PODSTAWY CYBERBEZPIECZEŃSTWA SYSTEMÓW IT

ANALIZA CELÓW I SKUTKÓW ATAKÓW SIECIOWYCH

Włamania, ataki DoS i DDoS

Materiał teoretyczny dla uczniów technikum

Trzy lekcje po 45 minut • Poziom wprowadzający • Bez instrukcji przeprowadzania ataków

PYTANIE NA POCZĄTEK

Wyobraź sobie, że logujesz się do dziennika elektronicznego, a strona nie odpowiada. Czy ktoś ukradł hasła? Czy serwer został zaatakowany? A może po prostu jednocześnie weszło na niego zbyt wielu uczniów? W cyberbezpieczeństwie **objaw nie jest tym samym co przyczyna**.

Czego nauczysz się po przeczytaniu materiału?

- Odróżniać **atak, włamanie, incydent** i zwykłą awarię usługi.
- Wyjaśniać cele sprawców i przewidywać skutki incydentów dla użytkowników oraz organizacji.
- Opisywać **DoS i DDoS** oraz podstawowe sposoby zakłócania działania usług.
- Interpretować proste dane o ruchu i wskazywać działania obronne.
- Rozumieć, dlaczego analiza dowodów wymaga ostrożności, a testy tylko uprawnienia.

Plan nauki

LEKCJA 1 • 45 MIN	LEKCJA 2 • 45 MIN	LEKCJA 3 • 45 MIN
Cele sprawców, triada CIA, włamania i incydenty.	Jak działa DoS/DDoS, rodzaje przeciążenia i objawy.	Obrona, analiza logów, reakcja i studia przypadków.

Opracowanie dydaktyczne na podstawie literatury naukowej, standardów technicznych i raportów instytucji cyberbezpieczeństwa. Stan źródeł: 18.10.2026.

LEKCJA 1 / ZAGROŻENIA I MOTYWACJE

1. Dlaczego dochodzi do ataków sieciowych?

Współczesna szkoła, sklep internetowy, bank i szpital korzystają z systemów informatycznych do codziennych zadań. System jest wartościowy nie tylko ze względu na przechowywane dane, ale także dlatego, że **musi działać w odpowiednim czasie**. Nawet kilkunastominutowa niedostępność może opóźnić pracę wielu osób. Właśnie dlatego cyberbezpieczeństwo dotyczy zarówno ochrony informacji, jak i ciągłości działania usług. [5, 10]

1.1. Trzy filary bezpieczeństwa informacji – CIA

W literaturze i standardach bezpieczeństwa wyróżnia się trzy podstawowe cele: poufność (confidentiality), integralność (integrity) i dostępność (availability). Razem tworzą **triadę CIA**. Każdy z tych celów odpowiada na inne pytanie. [10]



Rysunek 1. Triada CIA – trzy różne wymiary bezpieczeństwa informacji.

Poufność: Czy informacja trafia wyłącznie do uprawnionych osób? Przykładem naruszenia jest ujawnienie danych osobowych uczniów. **Integralność:** Czy dane pozostają poprawne i niezmienione bez zgody właściciela? Przykładem jest nieuprawniona zmiana ocen. **Dostępność:** Czy uczeń lub nauczyciel może skorzystać z usługi wtedy, gdy jej potrzebuje? Atak DoS godzi przede wszystkim w tę trzecią właściwość.

WAŻNE ROZRÓŻNIENIE

Nie każda niedostępność jest atakiem, a nie każdy atak prowadzi do wycieku danych. Jedno zdarzenie może jednak naruszać kilka elementów triady CIA jednocześnie.

