Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť konfigurácií

Technické opatrenia (BLOK IV)
Kurz: Manažér kybernetickej bezpečnosti

Ing. Matúš Madleňák

KC KYB UNIZA, https://kc.uniza.sk/

kcskolenia@uniza.sk

Obsah

1. Bezpečnosť pri nadobúdaní, vývoji a údržbe konfigurácií

- Životný cyklus konfigurácie

2. Techniky a metódy riadenia konfigurácií

- Šablóny, zálohovanie, schvaľovanie zmien a automatizácia konfigurácií

3. Vplyv konfigurácií na bezpečnosť

- Praktické príklady

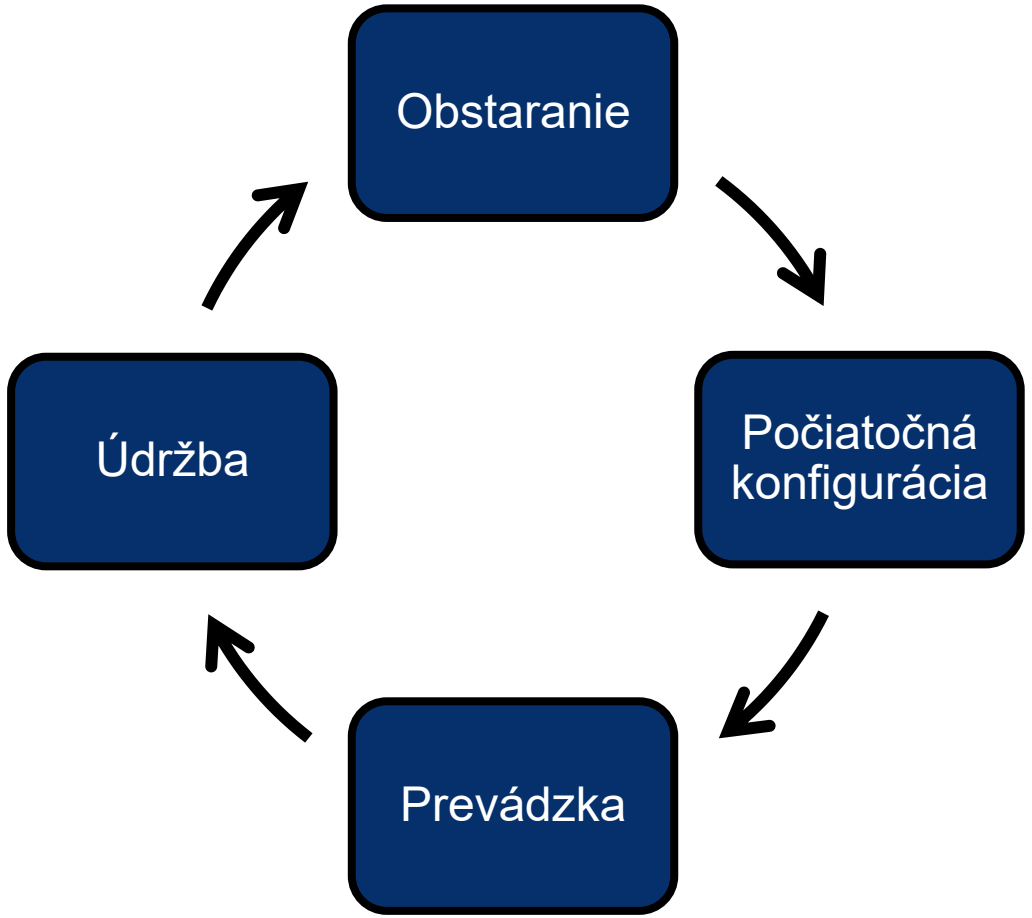
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť pri nadobúdaní, vývoji a údržbe konfigurácií

Životný cyklus konfigurácie

- **Konfigurácia** v kontexte počítačových sietí znamená nastavenie hardvéru a softvéru tak, aby sieťové zariadenia (routery, prepínače, firewally, Wi-Fi AP) fungovali podľa požiadaviek organizácie.

- Tento cyklus je **nekonečný** – keď sa zariadenie opotrebí alebo prestane byť podporované, organizácia opäť prechádza fázou obstarania.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Obstaranie

- **Obstaranie** je prvý krok v životnom cykle konfigurácie.
- Už v tejto fáze sa rozhoduje o tom, **ako bezpečná bude celá infraštruktúra**.

