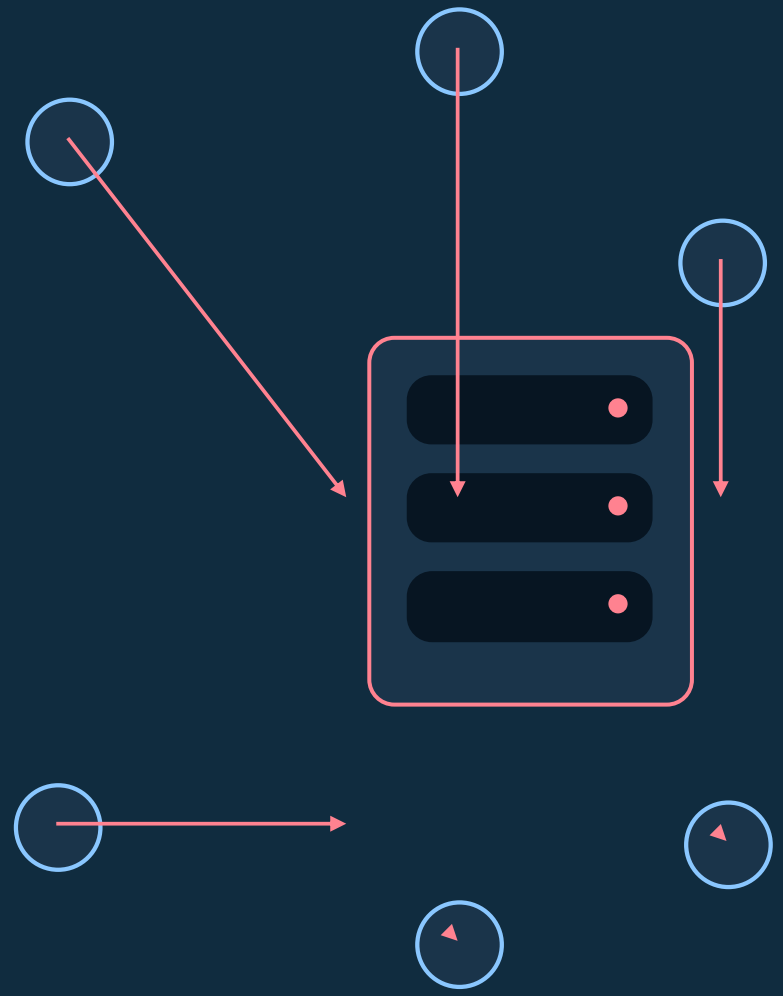
CYBERBEZPIECZEŃSTWO • KLASA 1TC

ATAKI

DoS / DDoS

Jak zatrzymać usługę?
Jak ją ochronić?



BOTNETY • DETEKCJA • OBRONA

E-dziennik nie odpowiada

Uczniowie widzą komunikat „Serwer niedostępny”.

AWARIA

Problem z serwerem lub aplikacją.

DUŻY RUCH

Wiele osób loguje się w tym samym czasie.

ATAK

Ktoś celowo przeciąża usługę.

Sam błąd 503 NIE oznacza automatycznie DDoS.

Klient, serwer i usługa

Zanim poznamy ataki, zobaczmy, jak działa zwykła strona.

KLIENT

Twoja przeglądarka, np. w telefonie ucznia.

SERWER

Komputer, który obsługuje stronę WWW.

USŁUGA

To, z czego korzystasz, np. e-dziennik.

DoS i DDoS utrudniają korzystanie z USŁUGI.

Czego nauczysz się dzisiaj?

Po zajęciach będziesz potrafić:

01	**WYJAŚNIĆ**	DoS, DDoS, botnet i zombie.
02	**ROZPOZNAĆ**	Objawy przeciążenia i typy ataków.
03	**ZAREAGOWAĆ**	Wskazać właściwe działania obronne.

Triada CIA: co atakuje DoS?

Głównym celem jest naruszenie DOSTĘPNOŚCI.

C

POUFNOŚĆ

Kto odczytuje dane?

I

INTEGRALNOŚĆ

Czy dane są poprawne?

