaos Communication Camp 2011 a školení webové aplikační bezpečnosti.

Vyúčtování provedlo ekonomické oddělení ZČU v Plzni dle platných předpisů. Doklady o nákupech a platbách jsou uloženy taktéž na ekonomickém oddělení ZČU.

Materiál	Cena	Hrazeno	Kategorie
Literatura	4 653,-	ZČU	knihy, uč. pomůcky
Náklady peněžního styku IETF.ORG	651,-	ZČU	cestovné
Doprava na konferenci IETF.ORG (kapesné)	714,-	ZČU	cestovné
Stravné na konferenci CCC 2011	13 644,-	ZČU	cestovné
Školení webové aplikační bezpečnosti	42 491,-	ZČU	ostatní služby
Vložné a doprava na konferenci CCC 2011	11 721,-	CESNET	cestovné
Mzdy řešitelům	78 000,-	CESNET	mdzy
Sociální a zdrav. poj.	27 000,-	CESNET	soc. zdrav. poj.
Celkem CESNET	116 721,-	-	-
Celkem ZČU	62 153,-	-	-
Celkem	178 874,-	-	-

Celkem bylo čerpáno 178 874,- Kč, z toho z Fondu rozvoje CESNETu 116 721,- Kč a ze strany Západočeské univerzity 62 153,- Kč, čímž spoluúčast ZČU činí 34,75%.

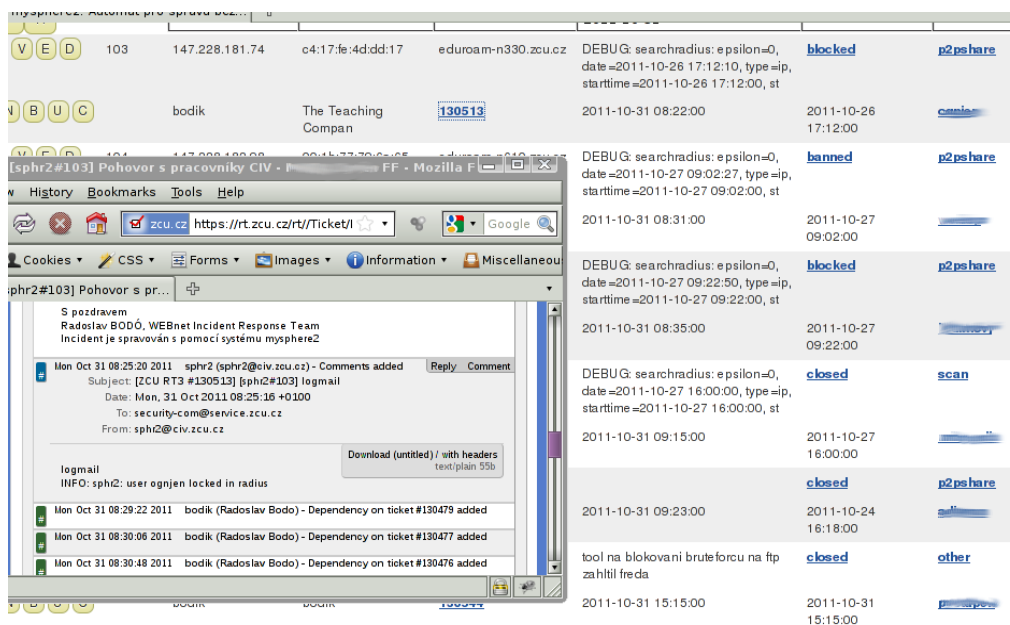
Rozdíl skutečných nákladů (178 tis,-) oproti plánovaným (241 tis.) je tvořen nevyčerpáním všech prostředků na cestovné na vybranou konferenci CCC2011 (původní odhad nákladů byl stanoven na základě jiného typu konference) a prostředků na vložné a školení.

## Literatura a odkazy

- [1] *Pavel Vachek*: LaBrea – Technická zpráva CESNETu č. 5/2006  
<http://www.cesnet.cz/doc/techzpravy/2006/ids/>
- [2] *Jan Goebel, Jens Hektor, Thorsten Holz*: *Advanced honeypot-based intrusion detection* ;login: v.31 n.6 – <http://www.usenix.org/publications/login/>
- [3] *Aleš Padrta*: Zvýšení odborné kvalifikace specialistů ZČU v Plzni v oblasti bezpečnost počítačových sítí a systémů  
Závěrečná zpráva FR CESNET projektu 155/2005  
<http://fondrozvoje.cesnet.cz/projekt.aspx?ID=155>
- [4] *Pavel Vachek*: CESNET Intrusion Detection System  
Technická zpráva CESNETu číslo 5/2006  
<http://www.cesnet.cz/doc/techzpravy/2006/ids/>
- [5] *Michal Petrovič, Aleš Padrta*: Řešení bezpečnostních incidentů v počítačové síti Západočeské univerzity  
Závěrečná zpráva FR CESNET projektu 218/2007  
<http://fondrozvoje.cesnet.cz/projekt.aspx?ID=218>
- [6] *Radoslav Bodó, Aleš Padrta*: Rozvoj systémů pro detekci průniků v síti WEBnet  
Závěrečná zpráva FR CESNET projektu 230R2/2007  
<http://fondrozvoje.cesnet.cz/projekt.aspx?ID=230>
- [7] PacketFence: Open Source NAC (Network Access Control)  
<http://www.packetfence.org>
- [8] *Tom Podermański, Matěj Grégr*: Tom Podermański, Matěj Grégr  
Seminář Monitorování provozu kampusových sítí, 2011  
<http://www.cesnet.cz/akce/2011/monitorovani-kampusovych-siti/p/podemanski-monitoring-ipv6-toku.pdf>
- [9] NAV: Network Administration Visualized  
<http://metanav.uninett.no/>
- [10] *Aleš Padrta, Jan Mach, Radek Orkáč*: Využití loggingu  
Seminář Monitorování provozu kampusových sítí, 2011  
<http://www.cesnet.cz/akce/2011/monitorovani-kampusovych-siti/p/padrta-logging.pdf>
- [11] *Greg Conti*: Security Data Visualization  
ISBN: 978-1-59327-143-5
- [12] The Intrusion Detection Message Exchange Format (IDMEF)  
<http://tools.ietf.org/html/rfc4765>
- [13] *Radoslav Bodó, Daniel Kouřil*: EGI Security Challenge 5: Lehce na cvičišti  
Sborník konference Europol.cz, podzim 2011, Želiv  
ISBN: 978-80-86583-22-8
- [14] *Radoslav Bodó*: Zkušenosti s IDS  
Seminář Monitorování provozu kampusových sítí, 2011  
<http://www.cesnet.cz/akce/2011/monitorovani-kampusovych-siti/p/bodo-ids-zkusenosti.pdf>
- [15] *Michal Kostěnek*: Honeypoty Kippo a Dionaea  
Seminář Monitorování provozu kampusových sítí, 2011  
<http://www.cesnet.cz/akce/2011/monitorovani-kampusovych-siti/p/kostenec-honeypot.pdf>
- [16] *Michal Kostěnek*: Řešení bezpečnostních incidentů v síti  
Diplomová práce, 2009, Plzeň

