

Zabezpieczenia domowego punktu dostępowego

Jak zabezpieczyć domowy punkt dostępowy (router)?

Dlaczego to ważne?

- Chroni prywatność i dane osobiste.
- Zapobiega nieautoryzowanemu dostępowi do sieci.
- Minimalizuje ryzyko cyberataków.

Zmiana domyślnych danych logowania

Dlaczego to ważne?

- Domyślne dane są publicznie dostępne (np. admin/admin).
- Łatwy cel dla ataków typu "brute force" lub skryptów automatycznych.

Jak zmienić dane logowania?

1. Zaloguj się do panelu administracyjnego (adres IP np. 192.168.0.1).
2. Przejdź do sekcji System / Security / Administrator Settings.
3. Zmień login i hasło na unikalne, silne hasło.

"Silne hasło": minimum 12 znaków, litery, cyfry, znaki specjalne.

„Silne” hasło

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD					
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

<https://www.hivesystems.io/password>

„Silne” hasło



Using ChatGPT hardware to brute force your password in 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	instantly	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	instantly	instantly
7	instantly	instantly	instantly	instantly	instantly
8	instantly	instantly	instantly	instantly	1 sec
9	instantly	instantly	4 secs	21 secs	1 min
10	instantly	instantly	4 mins	22 mins	1 hour
11	instantly	6 secs	3 hours	22 hours	4 days
12	instantly	2 mins	7 days	2 months	8 months
13	instantly	1 hour	12 months	10 years	47 years
14	instantly	1 day	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Source: hivesystems.io



<https://www.hivesystems.io/password>

„Silne” hasło



security awareness



Security Awareness Episode 1: Passwords

<https://www.youtube.com/watch?v=0Wd3JoUHXno&list=PL7QHbjPSF0r6qJonaROIxVaMLzwDnZyOL>

Wyłączenie rozgłaszania SSID

Dlaczego to ważne?

- Ukrycie nazwy sieci utrudnia jej znalezienie przez osoby postronne.
- Zmniejsza ryzyko ataków na sieć.

Jak wyłączyć rozgłaszanie SSID?

1. Zaloguj się do panelu administracyjnego.
2. Przejdź do sekcji **Wireless Settings / SSID Broadcast**.
3. Odznacz opcję **Enable SSID Broadcast** lub włącz **Hide SSID**.

Włączenie szyfrowania danych

Dlaczego to ważne?

- Szyfrowanie chroni przesyłane dane przed podsłuchiwaniami.
- Minimalny standard: **WPA2-PSK** (lub **WPA3**, jeśli dostępne).

Jak włączyć szyfrowanie?

1. Przejdź do sekcji **Wireless Settings / Security**.
2. Wybierz tryb szyfrowania **WPA2-PSK** (lub **WPA3**, jeśli dostępne).
3. Wprowadź silne hasło sieciowe (min. 12 znaków, unikalne).

Wskazówka: Unikaj szyfrowania WEP, jest przestarzałe i niebezpieczne.

Jak działa szyfrowanie WPA3

WPA3 (*Wi-Fi Protected Access 3*) to najnowszy standard zabezpieczeń sieci bezprzewodowych, wprowadzony przez **Wi-Fi Alliance** w 2018 roku. Jest następcą WPA2 i oferuje znacznie lepszą ochronę przed atakami, w tym atakami słownikowymi i podsłuchiowaniem transmisji.

Kluczowe ulepszenia WPA3 względem WPA2

WPA3 wprowadza kilka fundamentalnych zmian i nowych mechanizmów bezpieczeństwa:

- **SAE (Simultaneous Authentication of Equals)** – odporny na ataki słownikowe mechanizm uwierzytelniania, zastępujący **PSK (Pre-Shared Key)**.
- **Forward Secrecy** – każda sesja korzysta z unikalnego klucza szyfrującego.
- **Ochrona przed atakami offline** – atakujący nie może przechwycić i wielokrotnie odtwarzać ruchu, by złamać hasło.
- **Lepsza ochrona sieci otwartych** – szyfrowanie ruchu nawet w sieciach bez hasła (*OWE – Opportunistic Wireless Encryption*).
- **256-bitowe klucze w WPA3-Enterprise** – znacznie mocniejsze szyfrowanie niż w WPA2-Enterprise.

