Szanse i zagrożenia związane z rozwojem informatyki i technologii – rozpraszanie danych

Szanse i zagrożenia związane z rozwojem informatyki i technologii – rozpraszanie danych

Źródło: Nicolas Picard, dostępny w internecie: unsplash.com, domena publiczna.

Podłączanie do internetu kolejnych serwerów przynosi oczywiste korzyści, wynikające choćby z możliwości gromadzenia oraz przesyłania danych bądź świadczenia rozmaitych usług. Rozwój sieci wiąże się jednak także z zagrożeniami i sprawia, że na firmach – będących operatorami serwerów – spoczywa wielka odpowiedzialność.

Każde włamanie na serwer lub przerwanie jego działania może pociągnąć za sobą konsekwencje prawne oraz finansowe. Słabo zabezpieczone serwery i sieci komputerowe stały się celem cyberataków. Hakerzy wykradając dane albo zakłócając pracę przesiębiorstw, czerpią z tego wymierne zyski.

W jaki sposób przeciwdziałać atakom hakerskim? Jakimi technikami posługują się cyberprzestępcy? Czy rozproszona baza danych pozwala zminimalizować skutki włamania lub zakłócenia pracy serwerów? Na takie właśnie pytania odpowiemy w e-materiale.

Więcej informacji na temat poruszanych zagadnień znajdziesz w e-materiałach:

- Rozwój informatyki,
- Podstawy sieci komputerowych,
- Przestępczość komputerowa.

Twoje cele

- Określisz, jak działa rozproszona baza danych oraz jak jej wykorzystanie może zapobiec atakom hakerskim.
- Przeanalizujesz, czym charakteryzują się najczęstsze typy cyberataków.
- Przesledzisz sposoby obrony przed cyberatakami.

Przeczytaj

Rozproszona baza danych

Rozproszona baza danych jest bazą podzieloną na części umieszczone na wielu komputerach. Taka architektura jest szczególnie przydatna, gdy z informacji przechowywanych w bazie korzystają osoby zamieszkujące oddalone od siebie miejsca – np. różne miasta, kraje bądź kontynenty.

Rozdzielenie danych pozwala m.in. **zmniejszyć czas oczekiwania na odpowiedź serwera** (co z kolei przekłada się na szybkość wczytywania informacji i jest ważne w przypadku, kiedy czas odpowiedzi ma znaczący wpływ na czynności wykonywane w sieci – jak choćby podczas gier online lub prowadzenia widekonferencji).

Z punktu widzenia użytkownika baza rozproszona jest strukturą **jednolitą**. Oznacza to, że pomimo umieszczenia fragmentów bazy na wielu serwerach użytkownik nie jest w stanie określić, z którego komputera otrzymuje odpowiedź.

Zarządzając bazą rozproszoną, wykorzystuje się dwie metody rozdzielania informacji: **fragmentaryzację** oraz **replikację** (zazwyczaj stosowane są one wspólnie jako tzw. metoda hybrydowa).

Fragmentaryzacja danych

Fragmentaryzacja danych polega na **podzieleniu informacji na podzbiory**, które są przechowywane w różnych węzłach sieci. Metoda ta jest wykorzystywana głównie wtedy, gdy **dane zbierane są lokalnie** – np. baza danych w mieście A przechowuje wyłącznie informacje na temat miasta A, zaś baza danych B służy do przechowywania informacji o miejscowości B. Stale możliwe jest przy tym uzyskanie dostępu do całej bazy danych AB.

Zaletą przedstawionej metody jest przechowywanie **oryginalnych kopii** informacji. Nie muszą być one aktualizowane w wielu miejscach po dokonaniu zmian (jak ma to miejsce w przypadku replikacji). W razie wystąpienia awarii dane są przesyłane do innego, tymczasowego serwera.

Replikacja danych

Replikacja danych polega na **przechowywaniu identycznych kopii informacji** na kilku serwerach równocześnie. Warto zaznaczyć, że istnieje w tym przypadku podział danych na kategorie. Wynika on z praw dostępu do informacji:

- **dane do odczytu** – informacje, z których serwerowi drugorzędnemu wolno korzystać, bez możliwości wprowadzania jakichkolwiek zmian;
- **dane do zapisu** – informacje, które mogą zostać zmienione na każdym serwerze drugorzędnym. Po wprowadzeniu poprawek serwer ten staje się automatycznie serwerem macierzystym.

