

WIRT

WEBnet Incident Response Team

apadrta@civ.zcu.cz

10.5.2007, Praha

Obsah

- Co je to WIRT?
 - Z historie
 - Vznik
 - Filosofie přístupu k incidentům
 - Řešení incidentů
 - Logování
 - Ohlédnutí 2006-1Q2007
 - Zhodnocení funkčnosti
 - Přehled incidentů
 - Zajímavosti
 - Shrnutí
-
-

Co je to WIRT a proč ho milujeme?

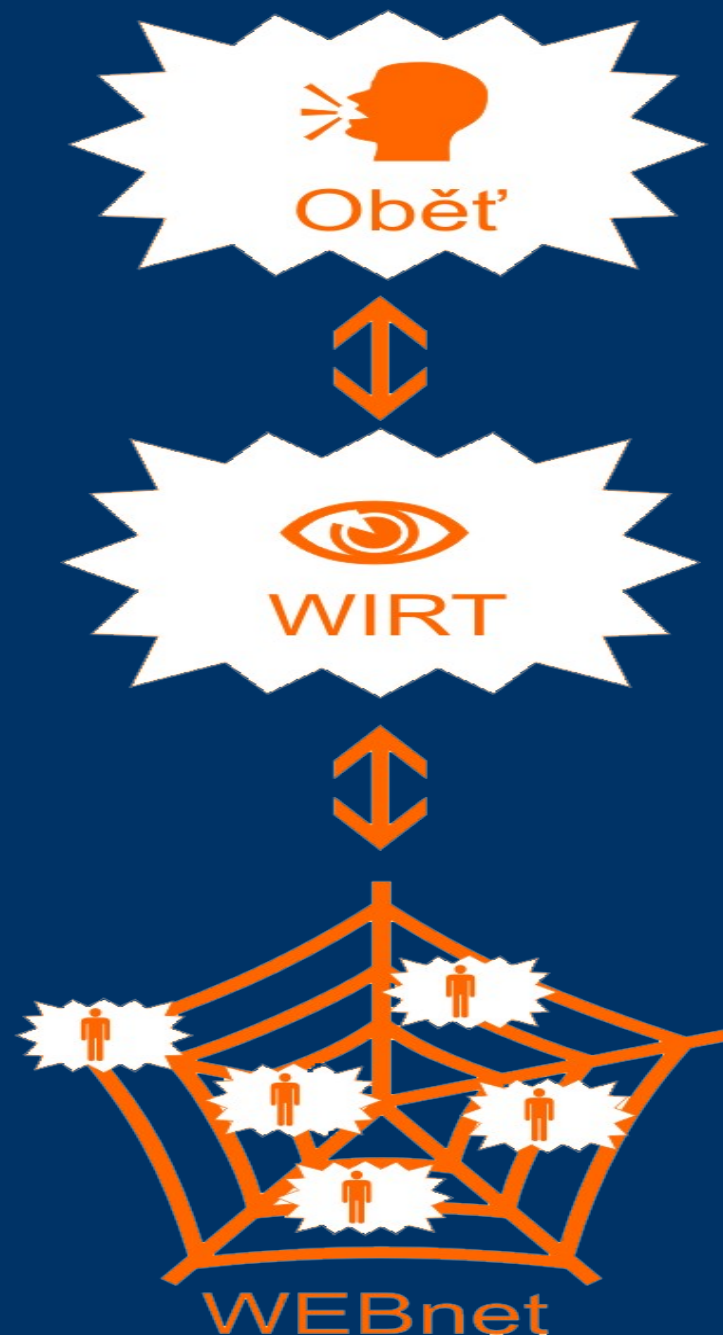
- WEBnet Incident Response Team
 - Aleš Padrta apadrta@civ.zcu.cz
 - Radoslav Bodó bodik@civ.zcu.cz
 - WEBnet
 - Síť Západočeské univerzity v Plzni
 - 147.228.0.0/16
 - Řešení bezpečnostních incidentů
 - Síťové útoky
 - Spamy
 - Viry
 - Porušování (autorského) zákona
 - ...
-
-

