

# Lekcja

## Temat: Wprowadzenie do cyberbezpieczeństwa



**Cyberbezpieczeństwo (ang. cybersecurity)** to **zbiór praktyk, procesów, technologii i środków organizacyjnych mających na celu ochronę systemów informatycznych, sieci, programów, urządzeń i danych przed atakami, uszkodzeniem lub nieautoryzowanym dostępem**. Jego celem jest zapewnienie poufności, integralności i dostępności informacji (tzw. triada CIA):

-  **C (Confidentiality)** – Poufność: dane dostępne tylko dla uprawnionych.
-  **I (Integrity)** – Integralność: dane są kompletne, dokładne i niezmienione bez autoryzacji.
-  **A (Availability)** – Dostępność: systemy i dane są dostępne dla uprawnionych użytkowników, gdy są potrzebne.



## Zastosowanie w informatyce



**Cyberbezpieczeństwo znajduje zastosowanie w każdej dziedzinie IT, m.in.:**

- **Ochrona infrastruktury sieciowej** (routery, przełączniki, firewalle).
- **Bezpieczeństwo aplikacji** (testy penetracyjne, bezpieczny kod, ochrona przed atakami na aplikacje webowe).
- **Bezpieczeństwo danych** (szyfrowanie, zarządzanie dostępem, backup).
- **Bezpieczeństwo chmury obliczeniowej** (ochrona danych i aplikacji hostowanych w chmurze).
- **Bezpieczeństwo operacyjne** (monitoring, zarządzanie incydentami, polityki bezpieczeństwa).
- **Bezpieczeństwo urządzeń końcowych** (komputery, smartfony, IoT).
- **Bezpieczeństwo tożsamości i dostępów** (uwierzytelnianie wieloskładnikowe – MFA, zarządzanie tożsamością).



## Ochrona infrastruktury sieciowej (routery, przełączniki, firewalle).

Infrastruktura sieciowa to m.in.: **routery, przełączniki, firewalle**.

Każde z tych urządzeń ma inną rolę w ochronie sieci.

2



### Router – pierwsza linia obrony w sieci

**Router** łączy sieć lokalną (LAN) z Internetem (WAN).

**Jak chroni:**

#### 1. Filtrowanie ruchu (Access Control Lists – ACL)

- Router może blokować ruch przychodzący lub wychodzący na podstawie adresu IP, portu lub protokołu.
- Przykład:
  - Blokujemy wszystkie połączenia przychodzące na port 23 (Telnet)
  - Pozwalamy tylko na porty 80 (HTTP) i 443 (HTTPS)

#### 2. Network Address Translation (NAT)

- Ukrywa wewnętrzne adresy IP przed Internetem
- Haker nie widzi dokładnie, jakie urządzenia są w sieci wewnętrznej

#### 3. Routing bezpieczny

- Routery mogą używać protokołów, które **chronią przed podszywaniem się w sieci** (np. OSPF authentication)

3



### Przełącznik (Switch) – ochrona wewnętrznej sieci LAN

**Switch** rozdziela ruch w sieci lokalnej.

**Jak chroni:**

#### 1. Segmentacja sieci (VLAN)

- Można podzielić sieć na różne grupy np. IT, księgowość, goście
- Atak z jednego VLANu **nie przechodzi automatycznie** do innych VLANów

#### 2. Port Security

- Ogranicza dostęp do portu tylko dla zdefiniowanych adresów MAC,

b. Jeśli ktoś podłączy obcy komputer, nie dostanie dostępu do sieci

### 3. Ochrona przed ARP spoofing i MAC flooding

a. Zapobiega podszywaniu się hakerów pod inne urządzenia w LAN



## Firewall – ochrona przed atakami z zewnątrz

**Firewall** to strażnik między siecią wewnętrzną a Internetem.

**Jak chroni:**

### 1. Blokowanie nieautoryzowanego ruchu

- a. Firewall przepuszcza tylko ruch zgodny z regułami
- b. Przykład: blokuje połączenia przychodzące spoza zaufanych IP

### 2. Ochrona przed atakami typu DoS / DDoS

- a. Limituje liczbę połączeń z jednego IP, żeby **nie zablokować serwera przeciążeniem**

### 3. Analiza ruchu i filtrowanie pakietów

- a. Sprawdza, czy pakiet jest „legalny”
- b. W niektórych firewallach NGFW analizuje **aplikacje i złośliwe wzorce ruchu**



