# Bezpečnost aktivně

–

# štěstí přeje připraveným

Andrea Kropáčová, andrea@cesnet.cz
CESNET, z. s. p. o.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI
2007–13
OP Výzkum a vývoj pro inovace

# Aktuální trendy

- Krátké, ale intenzivní DoS útoky
- Útoky na bázi amplifikace, zneužití zranitelností
- Cílené útoky na uživatele
- Více útoků -> Více bezpečnostních nástrojů -> více dat a informací

# Směr vývoje (nejen v CESNET)

- Schopnost včas zasáhnout (**reaktivní** -> **proaktivní, automatizace**)
- **Semi-automatická obrana** na bázi spolehlivé detekce
- **Eliminace zařízení** náchylných na **amplifikaci** nebo **zranitelnost**
- **Data** – lepší sběr, validace, klasifikace, analýza, obohacení, distribuce
- **Služby zaměřené na prevenci, školení**

FTAS LAB Forenzní laboratoř

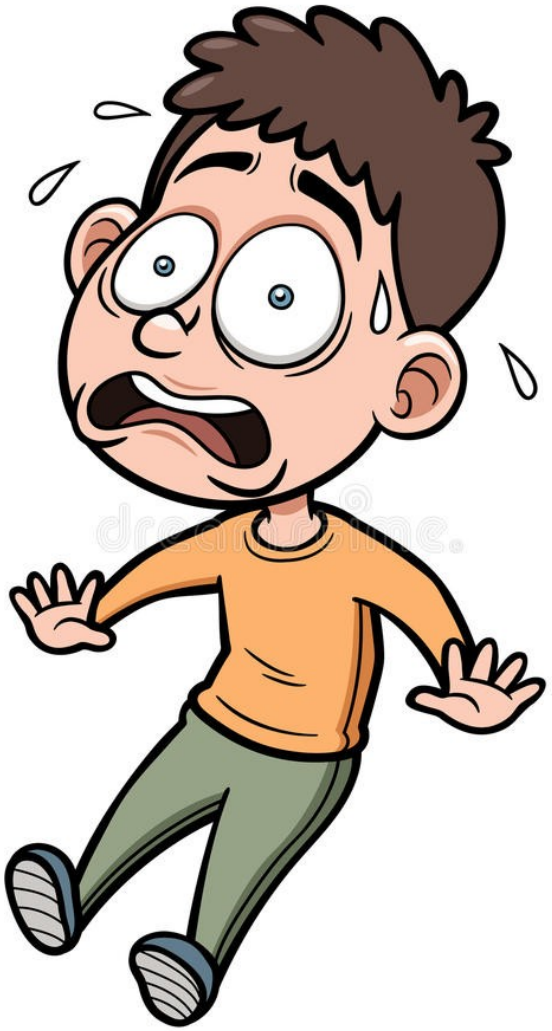
