## **Bezpieczny Mikrotik – RouterOS**

Podobnie jak w przypadku innych producentów sprzętu sieciowego, Mikrotika zaraz po wyjęciu z pudełka należy skonfigurować pod kątem bezpieczeństwa. Niestety w ostatnim czasie pojawiło się sporo zagrożeń związanych z przejęciem całkowitej kontroli nad urządzeniem. Podobne problemy dotyczą praktycznie wszystkich producentów sprzętu, dlatego niezależnie od vendora, zawsze warto poświęcić trochę czasu na zabezpieczenie sprzętu.

Zaczniemy od rzeczy, które należy wykonać **przed** podłączeniem Mikrotika do Internetu.

### 1. Zmiana kont systemowych

Domyślnym kontem w RouterOS jest admin, bez hasła. Zaczynamy od zmiany nazwy usera z admin na dowolnie inną. Używamy silnego hasła, najlepiej z generatora. Znam adminów, co mają kilka ulubionych haseł i tworzą z nich kolejne nowe odmiany, ale lepiej używać menadżera haseł np. <u>KeePass</u>. Konta userów zmieniamy w menu **System**->*Users*.

| A LODGE AND ADDRESS OF ADDRESS OF ADDRESS ADDR |  |       |  |
|--|--|-------|--|
| him may be a second  |  |       |  |
|  | No and<br>The Annual State<br>State State State<br>State State<br>State State<br>State State<br>State State<br>State State<br>State State<br>State State<br>State State<br>State State State<br>State State<br>State State<br>State State State<br>State State State<br>State State State<br>State State State<br>State State State State<br>State State State State<br>State State State State State State<br>State State State State State State State<br>State State State State State State<br>State State | 100   |  |
| 4-08.<br>27  | -  | 10-10 |  |

Terminal:

[code]/user print[/code] Powinieneś zobaczyć listę wszystkich userów w systemie [code] Flags: X – disabled **# NAME GROUP** 0 ;;; system default user grzegorz full 1 admin\_zapasowy read [/code] Wybierając 0 edytujemy ustawienia usera grzegorz, natomiast 1 to user admin\_zapasowy [code] /user set 0 name=nowaNazwaUsera /user set 0 password="HasloZGeneratora!!!" [/code] Dodatkowym zabezpieczeniem jest ustawienie dozwolonych adresów IP, z których można zalogować się do konta. [code] /user set 0 allowed-address=x.x.x.x/yy [/code]

## 2. Aktualizacja RouterOS'a oraz Winbox'a

W ostatnim czasie pojawiło się sporo <u>explitów</u>, dlatego koniecznie zaktualizuj wersje routerOS do najnowszej, najlepiej z gałęzi **current**. Aktualizację możemy wykonać na kilka sposobów, ponieważ skupiliśmy się na krokach jakie należy zrobić przed podłączeniem Mikrotika do Internetu, pozostaje nam manualna instalacja. Przechodzimy na stronę

<u>https://mikrotik.com/download</u> i pobieramy najnowszą wersję. Paczkę wybieramy w zależność od architektury sprzętu, którą najszybciej znajdziemy w nazwie okna winbox'a.



Sama instalacja paczki działa na zasadzie przeciągnij&upuść. Plik należy dodać do **Files**, ważne, aby był w głównym katalogu. Instalacja następni po ponownym uruchomieniu routera. **Uwaga!!!** *instalacja paczki wydłuża pierwszy start routera*.

## 3. Wyłączenie nieużywanych usług(packages)

Jeżeli nie korzystasz z opcji hotspot albo z ipv6, to nie ma sensu, aby były aktywne w systemie. Przechodzimy na **System**->*Package*, podświetlamy paczkę ipv6 i klikamy w **disable**.

