Analiza celów i kompromisów technicznych

dr inż. Krzysztof Makles

Wstęp

- Typowe cele techniczne to skalowalność, dostępność, wydajność sieci, bezpieczeństwo, użyteczność, zdolność do przystosowania się i dostępność finansowa;
- Kompromisy, np. spełnienie surowych wymagań dotyczących wydajności może być trudne z punktu widzenia dostępnych finansów;

Skalowalność

- Odnosi się do przyszłego rozwoju sieci, który należy uwzględnić w projekcie;
- Często jest celem podstawowym dla przedsiębiorstwa;
- Związana jest z rozwojem przedsiębiorstwa, rosnącą liczbą użytkowników, aplikacji, dodatkowymi lokalizacjami, zewnętrznymi połączeniami sieciowymi;

Skalowalność – planowanie rozbudowy

- Klient powinien być w stanie przewidzieć, w jakim stopniu sieć rozszerzy się w ciągu następnego roku i następnych dwóch lat;
- Ile lokalizacji będzie dodanych w ciągu następnego roku? Następnych dwóch lat?
- Jak rozległe będą sieci w każdej z tych lokalizacji?
- Ilu użytkowników więcej będzie miało dostęp do sieci korporacyjnej w ciągu następnego roku? Następnych dwóch lat?
- Ile więcej serwerów będzie dodanych do sieci korporacyjnej w ciągu następnego roku? Następnych dwóch lat?

Skalowalność – zwiększanie dostępu do danych

- Dawniej dane ważne dla działania firmy były przechowywane w wydziałowych sieciach LAN, obecnie często są przechowywane na scentralizowanych serwerach;
- Stosowano wówczas podział 80/20 – 80% ruchu pozostaje w wydziałowych sieciach LAN, a 20% jest przeznaczone dla innych wydziałów bądź sieci zewnętrznych;
- W chwili obecnej następuje przesunięcie tych proporcji w odwrotnym kierunku. Wiele firm posiada scentralizowane serwery umieszczone na farmach serwerów usytuowanych w szkieletowych sieciach budynków lub sieciach kampusowych;
- Głównym elementem zaburzającym wspomniane proporcje jest ruch na serwerach WWW przedsiębiorstwa (szkolenia, zamówienia, przeglądanie danych itd.);

Skalowalność – zwiększanie dostępu do danych

- Cel biznesowy: udostępnianie użytkownikom większej ilości danych, prowadzi do celów technicznych:
  - Połączenie oddzielnych wydziałowych sieci LAN w sieć korporacyjną;
  - Rozwiązanie problemu wąskiego gardła LAN/WAN spowodowanego przez duży wzrost ruchu sieciowego;
  - Zastosowanie scentralizowanych serwerów umieszczonych na farmach serwerów bądź w sieci zewnętrznej;
  - Połączenie niezależnej sieci SNA (mainframe) z siecią IP przedsiębiorstwa;
  - Dodanie nowych lokalizacji do obsługi biur terenowych i telepracowników;
  - Dodanie nowych lokalizacji i usług, aby obsługiwać bezpieczną komunikację z klientami, przedstawicielami i innymi partnerami biznesowymi.

Skalowalność – ograniczenia

- Wybór technologii spełniających wymagania klienta dotyczące skalowalności jest procesem skomplikowanym, który może mieć znaczące konsekwencje, jeżeli nie zostanie wykonany poprawnie;
- Pod uwagę należy wziąć:
  - Wpływ ruchu rozgłoszeniowego na skalowalność;
  - Skalowalność protokołów routingu i przełączania;
  - Skalowalność technologii sieci LAN i WAN oraz urządzeń sieciowych.

Dostępność

- Czas, w jakim sieć jest dostępna dla użytkowników;
- Często jest to cel krytyczny dla klientów zamawiających projekt sieci;
- Może być wyrażona jako procentowy czas prawidłowego działania w ciągu roku, miesiąca, tygodnia, dnia bądź godziny w stosunku do całkowitego czasu w tym okresie;
- Dostępność jest związana z niezawodnością, ale ma węższe znaczenie;
- Wiąże się również z nadmiarowością, która jest sposobem uzyskania wysokiej dostępności (duplikowanie połączeń lub urządzeń);
- Jest również powiązana z odpornością na uszkodzenia określającą, z jakim obciążeniem sieć może sobie poradzić, oraz jak szybko można przywrócić jej prawidłowe działanie po naruszeniu bezpieczeństwa, naturalnych lub wywołanych katastrofach, błędzie człowieka, poważnej awarii oprogramowania i sprzętu.