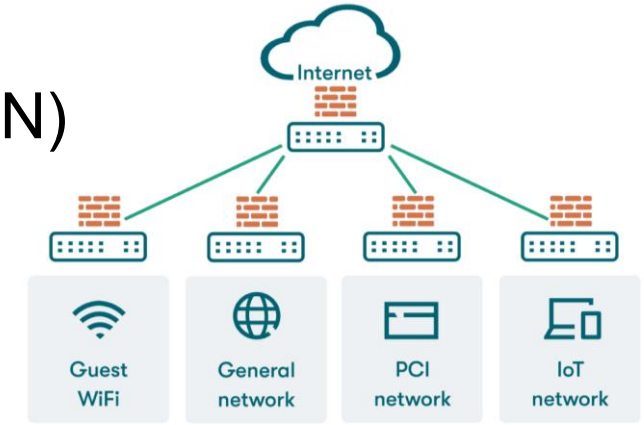
Kľúčové kritériá pri výbere zariadení:

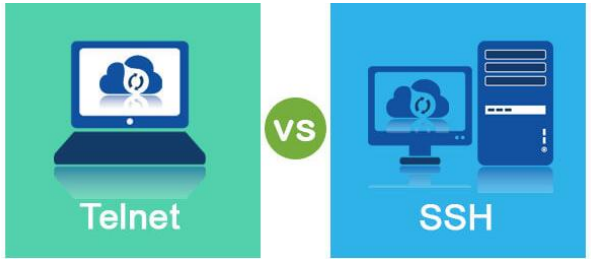
- Podpora bezpečnostných štandardov:
  - WPA3
  - IPv6
  - VPN
  - Firewall
  - IDS/IPS
- Podpora výrobcu
  - Pravidelné aktualizácie firmware
  - Dĺžka podpory
- Certifikácie a dôveryhodnosť
  - Reputácia
  - Certifikácie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Počiatočná konfigurácia

- Odstrániť alebo zmeniť „**defaultné účty“ a heslá** (admin/admin; user/password)
- Nastaviť silné **autentizačné mechanizmy**
- Oddeliť siete – **segmentácia** (VLAN)
- Zakázať **nepotrebné služby**