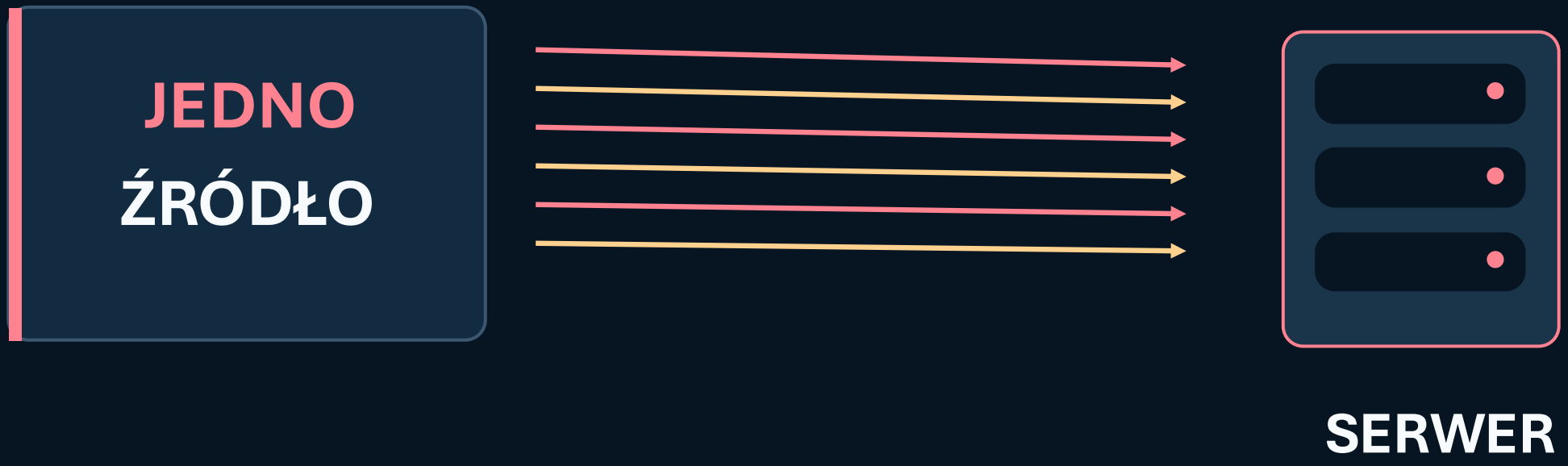
A

DOSTĘPNOŚĆ

Czy usługa działa?

DoS = odmowa usługi

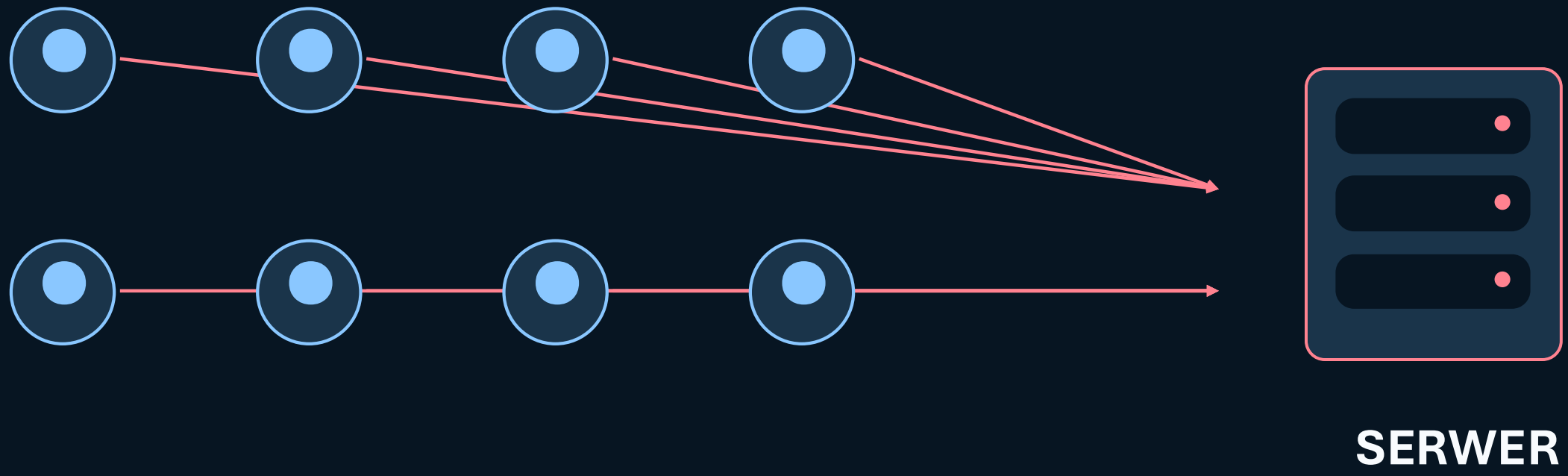
Denial of Service • zwykle jedno źródło ruchu.



