Bezpečný router

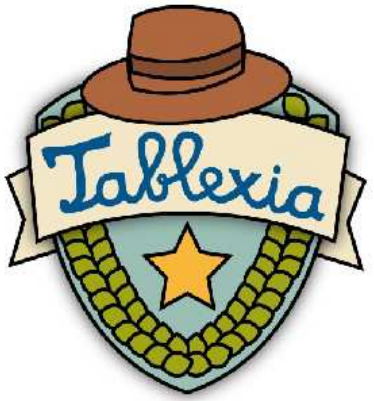
Pro malé úřady a školy

Pavel Bašta • pavel.basta@nic.cz • 05.04.2016

CZ.NIC | SPRÁVCE DOMÉNY CZ

CZ.NIC, z.s.p.o.

- Hlavní činnost správa doménových jmen .CZ



Knot DNS

Motivace

- Vytvoření bezpečného routeru
  - Současný stav v této oblasti je tristní
    - Nezáplatované zranitelnosti
    - Neexistující podpora nových protokolů a technologií
- Bezpečnost koncových uživatelů
  - Souvisí s podporou nových technologií
  - Sledování některých markantů v síťovém provozu
  - Schopnost rychlé reakce na nové hrozby
- Bezpečnostní výzkum

Výstupy z projektu

- Identifikace botnetu vytvořeného útočníky ze SoHo routerů
- Identifikace klientů nakažených bankovním trojským koněm
- Objevení manipulace s certifikáty
- Nebezpečné webové stránky (Malicious Domain Manager)