## A Přílohy

### A.1 Ukázka časování zpracování incidentů



ID	IP	MAC	Organization	Incident Description	Status	Tool
103	147.228.181.74	c4:17:fe:4d:dd:17	eduroam-n330.zcu.cz	DEBUG: searchradius: epsilon=0, date=2011-10-26 17:12:10, type=ip, starttime=2011-10-26 17:12:00, st	blocked	p2pshare
bodik	The Teaching Compan	130513		2011-10-31 08:22:00	2011-10-26 17:12:00	scan
[sphr2#103] Pohovor s pracovníky CIV				DEBUG: searchradius: epsilon=0, date=2011-10-27 09:02:27, type=ip, starttime=2011-10-27 09:02:00, st	banned	p2pshare
				2011-10-31 08:31:00	2011-10-27 09:02:00	
				DEBUG: searchradius: epsilon=0, date=2011-10-27 09:22:50, type=ip, starttime=2011-10-27 09:22:00, st	blocked	p2pshare
				2011-10-31 08:35:00	2011-10-27 09:22:00	
				DEBUG: searchradius: epsilon=0, date=2011-10-27 16:00:00, type=ip, starttime=2011-10-27 16:00:00, st	closed	scan
				2011-10-31 09:15:00	2011-10-27 16:00:00	
				2011-10-31 09:23:00	2011-10-24 16:18:00	p2pshare
				tool na blokovani bruteforcu na ftp zahitil freda	closed	other
				2011-10-31 15:15:00	2011-10-31 15:15:00	

Obrázek 17: Ukázka načasování zpracování incidentů

## A.2 Množiny incidentů pro vyhodnocení změny procesu

bez mysphere2 Incident	RT	pocatecni oznameni	informovani uzivatele	prvni reakce uzivatele	vyreseni incidentu		TTIU [m]	TTFR [m]	TTR [m]
p2pshare4	115280	Nov 11 14:26:04 2010	Nov 12 07:06:59 2010	Nov 20 10:30:55 2010	Nov 23 13:12:24 2010		1001	11724	17206
p2pshare5	92311	May 04 12:15:31 2009	May 04 14:18:24 2009	May 06 15:14:30 2009	May 06 15:14:30 2009		123	2936	3059
p2pshare6	105914	May 11 15:24:43 2010	May 12 08:03:56 2010	May 12 16:50:44 2010	May 17 12:10:11 2010		999	527	8445
botnet4	116135	Dec 06 05:17:32 2010	Dec 06 17:23:53 2010	Dec 06 17:54:37 2010	Dec 06 20:14:05 2010		726	31	897
botnet5	115766	Nov 25 21:02:17 2010	Nov 26 13:54:16 2010	Nov 26 15:55:23 2010	Nov 30 15:53:10 2010		1012	121	6891
botnet6	117558	Jan 24 06:57:23 2011	Jan 24 09:17:44 2011	Jan 26 06:48:57 2011	Jan 26 13:50:36 2011		140	2731	3293
spam4	115213	Nov 10 17:11:08 2010	Nov 10 19:36:38 2010	Nov 14 14:07:30 2010	Nov 15 07:12:51 2010		146	5431	6602
spam5	103951	Mar 11 12:40:46 2010	Mar 11 14:07:54 2010	Mar 11 14:24:48 2010	Mar 19 12:07:21 2010		87	17	11487
spam6	113324	Sep 27 16:30:28 2010	Sep 29 07:55:05 2010	Nov 16 20:37:08 2010	Nov 17 11:42:00 2010		2365	69942	73212
scan4	113269	Sep 27 12:05:47 2010	Sep 27 13:13:14 2010	Oct 01 08:58:47 2010	Oct 01 09:08:55 2010		67	5506	5583
scan5	108410	Aug 04 08:23:48 2010	Aug 04 10:00:51 2010	Aug 04 11:32:53 2010	Oct 22 07:49:41 2010		97	92	113726
scan6	103132	Feb 23 13:05:39 2010	Feb 23 13:13:59 2010	Mar 31 11:38:11 2010	Apr 08 09:51:38 2010		8	51684	63106
						Průměr	564	12562	26126
						Medián	143	2834	7668
s mysphere2 Incident	RT	pocatecni oznameni	informovani uzivatele	prvni reakce uzivatele	vyreseni incidentu		TTIU [m]	TTFR [m]	TTR [m]
p2pshare1	130513	Oct 29 02:06:01 2011	Oct 31 08:24:31 2011	Nov 06 20:55:25 2011	Nov 07 11:20:14 2011		3319	9391	13574
p2pshare2	130754	Nov 03 14:38:45 2011	Nov 04 08:22:39 2011	Nov 04 11:24:45 2011	Nov 07 09:41:37 2011		1064	182	5463
p2pshare3	127905	Sep 15 12:44:55 2011	Sep 15 13:17:29 2011	Sep 22 16:36:50 2011	Sep 30 14:46:47 2011		33	10279	21722
botnet1	124504	Jul 01 07:58:04 2011	Jul 01 14:20:48 2011	Jul 12 11:37:44 2011	Jul 12 11:45:18 2011		383	15677	16067
botnet2	130638	Nov 02 06:59:45 2011	Nov 02 09:08:21 2011	Nov 02 10:47:17 2011	Nov 02 10:59:25 2011		129	99	240
botnet3	130399	Oct 27 07:59:48 2011	Oct 27 10:15:16 2011	Oct 27 12:48:09 2011	Oct 31 08:52:25 2011		135	153	5873
spam1	126309	Aug 22 15:38:36 2011	Aug 23 16:19:19 2011	Aug 23 20:55:16 2011	Aug 23 21:16:59 2011		1481	276	1778
spam2	124768	Jul 08 07:00:00 2011	Jul 11 22:16:36 2011	Jul 12 11:38:48 2011	Jul 12 13:33:23 2011		5237	802	6153
spam3	130402	Oct 27 07:00:00 2011	Oct 27 10:33:40 2011	Nov 13 12:09:24 2011	Nov 14 10:22:05 2011		214	24636	26182
scan1	122702	May 17 14:15:40 2011	May 17 20:57:06 2011	May 19 12:01:35 2011	May 19 14:00:01 2011		401	2344	2864
scan2	127033	Sep 05 07:00:00 2011	Sep 05 10:59:06 2011	Sep 05 14:50:51 2011	Sep 08 08:27:39 2011		239	232	4408
scan3	128627	Sep 23 07:00:00 2011	Sep 23 19:10:34 2011	Sep 26 15:40:00 2011	Oct 05 11:09:07 2011		731	4109	17529
						Průměr	1114	5682	10154
						Medián	392	1573	6013