**Bezpieczeństwo aplikacji** (testy penetracyjne, bezpieczny kod, ochrona przed atakami na aplikacje webowe).



## Testy penetracyjne (Penetration Testing)

**Cel:** sprawdzić, czy aplikacja ma luki bezpieczeństwa.

**Przykład:**

- Strona logowania do panelu administracyjnego.
- Tester próbuje wprowadzić w polu hasła:

' OR '1'='1

- Jeśli aplikacja **nie sprawdza poprawnie danych**, tester może się zalogować bez prawidłowego hasła → luka SQL Injection.
- Raport z testu zawiera opis luk i zalecenia: użycie **zapytania parametryzowanego**.



2

## Pisanie bezpiecznego kodu (Secure Coding)

**Cel:** tworzyć aplikacje w taki sposób, aby były odporne na ataki.

**Przykłady:**

### 1. Weryfikacja danych wejściowych

```
# zamiast wstawiać dane bezpośrednio do SQL  
cursor.execute("SELECT * FROM users WHERE username = ?", (username,))
```

a. Użycie **zapytania parametryzowanego** chroni przed SQL Injection.

### 2. Szyfrowanie wrażliwych danych

```
import hashlib  
password_hash = hashlib.sha256(password.encode()).hexdigest()
```

a. Hasła przechowywane w bazie są w formie **hasha**, nie w czystym tekście.

### 3. Używanie bezpiecznych protokołów

- a. HTTPS zamiast HTTP
- b. TLS/SSL dla komunikacji z API



3

## Ochrona przed atakami na aplikacje webowe

### Typ ataku

SQL Injection	Zapytania parametryzowane, ORM (np. Django ORM)
Cross-Site Scripting (XSS)	Escapowanie danych wyświetlanych w HTML, Content Security Policy (CSP)
Cross-Site Request Forgery (CSRF)	Tokeny CSRF w formularzach
Brute Force	Limitowanie prób logowania, CAPTCHA, MFA
Session Hijacking	Bezpieczne ciasteczka (HttpOnly, Secure), szyfrowanie sesji

### Przykład ochrony



## 4 Przykład praktyczny – strona logowania

1. Formularz logowania:
  - a. Użytkownik wpisuje login i hasło
2. Testy penetracyjne wykrywają lukę SQL Injection
3. Programista poprawia kod:
  - a. Używa zapytań parametryzowanych
  - b. Dodaje limit prób logowania i MFA
4. Strona jest teraz odporna na najczęstsze ataki



## 5 Podsumowanie

- **Testy penetracyjne** → sprawdzają luki w aplikacji
- **Bezpieczny kod** → minimalizuje ryzyko ataków (walidacja, szyfrowanie, HTTPS)
- **Ochrona przed atakami webowymi** → XSS, CSRF, SQL Injection, brute force



**Bezpieczeństwo danych** to zestaw działań mających na celu ochronę informacji przed nieautoryzowanym dostępem, utratą lub uszkodzeniem. Obejmuje m.in.:

1. **Szyfrowanie** – dane są kodowane w taki sposób, że bez odpowiedniego klucza nie da się ich odczytać.
  - a. *Przykład:* wiadomości w komunikatorach takich jak Signal czy WhatsApp są szyfrowane end-to-end.
2. **Zarządzanie dostępem** – kontrola, kto i w jakim zakresie może korzystać z danych.
  - a. *Przykład:* w firmie pracownicy działu księgowości mają dostęp do faktur, ale nie do danych kadrowych.
3. **Backup (kopie zapasowe)** – tworzenie kopii danych, aby można je było przywrócić w razie awarii lub utraty.



**Bezpieczeństwo chmury obliczeniowej** polega na ochronie danych, aplikacji i infrastruktury hostowanej w chmurze przed nieautoryzowanym dostępem, utratą lub atakami cybernetycznymi. Obejmuje kilka kluczowych obszarów:



1. **Szyfrowanie danych w chmurze** – chroni informacje zarówno w czasie przesyłania (transmisji), jak i przechowywania (w spoczynku).

a. *Przykład:* dane przechowywane w Amazon S3 lub Google Cloud Storage mogą być szyfrowane AES-256.



2. **Kontrola dostępu i uwierzytelnianie** – ogranicza, kto może logować się do chmury i korzystać z aplikacji.

a. *Przykład:* użycie uwierzytelniania wieloskładnikowego (MFA) dla kont administracyjnych w Microsoft Azure.