| Name         Fremon         Bulk Time         Scheduled           Imatescenepide         6.35.2         May 00.2001 to 109.25         Imatescenepide           Imates  | Creox for spones            | EL-MONE | Constant of | Cranes.   | traineute       | Color-dearen     | Criefin Presidenti |  |
|--|-----------------------------|---------|-------------|-----------|-----------------|------------------|--------------------|--|
| Operation expecte         6.55.2         May 00/2014 10.09.26           Ø showcest feelow         6.55.2         May 00/2014 10.09.26           Ø stop         6.55.2         May 00/2014 10.09.26           Ø spec         6.55.2         May 00/2014 10.09.26  | Name                        | 1       | Version     | Build Ter | e               | Scheduled        |                    |  |
| ● absurance transis         6.15.2         May 020/2014 10.05.26           ● drap         6.15.2         May 020/2014 10.05.26           ● hompost         6.15.2         May 020/2014 10.05.26           ● monitors cm <sup>2</sup> 6.15.2         May 020/2014 10.05.26           ● monitors cm <sup>2</sup> 6.15.2         May 020/2014 10.05.26  | B routerce-mpabe            |         | 6.35.2      | May-0     | 2/2016 10:09:26 |                  |                    |  |
| Ø drop         6.35.2         May 002/2016 10:05.26           Photopot         6.35.2         May 002/2016 10:05.26           Ø por 6         6.35.2         May 002/2016 10:05.26           Ø madrog         6.35.2         May 002/2016 10:05.26           Ø madrogen om 2         6.35.2         May 002/2016 10:05.26   | advanced tools              |         | 6.35.2      | May-G     | 2/2016 10:09:26 |                  |                    |  |
| Bit value         6.35.2         May 00/2016 10:05.36           Bit prof.         6.35.2         May 00/2016 10:05.26           Bit prof.         6.35.2         May 00/2016 10:02.36  | 🗃 shop                      |         | 6.35.2      | May-0     | 2/2016 10:09:26 |                  |                    |  |
| Opport         6.35.2         May 002/2014 10:02.35           Owner         6.35.2         May 002/2014 10:02.35         May 002/2014 10:02.35           Opport         6.35.2         May 002/2014 10:02.36         May 002/2014 10:02.36           Ownering         6.35.2         May 002/2014 10:02.36         May 002/2014 10:02.36           Ownering         6.35.2         May 002/2014 10:02.36         May 002/2014 10:02.36           Ownering         6.35.2         May 002/2014 10:02.36         May 002/2014 10:02.36           Optimizer         6.35.2         May 002/2014 10:02.36         May 002/2014 10:02.36           Optimizer orn2         6.35.2         May 002/2014 10:02.36         May 002/2014 10:02.36  | Compatibility of the second |         | 6.35.2      | May-10    | 0/2016 10:09:26 |                  |                    |  |
| Offmain         6.35.2         Mage/02/2016 10:09.36         Mask block has been block has block | Bavis                       |         | 6.35.2      | May 0     | 0/2016 10 09:26 |                  |                    |  |
| Opp         6.35.2         May 002/0016 10:02:36           Transfer         6.35.2         May 002/0016 10:02:36           Broachy         6.35.2         May 002/0016 10:02:36   | (Freis                      |         | 6.35.2      | May 0     | 2/2016 10 09 26 | attraction for d | Inable             |  |
| Bitsdarg         Inf         6.15.2         May/02/2016 10:01:36           Bitsdarg         6.15.5.2         May/02/2016 10:01:26         May/02/2016 10:01:26           Bystem         6.15.2         May/02/2016 10:01:26         May/02/2016 10:01:26           Characteristics         0.15.2         May/02/2016 10:01:26         May/02/2016 10:01:26           Characteristics         0.15.2         May/02/2016 10:01:26         May/02/2016 10:01:26   | Ø 300                       |         | 6.35.2      | May-0     | 2/2016 10:09:26 | 1.00             | 2.54               |  |
| Bysecurity         6.35.2         Mays 050,20718 10:02.36           Bysecurity         6.35.2         Mays 050,20718 10:02.36           Off members on 2         6.35.2         Mays 050,20718 10:02.36           Bysecurity         6.35.2         Mays 050,20718 10:02.36           Bysecurity         6.35.2         Mays 050,20718 10:02.36  | Badra 19                    |         | 635.2       | May-G     | 2/2016 10:09:26 |                  |                    |  |
| Ø system         6.35.2         Mage 02/2016 10:09.26           Ø soutiese cm2         6.35.2         Mage 02/2016 10:09.26           Ø soutiese de         5.35.2         Mage 02/2016 10:09.26   | @ security                  |         | 6.35.2      | Max 0     | 2/2016 10:09:26 |                  |                    |  |
| Orienteuro con 2         6.35.2         May 00:2016 10:09.26   | @ system                    |         | 6.35.2      | May-0     | 2/2016 10:09:26 |                  |                    |  |
| @ university 6, 25, 2 May 02, 2016 10:09, 26   | (9 violess cm2              |         | 635.2       | Max-0     | 2/2016 10:09:26 |                  |                    |  |
|  | (Passiens /p                |         | 6.35.2      | May-O     | 2/2016 10:09:26 |                  |                    |  |
|  | 🗗 utatiess-lp               |         | 6.35.2      | May G     | 2/2016 10:09:26 |                  |                    |  |