### A.3 Nastavení karanténního firewallu

```
# Generated by iptables-save v1.4.8 on Fri May 20 11:41:02 2011
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]

:BASE - [0:0]
:SHELL - [0:0]
:WEB - [0:0]

:QUARANTINEF - [0:0]

# zakladni prostredky pro ziskani konektivity a prihlaseni uzivatele
:KDC - [0:0]
:DNS - [0:0]
:LDAP - [0:0]
:AFS - [0:0]
:NTP - [0:0]
# aaa
:STROJE - [0:0]
:FAIS - [0:0]
:FTPZCU - [0:0]

# ciste webove filtry (aaa
:SUPPORT - [0:0]
:DOWNLOAD - [0:0]
:PHONE - [0:0]
:WEBKDC - [0:0]
:WEBMAIL - [0:0]
:EPO - [0:0]

-A INPUT -s 147.228.0.0/16 -j WEB
-A INPUT -s 147.228.0.0/16 -j SHELL
-A INPUT -j BASE

-A BASE -s 127.0.0.0/8 -i lo -j ACCEPT
-A BASE -m state --state RELATED,ESTABLISHED -j ACCEPT
-A BASE -p tcp -m tcp --dport 113 -j REJECT --reject-with icmp-port-unreachable
-A BASE -p icmp -j ACCEPT
-A SHELL -p tcp -m tcp --dport 22 -j ACCEPT
-A WEB -p tcp -m tcp --dport 80 -j ACCEPT
-A WEB -p tcp -m tcp --dport 443 -j ACCEPT

-A FORWARD -i eth1 -j QUARANTINEF
-A FORWARD -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT

-A QUARANTINEF -j KDC
-A QUARANTINEF -j DNS
-A QUARANTINEF -j LDAP
-A QUARANTINEF -j AFS
-A QUARANTINEF -j NTP
-A QUARANTINEF -j STROJE
-A QUARANTINEF -j FAIS

-A QUARANTINEF -j SUPPORT
-A QUARANTINEF -j PHONE
-A QUARANTINEF -j DOWNLOAD
-A QUARANTINEF -j WEBKDC
-A QUARANTINEF -j WEBMAIL
-A QUARANTINEF -j EPO

-A KDC -d 147.228.aa.aa/32 -m udp -p udp --dport 88 -j ACCEPT
-A KDC -d 147.228.aa.aa/32 -m udp -p udp --dport 88 -j ACCEPT
-A KDC -d 147.228.aa.aa/32 -m udp -p udp --dport 88 -j ACCEPT
# aa windowsi AD
-A KDC -d 147.228.aa.aa/32 -j ACCEPT
-A KDC -d 147.228.aa.aa/32 -j ACCEPT

-A DNS -d 147.228.aa.aa -m udp -p udp --dport 53 -j ACCEPT
-A DNS -d 147.228.aa.aa -m udp -p udp --dport 53 -j ACCEPT
-A DNS -d 147.228.aa.aa -m udp -p udp --dport 53 -j ACCEPT

-A LDAP -d 147.228.aa.aa -m multiport -p tcp --dports 389,636 -j ACCEPT
-A LDAP -d 147.228.aa.aa -m multiport -p tcp --dports 389,636 -j ACCEPT

-A AFS -p udp -m multiport --dports 7000:7010 -j ACCEPT
```



```
-A NTP -p udp -m multiport --port 123 -j ACCEPT

-A FAIS -d 147.228.aa.aa/32 -j ACCEPT
-A FAIS -d 147.228.aa.aa/32 -j ACCEPT
-A FAIS -d 147.228.aa.aa/32 -j ACCEPT

#TODO: port range ...
-A FTPZCU -d 147.228.aa.aa/32 -j ACCEPT

-A STROJE -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A SUPPORT -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A PHONE -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A DOWNLOAD -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A WEBKDC -d 147.228.aa.aa -m tcp -p tcp --dport 443 -j ACCEPT
-A WEBKDC -d 147.228.aa.aa -m tcp -p tcp --dport 443 -j ACCEPT
-A WEBKDC -d 147.228.aa.aa -m tcp -p tcp --dport 443 -j ACCEPT
-A WEBMAIL -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A EPO -d 147.228.aa.aa -m multiport -p tcp --dports 80,443,8443,8444 -j ACCEPT


COMMIT
# Completed on Fri May 20 11:41:02 2011
# Generated by iptables-save v1.4.8 on Fri May 20 11:41:02 2011
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
#tohle tady musi byt kvuli kradeni weboveho trafficu
:STROJE - [0:0]
:SUPPORT - [0:0]
:DOWNLOAD - [0:0]
:PHONE - [0:0]
:WEBKDC - [0:0]
:WEBMAIL - [0:0]
:EPO - [0:0]
:FTPZCU - [0:0]

-A PREROUTING -i eth1 -j STROJE
-A PREROUTING -i eth1 -j SUPPORT
-A PREROUTING -i eth1 -j PHONE
-A PREROUTING -i eth1 -j DOWNLOAD
-A PREROUTING -i eth1 -j WEBKDC
-A PREROUTING -i eth1 -j WEBMAIL
-A PREROUTING -i eth1 -j EPO
-A PREROUTING -i eth1 -j FTPZCU
-A PREROUTING -i eth1 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 80
-A PREROUTING -i eth1 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 443

-A STROJE -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A SUPPORT -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A PHONE -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A DOWNLOAD -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A WEBKDC -d 147.228.aa.aa -m tcp -p tcp --dport 443 -j ACCEPT
-A WEBKDC -d 147.228.aa.aa -m tcp -p tcp --dport 443 -j ACCEPT
-A WEBKDC -d 147.228.aa.aa -m tcp -p tcp --dport 443 -j ACCEPT
-A WEBMAIL -d 147.228.aa.aa -m multiport -p tcp --dports 80,443 -j ACCEPT
-A EPO -d 147.228.aa.aa -m multiport -p tcp --dports 80,443,8443,8444 -j ACCEPT
#TODO: port range ...
-A FTPZCU -d 147.228.aa.aa/32 -j ACCEPT

COMMIT
# Completed on Fri May 20 11:41:02 2011
```