Cel ataku: użytkownik nie może skorzystać z usługi.

DDoS = atak rozproszony

Distributed Denial of Service • wiele źródeł jednocześnie.



To odróżnia DDoS od zwykłego DoS: wiele źródeł.

DoS czy DDoS?

Dwa warianty ataku na dostępność.

DoS

Jedno źródło
→ jedna usługa.

DDoS

Wiele źródeł
→ jedna usługa.

DDoS trudniej ograniczyć blokadą jednego adresu IP.

Adres IP — do czego służy?

Adres IP pomaga kierować dane do właściwego urządzenia lub sieci.

ADRES IP

Numer używany w komunikacji sieciowej.

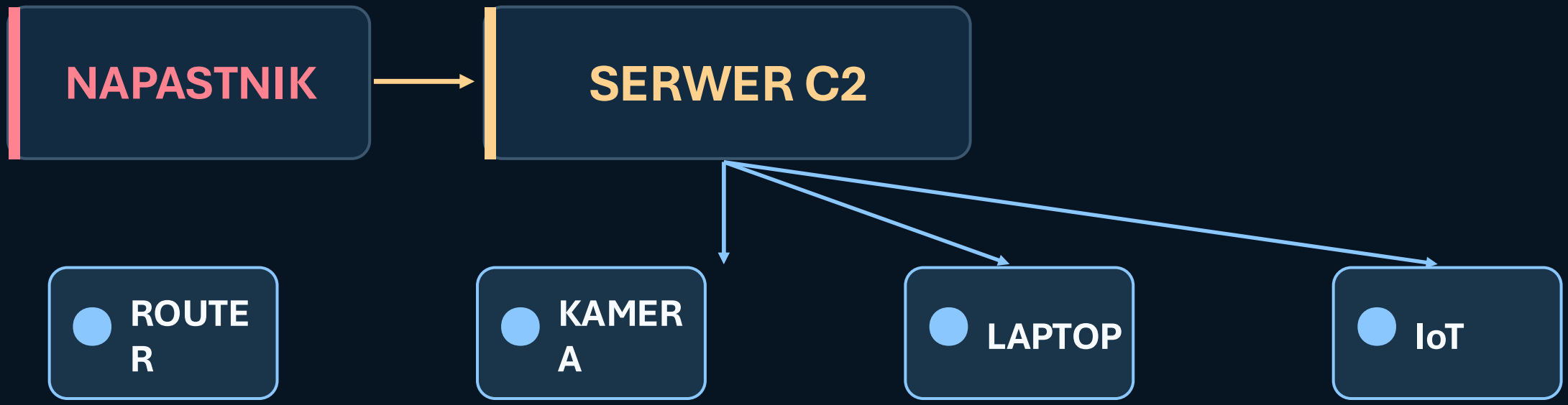
PRZYKŁAD

W logach serwera widać adres źródła ruchu.

Uwaga: jeden publiczny IP może służyć wielu urządzeniom.

Botnet: „armia zombie”

Sieć urządzeń zdalnie kontrolowanych przez napastnika.



C2 (Command and Control) przekazuje polecenia botom.

Bot, botnet, zombie i C2

Cztery nazwy używane na schematach ataku.

BOT

Urządzenie wykonujące polecenia napastnika.

BOTNET

Wiele botów działających jako sieć.

ZOMBIE

Potoczne określenie przejętego urządzenia.

C2

System dowodzenia wysyłający polecenia.

Zombiakiem może być...

Nie tylko komputer. Każde urządzenie narażone na przejęcie.

ROUTER

domowy

KAMERA

IP

KOMPUTER

biurowy

URZĄDZENIE

IoT

Jak urządzenie trafia do botnetu?

Najczęstsze zaniedbania ułatwiają przejęcie.