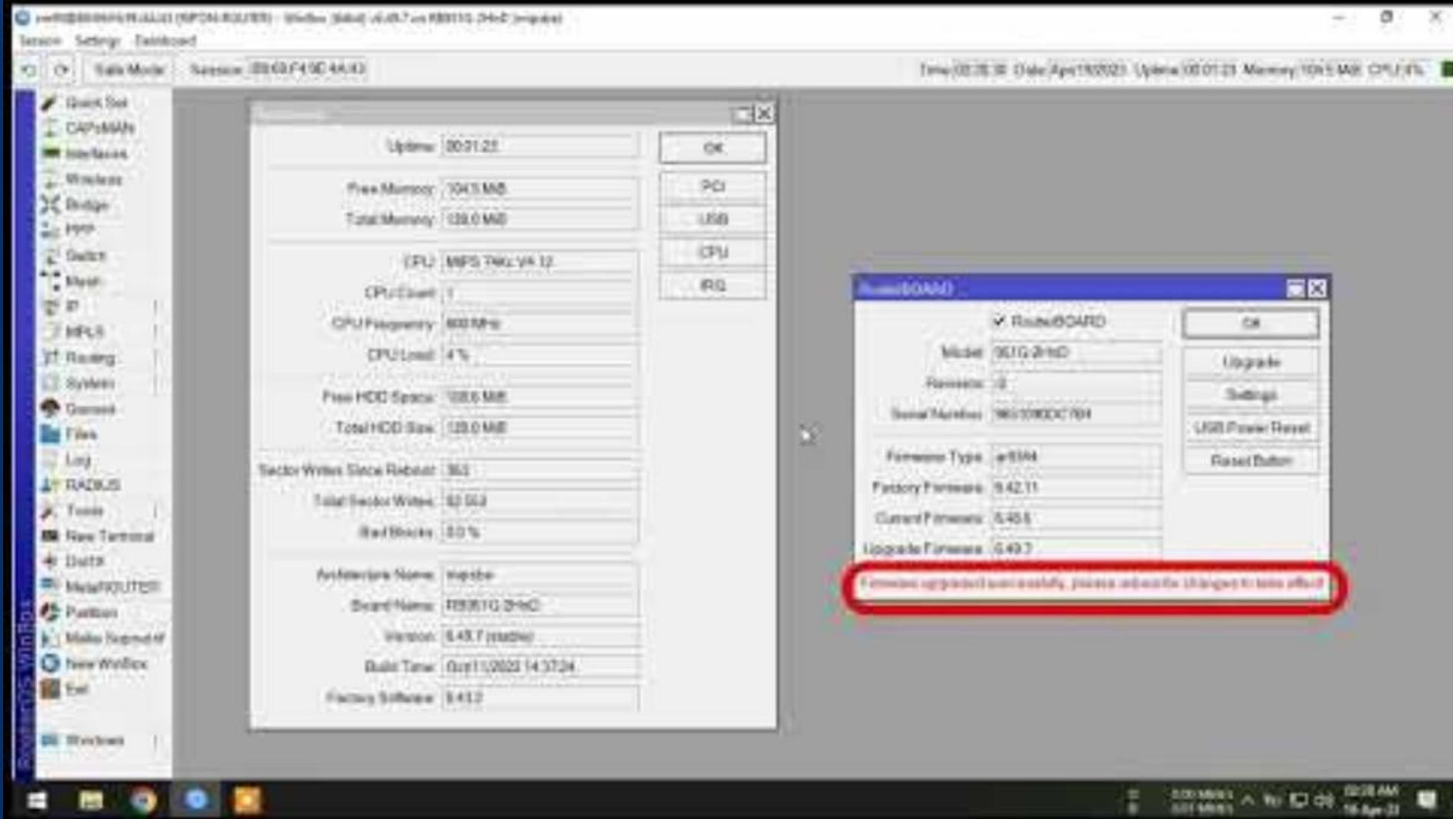




Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Údržba konfigurácií

- Pravidelné **aktualizácie firmvéru** a softvéru. Ideálne najprv v testovacom prostredí (spomeňte si napríklad na CrowdStrike)
- **Zálohovanie** konfigurácií – možnosť rýchlej obnovy pri poruche alebo útoku.
- **Audit** nastavení – kontrola, či zariadenia spĺňajú interné politiky, či sú nastavené tak ako majú byť
- Odstránenie **nepotrebných účtov/služieb**.


Session
Settings
Dashboard
Safe Mode
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Dot1X
Partition
Make Supout.rif
New WinBox
Exit
Windows
Uptime:
Free Memory:
Total Memory:
CPU:
CPU Count:
CPU Frequency:
CPU Load:
Free HDD Space:
Total HDD Size:
Sector Writes Since Reboot:
Total Sector Writes:
Bad Blocks:
Architecture Name:
Board Name:
Version:
Build Time:
Factory Software:
OK
PCI
USB
CPU
IRQ
RouterBOARD
Model:
Serial Number:
Firmware Type:
Factory Firmware:
Current Firmware:
Upgrade Firmware:
OK
Upgrade
Settings
USB Power Reset
Reset Button

Praktický príklad – Domáci Switch

Obstaranie:

- kúpa **managed switcha**, ktorý podporuje VLAN a má webové rozhranie,
- vyhýbanie sa lacným „unmanaged“ switchom, ktoré neumožňujú bezpečnostné nastavenia.

Počiatočná konfigurácia:

- zmena **defaultného hesla** do administrácie,
- vypnutie **nepotrebných služieb** (napr. Telnet, CDP, IPv6 – ak nepoužívame),
- vytvorenie VLAN – napr. oddelenie PC od smart TV a IoT zariadení.

Prevádzka:

- bežné používanie siete – PC, smart TV, herná konzola, IoT, všetko beží cez switch,
- dohľad, či všetko funguje a či sa nezapája cudzie zariadenie.