# Štěstí v CESNET

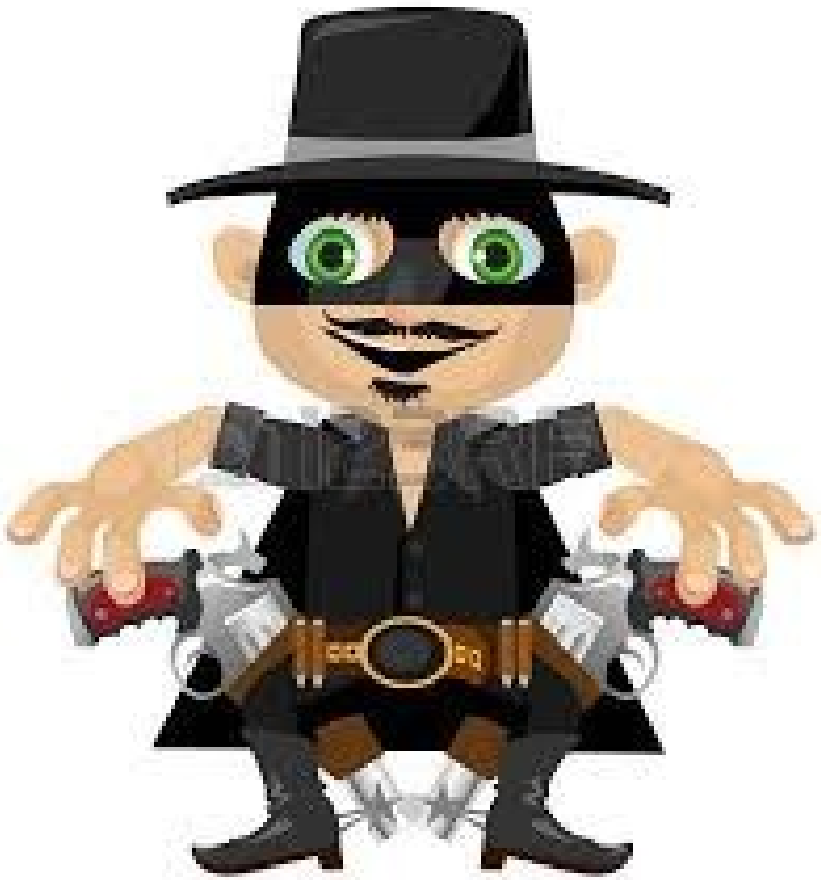
- Síťové sondy na perimetru sítě CESNET2
- Systémy FTAS a G3 (plošný monitoring na bázi toků)
- Detekční systémy – IDS, honeypoty, sondy ...
- Systémy pro sdílení informací z bezpečnostních nástrojů
- SIEM systém pro management bezpečnostních událostí
- Bezpečnostní tým CESNET-CERTS – řešení bi a pomoc při jejich zvládání
- Forenzní laboratoř – penetrační a zátěžové testy, testy sociálního inženýrství
- Antispam Gateway – ochrana před spamem
- Konzultace a pomoc při návrhu sítě a obrany
- Asistence při problému pro připojené organizace
- Vzdělávání, osvěta, (on-demand) školení
- Pracoviště stálé služby, NOC
  - dohled nad provozem sítě CESNET2
  - režim 24/7/365

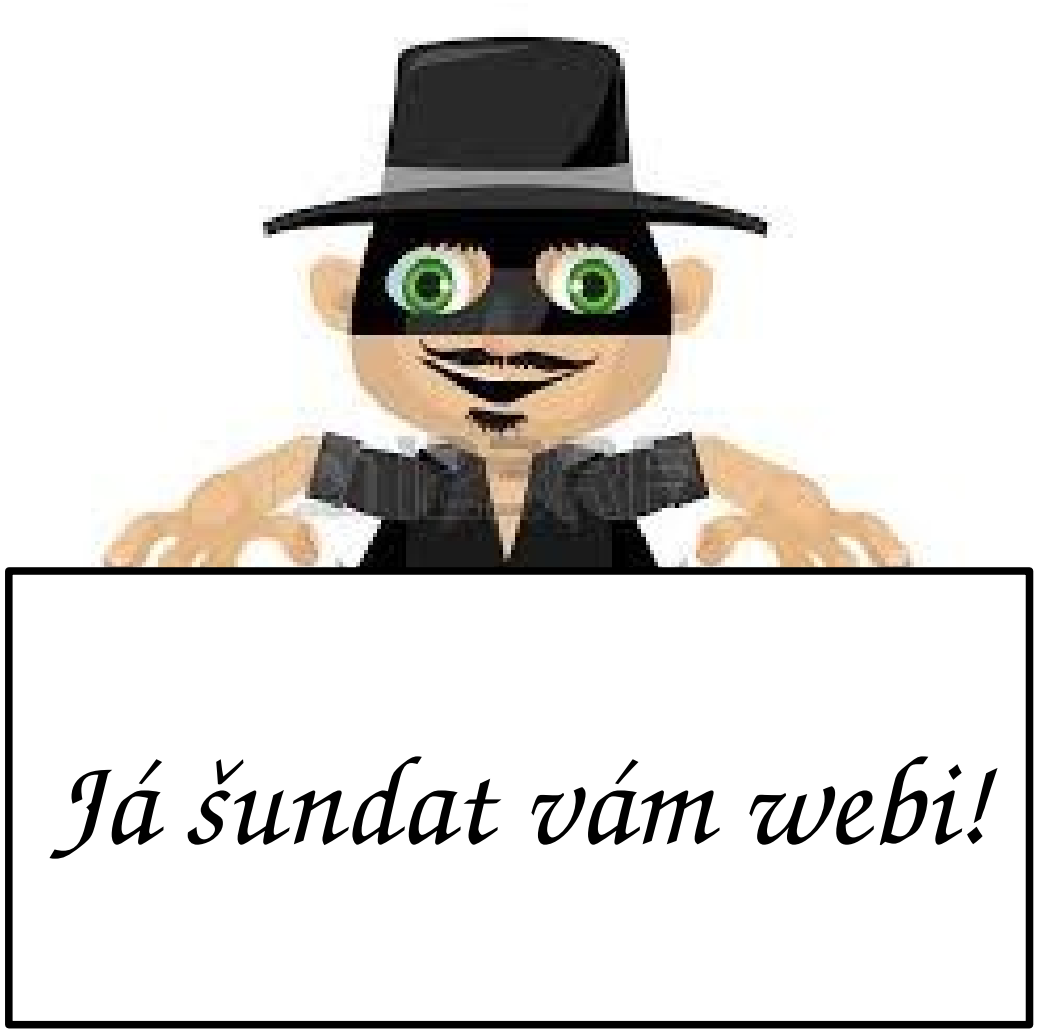
**+420 2 2435 2994**
**support@cesnet.cz**