Dostępność – przywrócenie sieci po awarii

- Plan przywrócenia prawidłowego działania obejmuje zarówno przechowywanie zapasowych kopii danych w jednym bądź wielu miejscach, w których prawdopodobieństwo katastrofy jest niewielkie, jak również metodę przełączania się na zapasowe technologie, jeżeli główne zostały dotknięte katastrofą;
- Nie należy lekceważyć znaczenia posiadania wystarczającego personelu do przeprowadzenia planu wznowienia poprawnej pracy sieci po katastrofie. Czy wiadomo, co należy zrobić, jeżeli administratorzy serwerów i sieci będą musieli być poddani kwarantannie? Uzasadnione może być zapewnienie szybkiego dostępu przez VPN z domów pracowników oraz przetestowanie jego wydajności, zanim dojdzie do awarii;
- Ważne jest testowanie nie tylko technologii, ale również pracowników – powinni być oni odpowiednio przeszkoleni na wypadek katastrofy;
- Należy zasymulować katastrofę, aby personel był przygotowany do pracy pod presją czasu i stresu, z wykorzystaniem nadmiarowych serwerów i lokalizacji.

Dostępność – określanie wymagań

- Klient powinien określić wymagania dotyczące dostępności;
- Czy może to być 99,70% (30 min. w tygodniu sieć nie działa), czy też 99,95% (sieć nie działa 5 min. w tygodniu);
- Wymagania powinny być określone z dokładnością co najmniej do drugiego miejsca po przecinku;
- Ważne jest określenie ram czasowych, w obrębie których nie może nastąpić brak dostępności sieci (godziny, pora dnia, dni tygodnia);
- Wymagania czasowe powinny być określone jako czas sprawności w ciągu roku, miesiąca, tygodnia, dnia bądź godziny (30 minut w tygodniu, 10,7 sekundy w ciągu każdej godziny).

Dostępność – 99,999

- Dostępność taka może być potrzebna okresowo (księgowość, okres świąteczny), a bywają firmy, które żądają jej ustawicznie;
- Jest to warunek trudny do spełnienia;
- Należy wytłumaczyć klientowi, że do osiągnięcia takiej dostępności potrzebna jest inwestycja w nadmiarowy sprzęt i infrastrukturę, oraz w dodatkowe etaty dla obsady, niezawodny sprzęt komputerowy i oprogramowanie;
- Szacuje się, że 80-90% usterek jest skutkiem błędów ludzi (lokalni administratorzy, pracownicy dostawcy usług, czy też słynny operator koparki);
- Konieczne jest opracowanie dobrych procedur i umiejętności personelu;
- Ważny jest dobór narzędzi, które będą powiadamiały administratorów sieci o usterkach natychmiastowo;
- Warto rozważyć zakup urządzeń, w których uszkodzone komponenty można wymieniać w czasie pracy urządzenia;
- Należy uświadomić klientowi, że należy uwzględnić czas na aktualizacje oprogramowania;

Dostępność – 99,999

- Czasami stosuje się potrójną nadmiarowość: jedna działa, druga jest w aktywnej rezerwie gotowa do natychmiastowej pracy, a trzecia w rezerwie bądź konserwacji;
- Można wówczas np. odłączyć rezerwowy router w celu uaktualnienia lub konserwacji. Wówczas można dokonywać uaktualnienia i konserwacji pozostałych routerów rotacyjnie;

Dostępność – koszt czasu przestoju

- Dla każdej aplikacji o decydującym znaczeniu dla przedsiębiorstwa należy udokumentować ile pieniędzy traci firma w ciągu godzinnego przestoju (lub innym czasokresie);
- Jeżeli usługi sieciowe obsługiwane są przez firmę zewnętrzną, określenie kosztu przestoju pozwoli zrozumieć jej krytyczność danej aplikacji dla działania firmy;
- Pozwoli także na określenie, czy uaktualnianie w czasie eksploatacji oraz potrójna nadmiarowość są konieczne.

Dostępność – MTBF, MTTR

- Średni czas pomiędzy awariami (MTBF);
- Średni czas potrzebny na naprawę (MTTR);
- Pozwalają precyzyjniej oszacować dostępność;
- Typowy cel MTBF – 4000 godzin, czyli sieć nie powinna ulegać awarii częściej niż raz na 4000 godzin, czyli co 166,67 dni;
- Typowy cel MTTR to 1 godzina, czyli naprawa sieci powinna nastąpić w ciągu jednej godziny, wówczas średnia dostępność wynosi 4000/4001=99,98%;
- Dostępność określamy stosując równanie: dostępność=MTBF/(MTBF+MTTR)
- Należy pamiętać, że szacowana jest średnia;
- Klienci mogą sobie życzyć oszacowania celów MTBF i MTTR dla różnych części sieci;
- Dla każdego programu o wysokim koszcie czasu przestoju należy udokumentować dopuszczalne wartości MTBF i MTTR;
- Dostawcy sprzętu najczęściej określają wartości MTBF i MTTR dla swoich produktów;
- Należy spróbować uzyskać pisemne zobowiązania dotyczące MTBF, MTTR i zmienności wartości od dostawców sprzętu i usług;