1.2. Atak, podatność, włamanie i incydent

Podatność to słabość systemu, konfiguracji lub procedury, którą można wykorzystać. **Atak** jest próbą zaszkodzenia systemowi, uzyskania nieuprawnionych korzyści albo zakłócenia jego działania. **Włamanie** w języku potocznym oznacza uzyskanie nieuprawnionego dostępu; nie jest synonimem każdego cyberataku. **Incydent bezpieczeństwa** to zdarzenie, które rzeczywiście lub potencjalnie narusza bezpieczeństwo i wymaga zbadania. [5, 6]

Przykładowo ktoś może próbować zgadnąć hasło do konta (próba ataku), ale nie uzyskać dostępu. Ktoś inny może wejść na konto za pomocą wykradzionego hasła (nieuprawniony dostęp). Natomiast wysycenie zasobów serwera może uniemożliwić korzystanie ze strony **bez odczytania ani jednej prywatnej wiadomości**.

1.3. Dlaczego sprawcy podejmują ataki?

Motywacji nie można wiarygodnie ustalić wyłącznie na podstawie objawów. Zdarzenia mogą wynikać z chęci uzyskania pieniędzy, kradzieży informacji, sabotażu, manifestacji ideologicznej, zdobycia rozgłosu lub ukrycia innej operacji. Badania nad DDoS oraz klasyfikacja MITRE opisują między innymi wymuszenia, działania o charakterze politycznym i odwracanie uwagi obrońców. [1, 2, 7, 8]

Motywacja	Przykładowy skutek dla ofiary
Korzyść finansowa	Przestój sklepu w kluczowym momencie sprzedaży; presja na zapłatę za przerwanie zakłóceń.
Kradzież informacji	Nieuprawnione ujawnienie danych klientów lub dokumentów firmy.
Sabotaż lub presja	Przerwa w działaniu strony, systemu rezerwacji albo platformy do nauki.
Odwrócenie uwagi	Zespół IT skupia się na niedostępności usług i może przeoczyć inne oznaki incydentu.

Oznacza to, że obrońca bada przede wszystkim **fakty i skutki**: co przestało działać, kiedy, dla kogo i jakie są dowody. Dopiero później może formułować hipotezy o sprawcy i jego celu.

1.4. Czym różni się włamanie od zakłócania dostępności?

Włamanie najczęściej dotyczy przekroczenia granicy uprawnień: ktoś uzyskuje dostęp do konta, systemu lub danych, do których nie powinien mieć dostępu. Może to prowadzić do odczytu poufnych informacji, zmiany konfiguracji lub utrwalenia obecności w systemie. Z kolei celem ataku DoS jest przede wszystkim uniemożliwienie lub utrudnienie normalnej pracy usługi. [7, 8]

Te zdarzenia mogą się łączyć. Przejęte wcześniej komputery mogą stać się częścią botnetu uczestniczącego w DDoS. W innej sytuacji DoS może służyć odciągnięciu uwagi od kradzieży danych. Nie oznacza to jednak, że każde zakłócenie działania serwera jest dowodem włamania.

HISTORIA Z ŻYCIA SZKOŁY

Dziennik elektroniczny działa bardzo wolno podczas wystawiania ocen. Użytkownicy mówią: „ktoś nas zaatakował”. Administrator powinien najpierw sprawdzić dane o obciążeniu, awariach i błędach aplikacji. **Nagły wzrost prawidłowych logowań** może mieć podobne objawy jak celowo wywołane przeciążenie.

1.5. Włamania – ogólny przebieg incydentu

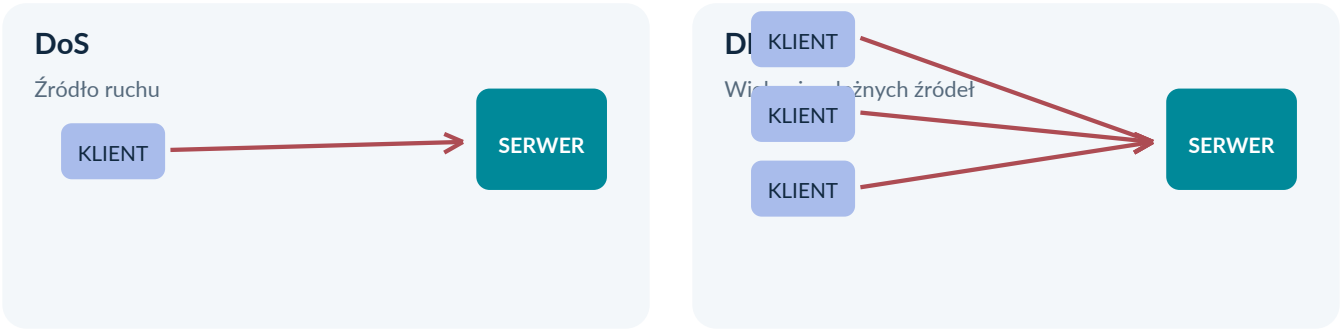
Z punktu widzenia analityka śledczego istotna jest rekonstrukcja kolejnych etapów zdarzenia. Nie jest to instrukcja dla sprawcy, lecz sposób porządkowania dowodów. Przykładowy incydent może obejmować: rozpoznanie otoczenia, znalezienie słabości, próbę dostępu, uzyskanie uprawnień, działania wewnątrz systemu i pozostawione ślady. Nie wszystkie incydenty przebiegają jednak według jednego schematu.