Zaletą tej metody jest zapewnienie większej **dostępności do danych z każdej lokalizacji**. Przekłada się to na zwiększenie szybkości działania serwerów oraz umożliwia wysyłanie większej liczby zapytań równocześnie.

Główną wadą replikacji jest natomiast konieczność dokonywania **wielu aktualizacji**. Informacje na serwerach drugorzędnych są aktualizowane nawet po wprowadzeniu najdrobniejszych zmian na serwerze macierzystym. W innym przypadku mogą pojawiać się niespójności w poszczególnych kopiach. Sam proces aktualizacji obciąża natomiast serwery.

> **Już wiesz**
>
> Omawialiśmy już pojęcie **redundancji** (nadmiarowości).
>
> O ile **zjawisko redundancji w bazach danych** nie jest zazwyczaj postrzegane jako pożądane (z uwagi na możliwość występowania pewnych anomalii przy modyfikacji danych), o tyle w przypadku replikacji jest oczekiwane i ma uzasadnienie. **Nadmiarowość informacji** może bowiem uchronić przed niespodziewaną utratą danych i być gwarancją bezpieczeństwa w przypadku ataku na jeden z serwerów.

Korzyści płynące z rozproszenia baz danych

W porównaniu ze scentralizowanym systemem bazy danych **rozproszona struktura pozwala przede wszystkim zminimalizować skutki awarii serwerów**. W razie wystąpienia problemów obniża się tylko wydajność serwerów. Nie przerywają one całkowicie pracy, tak jak dzieje się w przypadku systemów scentralizowanych.

Oprócz tego rozproszona baza danych zapewnia:

- **zwiększenie szybkości otrzymywanych odpowiedzi** na zapytania wysyłane przez użytkowników;
- **zwiększenie kontroli nad danymi w przypadku ich fragmentaryzacji na rejony** (serwer A odpowiedzialny jest wyłącznie za przechowywanie danych w mieście A);
- **możliwość rozbudowania serwerów w sposób modułowy**, a co za tym idzie, poprawienia logistycznej struktury serwerów oraz zwiększenia ich wydajności i bezawaryjności.

Ataki na serwery

Atak DoS

Jednym z najprostszych typów ataku na serwer jest DoS. Polega on na wysyłaniu pakietów zapytań na określony adres IP w celu całkowitego wysycenia dostępnego pasma. Skutkiem jest blokada dostępu do strony WWW lub serwisu. Częstym zjawiskiem jest również wykorzystanie błędów protokołów internetowych. Ułatwia to zablokowanie serwisu.

Atak typu DoS charakteryzuje się **niską efektywnością**. Warunkiem powodzenia jest bowiem dysponowanie znacznie większym pasmem internetowym niż to, które wykorzystuje atakowany obiekt. Ponadto cały atak przeprowadzany jest zazwyczaj z wykorzystaniem kilku adresów IP. Atakowany może je wpisać na tzw. **czarną listę** i zablokować pochodzące z nich zapytania.

Atak DDoS

Znacznie bardziej uciążliwym typem ataku na serwer jest DDoS. W tym przypadku atakujący wykorzystuje **bardzo dużą (teoretycznie nieograniczoną) liczbę komputerów**.

Aby to uczynić, cyberprzestępca rozsyła zawirusowane pliki do użytkowników sieci. Jeśli internauci je otworzą, ich systemy są infekowane, a atakujący przejmuje nad nimi kontrolę. W ten sposób powstaje sieć tzw. **komputerów-zombies**, którymi haker jest w stanie zarządzać za pomocą specjalnego oprogramowania.

Podczas ataku DDoS wszystkie zainfekowane komputery (działające niejednokrotnie w bardzo odległych zakątkach globu) wysyłają zapytana na adres IP ofiary. Szybko prowadzi to do zablokowania dostępu do strony lub serwisu.

