Co nového v Turrisu

Na čem jsme letos pracovali

Michal Hrušecký • michal.hrusecky@nic.cz
Miroslav Hanák • miroslav.hanak@nic.cz
Martin Prudek • martin.prudek@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ

Turris OS 5.3

- vydán ve čtvrtek
- hlavní téma - lepší integrace Turris Sentinel
- poslední major release založený na OpenWrt 19.07
- poslední release s Forisem
  - dost možná ho už nemáte

Co zrušíme dál?

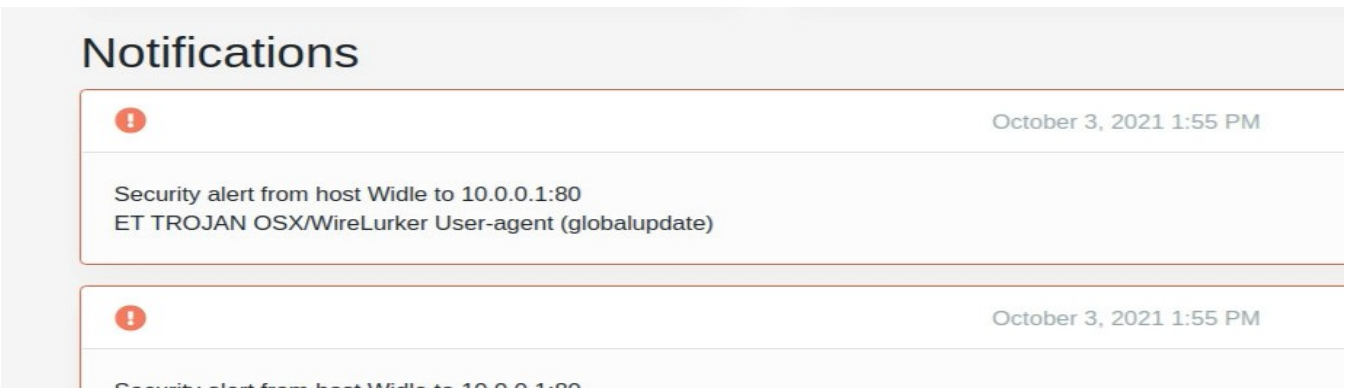
- Foris (úplně)
  - Server Side backups
  - Pakoň
- Turris OS 3.X
  - bude ale migrace
- portál project.turris.cz
  - máme Sentinel ;-)
  - máme sview

Na co se těšit? Pakoň!

- separátní web application
- nezávislá na Forisu/Turrisu
- CSV export
- nahradíme závislost na Surikatě
- časem bude i hezčí

Na co se těšit? Morče!

- další zvířátko do sbírky
- integrace IDS do systému
- první krok - notifikace
- časem bude i log/přehled
- časem spojíme s Pakoňem a vymyslíme normální jméno
  - snad normální….



Na co se těšit? Migrace!

- začínáme po 5.3
- začneme postupně zapínat pro Omnie
- zapneme pro Turrisy 1.X s Btrfs

Co Turris 1.X bez karty?

- chystáme migraci na externí USB

Omnia II

- nová vlajková loď
- víc jader a víc GHz
- víc RAM
- možná display?