Z historie WIRT

- Založen 11/2005
 - inspirace: seminář CESNETu
 - formalizace stávajícího stavu
 - definice postupů
- Činnost
 - Řešení bezpečnostních incidentů
 - Primární náplň práce
 - Prevence BI
 - Technická opatření
 - Vzdělávání uživatelů

Přístup k incidentům

- Stížnosti
 - Pouze přes WIRT
 - Vnitřní řešení
- Výhody
 - Jednotný kontakt
 - Konzistentní odpovědi
 - Kvalifikovaná reakce
 - Přehled o řešení



Postup při řešení BI

- Příchod stížnosti (stěžovatel → WIRT)
 - Ověření oprávněnosti (WIRT)
 - Odstrížení od sítě (WIRT)
 - Předání stížnosti dále (WIRT → lokální správce)
 - Provedení nápravy (lokální správce/správcové)
 - Zpráva o vyřešení (lokální správce → WIRT)
 - Připojení k síti (WIRT)
 - Zpráva o vyřešení (WIRT → stěžovatel)
-
-

Postup při řešení BI

- Příchod stížnosti (stěžovatel → WIRT)
 - Ověření oprávněnosti (WIRT)
 - Odstřižení od sítě (WIRT)
 - Předání stížnosti dále (WIRT → lokální správce)
 - Provedení nápravy (lokální správce/správcové)
 - Zpráva o vyřešení (lokální správce → WIRT)
 - Připojení k síti (WIRT)
 - Zpráva o vyřešení (WIRT → stěžovatel)
-
-

Informace pro řešení BI

Logování

- Bezpečnostní incident
 - Hlášena IP adresa
 - Kdo je pachatel?
 - Co provedl?
 - Jak to provedl?
- Řešení BI
 - Vyžaduje informace
 - Co nejdelší časový úsek
 - Potřeba logování

Informace pro řešení BI

Logy WIRT

- DHCP
 - Přiřazování IP adres v čase
 - Kerberos
 - Přístupy uživatelů
 - Netflow
 - Vnější chování strojů
 - Snort, Nepenthes
 - Hlubší analýza síťového provozu
 - Eduroam
 - Přístupy uživatelů
 - Systémové logy
 - Hlášení serverů o činnosti
-
-

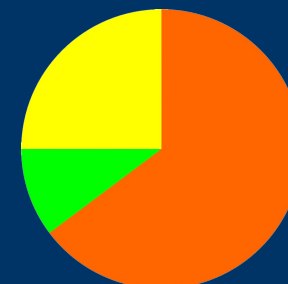
Ohlédnutí 2006 - 1Q2007

- Preventivní činnost
 - Devatero rad pro bezpečné používání sítě WEBnet
 - Seminář
 - Návody
 - Řešení BI
 - Vytvoření a sepsání postupů
 - Plná zastupitelnost členů
 - Vyřešeno 100% BI
 - Archív
 - Dokumentace vyšetřovaných případů
 - Články, postupy, ...
-
-