SŁABE HASŁO	np. fabryczne dane logowania
BRAK AKTUALIZACJI	niezałatane podatności
ZBĘDNE USŁUGI	otwarte i niechronione funkcje

Router, IoT i malware

Te trzy terminy często pojawiają się przy botnetach.

ROUTER

Kieruje ruchem między sieciami, np. w domu.

IoT

Urządzenia podłączone do sieci: kamera, czujnik.

MALWARE

Złośliwy program; może pomóc przejąć sprzęt.

Urządzenie online nie musi być zainfekowane.

Po co atakujący tworzy botnet?

Wiele przejętych urządzeń można wykorzystać równocześnie.

DDoS

Niedostępność usług.

SKANOWANIE

Poszukiwanie kolejnych podatnych urządzeń.

PRÓBY LOGOWAŃ

Automatyczne sprawdzanie wykradzionych haseł.

Przejęte urządzenie może działać „normalnie” dla właściciela.

Trzy rodzaje ataków DDoS

Różne techniki uderzają w różne zasoby.

WOLUMETRYCZNE

Zapychają łącze.

PROTOKOŁOWE

Wycieńczają zasoby połączeń.

APLIKACYJNE

Obciążają WWW i bazę danych.

Jeden incydent może łączyć kilka technik.

Pakiet i łącze — co to jest?

Można porównać sieć komputerową do drogi.

PAKIET

Mała porcja danych przesyłana przez sieć.

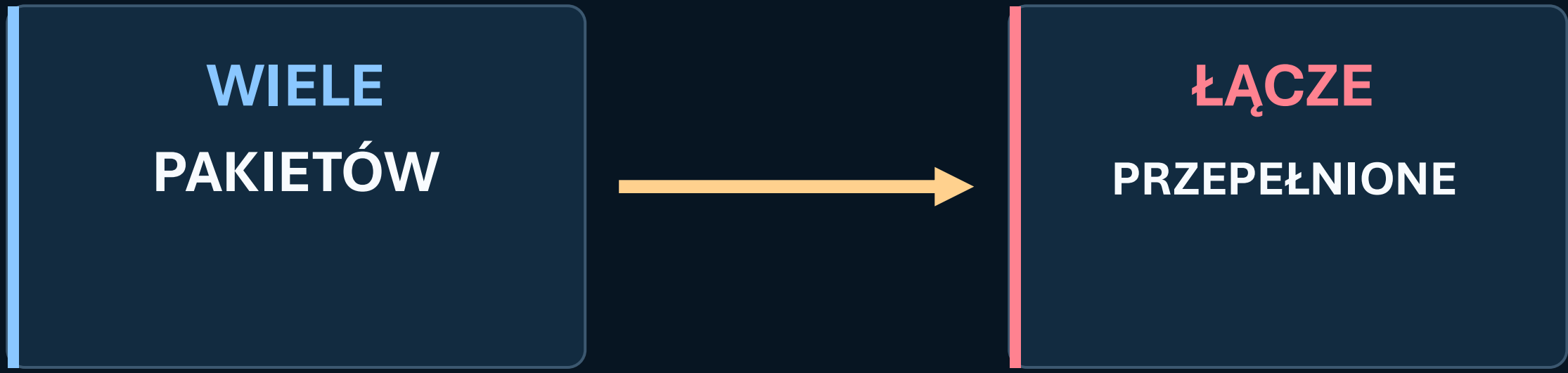
ŁĄCZE

Połączenie o ograniczonej szybkości przesyłania.

Pakiety są jak pojazdy, a łącze — jak droga.

Wolumetryczny: zalanie łącza

Przykład: ogromna ilość pakietów lub danych.



Zabezpieczenie: filtrowanie przed przeciążonym łączem.

TCP i SYN — na czym to polega?

TCP to protokół, który pomaga niezawodnie przesyłać dane.

1 SYN

Chcę się połączyć.

2 SYN-ACK

Słyszę cię.

3 ACK

Potwierdzam.

SYN flood: wiele prób połączenia nie zostaje dokończonych.

Protokołowy: SYN flood

Wiele rozpoczętych, ale niedokończonych połączeń TCP.

KLIENT	SERWER	SKUTEK
Wysyła SYN	Czeka na zakończenie	Zasoby połączeń zajęte

Obrona: m.in. SYN cookies i filtracja na brzegu sieci.

Aplikacyjny: HTTP flood

Pozornie zwykłe żądania mogą przeciążyć aplikację.