Ślady mogą znajdować się w dziennikach logowań, historii zmian kont, konfiguracji usług, zdarzeniach systemowych i informacjach sieciowych. Warto pamiętać, że pojedynczy adres IP zwykle nie wystarcza do pewnego ustalenia sprawcy: adres może być współdzielony, przekierowany lub należeć do urządzenia przejętego przez kogoś innego. [5, 6]

LEKCJA 2 / MECHANIZMY ZAKŁÓCENIA USŁUGI

2. Jak działają ataki DoS i DDoS?

DoS (Denial of Service) oznacza odmowę usługi: celowe działanie, które utrudnia lub uniemożliwia uprawnionym użytkownikom korzystanie z zasobu cyfrowego. **DDoS (Distributed Denial of Service)** jest odmianą rozproszoną, w której w zakłócaniu uczestniczy wiele źródeł ruchu lub wiele urządzeń. Sam fakt, że komputer nie działa, nie przesądza o DoS. [1, 2, 3]



Rysunek 2. Różnica pojęciowa: jedno źródło ataku (DoS) i wiele źródeł (DDoS). Rysunek jest uproszczony.

Najważniejsze jest nie to, ile „stron" zobaczy użytkownik, lecz **jaki ograniczony zasób staje się wąskim gardłem**. Może to być przepustowość łącza, pamięć przeznaczona na obsługę połączeń, liczba procesów serwera albo czas potrzebny na przygotowanie odpowiedzi aplikacji. [3, 7, 8]

2.1. Dlaczego serwer może przestać odpowiadać?

Wyobraź sobie szkolny sekretariat z jednym stanowiskiem obsługi. Przy kilku interesantach kolejka posuwa się sprawnie. Kiedy liczba osób przychodzących w każdej minucie stale przewyższa liczbę obsługiwanych, kolejka zaczyna rosnąć. Ostatecznie niektórzy odchodzą bez załatwienia sprawy. Serwer zachowuje się podobnie, choć rzeczywiste aplikacje mają wiele współpracujących mechanizmów obsługi zapytań.

W sieci można obserwować np. **opóźnienie odpowiedzi**, **udział nieudanych żądań** i **stopień wykorzystania zasobów**. Wzrost jednego z tych wskaźników nie musi oznaczać ataku; wskazuje jedynie, że trzeba zbadać problem.

PRZYKŁAD LICZBOWY – TYLKO MODEL DYDAKTYCZNY

Przyjmijmy, że laboratorium może obsłużyć maksymalnie 100 zapytań na minutę. Jeżeli regularnie napływa 140 zapytań na minutę, zaległości będą rosły, o ile system nie ograniczy ruchu lub nie zwiększy wydajności. **To ilustracja zależności, a nie rzeczywisty parametr konkretnego serwera.**

2.2. Trzy podstawowe grupy mechanizmów

Specjaliści rozróżniają zakłócenia na poziomie sieci, protokołów obsługujących komunikację oraz samej aplikacji. W praktyce te kategorie mogą się nakładać. Klasyfikacja MITRE ATT&CK oddziela przeciążenie sieci (T1498) od wyczerpywania zasobów usługi lub urządzenia (T1499). [7, 8]

Rodzaj	Na co oddziałuje	Jak widzi to użytkownik
Przeciążenie łącza np. ruch UDP	Ograniczona przepustowość połączenia i urządzeń sieciowych.	Usługa jest trudno osiągalna, mogą wystąpić duże opóźnienia.