Atak **DDoS jest trudny do odparcia**, ponieważ w jego przypadku należałoby przenieść na czarną listę tysiące adresów IP. Poza tym ruch generowany przez zwykłych (niezainfekowanych) użytkowników nie tylko wyczerpuje pasmo ofiary, ale także utrudnia wydzielenie grupy adresów IP wykorzystywanych przez atakującego.

DRDoS

Kolejnym bardzo niebezpiecznym typem ataku jest DRDoS. Polega on na wysyłaniu zapytań do losowych adresów IP w sieci oraz fałszowaniu adresu ich nadawcy: zastępuje się go adresem potencjalnej ofiary.

W przypadku jednoczesnego wysłania tysięcy takich zapytań następuje zablokowanie dostępu do serwisu będącego celem ataku: wszystkie odpowiedzi trafiają na adres ofiary, blokując jej pasmo internetowe.

Warto dodać, że za dokonanie ataku internetowego (w zależności od wyrządzonych szkód) grozi kara grzywny lub pozbawienia wolności nawet do **2 lat.**

> **Ciekawostka**
>
> Jedną z usług pozwalających zwiększyć bezpieczeństwo strony internetowej lub serwisu proponuje firma **CloudFlare.**
>
> Wykorzystywany jest przy tym pewien rodzaj **filtra**, dzięki któremu użytkownicy sieci (w tym boty lub cyberprzestępcy) nie łączą się bezpośrednio z docelowym adresem IP, lecz ich zapytania są wstępnie przetwarzane przez serwery firmy CloudFlare. Oddziela ona połączenia generowane przez zwykłych użytkowników od ruchu budzącego podejrzenia.
>
> Oprócz filtrowania usługa CloudFlare pozwala m.in. na **ukrycie adresu IP serwera, przyspieszenia działania strony WWW albo limitowanie zapytań** w przypadku ogromnego zwiększenia ruchu, co jest szczególnie ważne, gdy dochodzi do cyberataku.