3. **Monitoring i wykrywanie zagrożeń** – systemy monitorują aktywność w chmurze i wykrywają nietypowe działania lub próby włamań.

a. *Przykład:* AWS CloudTrail rejestruje wszystkie operacje na zasobach chmurowych, a Amazon GuardDuty analizuje podejrzane zachowania.



4. **Backup i odzyskiwanie danych** – tworzenie kopii zapasowych i planów odzyskiwania po awarii.

a. *Przykład:* Google Cloud Backup & DR pozwala przywrócić dane aplikacji w razie przypadkowego usunięcia lub awarii.



5. **Zabezpieczenie aplikacji** – ochrona przed atakami typu SQL injection, XSS, DDoS itp.

a. *Przykład:* korzystanie z Web Application Firewall (WAF) w chmurze do filtrowania niebezpiecznych żądań HTTP.



**Bezpieczeństwo operacyjne** to działania i procedury zapewniające ochronę systemów informatycznych w codziennej pracy organizacji. Skupia się na tym, aby procesy, infrastruktura i ludzie pracowali w bezpieczny sposób. Obejmuje m.in.:

- 
  1. **Monitoring** – ciągłe śledzenie systemów i sieci w celu wykrywania zagrożeń lub nieprawidłowości.
    - a. *Przykład:* system SIEM (Security Information and Event Management) analizuje logi serwerów i powiadamia administratora o podejrzanych próbach logowania.
- 
  2. **Zarządzanie incydentami** – proces reagowania na zdarzenia bezpieczeństwa, tak aby zminimalizować szkody i przywrócić normalne działanie systemu.
    - a. *Przykład:* po wykryciu ataku ransomware dział IT izoluje zainfekowane komputery i przywraca dane z kopii zapasowej.
- 
  3. **Polityki bezpieczeństwa** – zestaw zasad i procedur, które określają, jak pracownicy mają postępować, aby chronić dane i systemy.
    - a. *Przykład:* polityka wymaga zmiany hasła co 90 dni i zakazuje korzystania z niezaufanych nośników USB w firmie.

W skrócie: **bezpieczeństwo operacyjne to codzienna „tarcza” organizacji**, która chroni systemy i dane dzięki monitorowaniu, reagowaniu na incydenty i ustalonym zasadom postępowania.



**Bezpieczeństwo urządzeń końcowych** (ang. *endpoint security*) polega na ochronie komputerów, smartfonów, tabletów czy urządzeń IoT przed zagrożeniami takimi jak malware, kradzież danych czy nieautoryzowany dostęp. Chodzi o to, żeby każde urządzenie podłączone do sieci było bezpieczne, bo stanowi potencjalne wejście dla atakującego.

- 
  1. **Ochrona antywirusowa i antymalware** – instalacja programów, które wykrywają i usuwają złośliwe oprogramowanie.

*Przykład:* Windows Defender na komputerach z Windows lub Avast na laptopach i smartfonach.
  2. **Aktualizacje systemu i aplikacji** – regularne łatanie luk bezpieczeństwa, które mogą być wykorzystane przez atakujących.

*Przykład:* automatyczne aktualizacje Androida, iOS czy Windowsa, które naprawiają podatności.



3. **Szyfrowanie danych na urządzeniu** – zabezpiecza dane w razie kradzieży lub zgubienia sprzętu.

*Przykład:* BitLocker na komputerach z Windows lub szyfrowanie iPhone (FileVault w MacOS).



4. **Kontrola dostępu i uwierzytelnianie** – blokowanie dostępu osobom nieupoważnionym.

*Przykład:* logowanie do smartfona za pomocą PIN-u, odcisku palca lub Face ID.



5. **Bezpieczeństwo IoT** – zabezpieczenie inteligentnych urządzeń domowych lub przemysłowych.

*Przykład:* aktualizacja oprogramowania inteligentnych kamer, zablokowanie domyślnych haseł w smart TV lub czujnikach IoT.