Rodzaj	Na co oddziałuje	Jak widzi to użytkownik
Wyczerpywanie stanu połączeń np. SYN flood	Zasoby związane z obsługą nowych połączeń TCP.	Nowe połączenia nie powstają albo trwają bardzo długo.
Przeciążenie aplikacji np. HTTP flood	Praca aplikacji, serwera WWW lub systemów zaplecza.	Strona ładuje się wolno lub zwraca błędy.

Ruch wolumetryczny – kiedy problemem jest przepustowość

Sieć ma ograniczoną zdolność przesyłania danych. Jeżeli natężenie ruchu przewyższa możliwości danego odcinka, część pakietów może być opóźniana albo odrzucana. Ruch zakłócający może korzystać z różnych protokołów, w tym UDP. Duża liczba pakietów może nadmiernie obciążać urządzenia sieciowe, nawet jeśli sama aplikacja internetowa nie zużywa dużo procesora. [3, 7]

SYN flood – gdy obciążany jest mechanizm nawiązywania połączenia

W typowym połączeniu TCP strony wymieniają komunikaty potrzebne do rozpoczęcia komunikacji. Serwer musi obsługiwać wiele prób połączeń jednocześnie. Atak określany jako SYN flood nadużywa tego procesu, aby wyczerpywać zasoby przeznaczone dla nowych połączeń. Jedną z opisanych w literaturze metod ograniczania takiego problemu są **SYN cookies**. Szczegółowy opis i ograniczenia mechanizmów obronnych przedstawia RFC 4987. [4]

HTTP flood – gdy obciążana jest aplikacja

Przeglądarka wysyła żądania HTTP, kiedy użytkownik odwiedza witrynę. Ich obsługa może wymagać odczytu plików, wykonania programu lub zapytania do bazy danych. Jeżeli aplikacja otrzymuje zbyt wiele kosztownych operacji, czas odpowiedzi może rosnąć. Nie każdy taki przypadek powoduje przeciążenie samego łącza internetowego: wąskim gardłem może być np. baza danych lub liczba procesów obsługujących aplikację. [2, 8]

2.3. Czym jest botnet?

Botnet to grupa urządzeń, którymi ktoś może sterować zdalnie, często bez wiedzy ich właścicieli. W jego skład mogą wchodzić nie tylko komputery, lecz także źle zabezpieczone urządzenia sieciowe lub urządzenia Internetu Rzeczy (IoT). Jeśli wiele takich urządzeń jednocześnie generuje niepożądany ruch, rozproszenie utrudnia obronę. [1, 2]

Ważny wniosek: osoba, której adres IP pojawia się w zapisach ruchu, może być również **ofiarą przejęcia swojego urządzenia**. Adres źródłowy ruchu i tożsamość faktycznego sprawcy nie są tym samym.

2.4. Czy każdy nagły wzrost ruchu jest atakiem?

Nie. **Flash crowd** to sytuacja, w której duża liczba prawdziwych użytkowników pojawia się w krótkim czasie, np. przy publikacji wyników egzaminów. Dla administratora taki wzrost może wyglądać podobnie do przeciążenia wywołanego przez sprawcę. Sama liczba żądań nie odpowiada na pytanie o intencję i źródło problemu. [2, 3]

Przesłanka	Legalne duże zainteresowanie	Podejrzenie DoS/DDoS
Kontekst czasu	Znane wydarzenie: ogłoszenie wyników, ważna publikacja.	Nagły wzrost bez oczywistego wydarzenia.