[code]

/system package disable hotspot /system package disable ipv6 [/code]

## 4. Wyłączenie nieużywanych usług(services)

Podobnie jak w przypadku nieużywanych paczke, wyłączamy nieużywane usługi takie jak telnet, ftp, api. Przechodzimy na **IP**->*Services*, podświetlamy usługę, następnie klikamy w czerwony krzyżyk. W przypadku, gdy np. jest nam potrzebne połączenie po ssh, zmieniamy domyślny port usługi, oraz dodajemy ograniczenie logowania po konkretnym adresie IP bądź podsieci. Nie zalecam, a wręcz odradzamy wystawianie serwisów po publicznych adresach. Dedykowany vlan/adresacja do zarządzania(managmentu), to konieczność.

| etficate |
|----------|
| ne       |
| ne       |
|          |
|          |
|          |
|          |
|          |
|          |
| ne       |
|          |

/ip service disable telnet,ftp,www,api,api-ssl /ip service set ssh port=2020 /ip service set winbox address=192.168.66.0/24 /ip service set ssh address=192.168.66.0/24 [/code]

## 5. Wyłączenie logowania do winbox'a po mac addresie

Zarządzanie RouterOSem może odbywać się po adresie IP(L3), ale i także po warstwie drugiej czyli po mac addessie. Domyślnie ta opcja jest włączona na **wszystkich** interfejsach. Przechodzimy na **Tool**->*MAC Server*. Analogicznie jak w przypadku poprzednich ustawień czerwony X wyłącza opcję, ewentualnie dodajmy interfejsy, z których można się zalogować.

| MAC Server                          |                 |
|-------------------------------------|-----------------|
| Telnet Interfaces WinBox Interfaces | Active Sessions |
| + 1                                 | Find            |
| Interface 100 /                     | •               |
| X all                               |                 |
|                                     |                 |
|                                     |                 |
|                                     |                 |
|                                     |                 |
|                                     |                 |
|                                     |                 |
|                                     |                 |
| 1 item (1 selected)                 |                 |

[code]

/tool mac-server mac-winbox set [find] disabled=yes [/code]

## 6. Wyłączenie logowania MAC-Telnet

Zostając w tym samy oknie przechodzimy na zakładkę **Telnet Interfaces** zaznaczamy **all** i wyłączamy opcje. Uchroni to nas przed dalszym rozproszeniem się intruzów w sieci, ponieważ jeden skompromitowany router nie będzie otwartą bramą do pozostałej infrastruktury.

| Telnet Interfaces | WinBox Inte | afaces Ac | tive Sess | ions |
|-------------------|-------------|-----------|-----------|------|
| +                 |             | MAC Ping  | Server    | Find |
| Interface         | p.b.s       |           |           | •    |
| i idii            |             |           |           |      |
|                   |             |           |           |      |
|                   |             |           |           |      |
|                   |             |           |           |      |
|                   |             |           |           |      |
|                   |             |           |           |      |
|                   |             |           |           |      |
|                   |             |           |           |      |

/tool mac-server set [find] disabled=yes /tool mac-server ping set enabled=no [/code]

