Seminář o bezpečnosti provozu sítí a služeb

Datum konání: 25. 11. 2013

Čas: 10:00 - 16:00 (konec dle zájmu o diskusi)

Místo konání: v sídle Kraje Vysočina, Žižkova 57, Jihlava, budova B, kongresový sál

Cílová skupina: Seminář je určen informatikům ORP a PO Kraje Vysočina, tzn. IT odborníkům z menších sítí, kteří v rámci svých sítí zajišťují vše od opravy PC přes administraci, zálohování až po budování metropolitních sítí. Seminář je koncipován tak, aby podal základní principy "sebeobrany v oblasti sítí a služeb" s důrazem na to nejpodstatnější, a aby bylo dostatek prostoru na dotazy a diskusi.

Program:

- **Já anonym, aneb svoboda na síti** (30 min), 10:00 – 10:40
  ➔ *informační stopa, kterou za sebou jako uživatelé necháváme*
  - kde se o nás jako uživatelích sbírají jaké informace, jak se s nimi zachází a kdo k nim má přístup
  - možnosti zjištění, kdo v daný okamžik používal konkrétní počítač s konkrétní IP adresou, apod., kdo přistupoval k určité službě apod.

- **Obrana sítě – základní principy** (40 min), 10:40 – 11:20
  ➔ *postup při designování obrany sítě a služeb na ní umístěných*
  - Správný design sítě
  - Víceúrovňové filtrování provozu
  - Ochrana koncových stanic
  - Ochrana aktivních prvků
  - Monitorování služeb
  - Monitorování síťové komunikace
  - Ochrana klientů (před klienty)

- **Sledování provozu sítě a služeb (+ systémy FTAS a G3)** (cca 40 min), 11:40 – 12:20
  - základní principy sledování provozu sítí
  - mechanismy a možnosti sledování provozu sítí
  - co je dobré sledovat, logovat a jakým způsobem
  - k čemu je možné takto získané informace využít

  - Systémy FTAS a G3
    - monitoring sítě na úrovni páteřní sítě v síti CESNET2
    - přímé poskytování monitoringu jako služby, jaké informace lze získat a jaké ne
    - vzorové ukázky toho, co mají k dispozici uživatelé, kteří
      - využívají tuto službu ve vlastní instanci (klon služby běží u nich)

        - využívají služeb instance, která je nasazena na páteřní síti CESNET2
    - ukázky provozních dat
    - cílený monitoring anomálií
    - FTAS a G3 jako služba pro dvě cílové skupiny:
        - členové bezpečnostních týmů, administrátoři sítí a služeb = konkrétní informace, vzorky dat, možnosti využití při ladění sítě, aktivní obraně apod.
        - manažeři, designéři sítě a služeb = náhled na provoz sítě jako celku, její zdraví, architektura, vytížení, ukázky možnosti dělení těchto informací dle institucí (koncových sítí)

- **Obrana sítě – síťařské desatero** (40 min), 13:20 – 14:00
  ➔ *na co je potřeba myslet při připojování sítě do Internetu*
    - filtrování provozu, firewall, policing, shaping, access listy
    - RTBH, URPF
    - kontrola odchozího provozu
    - zajištění dostupnosti služeb - DNS RR, anycast
    - bezpečnostní prvky typu IDS, IPS, ...
    - **uRPF**

- **Antispamová ochrana** (40 min), 14:00 – 14:40
  ➔ *současný stav služeb na bázi el. pošty a možnosti ochrany*
    - doporučená architektura poštovních serverů
    - principy a možnosti antispamové ochrany
    - postfix, Postfwd, Sqlgrey, Blacklist, Spamassassin, MySql, nolisting, ClamAV, předřazené filtry, logování, monitoring

- **Právní sekce – svět IT a legislativa** (30 min), 15:00 – 15:30
  ➔ *aktuality z oblasti legislativy*
    - zákon o kyberbezpečnosti
    - ochrana citlivých dat
    - *cokoliv, na co se chcete zeptat*
        - *sledování provozu sítě?*
        - *uchovávání provozních údajů o dění v síti?*

FTAS – systém pro plošné souvislé sledování IP provozu rozsáhlých síťových infrastruktur na bázi zpracování provozních informací o IP tocích (netflow).

G3 – systém pro plošné souvislé sledování stavu a chování rozsáhlých výkonných infrastruktur primárně pro sledování provozu CESNET2.