Przesłanka	Legalne duże zainteresowanie	Podejrzenie DoS/DDoS
Wzorce korzystania	Użytkownicy wykonują zróżnicowane, sensowne operacje.	Nietypowe powtarzalne wzorce, anomalie sesji.
Wskaźniki	Możliwy wzrost opóźnień oraz błędów.	Również możliwy wzrost opóźnień oraz błędów.
Wniosek	Wymaga porównania z normalnym ruchem.	Wymaga weryfikacji, nie automatycznego wyroku.

PUŁAPKA INTERPRETACJI

Wysoki ruch, komunikat „503 Service Unavailable" lub bardzo wolna strona **nie dowodzą samodzielnie** DoS. Potrzebujemy kontekstu, historii ruchu i danych z kilku warstw infrastruktury.

2.5. Jakie szkody może spowodować niedostępność?

Skutki są zależne od roli usługi. Sklep internetowy może nie przyjmować zamówień. Szkoła może czasowo utracić dostęp do materiałów. Placówka medyczna może mieć problemy z dostępnością niektórych systemów obsługi pacjentów. Koszty nie ograniczają się do utraconej sprzedaży: organizacja musi poświęcić czas zespołu technicznego, powiadomić użytkowników i odbudować zaufanie. [2, 9]

Atak o krótkim czasie trwania może być bardzo uciążliwy w krytycznym momencie – np. w trakcie rejestracji na egzamin. Z drugiej strony czas trwania zdarzenia nie pozwala samodzielnie wnioskować o rozmiarach szkód; trzeba znać kontekst działalności.

2.6. Co mówią współczesne raporty?

Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) w raporcie *Threat Landscape 2026*, obejmującym zdarzenia analizowane za 2025 rok, zwraca uwagę m.in. na związane z hacktywizmem kampanie DDoS wobec ważnych podmiotów oraz wpływ zależności cyfrowych na odporność organizacji. Nie oznacza to, że każda awaria jest skutkiem takiej kampanii; raport służy do rozumienia skali i charakteru zagrożeń w Europie. [9]

PYTANIA DO ROZMOWY

- Dlaczego liczba źródeł odróżnia DDoS od typowego DoS?
- Co może wyczerpać się podczas ataku: łącze, pamięć połączeń czy zasoby aplikacji?
- Jakie dane sprawdzisz, by nie pomylić wzrostu zainteresowania wynikami egzaminu z atakiem?

LEKCJA 3 / OBRONA I REAKCJA NA INCYDENT

3. Jak rozpoznaje się i ogranicza skutki ataków?

Bezpieczeństwo to nie tylko „mocny firewall”. W praktyce potrzebne są przygotowanie, obserwowanie stanu usług, właściwe decyzje w trakcie incydentu i analiza po jego zakończeniu. NIST SP 800-61 Rev. 3 (2025) podkreśla powiązanie reakcji na incydenty z całym zarządzaniem ryzykiem organizacji. [5]

3.1. Co widać w logach i monitoringu?

Administrator nie obserwuje bezpośrednio „hakera”, lecz ślady techniczne. W logach WWW można znaleźć czas żądania, odpowiedź serwera, ścieżkę zasobu oraz – zależnie od konfiguracji – informację o źródle. Monitoring może pokazywać liczbę żądań na sekundę, liczbę błędów, opóźnienia, obciążenie procesora i transfer sieciowy. [6]

Sygnał	Co może oznaczać	Dlaczego nie wystarcza?
Bardzo wiele żądań	Nagły wzrost obciążenia aplikacji.	Może wynikać z popularności usługi.
Błędy HTTP 429 / 503	Ograniczanie żądań lub niedostępność usługi.	Może wynikać z konfiguracji lub awarii.
Wzrost opóźnień	Zatory w sieci lub aplikacji.	Mógł pojawić się problem z bazą danych.
Wiele nieudanych połączeń	Problem na warstwie transportowej lub w sieci.	Możliwa awaria albo błędna konfiguracja.
Wiele źródeł ruchu	Wzorzec rozproszony.	Również legalni klienci są rozproszeni.

Kod **429** często oznacza, że serwer ogranicza liczbę żądań. Kod **503** zwykle sygnalizuje tymczasową niedostępność usługi. Interpretacja zawsze zależy od konfiguracji serwera, bramki, proxy i aplikacji. Błędy HTTP nie są etykietą „potwierdzony atak”.