## Lekcja

### Temat: Rodzaje szkodliwego oprogramowania: wirusy



**Wirus komputerowy to złośliwe oprogramowanie**, które:

- Powiela się (kopiuje do innych plików/programów)
- Wymaga "nosiciela" (pliku, programu, dokumentu)
- Wykonuje niepożądane działania



## JAK DZIAŁA WIRUS?



### Prosty cykl życia:

1. **Zarażenie** → Wirus przyczepia się do zdrowego pliku
2. **Ukrywanie** → Czeka na aktywację
3. **Uaktywnienie** → Wykonuje złośliwy kod
4. **Rozprzestrzenianie** → Szuka nowych plików do zarażenia



## GŁÓWNE RODZAJE WIRUSÓW:



### 1. WIRUSY PLIKOWE

Przyczepiają się do programów:

- .exe, .dll, .com
- **Przykład:** Uruchamiasz grę, a wirus infekuje system



### 2. WIRUSY BOOT SEKTORA

Atakują obszar startowy dysku:

- Uaktywniają się przy starcie komputera
- Bardzo trudne do usunięcia
- **Przykład:** "Stoned", "Michelangelo"



### 3. MAKROWIRUSY

Ukryte w dokumentach:

- Głównie w plikach Office (Word, Excel)
- Używają makr do działania
- **Przykład:** "Melissa" (1999) - rozsyłał się mailem

## 4. WIRUSY SKRYPTOWE

Pisane w językach skryptowych:

- JavaScript, VBScript, PowerShell
- Działają w przeglądarkach/systemie
- **Przykład:** "Love Letter" (ILOVEYOU)

## JAK ROZPOZNAĆ ZARAŻONY KOMPUTER?

### Objawy infekcji:

- Komputer działa WOLNIEJ niż zwykle
- Pojawiają się DZIWNE OKNA/REKLAMY
- Programy CRASHUJĄ bez powodu
- PLIKI ZNIKAJĄ lub się uszkadzają
- Dziwne WIADOMOŚCI od Ciebie do znajomych
- WYSOKIE użycie procesora bez powodu
- ANTYWIRUS przestaje działać

## JAK SIĘ CHRONIĆ? - 5 ZŁOTYCH ZASAD

### 1. Antywirus

- Zawsze aktualizowany
- Regularne skanowanie
- **Przykłady:** Windows Defender, AVG, Avast



## 2. Aktualizacje systemu

- Windows Update zawsze włączony
- Aktualne wersje programów



## 3. Ostrożność w sieci

NIE KLIKAJ:

- Dziwnych linków w mailach
- "Nagród" i "alertów"
- Podejrzanych załączników



## 4. Backup danych

- Regularne kopie zapasowe
- Przechowywane offline



## 5. Zdrowy rozsądek

- Nie instaluj "cracków"
- Nie używaj pendrive'ów z nieznanego źródła
- Sprawdzaj, co pobierasz



## RÓŻNICA: WIRUS vs INNE ZŁOŚLIWE OPROGRAMOWANIE

Typ	Główna cecha	Przykład
Wirus	Przyczepia się do plików	ILOVEYOU
Robak	Roznosi się SAM (bez pliku)	Mydoom

<b>Trojan</b>	Udaje coś pozytecznego	Fake antywirus
<b>Ransomware</b>	Blokuje i żąda okupu	WannaCry
<b>Spyware</b>	Szpieguje użytkownika	Keylogger

## Lekcja

### Temat: Rodzaje szkodliwego oprogramowania szpiegującego

#### KLASYFIKACJA OPROGRAMOWANIA SZPIEGUJĄCEGO

Kategoria	Główny cel	Przykłady	Metoda działania
<b>Keyloggers</b>	Kradzież haseł i danych logowania	Snake, Advanced Keylogger	Rejestracja każdego uderzenia w klawiaturę
<b>Adware</b>	Wyświetlanie reklam, śledzenie aktywności	Gator, 180 Solutions	Niechciane pop-upy, przekierowania
<b>Banking</b>	Kradzież danych finansowych	BlankBot,	Nakładki na aplikacje bankowe,
<b>Trojany</b>		SpyNote	przechwytywanie transakcji
<b>System monitors</b>	Pełna inwigilacja użytkownika	Pegasus, Olimpic Vision	Nagrywanie ekranu, audio, wideo, lokalizacja GPS
<b>Browser hijackers</b>	Przejęcie kontroli nad przeglądarką	CoolWebSearch	Zmiana strony startowej, przekierowania wyszukiwania

<b>Stalkerware</b>	Cyberstalking, prześladowanie	FinSpy	Kompleksowa inwigilacja ofiary
<b>Tracking cookies</b>	Profilowanie behawioralne	-	Śledzenie nawyków zakupowych

## SZCZEGÓŁOWY OPIS I PRZYKŁADY

### 1. KEYLOGGERS (rejestratory klawiszy)

#### Jak działają:

Rejestrują każde uderzenie w klawiaturę, przechwytyując hasła, numery kart kredytowych i treść wiadomości. Wykorzystują niskopoziomowe hooki systemowe (np. SetWindowsHookEx z flagą WH\_KEYBOARD\_LL).