Jak działa szyfrowanie WPA3

Simultaneous Authentication of Equals (SAE) – Kluczowy mechanizm WPA3

WPA3-PSK (znany jako **WPA3-Personal**) nie używa już tradycyjnego klucza wstępnego **Pre-Shared Key (PSK)**. Zamiast tego stosuje **SAE (Simultaneous Authentication of Equals)** – mechanizm oparty na mechanizmie **Dragonfly Key Exchange**, który chroni przed atakami offline.

Jak działa SAE w WPA3?

1. Proces uwierzytelniania

- **Inicjalizacja** – Klient i punkt dostępu (AP) przeprowadzają **kluczową wymianę danych**, ale nie przesyłają haseł w jawnej postaci.
- **Generowanie kluczy** – Obie strony używają mechanizmu **Diffie-Hellmana** do wymiany danych i wygenerowania wspólnego klucza sesji.
- **Weryfikacja** – Klient i AP potwierdzają autentyczność, zanim nawiążą połączenie.

2. Ochrona przed atakami słownikowymi

- W przeciwieństwie do WPA2, gdzie hasło było przesyłane w postaci **klucza skrótu**, SAE zapobiega atakom **offline** – nawet jeśli atakujący przechwyci wymianę kluczy, nie może jej ponownie odtworzyć i sprawdzić różnych haseł.
- Klucz sesji jest **jednorazowy** – nawet jeśli atakujący zdobędzie jedno hasło, nie odszyfruje wcześniejszych sesji.

3 . Forward Secrecy – klucz do bezpieczeństwa

- Każda sesja w WPA3 jest zabezpieczona unikalnym kluczem sesji.
- Oznacza to, że złamanie klucza nie pozwala odszyfrować wcześniejszych komunikacji.

Jak działa szyfrowanie WPA3

Ochrona sieci otwartych – Opportunistic Wireless Encryption (OWE)

Sieci Wi-Fi w miejscach publicznych (np. kawiarniach, lotniskach) tradycyjnie nie stosowały szyfrowania, co umożliwiało ataki typu **Man-in-the-Middle (MITM)**. WPA3 wprowadza mechanizm **OWE**

(Opportunistic Wireless Encryption), który:

- Automatycznie szyfruje ruch w sieciach otwartych, nawet bez hasła.
- Zapewnia podstawową ochronę przed przechwytywaniem transmisji.
- Nie wymaga od użytkownika żadnej konfiguracji – działa automatycznie.

WPA3-Enterprise – Szyfrowanie klasy korporacyjnej

Dla firm i organizacji WPA3 oferuje **WPA3-Enterprise**, który:

- Wprowadza **szyfrowanie 192-bitowe** zamiast 128-bitowego.
- Korzysta z **szyfrowania CNSA (Commercial National Security Algorithm)** rekomendowanego przez NSA.
- Oferuje lepszą ochronę przed podsłuchiwaniami i atakami man-in-the-middle.

Jak działa szyfrowanie WPA3

Wady i ograniczenia WPA3

Wsteczna kompatybilność:

WPA3 obsługuje tryb **WPA3/WPA2 mixed mode**, ale starsze urządzenia mogą nadal działać w trybie WPA2.

Wymagania sprzętowe:

- Starsze routery wymagają aktualizacji oprogramowania lub całkowitej wymiany na sprzęt zgodny z WPA3.

Ataki Dragonblood:

- W 2019 roku badacze odkryli luki w implementacji **SAE (Dragonfly)**, które umożliwiały ataki side-channel. Aktualizacje firmware'u i poprawione implementacje WPA3 załatały te luki.