Údržba:

- občasná kontrola dostupnosti **firmvérových aktualizácií** na stránke výrobcu,
- uloženie (záloha) konfigurácie, ak switch túto možnosť podporuje,
- raz za čas prejsť nastavenia a vymazať nepotrebné VLAN alebo účty.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Techniky a metódy riadenia konfigurácií

Čo znamená riadenie konfigurácií – Tri piliere

PROCES

- Každá zmena konfigurácie musí mať jasne definovaný postup:
  - **kto** zmenu vykonáva,
  - **čo** sa mení,
  - **prečo** sa mení.
- Ide o súčasť **change managementu**
- Používa sa princíp „4 očí“ – zmenu navrhne jedna osoba, schváli iná a až potom sa zavedie.
- Zmeny by mali byť **plánované a testované**. Ad hoc zmeny môžu spôsobiť incidenty

TECHNOLÓGIA

- Napríklad:
  - **Centralizované platformy** (Cisco DNA Center, MikroTik CAPsMAN) – správa viacerých zariadení z jedného miesta.
- Výhodou je minimalizácia ľudských chýb a vyššia konzistentnosť konfigurácií.

Čo znamená riadenie konfigurácií – Tri piliere

DOKUMENTÁCIA

- Každá zmena konfigurácie musí byť **evidovaná**
- Inak sa stráca prehľad a vzniká tzv. „shadow IT“.
- Správna dokumentácia je nevyhnutná pri audite aj pri riešení incidentov – viete spätne zistiť, či za problém môže zmena konfigurácie.

- Formy dokumentácie:
  - **prevádzková dokumentácia** (aký je aktuálny stav),
  - **zápisy o zmenách** (kto a kedy spravil akú zmenu),
  - **verzionovanie** – uchovávanie histórie zmien, aby sa dala konfigurácia vrátiť späť.

Štandardizované šablóny

- Štandardizované šablóny znamenajú, že všetky zariadenia v sieti majú rovnaký základ konfigurácie.
- Inými slovami – namiesto toho, aby mal každý admin „svoj vlastný štýl“, existuje **centrálne definovaná šablóna**, ktorú sa všetci držia.
- Šablóny môžu mať formu obyčajného textu (inštrukcie, príkazy), tabuľka, konfiguračný súbor (napr. startup config), skripty

Výhody

- **Jednoduchšie riadenie** – jednotné zásady pre všetky zariadenia, konzistentnosť pri nasadzovaní nových.
- **Menej chýb** – konfigurácia je otestovaná, zabráni sa ad hoc nastaveniam.
- **Rýchlejšia obnova** – nové zariadenie sa nasadí podľa šablóny, rýchly návrat do prevádzky.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Štandardizované šablóny - Príklad

- **Hostname zariadenia** – každé zariadenie dostane štandardizovaný názov podľa interných pravidiel (napr. SW-Admin-01).
- **Heslo pre privilegovaný EXEC režim** – definované silné heslo, rovnaký štandard pre všetky zariadenia.
- **Heslo na konzolový port** – prístup cez konzolu chránený heslom, aby sa predišlo neautorizovaným zmenám.
- **Heslo na VTY (virtuálne terminály)** – zabezpečený vzdialený prístup, štandardne len cez SSH, nie Telnet.
- **Šifrovanie hesiel** – všetky uložené heslá sú šifrované, aby neboli čitateľné v konfigurácii.
- **Banner** – jednotná správa (napr. varovanie o monitorovaní prístupu).
- **Nastavenie času** – synchronizácia cez NTP server, aby logy a záznamy mali správny čas.
- **Zakázanie vyhľadávania DNS** – príkaz *no ip domain-lookup*, aby sa switch nepokúšal prekladať chybne zadané príkazy ako DNS dotazy.
- **Konzolové hlásenia** – podľa potreby sa zapnú alebo vypnú systémové hlásenia na konzole, aby nerušili administrátora pri práci.

Zálohovanie konfigurácií

- Konfigurácia sieťového zariadenia je často **rovnako cenná ako samotný hardvér**.
- Bez zálohy môže byť obnova siete po incidente zdĺhavá a nákladná.
- Správne zálohovanie je preto súčasťou **plánu kontinuity prevádzky** a **incident response**.

- **Ochrana pred stratou dát pri poruche** – bez zálohy treba zariadenie konfigurovať odznova.
- **Rýchla obnova po útoku alebo chybe administrátora** – obnova zo zálohy je najrýchlejší spôsob návratu do funkčného stavu.
- **Historické porovnanie konfigurácií** – možnosť zistiť, kedy a čo sa zmenilo, dôležité pri audite alebo incidente.

Zálohovanie konfigurácií

Ako:

- **manuálne**: admin si stiahne konfiguráciu (napr. copy running-config tftp). Vhodné pred jednorazovou zmenou.
- **automatizovane**: pravidelné scripty, centrálne nástroje (RANCID, Oxidized, Cisco Prime).