Wydajność sieci

- Należy wyodrębnić wymagania klienta dotyczące akceptacji wydajności sieci, w tym zdolności przepustowej, dokładności, sprawności, opóźnienia i czasu odpowiedzi;
- Istnieją wypracowane metody matematyczne szacowania wydajności sieci;
- Analizowanie istniejącej sieci pomoże określić, jakich zmian trzeba dokonać, aby spełnić cele wydajności sieci;
- Cele te są ściśle związane z celami dotyczącymi skalowalności;
- Należy zrozumieć plany rozbudowy sieci przed analizowaniem wydajności;

Wydajność sieci

- **Pojemność (szerokość pasma).** Zdolność przenoszenia danych obwodu bądź sieci, mierzona zazwyczaj w bit/s;
- **Wykorzystanie.** Procent całkowitej pojemności będącej w użyciu;
- **Optymalne wykorzystanie.** Maksymalne średnie wykorzystanie zanim sieć zostanie uznana za nasyconą;
- **Zdolność przepustowa.** Ilość bezbłędnych danych poprawnie przetransportowanych pomiędzy węzłami sieci w jednostce czasu, najczęściej sekundach;
- **Oferowane obciążenie.** Suma danych, które wszystkie węzły sieci mają przygotowane do wysłania w określonym czasie;
- **Dokładność.** Ilość użytecznego, poprawnie przetransmitowanego ruchu w stosunku do całkowitego ruchu;
- **Sprawność.** Miara tego, ile wysiłku trzeba włożyć, aby uzyskać określoną zdolność przepustową;
- **Opóźnienie (czas oczekiwania).** Czas między chwilą, gdy ramka jest gotowa do wysłania z jednego węzła, a jej dostarczeniem do innego miejsca sieci;
- **Wahania opóźnień.** Określa, jak bardzo waha się średni czas opóźnień;
- **Czas odpowiedzi.** Okres czasu pomiędzy żądaniem usługi sieciowej a odpowiedzią na to żądanie.

Wydajność sieci – optymalne wykorzystanie

- Optymalne wykorzystanie jest miarą tego, jak duża szerokość pasma jest używana w konkretnym czasie;
- Narzędzia do analizy sieci używają różnych metod do mierzenia wykorzystania pasma i uśrednia go w czasie(uśrednianie co milisekundę, sekundę, itd., średnie ważone);
- Przy tworzeniu projektu sieci celem klienta może być maksymalne średnie wykorzystanie sieci dozwolone dla segmentu;
- Dla rozległych sieci komputerowych (WAN), optymalne średnie wykorzystanie sieci wynosi około 70%;
- Typową regułą dla współdzielonych, opartych na koncentratorach ethernetowych, sieciach jest średnie wykorzystanie nie przekraczające 37% (kolizje);
- Łącze punkt-punkt, które łączy przełącznik z serwerem bądź innym przełącznikiem, może zużyć całą szerokość pasma, w zależności od wzorców ruchu. Jeżeli wykorzystanie przekracza 70%, to prawdopodobnie nadszedł czas, aby zwiększyć szerokość pasma;
- Ruch sieciowy ma wiele szczytów. Należy planować pojemność sieci LAN i WAN z założeniem, że średnie wykorzystanie będzie zwiększało się w czasie podczas szczytów ruchu;
- Pełnodupleksowy ethernet stał się standardowym trybem przy łączeniu serwerów, przełączników, a nawet komputerów użytkowników;
- Bezwzględnie podczas modernizacji istniejącej sieci należy koncentratory zastąpić przełącznikami;

Wydajność sieci – zdolność przepustowa

- Definiuje się ją dla konkretnego połączenia lub sesji, ale w niektórych przypadkach określa się całkowitą zdolność przepustową sieci;
- W idealnym przypadku zdolność przepustowa powinna być taka sama jak pojemność. Teoretycznie zdolność przepustowa powinna się zwiększać wraz ze wzrostem oferowanego obciążenia, aż do maksymalnej wartości pojemności sieci;
- W rzeczywistości zdolność przepustowa sieci zależy od metody dostępu, obciążenia sieci i współczynnika błędów.