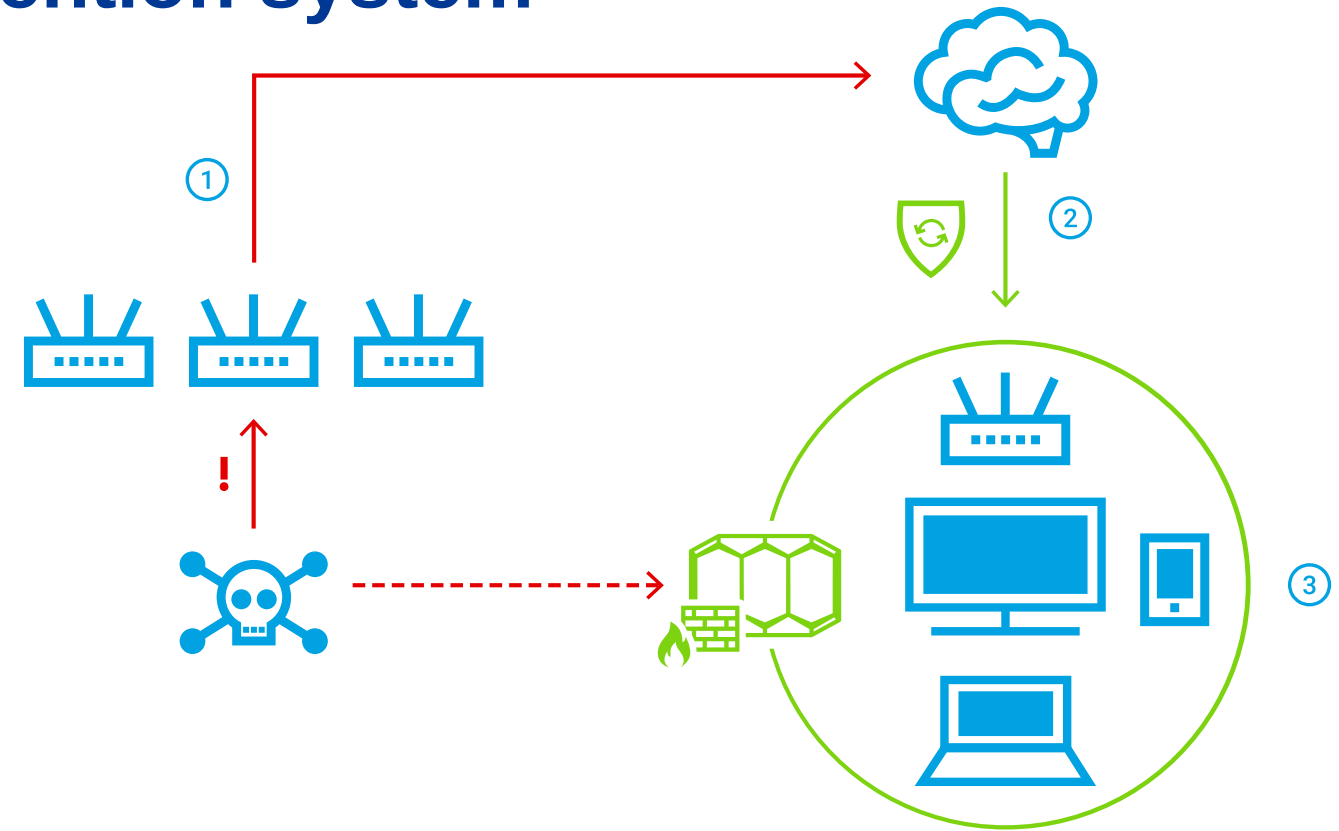
Omnia II

- 10 Gbps metalika
- 10 Gbps SFP
- 2.5 Gbps metalika
- WiFi 6
- 5G ready
- Kdy? Velmi možná konec 2022

Co do tý doby?

- Turris OS 6.0
  - založen na OpenWrt 21.02
  - s trochou štěstí k Vánocům
- Omnia s WiFi 6
  - v průběhu 2022
- novinky v Sentinelu ;-)

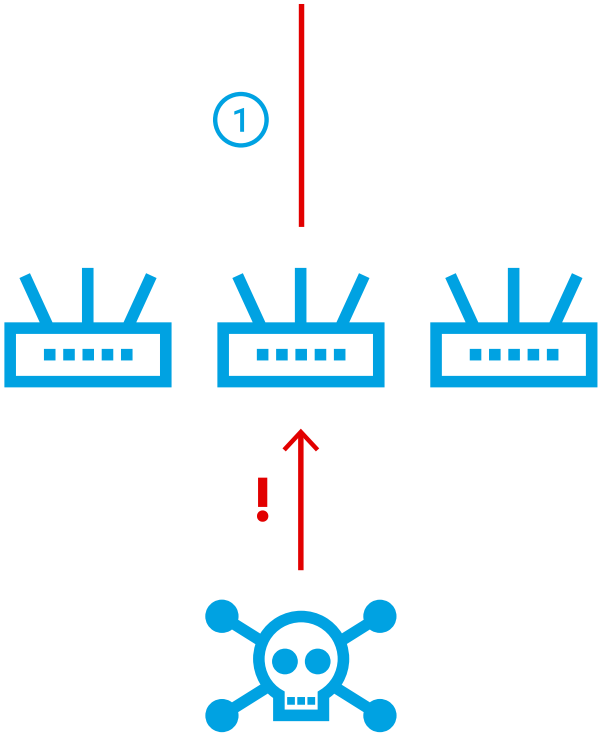
Sentinel – threat detection and cyberattack prevention system