LOGOWANIE

Żądania do formularza.

WYSZUKIWANIE

Kosztowne zapytania do bazy.

RAPORTY

Generowanie plików i treści.

Tutaj liczy się zachowanie aplikacji, nie tylko ilość danych.

HTTP: przeglądarka prosi, serwer odpowiada

HTTP to zestaw zasad komunikacji ze stroną WWW.

ŻĄDANIE

Przeglądarka: „Pokaż mi stronę z ocenami”.

ODPOWIEDŹ

Serwer: „Oto strona” albo komunikat błędu.

HTTP flood: bardzo dużo żądań obciąża aplikację.

Reflection / amplification

Małe zapytanie może wywołać dużą odpowiedź.



Mechanizm: podszycie pod adres źródłowy + większa odpowiedź.

Odbicie i wzmocnienie DDoS

Dwa różne pomysły, które mogą wystąpić razem.

ODBICIE

Odpowiedź z pośrednika trafia do ofiary.

WZMOCNIENIE

Odpowiedź jest znacznie większa niż zapytanie.

Odbicie = dokąd idzie odpowiedź; wzmocnienie = jej wielkość.

Który zasób jest „wąskim gardłem”?

Powiąż rodzaj ataku z jego głównym skutkiem.

WOLUMETRYCZNY	→	ŁĄCZE
PROTOKOŁOWY	→	TABLICE POŁĄCZEŃ
APLIKACYJNY	→	CPU / BAZA / WWW

Po czym poznasz podejrzany ruch?

Pojedynczy objaw nie przesądza o DDoS.

NAGŁY WZROST

RPS, pps lub bps

BŁĘDY

np. 502 lub 503

OPÓŹNIENIA

strona długo odpowiada

WZORCE

powtarzalne żądania

Log, monitoring i alert

Jak administrator zauważa problemy i je sprawdza?

LOG

Dziennik zdarzeń: zapis np. czasu i wyniku żądania.

MONITORING

Obserwowanie stanu serwera na bieżąco.

ALERT

Ostrzeżenie: coś może wymagać sprawdzenia.

Błąd 503 oznacza czasową niedostępność obsługi żądania.

bps i pps: dwa różne wskaźniki

Narzędzia monitorujące pokazują oba.

bps

Bity na sekundę
→ obciążenie łącza.

pps

Pakiety na sekundę
→ natężenie pakietów.

Wysokie bps i wysokie pps to nie to samo.

RPS i opóźnienie

Dwa ważne wskaźniki dla aplikacji WWW.

RPS

Żądania na sekundę.
Ile pracy ma serwer?

LATENCY

Czas odpowiedzi.
Jak długo czeka użytkownik?

1000 RPS może być normą lub anomalią — zależy od serwisu.

bps, pps i RPS — nie myl pojęć!

Każdy wskaźnik mierzy coś innego.

bps

Ile bitów danych przechodzi w sekundę?

pps

Ile pakietów przechodzi w sekundę?