## A.4 Ukázky obrazovek pro získání zpětné vazby od uživatele


**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 odvírování 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).

- ▶ <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](#).

Obrázek 18: Informační stránka responses/virus.


**Mysphere2: Automat pro správu bezpečnostních incidentů**
[studentx]

**INFO: Přihlášení bylo úspěšné**

**Reagovat na incident (sphr2 l#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>

Dobry den, rad bych si s Vami smluvil schůzku ohledně incidentu [sphr2#119]  
K pohovoru se mohu dostavit kterýkoli den, nejlépe však

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](https://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](mailto:abuse@zcu.cz) ručně. Zprávu formulujte podle vzoru:

Subject: [ZCU RT3 #131555] [sphr2#119] Pohovor s pracovníky CIV - Test Konto NENI\_PRACOVISTE  
AddRequestor: studentx@civ.zcu.cz

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

-----

Dobry den, rad bych si s Vami smluvil schůzku ohledně incidentu [sphr2#119]  
K pohovoru se mohu dostavit kterýkoli den, nejlépe však

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.

Obrázek 19: Informační stránka [responses/p2pshare](#).

## A.5 support.zcu.cz :: Jak postupovat v případě zavirování počítače

### Jak postupovat v případě zavirování počítače

#### Obsah

- 1 Proč mi virus zavíroval počítač ?
- 2 Jak k tomu mohlo dojít ?
- 3 Jak se zachovat v případě napadení ?
- 4 Jak napadení předcházet ?

#### Proč mi virus zavíroval počítač ?

Díky internetu, celosvětové komunikační sítí, 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 útočnickovy účely a
- využití počítače pro uložení útočnickových 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 uživatelskou plochu, slibují bezplatnou antivirovou ochranu nebo zrychlené připojení k internetu. Dalším případem to bývají tzv. *crack*y pro 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 zavírovaného dokumentu (hromadné přeposílání vtipných prezentací), zavírovaného emailu nebo jeho přílohy. Případně může útočník využít některou z chyb operačního systému vzdáleně po síti, aniž byste se o nákazu museli sami přičinit.

#### Jak se zachovat v případě napadení ?

Je potřeba počítač preinstalovat, tento (mnohdy velmi nepříjemný) krok představuje nejbezpečnější postup jak se viru zbavit. Pouhé odvírování pomocí některého z antivirových programů nemusí být dostačující.

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 soubory vašich oblíbených programů.
- ihned po instalaci operačního systému byste měli nainstalovat
  - antivirový software ( Kaspersky Anti-Virus, McAfee, Avast (<http://www.avast.com/cs-cz/free-antivirus-download>) )
  - firewall ( Kaspersky Anti-Virus, McAfee, Avast (<http://www.avast.com/cs-cz/free-antivirus-download>) ), nebo využívat ochranu poskytovanou operačním systémem
  - aktualizovat operační systém a zapnout automatické aktualizace (MS Windows ([http://www.microsoft.com/cze/athome/security/update/msupdate\\_keep\\_current.mspx](http://www.microsoft.com/cze/athome/security/update/msupdate_keep_current.mspx)) )

- v případě instalace 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 (připojil se k php aplikaci podobně jako k exe souboru).
- po instalaci (nebo i před ní, ale z bezpečného počítače) byste měli změnit všechna důležitá používaná hesla (Orion heslo, heslo pro internetbanking, ...)
- před natažením zazálohovaných osobních dat byste měli udělat jejich důkladnou antivirovou kontrolu
- provést antivirovou kontrolu všech mobilních zařízení (mobilní telefon, mp3 přehrávač, ...) a úložišť dat (USB disky, fotoaparáty, ...)
- zamyslet se nad způsobem, jak a kdy mohlo dojít k napadení počítače a pro příště se takové činnosti vyvarovat