## 7. Wyłączenie Neighbor Discovery

Kolejną dobrą praktyką jest wyłączenie możliwości wyszukania routera za pomocą Mikrotik Neighbor Discovery Protocol (NDP) albo Cisco Discovery Protocol (CDP). Przechodzimy na zakładkę **IP**->*Neighbors* następnie **Discovery Interfaces**, zaznaczamy interfejsy i czerwonym krzyżykiem wyłączamy.

| Neighbor List  | E 8  |
|--|------|
| Neighbors Decovery Interfaces  | Find |
| Interface         ↓           ▲ ether1         ↓           □ ether2         ↓           □ ether3         ↓ | •    |
| Do Rema (S salected)   |      |

[code]

/ip neighbor discovery settings set default=no default-for-dynamic=no /ip neighbor discovery set [find] discover=no [/code]

## 8. DNS Remote Requests

Domyślnie ta opcja jest odznaczona, ale warto sprawdzić. Przechodzimy na **IP-**>*DNS* i sprawdzamy czy checkbox przy **Allow Remote Requests** jest odznaczony.

| DNS Settings          |                    |     |        |
|-----------------------|--------------------|-----|--------|
| Servers:              |                    | ¢   | 2K     |
| Dynamic Servers:      | 85.237.160.6       |     | Cancel |
|                       | 85.237.160.7       |     | Apply  |
|                       | Allow Remote Reque | sts | Static |
| Max UDP Packet Size:  | 4096               |     | Cache  |
| Query Server Timeout: | 2.000              | s   |        |
| Query Total Timeout:  | 10.000             | 5   |        |
| Cache Size:           | 2048               | KIB |        |
| Cache Max TTL:        | 7d 00:00:00        |     |        |
| Cache Used:           | 9                  |     |        |

/ip dns set allow-remote-requests=no [/code]

## 9. Domyślna konfiguracja Firewall'a

Warto zostawić domyślna konfigurację firewall oraz ograniczyć dostęp do router tylko adresom z allow\_list(dzięki temu nie będziesz musiał ograniczać dostępu do usług per ip/sieć, zrobi to za nas allow lista) [code] /ip firewall filter add action=accept chain=input comment="default configuration" connectionstate=established,related add action=accept chain=input src-address-list=allowed\_to\_router add action=accept chain=input protocol=icmp add action=drop chain=input /ip firewall address-list add address=192.168.66.2-192.168.66.254 list=allowed\_to\_router [/code] Dodatkowe ograniczenia wewnątrz sieci [code] /ip firewall filter add action=fasttrack-connection chain=forward comment=FastTrack connectionstate=established,related add action=accept chain=forward comment="Established, Related" connectionstate=established,related add action=drop chain=forward comment="Drop invalid" connection-state=invalid log=yes log-prefix=invalid add action=drop chain=forward comment="Drop tries to reach not public addresses from LAN" dst-address-list=not\_in\_internet in-interface=bridge1 log=yes log-prefix=! public\_from\_LAN out-interface=!bridge1 add action=drop chain=forward comment="Drop incoming packets that are not NATted" connection-nat-state=!dstnat connection-state=new in-interface=ether1 log=yes log-

#### prefix=!NAT

add action=drop chain=forward comment="Drop incoming from internet which is not public IP" in-interface=ether1 log=yes log-prefix=!public src-address-list=not\_in\_internet add action=drop chain=forward comment="Drop packets from LAN that do not have LAN IP" in-interface=bridge1 log=yes log-prefix=LAN\_!LAN src-address=!192.168.88.0/24