#### Przykład: Snake Keylogger

- **Cel:** Systemy Windows, przeglądarki Chrome, Edge, Firefox
- **Zasięg:** Ponad 280 milionów prób infekcji w 2025 roku
- **Mechanizm:**
  - Wykorzystuje AutoIt do ukrycia przed skanowaniem
  - Stosuje **process hollowing** – wstrzykuje kod do legalnych procesów (regsvcs.exe)
  - Eksfiltruje dane przez SMTP lub Telegram BOT (omija firewalle)
  - Utrzymuje się poprzez wpis w folderze startowym (ageless.vbs)
  - Pobiera geolokalizację ofiary z checkip.dyndns.org

Inne przykłady: Advanced Keylogger, Go Keyboard (fałszystwa klawiatura Android)

### 2. BANKING TROJANY / RAT (zdalny dostęp)

#### Jak działają:

Udają legalne aplikacje, a po instalacji przejmują kontrolę nad urządzeniem. Wykorzystują usługi dostępności (Accessibility Services) w Androidzie do automatyzacji kliknięć i przechwytywania ekranu.

#### Przykład: BlankBot

- **Odkryty:** Lipiec 2024, celuje głównie w Turcję
- **Zaawansowane techniki:**
  - **Własna wirtualna klawiatura** – przechwytuje naciśnięcia niezależnie od systemowej

- **Screen recording** – nagrywa ekran przez MediaProjection API (format MP4)
- **Custom injection** – tworzy nakładki imitujące ekrany logowania ING Banku z polami na dane kart i wzór blokady
- **HVNC** – zdalne sterowanie gestami (kliknięcia, swipe)
- **Omijanie zabezpieczeń** – na Android 13+ instaluje pakiety mimo Restricted Settings

### Przykład: SpyNote (Android RAT)

- **Mechanizm:**

- Dekrypcja payloadu AES z folderu assets
- **DEX Element Injection** – podmienia ClassLoader, by wykonać własny kod przed legalnym
- Komunikacja WebSocket z C2, zaciemnianie identyfikatorów (0 vs 0)
- Udaże legalne apki: Chrome, 8 Ball Pool, Block Blast, iHappy

## 3. SYSTEM MONITORS (monitory systemowe)

### Jak działają:

Kompleksowa inwigilacja – nagrywanie dźwięku, wideo, zrzuty ekranu, śledzenie GPS, logi połączeń.

### Przykład: Pegasus

**Pegasus** to zaawansowane oprogramowanie szpiegujące (spyware) stworzone przez izraelską firmę **NSO Group**. Był sprzedawany rządom jako narzędzie do walki z terroryzmem i przestępcością, ale według wielu śledztw był używany także przeciw dziennikarzom, opozycji i aktywistom.

- **Cel:** Dziennikarze, politycy (ataki celowane)

- **Mechanizm:**

- Zero-click installation – bez interakcji użytkownika
- Jailbreak iOS, dostęp do kamery, mikrofonu, iMessage, GPS
- Sprzedawany legalnym rządom, następnie nadużywany

**Inne:** Olimpic Vision, Zlob (rejestracja schowka, historia przeglądania)

Oprogramowanie ma dostęp praktycznie do wszystkiego, co robi użytkownik i co dzieje się w systemie.