3.2. Zabezpieczenia i ich ograniczenia

W obronie przed przeciążeniem stosuje się wiele mechanizmów. Nie zastępują one aktualizacji oprogramowania, kontroli dostępu i przygotowanego planu reagowania. Badania pokazują, że skuteczna ochrona wymaga dobrania metody do **rodzaju zagrożenia i miejsca powstawania wąskiego gardła**. [1, 2, 3]

Mechanizm	Do czego służy	Na co uważać
Rate limiting	Ogranicza liczbę żądań do usługi w określonym czasie.	Może przypadkowo ograniczyć także legalnych użytkowników.
WAF	Analizuje ruch do aplikacji WWW na podstawie reguł.	Nie jest ochroną przed każdą formą przeciążenia łącza.
CDN / caching	Rozprasza obsługę wybranych zasobów i zmniejsza obciążenie serwera.	Nie każda odpowiedź może być bezpiecznie buforowana.
SYN cookies	Pomagają ograniczać zużycie stanu połączeń TCP.	Nie rozwiązują problemów wszystkich warstw.

Mechanizm	Do czego służy	Na co uważać
Filtracja u operatora	Może ograniczać duży ruch, zanim dotrze do wąskiego łącza.	Wymaga współpracy infrastruktury i reguł filtracji.
Monitoring + plan	Umożliwiają szybką identyfikację i sprawne decyzje.	Alarm bez kontekstu może prowadzić do błędnych działań.

3.3. Pięć kroków rozumnej reakcji



Rysunek 3. Uproszczony cykl postępowania w ćwiczeniu szkolnym, spójny z zasadami NIST.

Zauważ: system zgłasza wzrost opóźnień lub brak dostępu. **Sprawdź:** zespół porównuje logi, wykresy oraz informacje o planowanym ruchu. **Ogranicz:** uruchamia odpowiednie mechanizmy ochrony, ostrożnie obserwując wpływ na prawdziwych użytkowników. **Przywróć:** potwierdza, że usługa odpowiada i klienci mogą z niej korzystać. **Wyciągnij wnioski:** dokumentuje przebieg, ustala możliwe przyczyny oraz zmienia plan ochrony. [5, 6]

Do dobrych praktyk należy zachowanie danych potrzebnych do rekonstrukcji zdarzenia. Analiza powinna respektować prywatność użytkowników, uprawnienia zespołu i przepisy dotyczące przetwarzania danych. Nie należy udostępniać uczniom produkcyjnych logów zawierających prawdziwe dane osobowe.

3.4. Analiza incydentu – nie wyciągaj pochopnych wniosków

W informatyce śledczej ważne jest oddzielenie **obserwacji** od **hipotezy**. Obserwacja: „od 10:15 do 10:25 liczba żądań wyraźnie wzrosła”. Hipoteza: „możliwe, że ktoś próbował przeciążyć usługę”. Wniosek można formułować dopiero po zestawieniu wielu danych. Atrybucja, czyli przypisanie zdarzenia konkretnemu sprawcy, wymaga osobnego procesu dowodowego i nie wynika z jednego wpisu w logu.

ETYKA I GRANICE ĆWICZEŃ

Próba przeciążenia publicznie dostępnej strony może zaszkodzić prawdziwym użytkownikom, nawet jeśli uczeń twierdzi, że robi to „dla nauki”. Ćwiczenia wykonuje się **wyłącznie w środowisku, do którego ma się wyraźne upoważnienie**, z kontrolą obciążenia i możliwością natychmiastowego przerwania testu.

3.5. Trzy krótkie studia przypadku

Przypadek A – e-dziennik w dniu wystawiania ocen

O 16:00 rośnie liczba logowań, a czas odpowiedzi zwiększa się kilkukrotnie. Użytkownicy widzą błędy, ale w tym samym czasie nauczyciele masowo wprowadzają oceny. **Wstępna interpretacja:** możliwe przeciążenie legalnym ruchem. **Do sprawdzenia:** harmonogram, liczba unikatowych sesji, rozkład operacji, stan bazy danych. **Wniosek:** na obecnym etapie brak podstaw, aby potwierdzić DoS.