#### /ip firewall address-list

```
add address=0.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=172.16.0.0/12 comment=RFC6890 list=not in internet
add address=192.168.0.0/16 comment=RFC6890 list=not_in_internet
add address=10.0.0.0/8 comment=RFC6890 list=not in internet
add address=169.254.0.0/16 comment=RFC6890 list=not_in_internet
add address=127.0.0.0/8 comment=RFC6890 list=not_in_internet
add address=224.0.0.0/4 comment=Multicast list=not_in_internet
add address=198.18.0.0/15 comment=RFC6890 list=not in internet
add address=192.0.0.0/24 comment=RFC6890 list=not in internet
add address=192.0.2.0/24 comment=RFC6890 list=not_in_internet
add address=198.51.100.0/24 comment=RFC6890 list=not in internet
add address=203.0.113.0/24 comment=RFC6890 list=not_in_internet
add address=100.64.0.0/10 comment=RFC6890 list=not in internet
add address=240.0.0/4 comment=RFC6890 list=not_in_internet
add address=192.88.99.0/24 comment="6to4 relay Anycast [RFC 3068]"
list=not in internet
[/code]
```

## 10. Wyłączenie nieużywanych interfejsów

Nieużywane port należy wyłączyć, a najlepiej w ogóle nie dodawać do konfiguracji.



[code] /interface set 2,3,4,5,6,7,8 disabled=yes [/code]

## 11. Włączenie klienta NTP

Aktualna data i godzina jest bardzo ważna, bez nich analiza logów będzie mocno utrudniona, a czasami wręcz niemożliwa.

| SNTP Client             |                             |         |
|-------------------------|-----------------------------|---------|
|                         | <ul> <li>Enabled</li> </ul> | OK      |
| Mode:                   | unicast                     | Cancel  |
| Primary NTP Server:     | 153.19.250.123              | Apply   |
| Secondary NTP Server:   | 0.0.0.0                     | hanning |
| Server DNS Names:       |                             | \$      |
| Dynamic Servers:        |                             |         |
| Poll Interval:          | 32 s                        |         |
| Active Server:          | 153.19.250.123              |         |
| Last Update From:       | 153.19.250.123              |         |
| Last Update:            | 00:00:01 ago                |         |
| Last Adjustment:        | -5 881 980 us               |         |
| Last Bad Packet From:   |                             |         |
| Last Bad Packet:        |                             |         |
| Last Bad Packet Reason: |                             |         |

/system ntp client set enabled=yes server-dns-names=ntp.task.gda.pl
[/code]

## 12. Logowanie zdarzeń

Najlepszym i najbezpieczniejszym rozwiązaniem jest logowanie zdarzeń do zewnętrznego <u>sysloga</u>. W innym przypadku zdarzenia można logować na dysk, ale wbudowana pamięć jest bardzo mała, dlatego do Mikrotików z portem usb możemy podłączyć pendriva.

## 13. Szyfruj kopie zapasową przy użyciu hasła

Przy eksporcie konfiguracji zawsze podawaj hasło.