# Use – case

# „instituce v ohrožení“






Já šundat vám webi!

# Reakce

Zacílení monitoringu na síťové úrovni

Předpřipravení potřebných filtračních mechanismů

Zvýšení míry detailu logování potenciálních cílů

Pohotovost na úrovni správců

Kontrola zabezpečení webových služeb

Rychlý scan na známé zranitelnosti

Penetrační testy webové prezentace/aplikace

Odstranění nálezů z provedených penetračních testů

# Je potřeba být připraven!

# Proaktivní služby

- Penetrační testy sítě a služeb
- Testy pomocí metod sociálního inženýrství
- Zátěžové testy


**https://flab.cesnet.cz/**

# Penetrační testy

- Cíl: Hledání chyb a zranitelností
  - nikoliv potvrzení bezchybnosti (audit)!

- Co by mělo být v centru zájmu správců?
  - lze infrastrukturu zneužít pro další útoky?
  - lze získat, poškodit, smazat data, systémy, služby?
  - lze získat autentizační údaje uživatelů?
  - existují v prostředí zneužitelné zranitelnosti?
  - kde udělal administrátor chybu při konfiguraci?
  - co by mělo/mohlo být zabezpečeno lépe a efektivněji?
  - ...

# Penetrační testy

- Průběh:
  1. fáze: **zadání**: specifikace požadavků, očekávání, rozsahu prací
  2. fáze: **aktivity v síti zadavatele**
     - scan sítě
     - sběr dat
     - testování specifikovaných služeb
  3. fáze: **následné zpracování**
     - dat, nálezů a zjištění
     - návrh a formulace doporučení

     ⟹ vytvoření a validace závěrečné zprávy
- Závěrečná zpráva & workshop
  - přehled provedených testů
  - zhodnocení výsledků
  - doporučení nápravných opatření

# Testy sociálního inženýrství

- Průběh:
  1. fáze: **zadání**: specifikace požadavků, očekávání, rozsahu prací
  2. fáze: **aktivity v síti zadavatele**
     - interakce s uživateli
     - „házení žížalek“, „pokládání nástrah“ ...
     - testování specifikovaných procesů/služeb
  3. fáze: **následné zpracování**
     - dat, nálezů a zjištění
     - návrh a formulace doporučení

     ⇒ vytvoření a validace závěrečné zprávy
- Závěrečná zpráva & workshop
  - přehled provedených testů
  - zhodnocení výsledků
  - doporučení nápravných opatření

# Zátěžové testy

- Cíl: Testování odolnosti služby (www, DNS)
  - Sekundární efekt – testování odolnosti sítě a obranných prvků
- Průběh
  - specifikace: cíle, požadavky a očekávání, pravidla, režim
  - průzkum terénu (ve spolupráci se správcem testované sítě)
  - návrh průběhu testů
  - kalibrace nástrojů a prostředí
  - výběr termínu
  - provedení testů
  - vyhodnocení výsledků
- Závěrečná zpráva & workshop
  - přehled provedených testů
  - zhodnocení výsledků
  - doporučení nápravných opatření