## Jak napadení předcházet ?

Měli byste dodržovat několik zásad bezpečného chování při práci s počítačem:

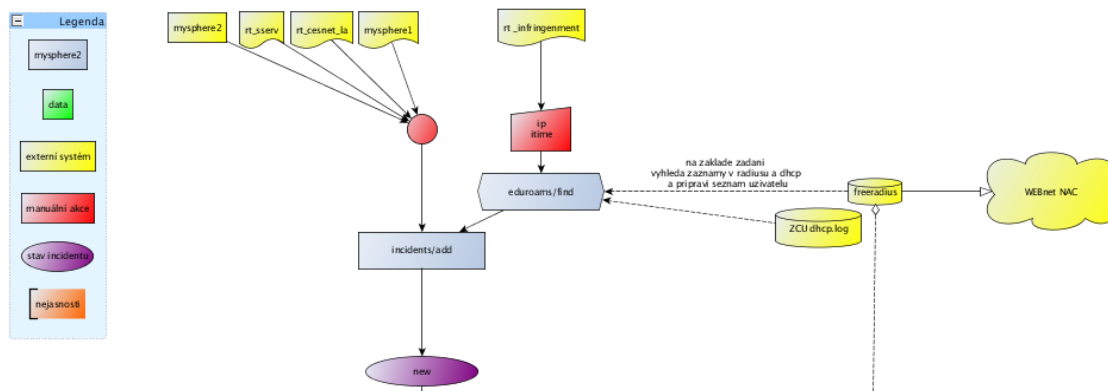
- používat aktualizovaný operační systém a aktualizované verze používaných programů
- vždy používat systém antivirové ochrany a firewall
- pro běžnou práci používat neprivilegovaný účet (nepracovat pod administrátorem)
- upřednostňovat bezpečné varianty internetových protokolů (https, ssh, ftps, ...)
- správně zacházet s přístupovými hesly
- neotevírat nevyžádané emaily
- používat pouze ověřené programy z ověřených zdrojů
- používat legálně nabitý SW. V dnešní době existuje téměř ke každému komerčnímu produktu jeho volně šiřitelná varianta
- administrátoři serverů nebo většího počtu stanic by měli sledovat bezpečnostní zprávy týkající se jimi provozovaných produktů nebo jiné portály zabývající se aktuální bezpečnostní situací v internetu ISC - Internet Storm Center (<https://isc.sans.edu>)

**Přehled nejčastěji používaných volně šiřitelných variant SW**

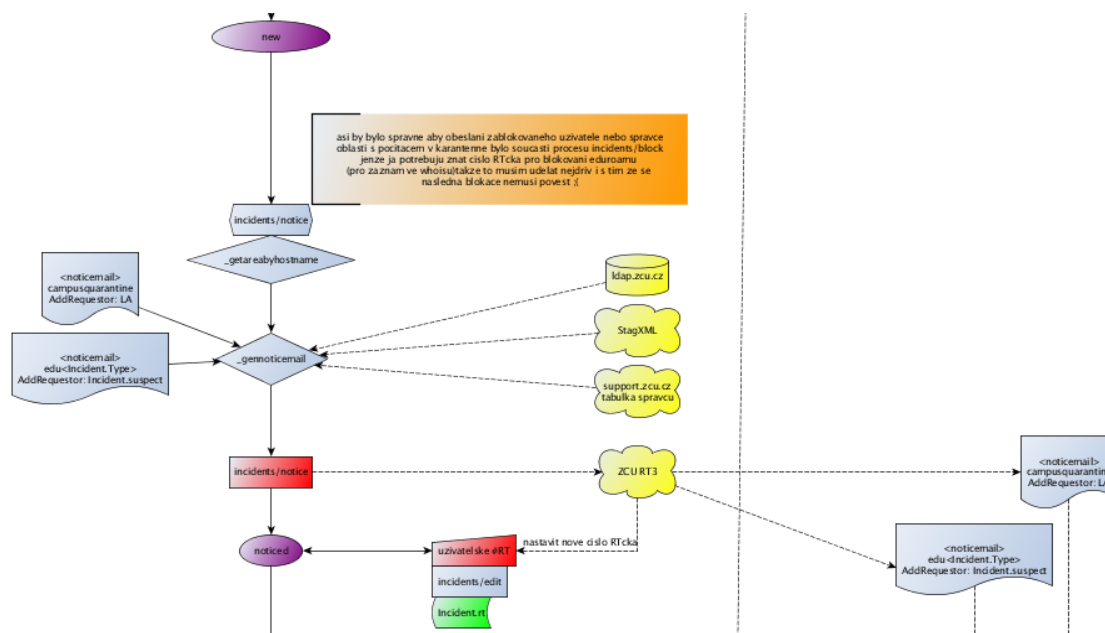
Program	Produkt	Alternativa
<b>Operační systém</b>	MS Windows	Debian GNU/Linux ( <a href="http://www.debian.org/distrib/index.cs.html">http://www.debian.org/distrib/index.cs.html</a> ) ; Ubuntu ( <a href="http://www.ubuntu.cz/ziskejte/stahnout">http://www.ubuntu.cz/ziskejte/stahnout</a> )
<b>Textový procesor</b>	MS Office	OpenOffice ( <a href="http://www.openoffice.cz/stahnout">http://www.openoffice.cz/stahnout</a> )
<b>Emailový klient</b>	MS Outlook	Mozilla Thunderbird ( <a href="http://czilla.cz/produkty/thunderbird/">http://czilla.cz/produkty/thunderbird/</a> )
<b>Webový browser</b>	MS Internet Explorer	Mozilla Firefox ( <a href="http://czilla.cz/produkty/firefox/">http://czilla.cz/produkty/firefox/</a> )
<b>Editor obrázků</b>	Adobe Photoshop	GIMP ( <a href="http://www.gimp.cz">http://www.gimp.cz</a> )
<b>Editor vektorové grafiky</b>	Corel Draw	Inkscape ( <a href="http://inkscape.org/download/?lang=cs">http://inkscape.org/download/?lang=cs</a> )
<b>Videostřížna</b>	Adobe Premiere	Kino
<b>Editor hudby</b>	SoundForge	Audacity ( <a href="http://audacity.sourceforge.net/?lang=cs">http://audacity.sourceforge.net/?lang=cs</a> )