Może obejmować:

### 1 Rejestrowanie klawiszy (keylogging)

- zapisywanie wpisywanych haseł
- przechwytywanie loginów
- zapisywanie wiadomości

## **2** Monitorowanie aplikacji

- jakie programy są uruchamiane
- jak długo są używane
- jakie strony internetowe są odwiedzane

## **3** Przechwytywanie danych systemowych

- lista plików
- historia przeglądarki
- zapisane hasła
- dane formularzy

## **4** Zrzuty ekranu i nagrywanie ekranu

- robienie screenshotów
- nagrywanie aktywności

## **5** Dostęp do sprzętu

- mikrofon (nagrywanie rozmów)
- kamera
- lokalizacja (GPS)

## **6** Wysyłanie danych do zewnętrznego serwera

- dane są przekazywane do atakującego (C&C – Command and Control)

## **Co potrafił Pegasus?**

### **1** Przejmował pełną kontrolę nad telefonem

Po zainfekowaniu urządzenia (iPhone lub Android) miał dostęp do:

- wiadomości SMS
- komunikatorów (WhatsApp, Signal, Messenger, iMessage)
- e-maily
- listy kontaktów
- kalendarza
- zdjęć i plików

## **2 Podsłuch i podgląd w czasie rzeczywistym**

- włączał **mikrofon** (nagrywanie rozmów)
- włączał **kamerę**
- rejestrował lokalizację GPS
- robił zrzuty ekranu

Użytkownik nie był o tym informowany.

## **3 Odczytywał zaszyfrowane wiadomości**

Nie łamał bezpośrednio szyfrowania – zamiast tego:

- przejmował dane **po odszyfrowaniu na urządzeniu**  
czyli czytał wiadomości tak, jak widział je użytkownik.

## **4 Ataki „zero-click”**

Jedna z najgroźniejszych cech:

- nie trzeba było kliknąć w link
- wystarczył np. specjalnie przygotowany iMessage
- infekcja mogła nastąpić bez wiedzy ofiary

## **5 Ukrywał swoją obecność**

- usuwał ślady z systemu
- działał w pamięci operacyjnej
- potrafił się sam dezaktywować

# **4. ADWARE I BROWSER HIJACKERS**

**Jak działają:**

Wyświetlają niechciane reklamy, modyfikują ustawienia przeglądarki. Często instalowane świadomie jako "darmowe narzędzia" z ukrytą klauzulą EULA.

**Przykład: CoolWebSearch**

- Zmieniał stronę startową i przekierowywał zapytania na serwery atakujących
- Wykorzystywał luki w Internet Explorer (ActiveX)

**Inne:** Gator, 180 Solutions – profilowanie behawioralne bez zgody

## 5. STALKERWARE

### Jak działają:

Oprogramowanie do prześladowania, instalowane fizycznie na urządzeniu ofiary przez osobę z bliskiego otoczenia.

### Przykład: FinSpy (FinFisher)

- Kompleksowy pakiet inwigilacyjny sprzedawany służbom
- Możliwości: kamera, mikrofon, zrzuty ekranu, keylogging
- Ironia: sam FinFisher padł ofiarą mega-wycieku danych

## 6. TRACKING COOKIES (pasywne śledzenie)

### Jak działają:

Nie instalują kodu – wykorzystują istniejącą funkcjonalność przeglądarek. Piksele śledzące w emailach informują nadawcę, kiedy otwarto wiadomość i z jakiego adresu IP.

## JAK ROZPOZNAĆ INFEKCIĘ?

Symptom	Typowy sprawca
Spowolnienie systemu, wysoki transfer	Keylogger, RAT
Dioda kamery świeci bez powodu	Stalkerware, Pegasus
Nowe paski narzędzi w przeglądarce	Browser hijacker
Autentykacja MFA przestaje działać	Banking trojan (przechwytuje 2FA)
Niewyjaśnione opłaty na karcie	BlankBot, SpyNote

## **PODSUMOWANIE – JAK SIĘ BRONIĆ?**

1. **Menadżer haseł** – automatyzuje logowanie, keylogger nie przechwyci wpisywanego hasła
2. **Tylko oficjalne sklepy** – Google Play, App Store (ale i tam bywają wpadki, jak Overseer)
3. **Ogranicz uprawnienia** – aplikacja do latarki nie potrzebuje dostępu do kontaktów
4. **Aktualizacje** – łatanie dziur zero-day
5. **Antywirus** – skanowanie behawioralne, nie tylko sygnaturowe
6. **Uwaga na maile** – nawet jeśli nadawca wygląda znajomo

## **Lekcja**

### **Temat: Rola administratora sieci**

#### **Rola administratora sieci**

Administrator sieci (ang. network administrator) to specjalista IT odpowiedzialny za zarządzanie, utrzymanie i optymalizację sieci komputerowych w organizacji. Obejmuje to sieci lokalne (LAN), szerokopasmowe (WAN), serwery oraz połączenia z internetem. Jego praca zapewnia płynne funkcjonowanie infrastruktury IT, co jest kluczowe dla codziennych operacji firmy, instytucji czy szkoły.

