10 KROKOV K VYŠŠEJ BEZPEČNOSTI SYSTÉMU CISCO IOS

Je to žiaľ krutá realita, že takmer každý deň čítame alebo počúvame správy o rôznych útokoch na IT infraštruktúru malých ale aj veľkých spoločností. Musíme sa zmieriť s faktom, že nie každý používateľ na sieti má dobré úmysly. Nezostáva nám nič iné, ako zapracovať na vyššej bezpečnosti nám zverených systémov a zariadení. V tomto blogu sa pozrieme na 10 možných krokov ako zvýšiť bezpečnosť sieťového operačného systému Cisco IOS.

1. AKTIVÁCIA FUNKCIE ŠIFROVANIA SYSTÉMOVÝCH HESIEL

Tento globálny konfiguračný príkaz automaticky zašifruje heslá v aktívnej beži konfigurácii zariadenia so systémom IOS. Keďže je však použitá šifra pomerne slabá, táto funkcia zabraňuje len náhodnému pozorovateľovi prečítať nepozorovane heslo. Konfiguráciu zariadenia je stále potrebné dôkladne chrániť pred únikom.

```
Router(config)#service password-encryption
```

VYPNUTIE FUNKCIE MANUÁLNEJ OBNOVY HESLA (PASSWORD RECOVERY)

Ak má sieťové zariadenie dostupný tzv. konzolový port, je možné pre každú osobu s fyzickým prístupom k tomuto portu vykonať procedúru na obnovu hesla (Password Recovery). Týmto krokom sa môže neoprávnená osoba dostať ku konfigurácii zariadenia a získať tak citlivé informácie. V systéme IOS je možné túto procedúru deaktivovať uvedeným konfiguračným príkazom. Pripomínam, že je vhodné mať offline zálohu konfigurácie zariadenia, pretože pri obnove hesla systém automaticky zmaže pôvodnú konfiguráciu.

```
Router(config)#no service password-recovery
```

2. VYPNUTIE NEPOTREBNÝCH SIEŤOVÝCH SLUŽIEB

Sieťový systém IOS poskytuje viacero sieťových služieb a protokolov. Ak však tieto služby nevyužívame, môžu poslúžiť ako ďalší spôsob útoku (Attack Vector). Samozrejme, treba si dôkladne zvážiť, ktoré sieťové služby využívame na zariadení, aby sme neprerušili ich produkčnú činnosť a funkciu.

PRÍKAZ VYPNE SLUŽBU TCP-SMALL-SERVERS

```
Router(config)#no service tcp-small-servers
```

PRÍKAZ VYPNE SLUŽBU UDP-SMALL-SERVERS

```
Router(config)#no service udp-small-servers
```

PRÍKAZ VYPNE SLUŽBU FINGER PROTOCOL

```
Router(config)#no ip finger
```

PRÍKAZ VYPNE SLUŽBU BOOTP SERVER

```
Router(config)#no ip bootp server
```

PRÍKAZ FILTRUJE PRIJATÉ PAKETY BOOTP PROTOKOLU

```
Router(config)#ip dhcp bootp ignore
```

PRÍKAZ VYPNE SLUŽBU DHCP SERVER A RELAY

```
Router(config)#no service dhcp
```

PRÍKAZ VYPNE FUNKCIU DNS PREKLADOV (LEN NA ROUTERI)

```
Router(config)#no ip domain-lookup
```

PRÍKAZ VYPNE SLUŽBU X.25 PACKET ASSEMBLER/DISASSEMBLER

```
Router(config)#no service pad
```

PRÍKAZ VYPNE SLUŽBU HTTP SERVER

```
Router(config)#no ip http server
```

PRÍKAZ VYPNE SLUŽBU HTTPS SERVER

```
Router(config)#no ip http secure-server
```

PRÍKAZ VYPNE SLUŽBU PROTOKOLU CDP

```
Router(config)#no cdp run
```

PRÍKAZ VYPNE SLUŽBU PROTOKOLU LLDP

```
Router(config)#no lldp run
```

PRÍKAZ VYPNE SLUŽBU SMART INSTALL VSTACK

```
Router(config)#no vstack
```

PRÍKAZ NA SIEŤOVOM ROZHRANÍ VYPNE SLUŽBU PROTOKOLU MOP

```
Router(config-if)#no mop enabled
```

3. ZAPNUTIE FUNKCIE NA UDRŽIAVANIE TCP RELÁCIÍ (TCP KEEPALIVE)

Tieto globálne konfiguračné príkazy aktivujú funkciu TCP Keepalive, ktorá udržiava aktívne TCP relácie a zabraňuje vzniku tzv. „half-open“ a „orphaned“ TCP relácií, ktoré sa dajú zneužiť na vyčerpanie sieťových a výpočtových zdrojov zariadenia.

```
Router(config)#service tcp-keepalives-in
```

```
Router(config)#service tcp-keepalives-out
```