Kategorie: Bezpečnost | Bodikoviny

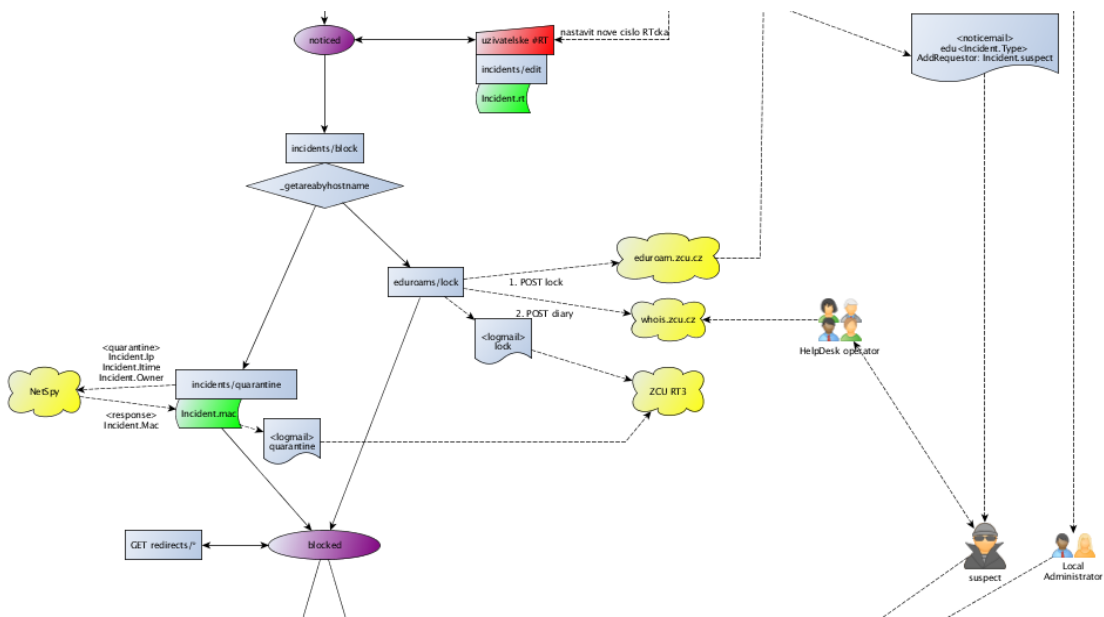
## A.6 Podrobný vývojový diagram



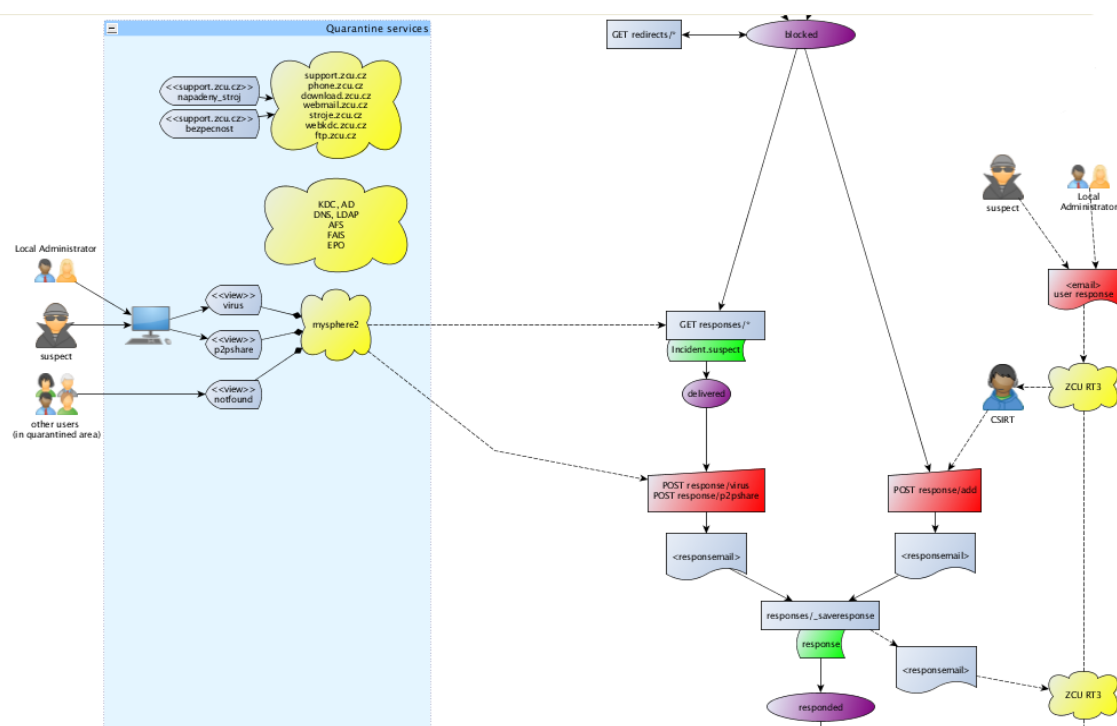
Obrázek 20: Vývojový diagram: Založení incidentu.