Ideálny scenár:

- Automatické denné zálohy + manuálne zálohy pred každou väčšou zmenou.
- Manuálne zálohy pred každou väčšou zmenou - ak sa zmena nepodarí, dá sa vrátiť späť.
- Uchovávanie záloh mimo produkčného prostredia (napr. na bezpečnom serveri).
- Kontrola prístupov – k zálohám majú prístup iba oprávnené osoby.

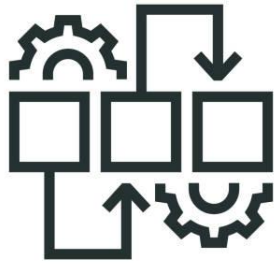
Schvaľovanie zmien

- Každá väčšia zmena musí prejsť procesom schválenia. Nie ad hoc
- Cieľom schvaľovania zmien:
  - **Predchádza výpadkom a chybám** – napr. nesprávne nastavenie VLAN môže spôsobiť nedostupnosť časti siete.
  - **Znižuje riziko konfliktov** – ak viacerí admini robia zmeny bez koordinácie, môžu si ich navzájom „prepisovať“.
  - **Zvyšuje zodpovednosť** – je jasné, kto zmenu navrhol a kto ju schválil.
  - **Spätná dohľadateľnosť** – ak dôjde k incidentu, dá sa zistiť, či jeho príčinou bola posledná zmena konfigurácie.

Proces:

1. **Navrhnúť** – admin popíše, čo sa má zmeniť.
2. **Posúdiť** – iný admin alebo manažér preverí, či zmena nemá negatívny dopad.
3. **Schváliť** – až potom sa zmena realizuje.
4. **Zdokumentovať** – výsledok sa uloží do záznamu zmien.

Automatizácia konfigurácií



Výhody:

- **Konzistentnosť** – všetky zariadenia majú rovnaké nastavenia.
- **Rýchlosť** – zmena sa dá aplikovať na stovky zariadení naraz.
- **Zníženie chybovosti** – ľudské chyby sa minimalizujú.

Nástroje:

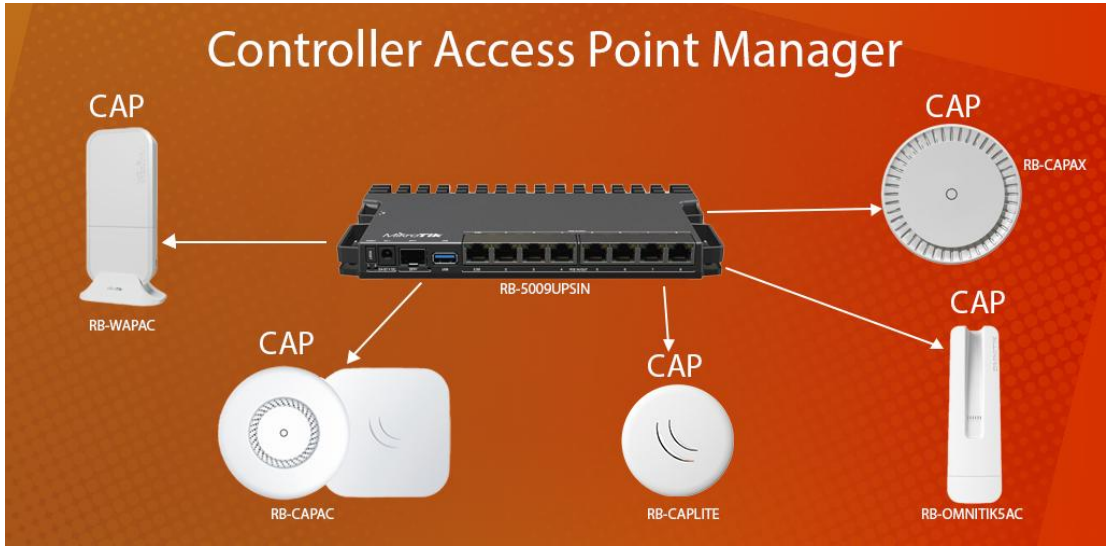
- **Cisco DNA Center** – centrálne riadenie celej infraštruktúry Cisco.
- **MikroTik CAPsMAN** – riadenie viacerých Wi-Fi AP z jedného miesta.
- **Ansible, Puppet, Chef** – open-source nástroje pre „Infrastructure as Code“ (IaC).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Automatizácia konfigurácií

MikroTik CAPsMAN

- Umožňuje spravovať desiatky až stovky Wi-Fi access pointov (AP) centrálne z jedného MikroTik routera alebo zariadenia.