### 14. Wyłącz LCD

15. Wyłącz BTest Server

## Podsumowanie

| 14 C   |  | 80  |
|--|--|-----|
| freeze   |  | 4 1 |
| Then TO TO TO ALL COMMAND AND ADDRESS OF ADDRESS OF ADDRESS ADDRES   | controllation for case or units from 10, 100, 211, 107, on refuse  | 1.  |
| Aug. (2). (2) (2) (2) (4) (1) partners, making provident   | supplication for user shall from 10, 104 201 107 on rates!   |     |
| Aug. 20 (2012) (2014) 12 manutory makes are taken  | loads/fail.org/her.commond/from 28 128 2771 167 up (advanced   |     |
| And TALENAL AND AN ALL ADDRESS OF ADDRESS ADDR | Institution for one production from 10 100, 211, 107 do instant  |     |
| Aug. 20. 2012 (2014) 14 mercery makes, provinced   | anti-fail are for case and free 18, 124 201 147 on taken   |     |
| Aug. 20. 2018 (M. H. H. Harrison, March 1999) (Mind  | test-false for star and free \$1,734,271 167 statistical   |     |
| Aug (20.2010/2014) 17 metalogy makes are adout   | supplied on his case studie have \$1,120,211,167 on telest   |     |
| Aug 20 2010 00 40 10 remove and an eric related  | instruction for user and from 20, 100 201 307 on Infrast   |     |
| Aug. 20.2012 (2014) 20 meters and an address arear address   | materializes for case and from 38 124 277 367 management   |     |
| And The COLUMN IS NOT A REAL PROPERTY AND ADDRESS OF AD | benefatigation for some en state have 10, 2000 277, 2017 og behadt   |     |
| And TO TOTAL CO. 41 27 annual states and referal   | supplied on the case and them 20, 724, 221, 267 on taken   |     |
| And the local division of the second se   | and the owner and they fill "24 277 167 statement  |     |
| And M. State State 1.1 merces and an ender state of the other  | some find and har a new set of the firsts 10, 1000, 211, 1077 and indicate   |     |
| And Mildford Mildl 27 mercers and an entry official  | supplied on the case and have \$1. UP \$21 MT on taken   |     |
| Anno 2012/2012 (2018) 22 memory modern arrivational  | second advectory and advectory (0) 121 211 207 one parts   |     |
| And TO COMPANY AND AND AND AND AND AND AND   | tradiction for one would have \$1,500 (21,507 on interior  |     |
| And TO CONTROL IN AN ADDRESS AND ADDRESS AND ADDRESS ADDRE   | particular for one and then \$1.54 \$15 MT on sales  |     |
| And M. Month M. 41 To manage in states and a state of  | termination of the same in and from \$60 King \$1.5 King? on address   |     |
| And the balance of the second se   | provided on the case another how M. 201 (2-1 147) on patient   |     |
| And TR. MARKED AT THE DESIGN AND ADDRESS OF COMPANY  | conclusion for one shall from \$5, 124 \$21 \$67 on taken  |     |
| And TRADING AND AN AVAILABLE AND ADDRESS A | and the owner was been been 10, 100, 201, 207, and along   |     |
| And the little and the second section where we are related   | territorial conference and the face. In 1919 211 1977 on factorial   |     |
| Aug. 20, 2018 (Multi Managers) and an and added  | increasing on the uncertaint time 10, 104 201 147 on adapt   |     |
| ton 10, 1014 (0-40 4) memory makes any other   | periodial on the case and time AL Via 2011 Self statement  |     |
| And TR. 2014 (Bull 4) 42 menory waters and refused   | some find om her opperaturation here. M. 1000, 2011 1877 og stationet  |     |
| And the State of the second section and referred   | controlled on her using shad lines (M. Chi 201) (M7 and failured   |     |
| A CONTRACTOR AND AN OWNER AND  | deared an operation of their section of the section |     |

Stawiaj bezpieczeństwo na pierwszym miejscu, lepiej jest posiedzieć dłużej nad konfiguracją, dodaniem sieci managmentowej, ale później spać spokojnie. W większej części przejęte routery robiły za koparki kryptowalut, czasami za dnsy do phisingowych stron, ale to chyba najlepsze co może Cię spotkać. Inwigilacja sieci za routerem, kradzież danych osobnych, to tylko jedne z nielicznych konsekwencji złego zabezpieczenia RouterOSa.

# Polecany sprzęt

Z własnego doświadczenia mogę wam polecić poniższy sprzęt, z podziałem na ewentualne przeznaczenie routera.

**Do domu i małej firmy(SOHO):** <u>hAP AX Lite</u>, <u>hAP AC3</u>, <u>RB4011</u>, <u>RB260GS</u>, <u>RB2011</u> <u>hAP AC3 LTE</u>, <u>hAP AX2</u>, <u>hAP AX3</u>, <u>L009UiGS-2HaxD-IN</u>, <u>RB5009UG+S+IN</u>, <u>Audience</u>

**LTE:** <u>SXT LTE kit</u>, <u>SXT LTE6 kit</u>, <u>LHG 5</u>, <u>LHG LTE kit</u>, <u>Audience LTE</u>, <u>Chateau LTE6 ax</u>, <u>LTAP</u> <u>LTE6</u>

Access Pointy: <u>mAP lite</u>, <u>mAP</u>, <u>cAP AX</u>, <u>cAP XL AC</u>

POE: <u>hEX PoE</u>

LAB: <u>hEX lite</u>

Średnia/Duża firma: CCR1036-12G-4S, CCR2004-16G-2S+