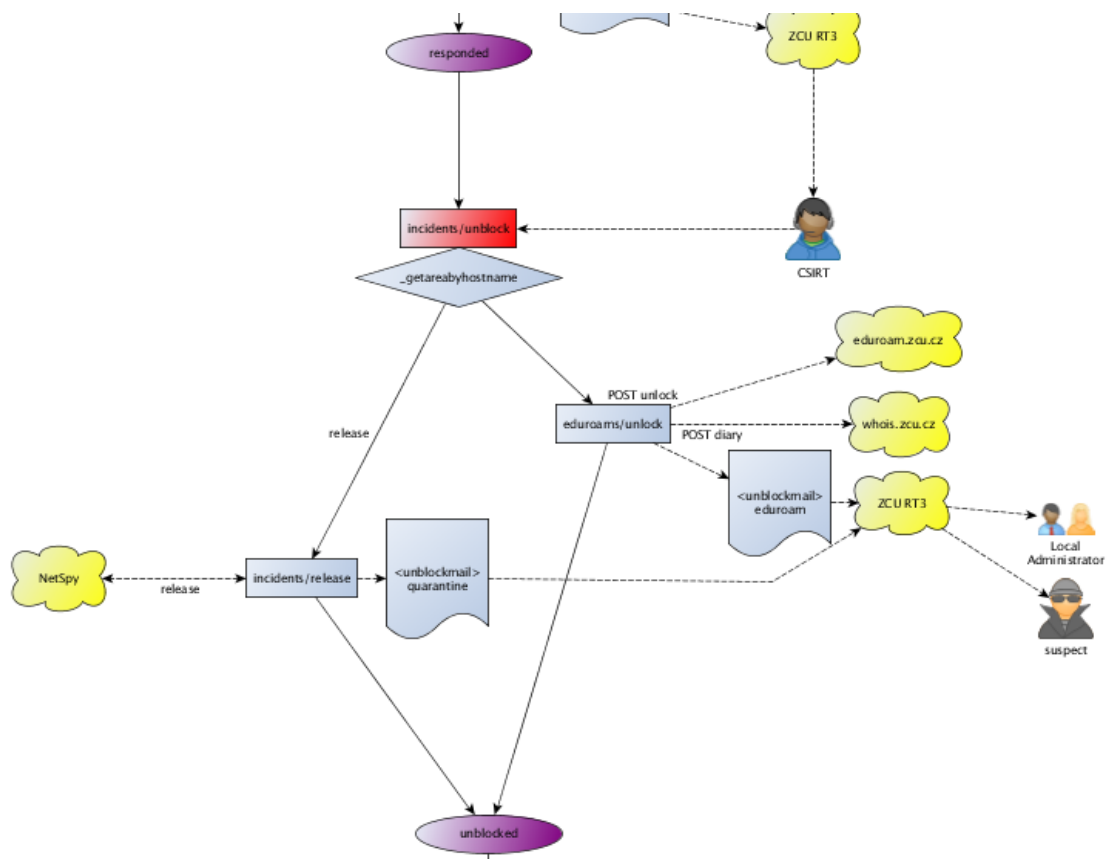
Obrázek 21: Vývojový diagram: Informování uživatele.



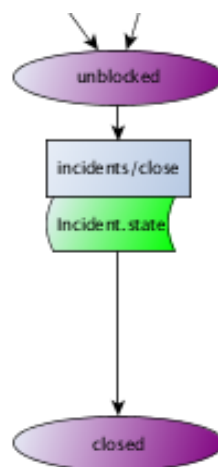
Obrázek 22: Vývojový diagram: Zablokování uživatele.



Obrázek 23: Vývojový diagram: Získání zpětné vazby.



Obrázek 24: Vývojový diagram: Odblokování uživatele.



Obrázek 25: Vývojový diagram: zavření incidentu.



## A.7 Ukázky administrátorské části aplikace Mysphere2

**INFO: The incident has been saved**

Incident Actions: [NOTICE](#) [BLOCK](#) [ADDRESSP](#) [UNBLOCK](#) [UNBLOCKMAIL](#) [CLOSE](#) [Edit Incident](#) [Delete Incident](#) [List Incidents](#) [New Incident](#) [List Responses](#) [New Response](#)

Id	119
Ip	147.228.53.147 <a href="#">netspy</a>
Mac	
Hostname	ui505p02-lps.civ.zcu.cz
State	<a href="#">new</a>
Type	<a href="#">p2pshare</a>
Owner	bodik
Claimant	<a href="#">bodik</a>
Rt	<a href="#">666</a>
Ctime	2011-11-18 14:34:00
Itime	2011-11-18 14:34:00
Suspect	
Text	pro screenshoty

**Related Responses** [New Response](#)

Obrázek 26: View incidents/view

Seznam lokálních spravců

**Notice Incident**

id:

Requestor:

Givenname:

Surname:

Department:

Subject: [sphr2#119] ui505p02-lps.civ.zcu.cz - porušování autorských práv  
 AddRequestor: CIV <abuse@zcu.cz>  
 AddDependsOn: 666

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

stroj ui505p02-lps.civ.zcu.cz (147.228.53.147),  
 který je pravděpodobně ve vaší správě, byl z důvodů nevhodného  
 chování na síti odpojen od sítě WEBnet.

Konkrétně sdělení obsahu pomocí P2P sítě, na které se vztahuje autorský zákon.

Informace o dalším postupu můžete vy nebo uživatel stroje získat pomocí  
 browseru na zmíněném stroji pomocí webového rozhraní karanténí sítě  
 do které byl stroj přesunut.

Na tento email neodpovídejte, pro reakci použijte webové rozhraní  
 karanténího systému.