Ohlédnutí 2006 - 1Q2007

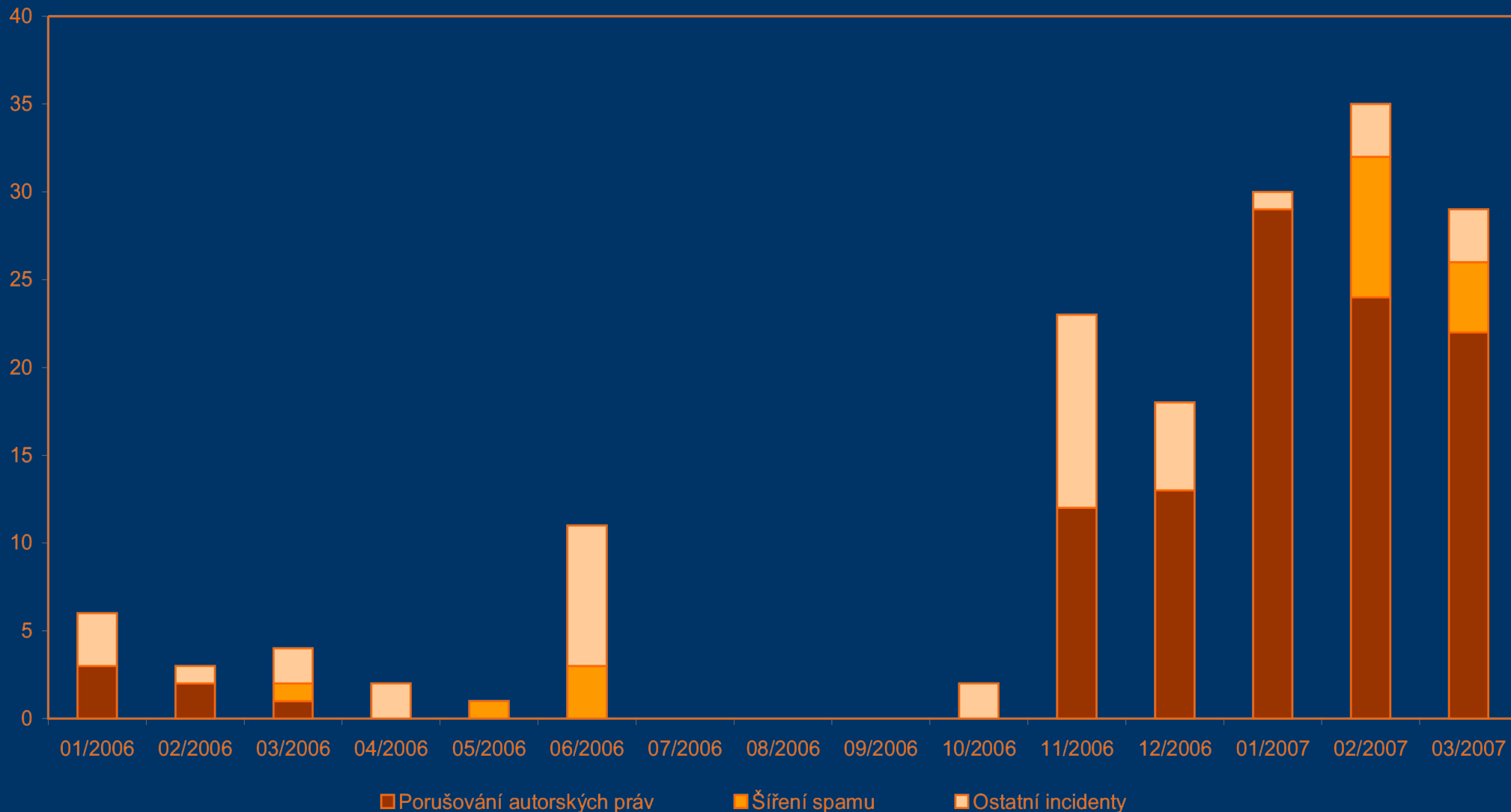
Přehled incidentů

- Detekované / hlášené incidenty - 164
- Původce incidentů
 - Mobilní připojení
 - Pracovní stanice
 - Počítačové učebny
 - Koleje
- Druhy incidentů
 - Nelegální sdílení 106 (65%)
 - Šíření spamů 17 (10%)
 - Ostatní incidenty 41 (25%)
 - nerozlišovány detailněji
 - šíření virů, zahlcení kapacity, nevhodné chování, ...



Ohlédnutí 2006 - 1Q2007

Počty bezpečnostních incidentů



Ohlédnutí 2006 - 1Q2007

Zajímavosti

- Uživatelé - mýty a výmluvy
 - Wi-fi je anonymní
 - Vinu nelze prokázat
 - Zábavné výmluvy
 - Půjčil jsem někomu na týden notebook, nevím komu
 - P2P síť se mi tam spouští sama
 - To co je v televizi je volně šířitelné
 - Před týdnem jsem to přeninstaloval, virus tam teď určitě není
 - ...
 - Efektivní metody
 - Možné vyšetřování Policií ČR
 - Disciplinární komise fakulty
 - Zablokování přístupu
-
-

Shrnutí

- Bezpečností incidenty
 - Byly, jsou a budou
 - Jejich řešení → *IRT
 - Vyšetřování → logy
 - WIRT
 - Jeden z Incident Response Teamů
 - Historie
 - Přístup k problematice
 - Zhodnocení
 - Statistika
 - *IRT do každé rodiny :-)
-
-