- Všetky AP (tzv. CAP – Controlled Access Point) sú pripojené k centrálnej jednotke CAPsMAN.
- Konfigurácia Wi-Fi (SSID, heslo, VLAN, bezpečnostné nastavenia) sa nastaví na CAPsMAN.
- CAPsMAN následne distribuuje konfiguráciu na všetky pripojené AP.

MikroTik CAPsMAN

Výhody oproti individuálnej konfigurácii AP:

- stačí spraviť zmenu iba raz na centrálnom manažéri,
- jednotné SSID a šifrovanie pre celú sieť,
- ľahšie riadenie VLAN a segmentácie,
- možnosť rýchlej zmeny hesiel alebo politiky zabezpečenia na celej sieti.

Bezpečnostný prínos:

- zabraňuje tomu, aby boli jednotlivé AP nakonfigurované rôzne (čo je častý problém pri manuálnom nastavovaní),
- umožňuje rýchlu reakciu – napr. okamžité nastavenie nového WPA3 kľúča na všetkých AP naraz.

Vplyv konfigurácií na bezpečnosť

Prečo je konfigurácia kľúčová pre bezpečnosť

- Každé nastavenie v sieti má priamy vplyv na dostupnosť, dôvernosť a integritu dát.
- Správna konfigurácia:
  - bezpečná a stabilná sieť.
- Nesprávna konfigurácia:
  - otvorené dvere pre útočníkov (tzv. misconfiguration).
- Veľa incidentov v sieťach nevzniká pre sofistikované útoky, ale pre chyby v konfiguráciách (defaultné heslá, nesprávne ACL, otvorené porty).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Firewall

- **Účel:** kontroluje a filtruje sieťovú komunikáciu medzi internou sieťou a internetom alebo medzi rôznymi časťami siete.

- **Správna konfigurácia:**
  - povolené sú len nevyhnutné porty a protokoly, pravidlá sú v súlade s politikou organizácie.

- **Nesprávna konfigurácia:**
  - firewall prepúšťa všetku komunikáciu bez obmedzení,
  - sú povolené zbytočné alebo nevyužívané porty,
  - pravidlá sú *príliš prísne* a blokujú aj legitímne služby.

- **Dôsledok**:
  - buď je sieť otvorená pre útočníkov,
  - alebo dochádza k výpadkom legitímnych služieb.

VLAN segmentácia

- **Účel:** logicky rozdeľuje sieť na segmenty (napr. hostia, administratíva, servery), aby sa komunikácia izolovala a znížilo sa riziko šírenia útokov.

- **Správna konfigurácia:**
  - každý typ zariadení alebo používateľov má vlastnú VLAN,
  - VLAN pre hostí je izolovaná od internej siete,
  - servery a kritické systémy sú oddelené od bežných používateľov.

- **Nesprávna konfigurácia:**
  - všetky zariadenia sú v jednej VLAN,
  - rozhrania sú priradené do nesprávnych VLAN,
  - chýba trunkovanie alebo je zle nakonfigurované.

- **Dôsledok:**
  - útočník alebo hosťovské zariadenie sa môže dostať k firemným systémom,
  - šírenie útoku naprieč celou sieťou.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

ACL

- **Účel:** definuje, aká komunikácia je povolená alebo zakázaná medzi zariadeniami, sieťami či aplikáciami.

- **Správna konfigurácia:**
  - prístup k serverom a citlivým systémom len pre autorizované IP adresy,
  - pravidlá vytvorené podľa zásady minimálnych práv.

- **Nesprávna konfigurácia:**
  - ACL je príliš voľná (umožňuje všetko),
  - ACL je príliš prísna (blokuje aj legitímnu prevádzku),
  - chýba dokumentácia alebo poradie pravidiel je zlé.

- **Dôsledok:**
  - útočník získa prístup k citlivým zdrojom,
  - alebo naopak legitímni používatelia stratia prístup k službám.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Wi-Fi

- **Účel:** poskytuje bezdrôtový prístup do siete.