#### **Główne zadania administratora sieci**

Zadania mogą się różnić w zależności od wielkości organizacji, ale zazwyczaj obejmują:

- **Konfiguracja i instalacja:** Projektowanie, instalowanie i konfigurowanie sprzętu sieciowego (routery, switche, firewalle) oraz oprogramowania. Obejmuje to ustawianie systemów operacyjnych, serwerów i połączeń.

#### **Przykładowe urządzenia, którymi zarządza:**

- Routery - kierują ruchem między sieciami
- Switch'e - łączą urządzenia w sieci lokalnej
- Firewalle - zabezpieczają sieć przed nieautoryzowanym dostępem
- Access point'y - zapewniają dostęp do WiFi
- Serwery - hostują usługi sieciowe

- **Utrzymanie i monitorowanie:** Codzienne monitorowanie wydajności sieci, wykrywanie problemów (np. wąskich gardeł), troubleshooting (rozwiązywanie awarii) i naprawy. Zapewnia to minimalny czas przestoju.

#### Typowe problemy do rozwiązania:

- "Nie mam internetu"
- "Drukarka nie drukuje"
- "Strona działa bardzo wolno"
- "Nie mogę połączyć się z serwerem"

- **Bezpieczeństwo:** Wdrażanie środków ochronnych, takich jak firewalle, antywirusy, audyty bezpieczeństwa i zarządzanie uprawnieniami dostępu. Chroni przed cyberatakami, wyciekami danych i nieautoryzowanym dostępem.
- **Aktualizacje i optymalizacja:** Aktualizowanie oprogramowania, hardware'u i systemów, aby poprawić prędkość, efektywność i skalowalność sieci. Obejmuje też planowanie rozbudowy sieci.
- **Wsparcie użytkowników:** Pomoc użytkownikom w rozwiązywaniu problemów z połączeniem, szkolenie personelu z obsługi sieci oraz zarządzanie kontami i uprawnieniami.
- **Backup i odzyskiwanie danych:** Tworzenie kopii zapasowych danych, zarządzanie chmurą obliczeniową i procedury odzyskiwania po awariach.
- **Analiza i raportowanie:** Ocena efektywności sieci, przygotowywanie budżetów na ulepszenia oraz raporty dla zarządzania.

W mniejszych firmach rolą może się pokrywać z administratorem systemów (system administrator), co obejmuje też zarządzanie stacjami roboczymi i oprogramowaniem.

Administrator sieci pomaga w zapewnieniu ciągłości działania organizacji poprzez:

- **Efektywność operacyjna:** Utrzymuje połączenia, co pozwala pracownikom na bezproblemową komunikację, dostęp do zasobów i pracę zdalną. Bez tego firma mogłaby stracić godziny lub dni na awarie.
- **Bezpieczeństwo danych:** Chroni przed zagrożeniami, minimalizując ryzyko utraty danych, co jest kluczowe w erze cyberataków i regulacji jak GDPR.
- **Oszczędności:** Optymalizuje zasoby, redukując koszty poprzez zapobieganie awariom i efektywne wykorzystanie bandwidthu.
- **Wsparcie biznesowe:** Umożliwia skalowanie firmy (np. dodawanie nowych urządzeń), integrację z chmurą i szybką adaptację do zmian technologicznych, jak IoT czy 5G.
- **Innowacje:** Pomaga we wdrażaniu nowych technologii, co wspiera rozwój firmy, np. w e-commerce czy zdalnej współpracy.

Podsumowując, administrator sieci to "strażnik" infrastruktury IT – bez niego sieć mogłaby być niestabilna, niebezpieczna i nieefektywna. Wymaga wiedzy z zakresu sieci, bezpieczeństwa i systemów operacyjnych, często certyfikatów jak CCNA czy CompTIA Network+.

## **Umiejętności potrzebne administratorowi sieci**

### **Techniczne:**

- Znajomość protokołów sieciowych (TCP/IP, DNS, DHCP, HTTP)
- Umiejętność konfiguracji sprzętu Cisco, MikroTik, Ubiquiti
- Znajomość systemów Windows Server i Linux
- Podstawy programowania (Python, Bash) do automatyzacji
- Znajomość zagadnień bezpieczeństwa