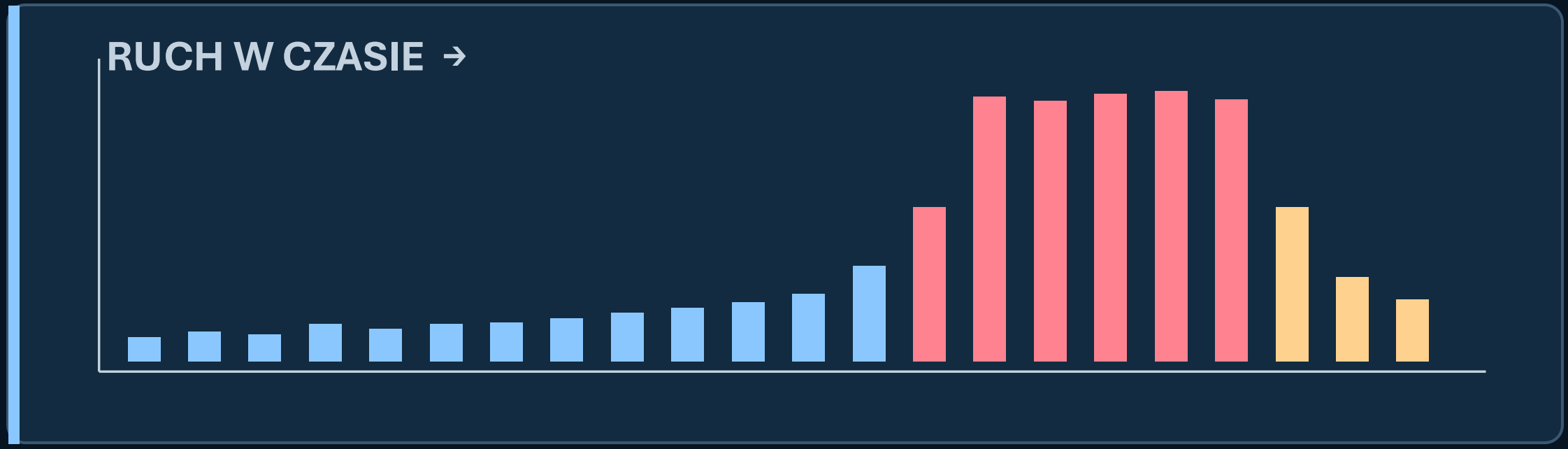
RPS

Ile żądań otrzymuje aplikacja w sekundę?

Jedno żądanie HTTP może wymagać wielu pakietów.

Naturalny wzrost ruchu czy DDoS?

Ten wykres nie wystarcza do postawienia diagnozy.



Co jeszcze sprawdzisz w logach i monitoringu?

Nie każdy skok to atak!

Podobne liczby, ale dwie różne sytuacje.

DUŻO UCZNIÓW

Publikacja ocen.
Wszyscy się logują.

PODEJRZANY RUCH

Powtarzalne zapytania.
Nietypowe źródła.

Pytanie: jakie dane rozróżnią te dwa przypadki?

ISP i firewall — kto za co odpowiada?

Obrona często zaczyna się jeszcze przed serwerem.

ISP

Dostawca Internetu, czyli operator łącza.

FIREWALL

Zapora sieciowa filtrująca ruch według reguł.

Gdy łącze jest zapchane, zapora może być za późno.

Ochrona warstwowa przed DDoS

Jeden firewall nie rozwiązuje wszystkich problemów.

01 ISP / OCHRONA DDoS

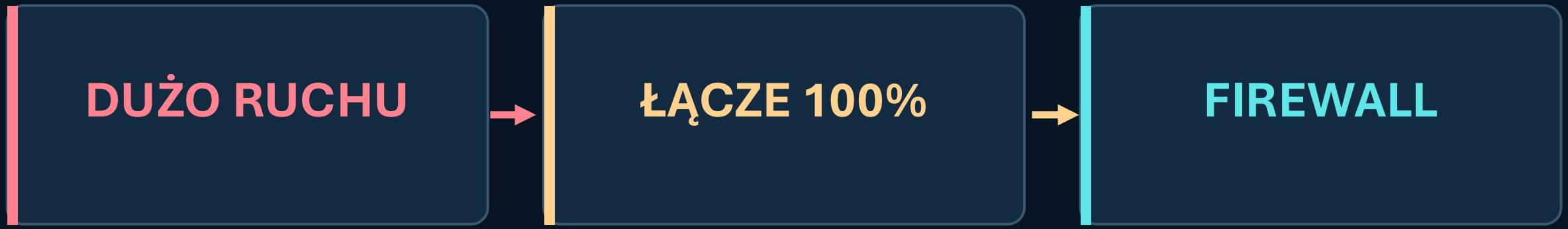
02 CDN / WIELE SERWERÓW

03 WAF / OCHRONA BOTÓW

04 LIMITY / CACHE

Czemu sam firewall nie wystarczy?

Gdy łącze jest już pełne, filtr może działać zbyt późno.



Często trzeba filtrować ruch u operatora Internetu.

WAF i CDN — co robią?

Dwa elementy mogą współpracować, ale mają różne role.

CDN

Rozkłada ruch.
Cache przyspiesza treści.

WAF

Analizuje żądania HTTP.
Blokuje podejrzane wzorce.

WAF nie zastępuje ochrony przed zalaniem łącza.

CDN, WAF i cache — prosta analogia

Wyobraź sobie szkolną bibliotekę z wieloma czytelnikami.

CDN

Filie biblioteki: obsługują czytelników w wielu miejscach.

WAF

Portier: sprawdza podejrzane prośby.