- **Správna konfigurácia:**
  - použitie WPA3 alebo silného WPA2 s dlhým heslom,
  - vypnuté WPS,
  - oddelená sieť pre hostí,
  - správne nastavená VLAN pre Wi-Fi SSID.

- **Nesprávna konfigurácia:**
  - otvorená Wi-Fi bez hesla,
  - použitie slabých alebo zastaraných protokolov (WEP, WPA2 so slabým heslom),
  - hostia majú prístup do internej siete.

- **Dôsledok:**
  - útočník sa ľahko pripojí a má prístup k internej sieti,
  - riziko odpočúvania alebo MITM útokov.

NTP (Network Time Protocol)

- **Účel:** synchronizuje čas na všetkých zariadeniach v sieti, čo je kľúčové pre logovanie, audit a bezpečnostné mechanizmy (napr. certifikáty).

- **Správna konfigurácia:**
  - synchronizácia času s dôveryhodným a overeným serverom (napr. vlastný NTP server, alebo autoritatívny časový zdroj),
  - zabezpečená komunikácia (NTP autentizácia).

- **Nesprávna konfigurácia:**
  - použitie neoverenéhо alebo nedôveryhodného NTP servera,
  - chýba synchronizácia - každé zariadenie má iný čas.

- **Dôsledok:**
  - problémy s logmi (nedajú sa korelovať incidenty),
  - zlyhanie autentizačných mechanizmov, nefunkčné certifikáty.

Bezpečnostné opatrenia

- Bezpečnosť siete nestojí len na firewalloch alebo antivíruse, ale priamo na tom, **ako sú nastavené bezpečnostné funkcie sieťových zariadení**.
- Ak sa nakonfigurujú nesprávne, riziko útoku alebo výpadku výrazne rastie.
- Správna konfigurácia bezpečnostných opatrení je preto rovnako dôležitá ako konfigurácia základných sieťových služieb.

Port Security:

- **Účel:** obmedzuje počet MAC adries na porte (ochrana pred útokom cez pripojenie neautorizovaných zariadení).
- **Správna konfigurácia:** port povoľuje len určitý počet známych MAC adries (napr. 1 PC = 1 MAC).
- **Nesprávna konfigurácia:** porty bez port-security - útočník môže pripojiť vlastné zariadenie alebo floodovať MAC tabuľku switcha.

Bezpečnostné opatrenia

Ochrana pred VLAN hoppingom:

- **Účel:** zabraňuje útočníkovi presunúť sa z jednej VLAN do inej (obchádzanie segmentácie).
- **Správna konfigurácia:** trunk porty sú striktne určené, nepoužívajú sa „dynamické trunky“, natvrdo nastavené VLAN ID.
- **Nesprávna konfigurácia:** ponechané default nastavenia - útočník môže preniknúť do inej VLAN.

DHCP Snooping:

- **Účel:** chráni pred falošným DHCP serverom v sieti.
- **Správna konfigurácia:** iba definované porty sú dôveryhodné pre DHCP, všetky ostatné sú nedôveryhodné.
- **Nesprávna konfigurácia:** chýbajúce pravidlá - útočník môže nasadiť vlastný DHCP a presmerovať prevádzku cez seba (Man-in-the-Middle).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnostné opatrenia

DAI (Dynamic ARP Inspection):

- **Účel:** zabraňuje ARP spoofingu/poisoningu - útočník sa vydáva za iné zariadenie.
- **Správna konfigurácia:** ARP odpovede sa overujú voči databáze (z DHCP Snooping).
- **Nesprávna konfigurácia:** ARP prevádzka sa nekontroluje - útočník môže presmerovať komunikáciu.

BPDU Guard (Bridge Protocol Data Unit Guard):

- **Účel:** chráni sieť pred nesprávnym alebo škodlivým zaslaním STP rámcov (Spanning Tree Protocol).
- **Správna konfigurácia:** BPDU Guard je zapnutý na prístupových portoch - ak sa objaví BPDU, port sa vypne.
- **Nesprávna konfigurácia:** chýba ochrana - útočník alebo omylom pripojený switch môže prebrať STP root rolu a spôsobiť výpadok siete.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Úvod k prevádzke elektronických komunikačných systémov

Technické opatrenia (BLOK IV)
Kurz: Manažér kybernetickej bezpečnosti

Ing. Matúš Madleňák

KC KYB UNIZA, https://kc.uniza.sk/

matus.madlenak@uniza.sk