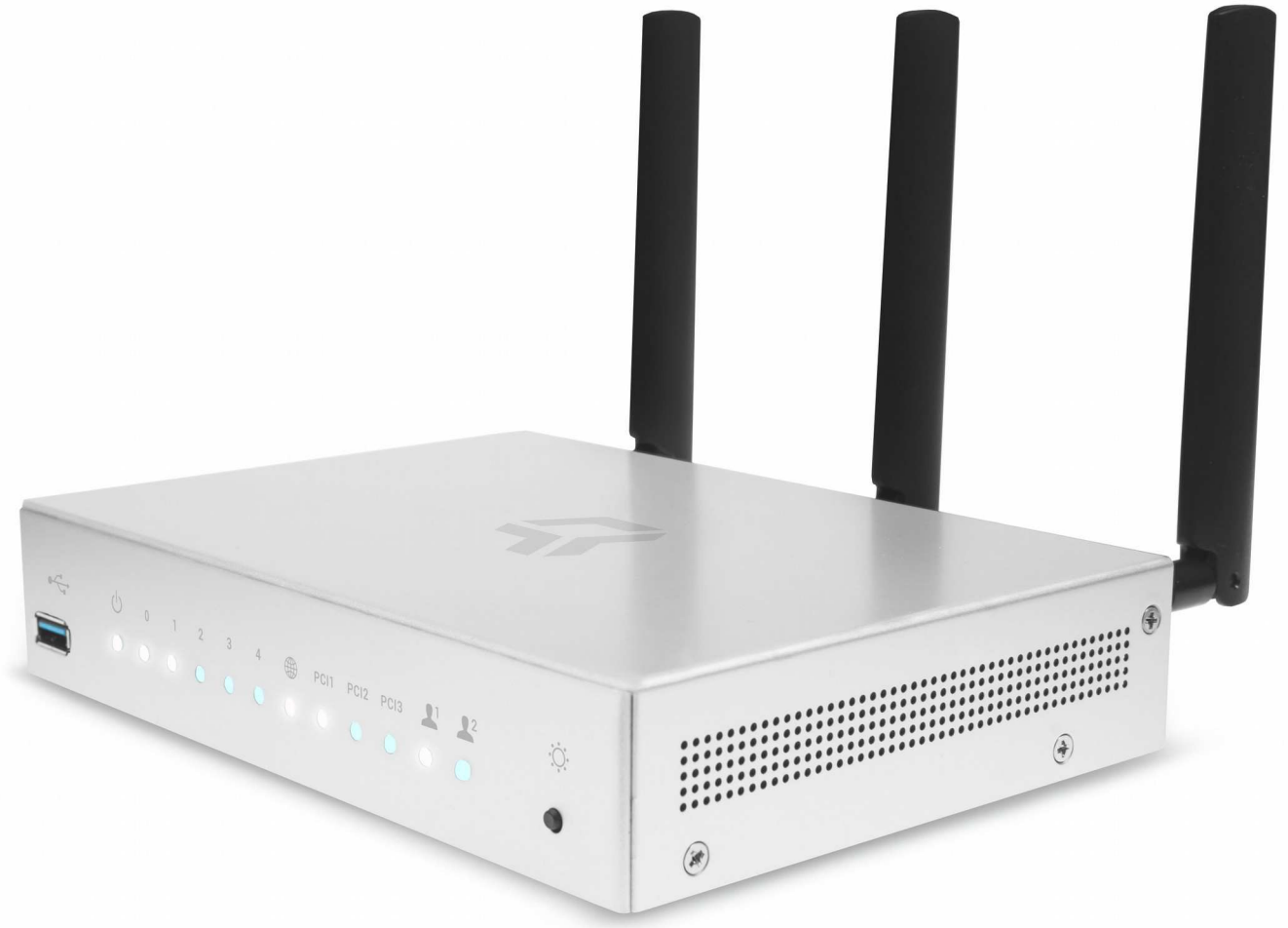
Zrození Turris Omnia

- Větší množství zájemců než routerů
- Užitek i pro ostatní
- Velký zájem v zahraničí
- Komunita
- Málo otevřeného hardware
- TurrisOS
- Rozšíření strojů v bezpečnostním výzkumu

Hlavní vlastnosti Turris Omnia

- Otevřený hardware i software
- Velký výkon (1.6 GHz dvoujádrový ARM, 1 GB DDR3)
- SFP konektor
- Bezpečnost
- Rozšiřitelnost

….proč byste se o něj měli zajímat?


0
1
2
3
4
PCI1
PCI2
PCI3
1
2

Obecné požadavky na moderní IT řešení

- Open-source, open-source, open-source
  - Možnost vlastních úprav
  - Nezávislost na dodavateli
- Podpora nových technologií
  - IPv6
  - DNSSEC
- Dlouhodobá udržitelnost
  - Ochota dodavatele podporovat projekt i po skončení záruky (bezpečnostní záplaty)
- Možnost identifikace zdroje incidentu

Zákon o kybernetické bezpečnosti (ZKB)

- Vyhláška 316/2014 k ZKB identifikuje požadavky pro subjekty definované v ZKB
- Definuje požadavky na celou řadu aspektů bezpečnosti
- Pro ostatní subjekty může posloužit jako vhodný průvodce při definici požadavků i pro Vaši organizaci

Požadavky na nástroj pro ochranu integrity komunikačních sítí § 17

- Řízení bezpečného přístupu mezi vnější a vnitřní sítí
- Segmentace vnitřní komunikační sítě (VLAN)
- Kryptografické prostředky pro vzdálený

přístup, vzdálenou správu nebo pro přístup po-

mocí bezdrátových technologií

Požadavky na ověřování identity uživatelů § 18

- Nástroj pro ověřování identity uživatelů (hlavně Wi-Fi)
  - Vysoký výkon a použitý systém umožňují snadné rozšíření o potřebné nástroje (Radius server)

Požadavky na ochranu před škodlivým kódem § 20

- Kontrola obsahu stahovaných stránek (proxy server, antivirus)
- Adaptivní firewall (MDM a další)

Požadavek na nástroj pro zaznamenávání činností informační infrastruktury § 21

- Možnost sledovat informace o síťovém provozu
- Sledování odchozí komunikace

Požadavek na nástroj pro detekci kybernetických bezpečnostních událostí

- Možnost vyhodnocování událostí na centrální úrovni

Požadavek na nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí § 23

- Možnost vyhodnocování událostí na centrální úrovni
- Adaptivní Firewall

Požadavky IROP

- V rámci IROP je ve vztahu k SC 2.4 (vnitřní konektivita škol a připojení k Internetu) připravován standard konektivity škol, specifikace opatření a aktivit, který definuje technická kritéria stavu školní síťové infrastruktury
- Mezi způsobilé výdaje se řadí též router splňující zejm. následující technické specifikace:
  - podpora přepínání/směrování protokolů IPv4 i IPv6
  - IDS, IPS
  - u vnitřní konektivity dále požadavek na monitorování IP datových toků
  - podpora protokolu IEEE 802.1X resp. ověřování uživatelů oproti databázi účtů přes protokol radius
  - podpora standardu IEEE 802.11n a případně novějších (ac, ad), současná funkce AP v pásmu 2,4 a 5 GHz

Děkuji za pozornost

Pavel Bašta • pavel.basta@nic.cz