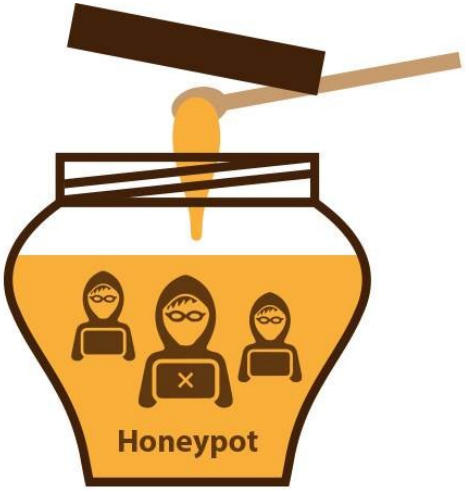
Sběr dat

- Na routeru:
  - Minipoty
  - Firewall logy
  - Dobrovolnost
- Externí zdroje:
  - HaaS – SSH Honeypot as a Service

    https://haas.nic.cz



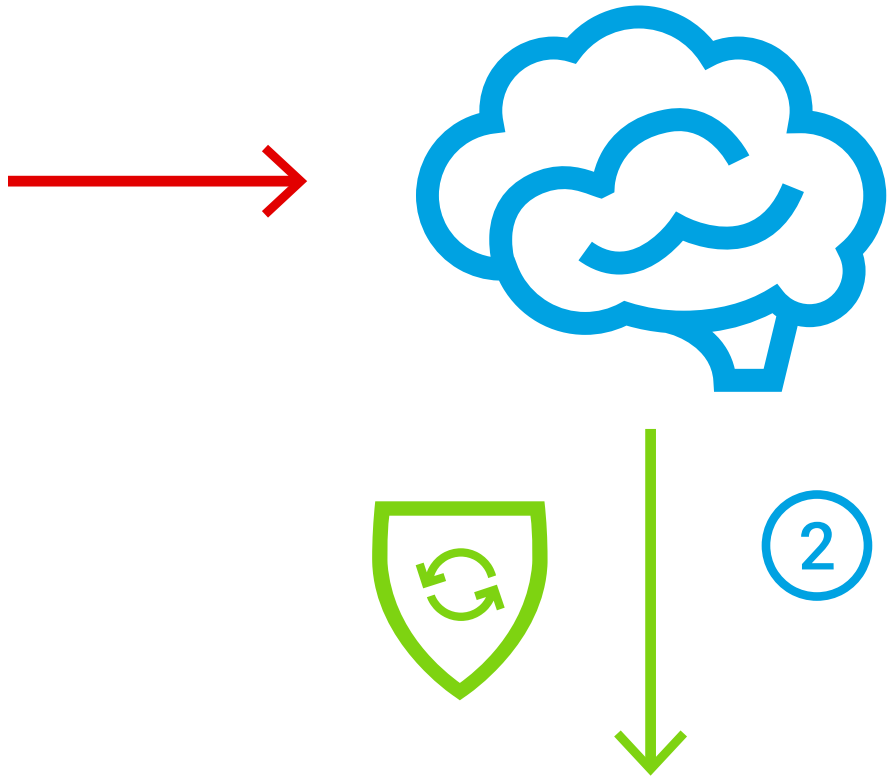
Minipot – minimální honeypot



- Honeypot – past
  - Kontrolované prostředí
  - Sledování útočníkovy aktivity
- Minimální
  - Emulace známých služeb na aplikační vrstvě – Telnet, HTTP, FTP, SMTP
  - Pokusy o připojení a přihlášení

Zpracování dat

- Proudově – data pipelines
  - Message queues
- Série propojených komponent
  - Obohacení dat
  - Analýza
  - Databáze
- Každá IP adresa má skóre
  - Práh



Výstupy

- Seznam škodlivých IP adres – Greylist
  - Veřejně dostupný
- Sentinel View
  - Statistiky dat
  - https://view.sentinel.turris.cz
- Spolupráce s národním CSIRT týmem