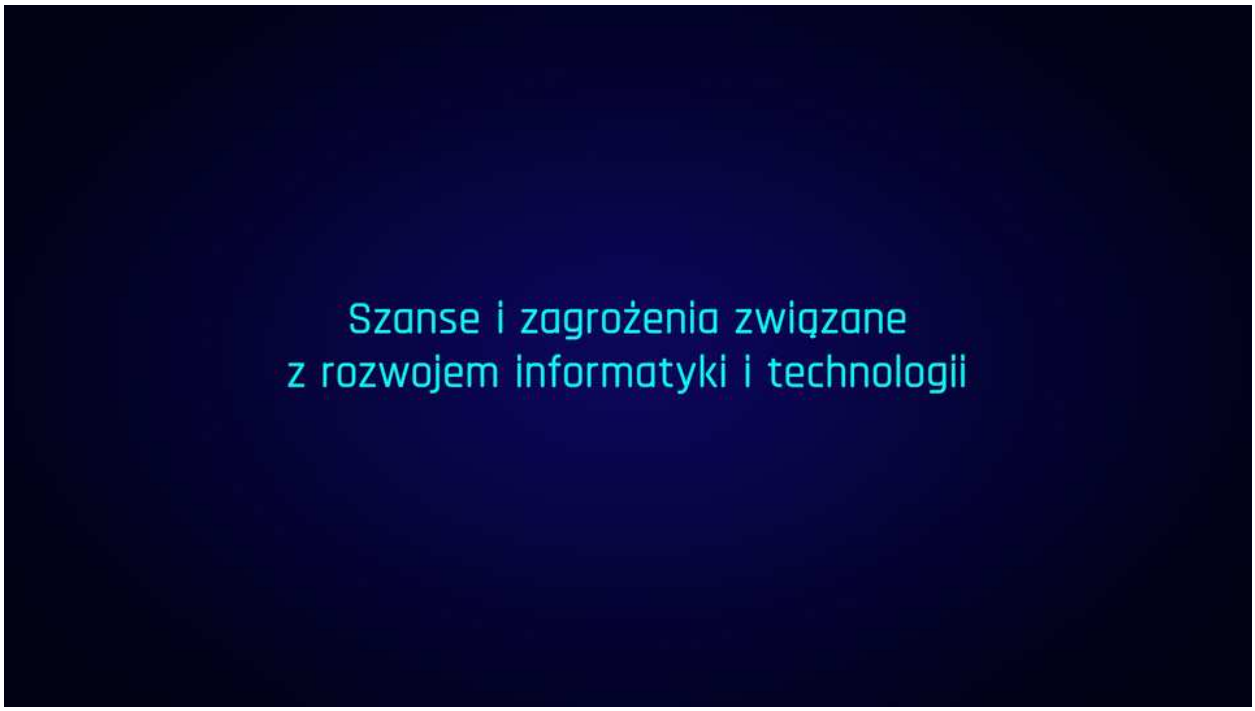
Słownik

> **DoS**
>
> (ang. *Denial of Service* – blokada usług); jeden z najprostszych typów ataku na serwer lub sieć komputerową, polegający na wysyłaniu pakietów zapytań na adres IP ofiary w celu zajęcia (wysycenia) całego jej pasma transmisyjnego
> **DDoS**
>
> (ang. *Distributed Denial of Service*); rozproszona blokada usług) typ ataku wykorzystujący zawirusowane komputery (*zombies*) w celu maksymalizacji efektów ataku
> **DRDoS**
>
> (ang. *Distributed Reflected Denial of Service*); odbita blokada usług) odmiana ataku, w przypadku której wykorzystuje się zjawisko „odbicia zapytania"; odpowiedzi pochodzące z wielu komputerów są przesyłane na serwer lub sieć komputerową ofiary

Animacja

Polecenie 1

Zapoznaj się z animacją i wykonaj **Ćwiczenie 1**.



Film dostępny pod adresem /preview/resource/RL5ka2y5OOJ9N

Film nawiązujący do treści materiału przedstawia szanse i zagrożenia związane z rozwojem technologii

Ćwiczenie 1

Poszukaj informacji na temat ataków DDoS. Przygotuj notatkę na temat jednego z nich.

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Wskaż, czym jest komputer-zombie.

- ◯ Bazą danych, która gromadzi dane wrażliwe użytkowników sieci.
- ◯ Zawirusowanym urządzeniem, które bez wiedzy użytkownika może być sterowane przez osobę z zewnątrz.
- ◯ Systemem wykorzystywanym do przechwytywania danych użytkownika, stosowanym najczęściej przy ataku DoS.

Ćwiczenie 2

Dokończ zdanie.

Fragmentaryzacja danych może być szczególnie opłacalna w wypadku, gdy...

- ◯ zależy nam na szybkości działania serwerów oraz łatwiejszym dostępie do nich z wielu lokalizacji.
- ◯ Obie odpowiedzi są błędne.
- ◯ dane zbierane są lokalnie, np. baza danych A zbiera wyłącznie informacje na temat miasta A.

Ćwiczenie 3

Połącz w pary pojęcia wraz z odpowiadającymi im opisami.

DDoS	Jeden z najprostszych typów ataku na serwer, który polega na wysyłaniu pakietów zapytań na adres IP ofiary.
DRDoS	Wykorzystuje zainfekowane komputery-zombie w celu zmaksymalizowania efektu ataku.
DoS	Wykorzystuje zjawisko odbicia zapytania, przesyłając odpowiedź na adres IP ofiary zamiast do prawdziwego nadawcy.

Ćwiczenie 4

Uporządkuj w odpowiedniej kolejności elementy procesu ataku DDoS.

- Rozesłanie programu do sieci, w celu zainfekowania systemu użytkowników
- Przeprowadzenie zmasowanego ataku na serwer lub sieć użytkownika
- Stworzenie bazy komputerów-zombie
- Stworzenie zawirusowanego programu

Ćwiczenie 5

Wyjaśnij różnice pomiędzy danymi do odczytu, a danymi do zapisu.

Ćwiczenie 6

Wyjaśnij pojęcia fragmentaryzacja oraz replikacja danych.

Ćwiczenie 7

Zaznacz wszystkie poprawne odpowiedzi. Wskaż, jakie są korzyści płynące z rozproszenia danych.