# Děkuji za pozornost.

Andrea Kropáčová, andrea@cesnet.cz

# Antispam Gateway

- Parametry
  - AG je monitorována Pracovištěm Stálé Služby v režimu 24/7
  - systematická kontrola provozu, uchovávání provozních informací (logování)
  - možnost individuálních nastavení pro konkrétní doménu
    - není nutné specifikovat seznam existujících mailových adres
    - whitelist
  - správce domény (organizace) má přístup k logům
- Výhody
  - více domén -> více zkušeností -> větší účinnost
  - váš e-mail provoz je „v bezpečí“
  - odpadají náklady na údržbu vlastní antispam ochrany
- Zřízení služby
  - masters@cesnet.cz
  - oboustranná akceptace pravidel
  - nastavení služby
  - testovací provoz

# Osvěta

- Semináře
  - velký seminář o bezpečnosti každý rok začátkem února
  - *!SecurityFest!* – osvětový seminář pro širokou veřejnost, říjen
- Školení (tématická)
  - správa a zabezpečení DNS
  - eduid.cz
  - systém FTAS (on-demand)
- Školení (semináře) pro uživatele
  - studenti
  - zaměstnanci-technici i netechnici

# Gramotné používání výpočetní techniky jako nejlepší prevence

Současný vývoj bezpečnosti v oblasti IT směřuje stále více k uživatelům, kteří tak při své práci musí každý den čelit různým. Přednáška se zabývá základními bezpečnostními riziky, které uživatelům při práci s výpočetní technikou a službami dostupnými prostřednictvím internetu hrozí, popisuje nejčastější chyby, kterých se dopouštějí a také neznalosti, ze kterých chyby pramení. Jsou popsány základní principy péče o výpočetní prostředek, principy ochrany identity, soukromí a dat, vlastností základních aplikací typu e-mail, prohlížeč apod. Stručně je probrána také oblast informační (digitální) stopy.

# Digitální stopa

Při používání počítačů a internetových online služeb za sebou každý den zanecháváme velmi silnou tzv. **digitální stopu**. Ta je složena z informací, které umožňují vysledovat činnost uživatele a získat o něm velké množství zajímavých informací – např. kdy se do sítě připojil, kdy používal jakou službu, kdy a komu napsal e-mail, kdy přistupoval na konkrétní www stránku. Co hůře ale také informace o tom, co dělal včera, co plánuje dělat zítra, kde je, kam jde atd. Některým digitálním stopám se vyvarovat nelze, ale za většinu z nich si můžeme sami svou činností v kombinaci s neznalostí. Přednáška demonstruje, kde všude po sobě tyto digitální stopy zanecháváme a proč a k čemu je možné informace z této digitální stopy využít.

# Aktuální kybernetické hrozby

V rámci prezentace jsou představeny a popsány aktuální kybernetické hrozby a útoky. Jedná se zejména o phishingové, ransomwarové a malwarové útoky, které se začaly objevovat v roce 2014, a které cílí na koncové uživatele. Posluchači jsou dále seznámeni s občansko a trestně právní odpovědností za jednání v kyberprostoru. Samostatná pozornost je věnována i problematice EULA, autorským právům a problematice sociálních sítí. Součástí prezentace jsou základní doporučení jak se chovat v prostředí Internetu, aby ne uživatel nestal obětí útoku nebo se nedopustil porušení legislativy.

# IT a legislativa

Přednáška představí vybrané pasáže z legislativy týkajících se prostředí Internetu, počítačových sítí a služeb. Je vysvětleno, jak na některé činy, kterých se jako uživatelé vědomě či nevědomě dopouštíme, pamatuje legislativa ČR a co by nám jako uživatelům mohlo hrozit, když spácháme např. bezpečnostní incident, nebo se staneme nedobrovolnými účastníky kybernetického útoku.

# Připravujeme

- **HaaS** (Honeypot as a Service)
  - předpřipravený image
  - zdroj dat pro Warden
  - dedikované nebo centrální řešení
- **Passive DNS**
  - sběr odpovědí z DNS serveru
  - vytváření „historie DNS“
  - *„řekni mi jak se IP adresa a.b.c.d jmenovala před měsícem“*
- **Reputační databáze**
  - databáze ***síťových entit*** (**IP adresy**, sítě, domény, …)
  - seznam známých zdrojů škodlivých aktivit a všeho, co o nich víme
  - shrnutí všech informací do „reputation score“