Sentinel novinky v TOS 5.3

- Turris Survey v0.2
- Minipoty v2.2 – sjednocení typů zpráv
- Nikola → FWLogs Collector
- Sentinel Proxy v1.4
- Sentinel Overview v reForisu
- Update serverové infrastruktury

Sentinel novinky v TOS 5.3 – Turris Survey

- Volitená část Sentinelu
- Informace o používaných funkcích
  - Nainstalované balíčky
  - Jazykové mutace
- Nově ve verzi 0.2

Sentinel novinky v TOS 5.3 – Minipoty

- Volitená část Sentinelu
- „Minimální honeypoty“ - Telnet, SMTP, FTP, HTTP
- Produkují eventy na základě chování útočníků
- Nově ve verzi 2.2 – sjednocení eventů
  - Connect
  - Login
  - Invalid
  - Message (pouze HTTP)

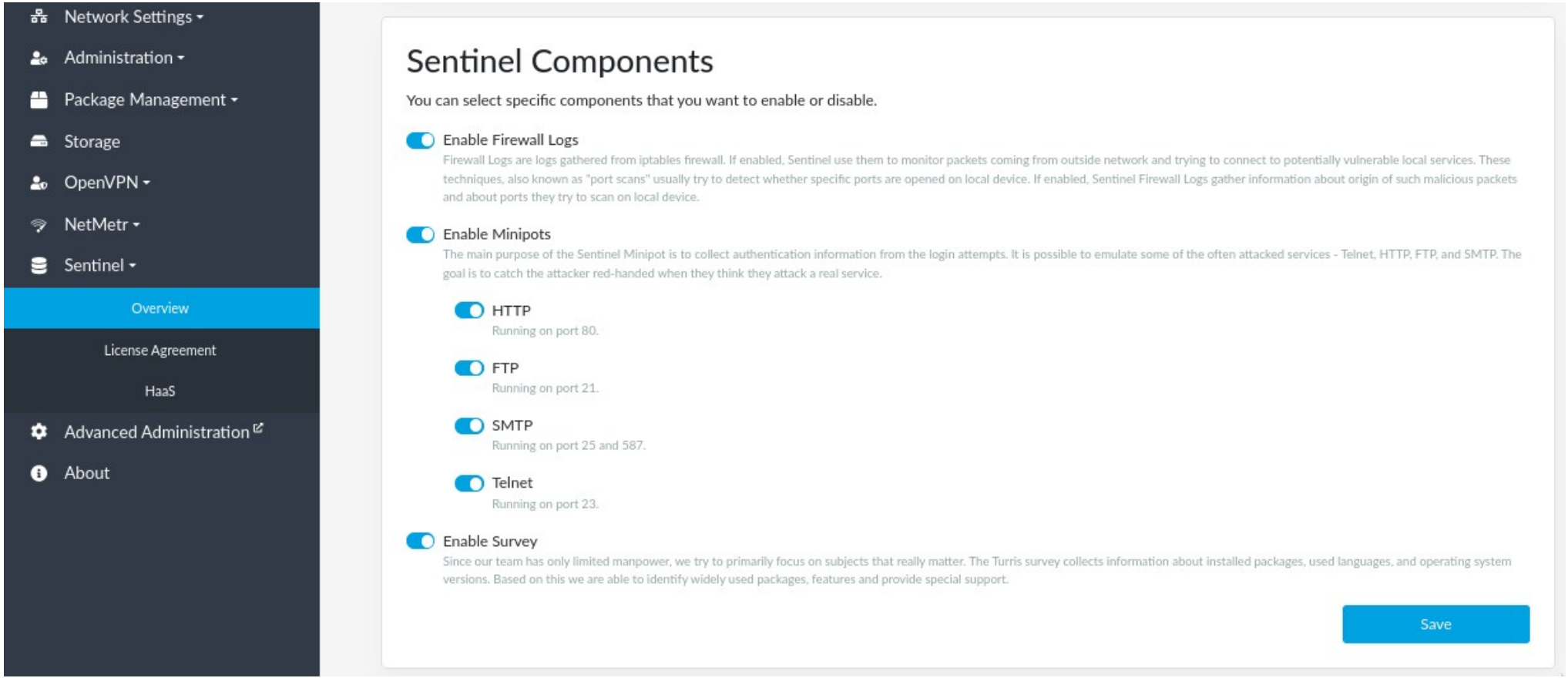
Sentinel novinky v TOS 5.3 – FWLogs collector