- [ ] Możliwość dalszej rozbudowy serwera w sposób modułowy.
- [ ] Zwiększenie szybkości otrzymywanych odpowiedzi na zapytania przez użytkowników sieci.
- [ ] Większa kontrola nad danymi w przypadku fragmentaryzacji na rejony lokalizacyjne.
- [ ] Większa awaryjność serwerów.

Ćwiczenie 8

Przedstaw dwa sposoby zapobiegania atakom typu DDoS lub metody niwelowania ich skutków.

Dla nauczyciela

Autor: Maurycy Gast
Przedmiot: Informatyka

Temat: Szanse i zagrożenia związane z rozwojem informatyki i technologii – rozpraszanie danych

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy

Podstawa programowa:

Cele kształcenia – wymagania ogólne

III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym: znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.

V. Przestrzeganie prawa i zasad bezpieczeństwa. Respektowanie prywatności informacji i ochrony danych, praw własności intelektualnej, etykiety w komunikacji i norm współżycia społecznego, ocena zagrożeń związanych z technologią i ich uwzględnienie dla bezpieczeństwa swojego i innych.

Treści nauczania – wymagania szczegółowe

IV. Rozwijanie kompetencji społecznych.

Zakres podstawowy. Uczeń:

2) podaje przykłady wpływu informatyki i technologii komputerowej na najważniejsze sfery życia osobistego i zawodowego; korzysta z wybranych e-usług; przedstawia wpływ technologii na dobrobyt społeczeństw i komunikację społeczną;

V. Przestrzeganie prawa i zasad bezpieczeństwa.

Zakres podstawowy. Uczeń:

4) opisuje szkody, jakie mogą spowodować działania pirackie w sieci, w odniesieniu do indywidualnych osób, wybranych instytucji i całego społeczeństwa.

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;

- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Określisz, jak działa rozproszona baza danych oraz jak jej wykorzystanie może zapobiec atakom hakerskim.
- Przeanalizujesz, czym charakteryzują się najczęstsze typy cyberataków.
- Przesledzisz sposoby obrony przed cyberatakami.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimedium i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Szanse i zagrożenia związane z rozwojem informatyki i technologii – rozpraszanie danych". Uczniowie mają zapoznać się z treściami w sekcji „Przeczytaj".

Faza wstępna:

1. Nauczyciel wyświetla i odczytuje temat lekcji oraz cele zajęć. Prosi uczniów o sformułowanie kryteriów sukcesu.

2. **Rozpoznanie wiedzy uczniów.** Nauczyciel prosi wybranego ucznia lub uczniów o przedstawienie sytuacji problemowej związanej z tematem lekcji.

Faza realizacyjna:

1. **Praca z tekstem.** Jeżeli przygotowanie uczniów do lekcji jest niewystarczające, nauczyciel prosi o indywidualne zapoznanie się z treścią zawartą w sekcji „Przeczytaj". Każdy uczestnik zajęć podczas cichego czytania wynotowuje najważniejsze kwestie poruszane w tekście.
2. **Praca z multimedium.** Nauczyciel wyświetla zawartość sekcji „Animacja". Uczniowie wspólnie zapoznają się z treścią multimedium. Zapisują ewentualne problemy i pytania. Po czym następuje dyskusja, w trakcie której nauczyciel wyjaśnia niezrozumiałe treści.
3. **Ćwiczenie umiejętności.** Uczniowie wykonują indywidualnie ćwiczenia nr 1-4 z sekcji „Sprawdź się", a następnie dzielą się wynikami swojej pracy z kolegą lub koleżanką.

Faza podsumowująca:

1. Nauczyciel wyświetla na tablicy temat lekcji i cele zawarte w sekcji „Wprowadzenie". W kontekście ich realizacji podsumowuje przebieg zajęć, a także wskazuje mocne i słabe strony pracy uczniów.
2. Wybrany uczeń podsumowuje zajęcia, zwracając uwagę na nabyte umiejętności.

Praca domowa:

1. Uczniowie wykonują ćwiczenia 5-8 z sekcji „Sprawdź się".

Wskazówki metodyczne:

- Treści w sekcji „Przeczytaj" można wykorzystać jako podsumowanie i utrwalenie wiedzy uczniów.