S pozdravem  
 Radoslav BODŮ, WEBnet Incident Response Team  
 Incident je spravován s pomocí systému mysphere2

[Notice](#)

Obrázek 27: View incidents/notice

Actions	Id	Ip	Mac	Hostname	Text	State	Type
[F] [R]						--	--
						Time	Suspect
[V] [E] [D] [N] [B] [U] [C]	59	147.228.53.150	00:11:09:d1:1a:18	u505p02-lps.civ.zcu.cz	testovací incident	unblocked	spam
		bodík	mysphere1	124412	2011-06-29 16:38:00	2011-06-29 16:38:00	
[V] [E] [D] [N] [B] [U] [C]	52	147.228.185.145	0c:ee:a6:a6:22:c0	zcu-mobile-n401.zcu.cz	/home/bodík/winearch2.pl Time sum(bytes) sum(pck) sp	blocked	scan
		bodík	mysphere1	123355	2011-06-02 08:01:00	2011-06-01 10:00:00	
[V] [E] [D] [N] [B] [U] [C]	56	147.228.180.131	00:16:ea:7b:e8:c6	eduroam-n131.zcu.cz	DEBUG: searchradius: epslon=0, date=2011-06-13 08:44:42, type=ip, starttime=2011-06-13 08:44:00, st	blocked	botnet
		bodík	SSERV	123975	2011-06-16 18:18:00	2011-06-13 08:44:00	
[V] [E] [D] [N] [B] [U] [C]	65	147.228.181.181	00:24:2b:04:7b:a3	eduroam-n437.zcu.cz	mysphere1 /home/bodík/winearch2.pl Time sum(bytes) sum(pck) si	noticed	botnet
		bodík	sserv	124821	2011-07-13 12:57:00	2011-07-11 15:43:00	
[V] [E] [D] [N] [B] [U] [C]	67	147.228.167.46	00:1a:92:f1:d1:8b	http://edison.fpe.zcu.cz/	Evidentiary Information: Notice ID: 22-156395469 Initial Infringement Timestamp: 8 Aug 2011 19	blocked	pcshare
		apadna	BayTSP	125702	2011-08-08 21:26:00	2011-08-09 22:58:00	
[V] [E] [D] [N] [B] [U] [C]	77	147.228.180.44	00:24:23:07:e8:4a	eduroam-n44.zcu.cz	inf time je o 5 minut jinde, ale predpokladam ze to byl on ... ..... DEBUG: search	banned	pcshare

Obrázek 28: View incidents/index

## A.8 Ukázky generovaných informačních emailů

**History**

# Fri Nov 18 14:51:34 2011 **sphr2 (sphr2@civ.zcu.cz) - Ticket created**

**Subject:** [sphr2#119] ui505p02-lps.civ.zcu.cz - porušování autorských práv  
**Date:** Fri, 18 Nov 2011 14:51:31 +0100  
**To:** security@service.zcu.cz  
**From:** sphr2@civ.zcu.cz

---

AddRequestor: CIV <abuse@zcu.cz>  
AddDependsOn: 122731

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

Dobrý den,

stroj ui505p02-lps.civ.zcu.cz (147.228.53.147),  
který je pravděpodobně ve vaší správě, byl z důvodů nevhodného  
chování na síti odpojen od sítě WEBnet.

Konkrétně sdělení obsahu pomocí P2P sítě, na které se vztahuje autorský zákon.

Informace o dalším postupu můžete vy nebo uživatel stroje získat pomocí  
browseru na zmíněném stroji pomocí webového rozhraní karanténní sítě  
do které byl stroj přesunut.

Na tento email neodpovídejte, pro reakci použijte webové rozhraní  
karanténního systému.

S pozdravem  
Radoslav BODÓ, WEBnet Incident Response Team  
Incident je spravován s pomocí systému mysphere2

#

Fri Nov 18 14:53:50 2011 **sphr2 (sphr2@civ.zcu.cz) - Comments added**  
**Subject:** [ZCU RT3 #131555] [sphr2#119] logmail  
**Date:** Fri, 18 Nov 2011 14:53:48 +0100  
**To:** security-com@service.zcu.cz  
**From:** sphr2@civ.zcu.cz

logmail  
INFO: sphr2: quarantined ui505p02-lps.civ.zcu.cz 147.228.53.147 00:11:09:d1:1c:35

#

Fri Nov 18 15:06:38 2011 **sphr2 (sphr2@civ.zcu.cz) - Requestor studentx added**  
Fri Nov 18 15:06:38 2011 **sphr2 (sphr2@civ.zcu.cz) - Comments added**  
**Subject:** [ZCU RT3 #131555] [sphr2#119] ui505p02-lps.civ.zcu.cz - napadený stroj  
**Date:** Fri, 18 Nov 2011 15:06:29 +0100  
**To:** security-com@service.zcu.cz  
**From:** sphr2@civ.zcu.cz

AddRequestor: studentx@civ.zcu.cz  
  
Text nad tímto řádkem ignorujte, následuje sdělení pro uživatele...  
Please ignore lines above, message for user follows ...  
-----  
<?xml version="1.0" encoding="utf-8"?>  
<xml>  
<response>  
<actiontaken>reinstalled</actiontaken>  
<notes>Kdo stahuje nelegálně, podporuje komunismus.</notes>  
<username>studentx</username>  
<incident\_id>119</incident\_id>  
<date>2011-11-18T15:06:29+01:00</date>  
</response>  
<incident>  
<id>119</id>  
<ip>147.228.53.147</ip>  
<mac>00:11:09:d1:1c:35</mac>  
<hostname>ui505p02-lps.civ.zcu.cz</hostname>  
<text>pro screenshoty</text>  
<state\_id>4</state\_id>  
<type\_id>3</type\_id>  
<owner>bodik</owner>  
<claimant>bodik</claimant>  
<rt>131555</rt>  
<ctime>2011-11-18 14:34:00</ctime>  
<itime>2011-11-18 14:34:00</itime>  
<suspect>studentx</suspect>  
</incident>  
</xml>

#

Fri Nov 18 15:13:15 2011 **sphr2 (sphr2@civ.zcu.cz) - Correspondence added**  
**Subject:** [ZCU RT3 #131555] [sphr2#119] napadený stroj  
**Date:** Fri, 18 Nov 2011 15:13:13 +0100  
**To:** security@service.zcu.cz  
**From:** sphr2@civ.zcu.cz

Text nad tímto řádkem ignorujte, následuje sdělení pro uživatele ...  
Please ignore lines above, message for user follows ...  
-----  
Počítač ui505p02-lps.civ.zcu.cz (147.228.53.147) byl odblokován.  
  
S pozdravem  
Radoslav BODÓ, WEBnet Incident Response Team  
Incident je spravován s pomocí systému mysphere2