- Volitená část Sentinelu
- = Firewall monitoring
- Sběr FW logů o odmítnutých nebo zahozených spojeních
- Náhrada „one shot“ skriptu Nikola za FWLogs collector
  - C
  - Netlink, knihovna libnetfilter_log
  - Rychlejší odezva na události
  - Nižší režie

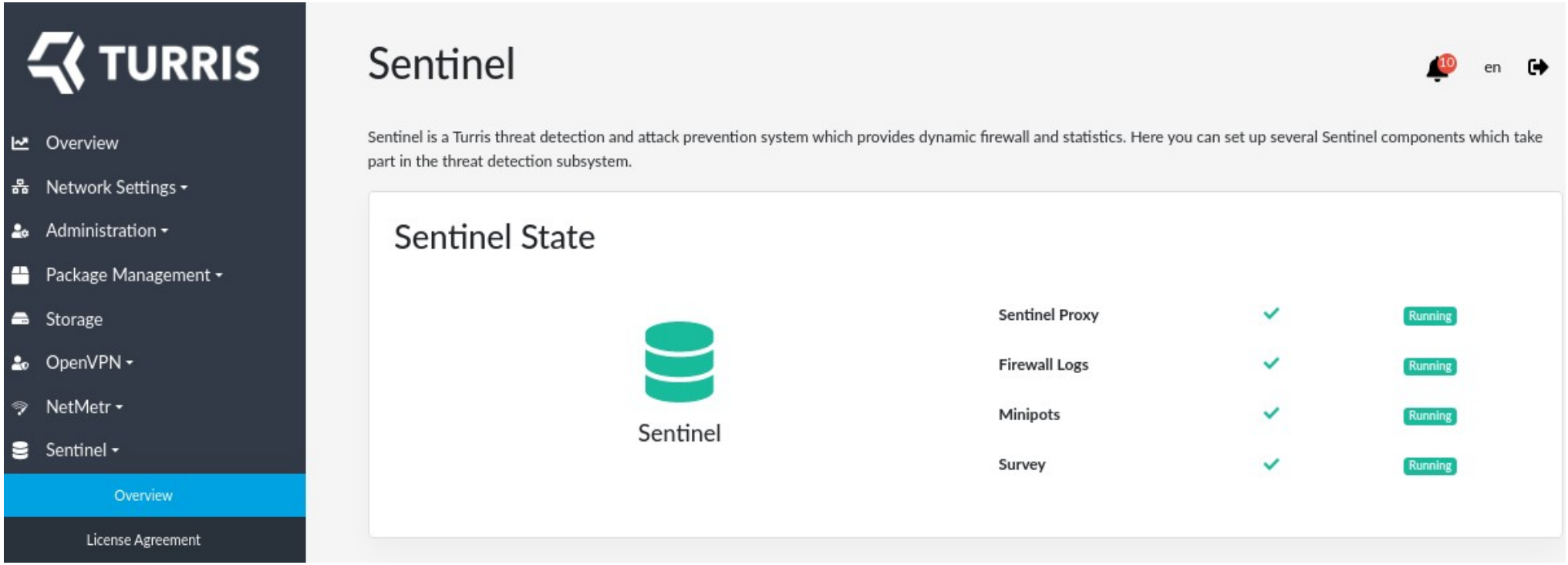
Sentinel novinky v TOS 5.3 – Sentinel Proxy

- Vychozí brána na routeru pro spojení na server
- Udržuje bezpečný komunikační kanál
- Nově ve verzi 1.4
  - Interní refactoring
  - Příprava pro zobrazení informací o aktivitě v reForisu

Sentinel novinky v TOS 5.3 – Sentinel Overview



Sentinel novinky v TOS 5.3 – Sentinel Overview



Nápady do budoucna

- Zobrazení poslední aktivity v reForisu
- Inspirace službou „Have I been pwned“
- Příprava na plnohodnotný běh Sentinelu mimo Turris
- Nasazení nového Sentinel View

Děkujeme za pozornost

Michal Hrušecký • michal.hrusecky@nic.cz
Miroslav Hanák • miroslav.hanak@nic.cz
Martin Prudek • martin.prudek@nic.cz
6.11.2021

CZ.NIC | SPRÁVCE DOMÉNY CZ