Podsumowanie

- **WPA3 zwiększa bezpieczeństwo Wi-Fi dzięki silniejszemu szyfrowaniu i ochronie przed atakami offline.**
- **Nowy mechanizm SAE zapobiega atakom słownikowym, a OWE szyfruje ruch w sieciach otwartych.**
- **Firmy mogą korzystać z WPA3-Enterprise z 192-bitowym szyfrowaniem klasy rządowej.**
- **Wymagana jest obsługa sprzętowa – starsze routery mogą nie wspierać WPA3.**
- **Pierwsze wersje miały luki w zabezpieczeniach, ale zostały poprawione.**

WPA3 to duży krok naprzód w zabezpieczeniach sieci Wi-Fi, jednak jego skuteczność zależy od wdrożenia przez producentów sprzętu i użytkowników.

Biała lista adresów MAC

Dlaczego to ważne?

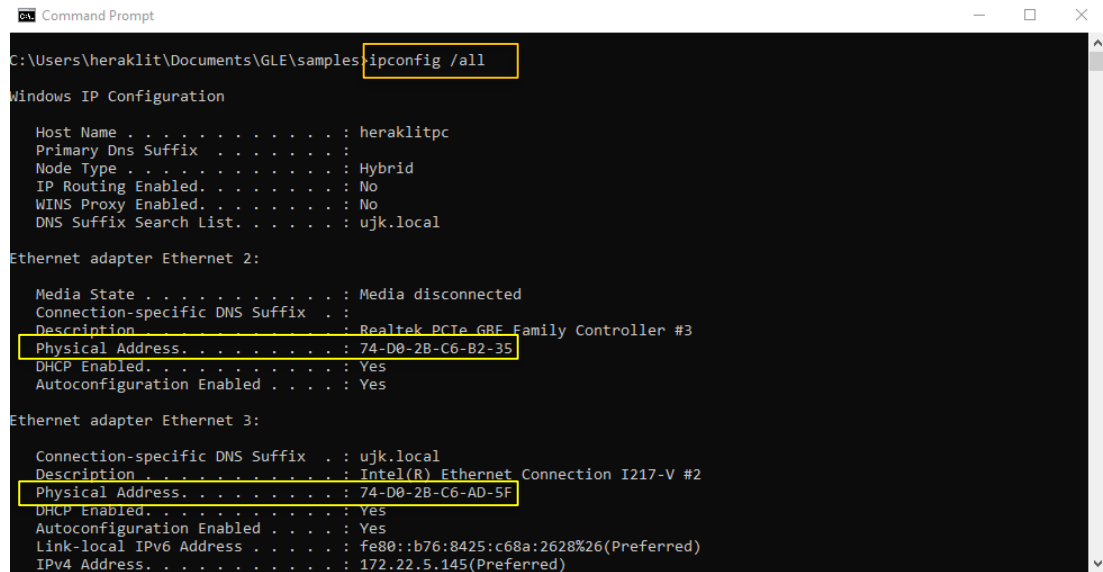
- Dodatkowa warstwa zabezpieczeń.
- Ogranicza dostęp tylko do zaufanych urządzeń.

Jak skonfigurować?

1. Przejdź do sekcji **Wireless Settings / MAC Filtering**.
2. Włącz opcję **Enable MAC Filtering**.
3. Dodaj adresy MAC urządzeń, które mają mieć dostęp.

Uwaga:

Adres MAC każdego urządzenia znajdziesz w jego ustawieniach sieciowych.



```
Command Prompt
C:\Users\heraklit\Documents\GLE\samples>ipconfig /all

Windows IP Configuration

Host Name . . . . . : heraklitpc
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ujk.local

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GBE Family Controller #3
Physical Address. . . . . : 74-D0-2B-C6-B2-35
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . : ujk.local
Description . . . . . : Intel(R) Ethernet Connection I217-V #2
Physical Address. . . . . : 74-D0-2B-C6-AD-5F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::b76:8425:c68a:2628%26(Preferred)
IPv4 Address. . . . . : 172.22.5.145(Preferred)
```

Podsumowanie

Kluczowe kroki:

1. Zmień dane logowania do panelu administracyjnego.
2. Wyłącz rozgłaszanie SSID.
3. Włącz szyfrowanie WPA2 lub WPA3.
4. Skorzystaj z białej listy adresów MAC.

Dodatkowe wskazówki:

- Aktualizuj oprogramowanie routera.
- Monitoruj urządzenia podłączone do sieci.

Pytania?