CACHE

Gotowa kopia: nie trzeba za każdym razem szukać od nowa.

To analogie — rzeczywiste systemy działają bardziej złożenie.

Rate limiting i cache

Jak ograniczyć koszt obsługi żądań?

RATE LIMITING

Ogranicza liczbę żądań w czasie.

CACHE

Przechowuje wyniki, aby nie liczyć ich wciąż od nowa.

Uwaga: zbyt ostre limity mogą blokować prawdziwych uczniów.

Nie pozwól, by urządzenie było zombie

Cztery podstawowe działania administratora.

01 SILNE HASŁA

02 AKTUALIZACJE

03 SEGMENTACJA

04 MONITORING

Mniej podatnych urządzeń = mniejsze możliwości botnetu.

Co zrobić podczas incydentu?

Najpierw ustal fakty. Potem ograniczaj skutki.

1 **POTWIERDŹ**
logi i monitoring

2 **OGRANICZ**
ISP, WAF, filtry

3 **KOMUNIKUJ**
zespół i użytkownicy

4 **ANALIZUJ**
wnioski i poprawki

Kto pomaga w Polsce?

W razie incydentu znaczenie ma prawidłowa ścieżka zgłoszenia.

CERT POLSKA

Zgłaszanie incydentów:
incydent.cert.pl

DOSTAWCY

Operator Internetu,
hosting, ochrona DDoS.

Stosuj procedury obowiązujące w organizacji.

Podatność i łatka — co oznaczają?

Podatności mogą ułatwiać przejęcie urządzeń do botnetu.

PODATNOŚĆ

Błąd lub słabość, którą można wykorzystać.

ŁATKA / PATCH

Aktualizacja, która naprawia problem.

CVE to identyfikator podatności, a CVSS — jej ocena.

CVE i CVSS a zagrożenia DDoS

Luki mogą pozwolić przejmować kolejne urządzenia.

CVE

Numer identyfikujący publicznie opisaną podatność.

CVSS

Ocena istotności podatności w skali 0–10.

CVSS NIE mierzy „siły ataku DDoS”.

E-dziennik szkoły przestał działać

Dane z ćwiczenia: sytuacja fikcyjna.

07:58

POCZĄTEK PROBLEMU

35 → 2900

ŻĄDANIA HTTP / s

38%

ODSETEK BŁĘDÓW 503

Czy te dane wystarczą, żeby stwierdzić atak?

Co zrobisz jako administrator?

Czas: 8 minut. Ustalcie odpowiedzi w parach.

01 **Podaj DWIE hipotezy.**

02 **Wskaż TRZY źródła danych.**

03 **Zaproponuj DWA działania.**

Który plan jest najlepszy?

Uzasadnij wybór, a nie tylko literę.

A. Odłącz Internet całej szkoły.

B. Sprawdź logi i uruchom właściwą ochronę.

C. Ignoruj problem — może minie sam.

DoS czy DDoS?

Wybierz A lub B, a potem wyjaśnij dlaczego.

Co odróżnia DDoS od DoS?

A **Wiele źródeł ruchu.**

B **System operacyjny serwera.**

Co to jest botnet?

Która definicja jest poprawna?

A. Program antywirusowy.

B. Sieć przejętych urządzeń.

Właściciel nie zawsze wie, że jego urządzenie jest botem.

Czy nagły wzrost RPS = DDoS?

Pomyśl o publikacji ocen lub wyprzedaży.

A **TAK — zawsze.**

B **NIE — trzeba sprawdzić kontekst.**

Analiza kilku źródeł danych jest ważniejsza niż jeden wykres.

5 rzeczy do zapamiętania

Powtórz je własnymi słowami.

1. DoS = jedno źródło; DDoS = wiele.
2. Botnet to sieć przejętych urządzeń.
3. Atak może uderzać w różne zasoby.
4. Objawy trzeba interpretować w kontekście.
5. Obrona jest warstwowa i zaplanowana.

Bibliografia

Materiały źródłowe i uzupełniające.

Paweł Kuraś

Kwalifikacje INF.11 i INF.12. Część 1. Podstawy, s. 78–80, 88–89.

„Wprowadzenie do bezpieczeństwa IT”, Sekurak

Modelowanie zagrożeń, s. 383–389.

Materiały uzupełniające: CERT Polska • CISA • NCSC