Bezpečná VLAN

Martin Semrád

IT 14

Praha, 22.5.2014

NIX·CZ

Představení NIX.CZ

- Neutrální propojovací platforma
- 5 datových center
- 119 připojených sítí
- 41 mezinárodních sítí
- 286,5 Gbps maximální datový tok
- Zaštiťuje projekt Bezpečná VLAN

Bezpečná VLAN

- Odpověď na útoky z 3/2013

  trvající 4 dny
- Mnoho cílů v CZ

  média, banky, mobilní operátoři, Seznam.cz
- Zdroj útoků mimo CZ
- Přes transit i NIX.CZ
- Žádná odpověď od zdroje

Bezpečná VLAN

- Klub vzájemně „důvěryhodných“
- Technický nástroj „Bezpečná VLAN“
- CZ uživatelé se potřebují dostat na CZ zdroje
  home banking, média, email …
- Možnost fungování v ostrovním režimu
  řešení poslední možnosti
- Dříve než přijde regulace
- Vysoká kritéria pro vstup

Bezpečná VLAN organizační pravidla

- Převedení pravidel až na koncového uživatele
  - spam, attacks
- 24x7 technický kontakt
  - žádné IVR
- CSIRT team
  - Zalistovaný u Trusted Introducer, Terena
- Více než 6 měsíců v NIX.CZ
- Aktivní účast na WG NIX.CZ
- Doporučení od 2 členů, žádné veto

Bezpečná VLAN technická pravidla

- BCP-38/SAC004 – granularita /24 (/48)
- RTBH využívající RS
- IPv6, DNSSEC – na důležitých doménách
- Plná redundance připojení do NIX.CZ
- Monitoring sítě (MRTG, NetFlow, …)
- Control plane policy RFC6192
- DNS, NTP, SNMP amplification protection
- Reakční čas na bezpečnostní incident <30min
- BGP – TCP MD5

Bezpečná VLAN
start

- 6 společností zakládá projekt – leden 14

  Active 24, CESNET, CZ.NIC, Dial telecom, Seznam.cz, Telefonica Czech Republic

- NIX.CZ jako arbitr dodržování pravidel

Bezpečná VLAN
aktuální stav

- První schůzka zakladatelů
- Úprava pravidel
- Jednaní s dalšími zájemci
- Základní struktura značky

~~**Bezpečná VLAN**~~

Nyní zapomeňme

název

Bezpečná VLAN

FENIX

propojujeme důvěryhodné sítě

Připojen
k důvěryhodné síti

Sledujte nás

.. a také na www.nix.cz ☺

Bezpečná VLAN organizační pravidla

- Převedení pravidel až na koncového uživatele
  - spam, attacks
- 24x7 technický kontakt
  - žádné IVR
- CSIRT team
  - Zalistovaný u Trusted Introducer, Terena
- Více než 6 měsíců v NIX.CZ
- Aktivní účast na WG NIX.CZ
- Doporučení od 2 členů, žádné veto

Bezpečná VLAN technická pravidla

- BCP-38/SAC004 – granularita /24 (/48)
- RTBH využívající RS
- IPv6, DNSSEC – na důležitých doménách
- Plná redundance připojení do NIX.CZ
- Monitoring sítě (MRTG, NetFlow, …)
- Control plane policy RFC6192
- DNS, NTP, SNMP amplification protection
- Reakční čas na bezpečnostní incident <30min
- BGP – TCP MD5