Przypadek B – sklep internetowy i gwałtowne wzrosty ruchu

Sklep nie prowadzi promocji, a monitoring wskazuje nienaturalny wzrost liczby zapytań i błędów. Ochrona zaczyna blokować część ruchu. **Wstępna interpretacja:** podejrzenie przeciążenia aplikacji, wymagające analizy. **Do sprawdzenia:** logi bramy, metryki aplikacji i ich korelacja w czasie. **Cel obrony:** utrzymać dostęp dla klientów i ograniczyć fałszywe blokady.

Przypadek C – szkoła widzi podejrzane logowania i przerwę w działaniu

Administrator dostrzega zarówno serie nieudanych logowań, jak i krótką niedostępność strony. **Ważne:** dwa objawy nie dowodzą wspólnego sprawcy. Zespół rozdziela analizy: osobno ocenia próby uzyskania dostępu, osobno bada dostępność usługi. Sprawdza, czy wystąpiła nieuprawniona sesja oraz jakie systemy były dotknięte. Dopiero po zebraniu dowodów można połączyć zdarzenia w jeden incydent.

3.6. Zastosowanie: interpretacja mini-raportu SOC

Poniższe dane są **fikcyjne** i służą ćwiczeniu analitycznemu, a nie opisowi realnego incydentu.

Godzina	Żądania/min	Śr. czas odpowiedzi	Błędy 5xx
09:55	80	120 ms	0%
10:00	105	150 ms	1%
10:05	180	600 ms	8%
10:10	260	1 700 ms	28%
10:15	110	210 ms	2%

Odpowiedz: co zmieniło się między 10:00 a 10:10? Jakie dodatkowe informacje pozwoliłyby odróżnić normalny wzrost ruchu od ataku? Dlaczego nie wolno automatycznie uznawać każdego żądania z tego okresu za złośliwe?

POWTÓRZENIE / ZAPAMIĘTAJ

4. Najważniejsze wnioski

- **Cyberbezpieczeństwo** obejmuje poufność, integralność i dostępność danych oraz usług.
- **Włamanie** wiąże się z nieuprawnionym dostępem; **DoS** z naruszeniem dostępności. To różne zjawiska, które mogą współwystępować.
- **DDoS** jest rozproszoną formą odmowy usługi, w której uczestniczy wiele źródeł ruchu.
- Atak może przeciążać **łącze, mechanizm połączeń TCP lub aplikację**; sposoby obrony zależą od wąskiego gardła.
- **Duży ruch ≠ dowód ataku**; prawdziwa popularność usługi też może doprowadzić do przeciążenia.
- Analiza incydentu wymaga **monitoringu, kontekstu, ostrożności w ocenach i zachowania dowodów**.
- Najlepsza obrona łączy **przygotowanie, wykrywanie, ograniczanie skutków i doskonalenie** zabezpieczeń.

Słowniczek

Termin	Znaczenie w jednym zdaniu
CIA	Poufność, integralność i dostępność informacji.
DoS	Celowe zakłócenie dostępności usługi.
DDoS	Rozproszony DoS, angażujący wiele źródeł ruchu.
Botnet	Grupa zdalnie sterowanych urządzeń, często przejętych.
HTTP	Protokół używany m.in. do komunikacji przeglądarki z serwerem WWW.
TCP	Protokół transportowy zapewniający m.in. nawiązywanie połączenia.
SYN flood	Przeciążanie zasobów związanych z tworzeniem połączeń TCP.
WAF	Zapora analizująca ruch kierowany do aplikacji WWW.
CDN	Sieć rozproszonych serwerów przyspieszających dostęp do treści.
Rate limiting	Ograniczenie natężenia żądań do usługi.
Log	Zapis zdarzeń systemu lub aplikacji.
SOC	Zespół/centrum obserwujące i analizujące zdarzenia bezpieczeństwa.