4. NASTAVENIE ČASOVAČA EXEC TIMEOUT

Stáva sa, že administrátor konfiguruje zariadenie alebo vykonáva diagnostiku a náhle musí odísť. Ak by nechal aktívne pripojenie na odomknutom PC, okoloidúca neoprávnená osoba môže naň získať plný prístup. Táto konfigurácia zabezpečí, že relácia sa po 5 minútach a 30 sekundách nečinnosti automaticky odpojí.

```
Router(config)#line vty 0 15
Router(config-line)#exec-timeout 5 30
```

5. POUŽITIE NA MANAŽMENT ZARIADENIA PROTOKOL SSHv2

Niekomu možno pripadá používanie protokolu SSHv2 ako úplná samozrejmosť, žiaľ musím konštatovať, že ešte stále sa stretávam so zariadeniami s nakonfigurovaným manažmentovým protokolom SSHv1 ba dokonca aj Telnet, čo už je naozaj riskantné. Ako hovorí klasik, opakovanie je matka múdrosti.

```
Router(config)#hostname Router
Router(config)#ip domain-name example.com
Router(config)#crypto key generate rsa modulus 2048
Router(config)#ip ssh time-out 60
Router(config)#ip ssh authentication-retries 3
Router(config)#ip ssh source-interface GigabitEthernet 0/1
Router(config)#ip ssh version 2
Router(config)#ip ssh dh min size 4096
Router(config)#line vty 0 15
Router(config-line)#transport input ssh
```

6. VYPNUTIE ASYNCHRÓNNEHO AUXILIARY (AUX) PORTU

Tento fyzický port sa dá zneužiť na neoprávnený útok na sieťové zariadenie, je preto vhodné ho vypnúť. Na vypnutie portu použijeme nasledujúcu príkazovú sekvenciu.

```
Router(config)#line aux 0
Router(config-line)#transport input none
Router(config-line)#transport output none
Router(config-line)#no exec
Router(config-line)#exec-timeout 0 1
Router(config-line)#no password
```

7. FILTROVANIE MANAŽMENTOVÉHO PRÍSTUPU

Nechávať otvorený manažmentový prístup SSHv2 do celého sveta naozaj nie je dobrý nápad. Je preto vhodné definovať si zoznam povolených IP adries a rozsahov, ktoré môžu pristupovať na SSHv2 server zariadenia. Použijeme nasledujúce príkazy.

```
Router(config)#ip access-list standard LINE-VTY-SSH-FILTER-IN
Router(config-std-nacl)#permit host 192.168.1.10
Router(config-std-nacl)#permit ip 192.168.2.0 0.0.0.255
Router(config-std-nacl)#line vty 0 15
Router(config-line)#access-class LINE-VTY-SSH-FILTER-IN in
```

8. REZERVÁCIA OPERAČNEJ PAMÄTE PRE KONZOLOVÝ PRÍSTUP

Pri útoku typu DDoS (Distributed Denial of Service), na sieťové zariadenie, môže byť veľký problém pristupovať na jeho manažmentové rozhranie, keďže väčšina jeho výpočtových zdrojov je vyčerpaných falošnými požiadavkami útočníkov. Je však možné rezervovať časť operačnej pamäte zariadenia práve na konzolový manažment zariadenia. V tomto príklade rezervujeme 4096 KiB pamäte.

```
Router(config)#memory reserve console 4096
```

9 .ZABEZPEČENIE SIEŤOVÝCH IP ROZHRANÍ

Na sieťových rozhraniach s IP konfiguráciou sú v systéme IOS automaticky aktivované funkcie, ktoré sa zvyčajne nevyužívajú, ale opäť sa dajú zneužiť na viacero škodlivých útokov. Je preto vhodné ich deaktivovať.

```
Router(config-if)#no ip unreachables
Router(config-if)#no ip redirects
Router(config-if)#no ip proxy-arp
```

10. VYPNUTIE FUNKCIE ZDROJOVÉHO IP SMEROVANIA (SOURCE ROUTING)

Pomocou špeciálnych IP paketov s nastaveným „IP Options“ príznakom je možné smerovať sieťovú prevádzku neočakávanou cestou a tak obchádzať bezpečnostné opatrenia ako sú napr. firewally alebo UTM (Unified Threat Management) zariadenia. Táto funkcia sa vypína nasledovným globálnym konfiguračným príkazom.

```
Router(config-if)#no ip source-route
```

Asi nikoho z vás neprekvapím, keď napíšem, že toto v žiadnom prípade nie je vyčerpávajúci zoznam bezpečnostných krokov. Samozrejme, postupov na zabezpečenie systému IOS je viac a vychádzajú z jeho konkrétnej konfigurácie pre danú aplikáciu. Tento blog poskytol základné minimum bezpečnej konfigurácie systému Cisco IOS. Určite viete aj o ďalších možnostiach zabezpečenia, prosím neváhajte a podeľte sa o ne v komentároch.