Pytania sprawdzające – do odpowiedzi własnymi słowami

1. Wyjaśnij różnicę między atakiem DoS a DDoS.

2. Dlaczego wyciek haseł i zablokowanie strony dotyczą różnych elementów triady CIA?

3. Podaj dwa możliwe cele sprawcy ataku na firmę.

4. Wymień trzy miejsca, w których może wystąpić przeciążenie.

5. Co oznacza botnet i dlaczego komplikuje analizę źródeł ruchu?

6. Dlaczego błąd HTTP 503 sam w sobie nie potwierdza cyberataku?

7. Jakie co najmniej trzy dane powinien zebrać analityk, zanim opisze incydent?

8. W jaki sposób rate limiting może pomóc, a w jakiej sytuacji może zaszkodzić?

9. Dlaczego adres IP nie jest automatycznie tożsamością sprawcy?

10. Jakie czynności należy wykonać po przywróceniu dostępności strony?

ZADANIE NA KONIEC

Wybierz jedną usługę: e-dziennik, sklep internetowy, system umawiania wizyt lub stronę szkoły. Opisz **jeden możliwy cel ataku, trzy skutki niedostępności, dwa sygnały w monitoringu i dwie metody obrony**. Wyjaśnij, jak sprawdzić, czy przyczyną nie jest legalne przeciążenie.

BIBLIOGRAFIA / WIARYGODNE ŹRÓDŁA

5. Literatura i źródła

Materiał jest **autorskim opracowaniem dydaktycznym**. Numery w nawiasach kwadratowych w tekście wskazują źródła, które wspierają przedstawione wyjaśnienia. Dwie pierwsze pozycje to recenzowane publikacje naukowe; pozostałe to standardy, dokumenty techniczne, bazy wiedzy i raporty.

Publikacje naukowe

[1] Mirković J., Reiher P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39–53.
doi.org/10.1145/997150.997156

[2] Zargar S. T., Joshi J. B. D., Tipper D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*, 15(4), 2046–2069.
doi.org/10.1109/SURV.2013.031413.00127

Standardy, dokumenty instytucjonalne i raporty

[3] Handley M. i in. (2006). RFC 4732: *Internet Denial-of-Service Considerations*. Internet Engineering Task Force.
rfc-editor.org/rfc/rfc4732

[4] Eddy W. (2007). RFC 4987: *TCP SYN Flooding Attacks and Common Mitigations*. Internet Engineering Task Force.
rfc-editor.org/rfc/rfc4987

[5] Nelson A., Rekhi S., Scarfone K., Souppaya M. (2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*. NIST SP 800-61 Rev. 3.
doi.org/10.6028/NIST.SP.800-61r3

[6] Scarfone K., Mell P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST SP 800-94.
doi.org/10.6028/NIST.SP.800-94

[7] MITRE ATT&CK. *Network Denial of Service*, T1498, baza wiedzy o technikach ataków.
attack.mitre.org/techniques/T1498

[8] MITRE ATT&CK. *Endpoint Denial of Service*, T1499, baza wiedzy o technikach ataków.
attack.mitre.org/techniques/T1499

[9] European Union Agency for Cybersecurity (2026). *ENISA Threat Landscape 2026* (opublikowano 22.09.2026; analiza danych za 2025 r.).
enisa.europa.eu / Threat Landscape 2026

[10] National Institute of Standards and Technology (2004). *Standards for Security Categorization of Federal Information and Information Systems*. FIPS 199.
nvlpubs.nist.gov / FIPS 199

JAK KORZYSTAĆ ZE ŹRÓDEŁ?

Artykuły [1] i [2] opisują podstawy i klasyfikację DoS/DDoS, ale ze względu na daty publikacji nie należy traktować ich jako katalogu najnowszych zagrożeń. Dokumenty MITRE i raport ENISA uzupełniają obraz o współczesne techniki i kontekst. W razie rozbieżności sprawdź datę i zakres danego dokumentu.

Materiał przeznaczony do edukacji obronnej. Diagramy, przykłady i dane z tabeli SOC są ilustracjami dydaktycznymi. Nie są one zapisem konkretnego cyberataku.