Zdolność przepustowa urządzeń

- Maksymalna szybkość, z jaką urządzenie może przekazywać pakiety bez ich gubienia (w pakietach na sekundę PPS);
- Większość sprzedawców publikuje wskaźniki PPS swoich produktów, bazując na swoich własnych oraz niezależnych testach;
- Wartości PPS dla małych ramek są znacznie wyższe niż w przypadku dużych ramek;
- Wiele urządzeń współdziałania międzysieciowego może przekazywać pakiety z teoretycznym maksimum, które jest nazywane prędkością przewodową;
- Maksimum teoretyczne obliczane jest poprzez podzielenie szerokości pasma przez rozmiar pakietu, łącznie z nagłówkiem, preambułą oraz odstępami pomiędzy ramkami, np. dla ethernetu 100 Mb/s:

rozmiar ramki	maksymalna wartość PPS
64	148800
512	23490
1024	11970
1518	8120

Zdolność przepustowa warstwy aplikacji

- Miara dobrych i użytecznych danych warstwy aplikacji przetransmitowanych w jednostce czasu;
- Czynniki wpływające na ograniczanie zdolności przepustowej warstwy aplikacji:
  - Współczynniki błędów na całej trasie;
  - Funkcje protokołów, takie jak uzgadnianie, okna i potwierdzenie odbioru;
  - Parametry protokołów, takie jak rozmiar ramki i zegary retransmisji;
  - Wskaźniki PPS i CPS dla urządzeń współdziałania sieciowego;
  - Pakiety bądź komórki utracone w urządzeniach współdziałania międzysieciowego;
  - Czynniki dotyczące wydajności stacji roboczych i serwerów:
    - Szybkość dostępu do dysku;
    - Rozmiar bufora dyskowego;
    - Wydajność sterownika urządzenia;
    - Wydajność magistrali komputera (pojemność i metody arbitrażu);
    - Wydajność procesora;
    - Wydajność pamięci;
    - Nieefektywność systemu operacyjnego;
    - Nieefektywność bądź błędy aplikacji.

Wydajność sieci - dokładność

- Celem jest, aby dane odebrane w punkcie przeznaczenia były takie same jak dane wysłane przez źródło;
- Typowe przyczyny występowania błędów w danych:
  - Przepięcia oraz nagłe skoki mocy;
  - Problemy z niezgodnością impedancji;
  - Połączenia fizyczne niskiej jakości;
  - Wadliwe urządzenia;
  - Szum spowodowany przez maszyny elektryczne;
  - Błędy w oprogramowaniu;
- Dla łączy sieci WAN cele dokładności określa się jako próg bitowego współczynnika błędu (Bit Error Rate, BER), np. dla światłowodu 1 na 10^{11}, dla kabla miedzianego 1 na 10^{6};
- Dla sieci LAN określamy współczynnik dla utraconych ramek;
- Dla ethernetu celem związanym z kolizjami pakietów jest uzyskanie mniej niż 0,1% ramek z kolizją właściwą;
- Kolizje nie powinny występować w łączu pełnodupleksowym. Jeżeli się pojawiają, świadczy to o konflikcie dupleksów;
- Dokładność może również określać, jak często sieć zmienia uporządkowanie kolejności pakietów. Korekcja uporządkowania pakietów (na poziomie protokołu) wprowadza nieznaczne spadki wydajności. Można ją badać na końcowych hostach.

Wydajność sieci - sprawność

- Jest miarą tego, jak skuteczna jest eksploatacja w porównaniu z włożonym wysiłkiem, energią, czasem i pieniędzmi;
- Określa, jak duże koszty ogólne są konieczne do osiągnięcia wymaganego wyniku;
- Sprawność sieci określa, jak duże są koszty przesłania ruchu oraz czy są one spowodowane przez kolizje, przekazywanie znacznika, raportowanie błędów, ponowny routing, potwierdzenia odbioru, duże nagłówki ramek, zły projekt sieci itd.;
- Jednym z powodów małej sprawności są duże nagłówki ramek;
- Używanie dużych ramek maksymalizuje ilość użytecznych danych w stosunku do danych nagłówka i poprawia zdolność przepustową warstwy aplikacji;
- Z drugiej strony, im większa ramka, tym większa szerokość pasma zużywana na ponowną transmisję w przypadku uszkodzenia pakietu;
- W wolnych łączach WAN czas wyprowadzenia dużej ramki jest znaczny, co generuje opóźnienie szeregowe, mające wpływ na transmisję głosu i obrazu. Rozwiązaniem jest zastosowanie ATM, albo fragmentacja w warstwie łącza oraz operacja przeplatania, np. Frame Relay FRF.12, wielopołączeniowe Frame Relay (FRF.16) oraz wielopołączeniowy PPP.

Wydajność sieci – opóźnienia i ich wahania

- Opóźnienie musi być stałe w przypadku aplikacji pracujących z dźwiękiem oraz obrazem wideo;
- Wahania opóźnień (jitter) powodują przerwy w brzmieniu głosu oraz skoki w strumieniach wideo;
- Aplikacje wykorzystujące protokół Telnet również są wrażliwe na opóźnienia (oczekiwanie na odpowiedź zwrotną);Aby ułatwić rozpoznanie, czy istnieje potrzeba projektowania sieci z niewielkimi opóźnieniami, należy ustalić, czy klient planuje wykorzystywać aplikacje opierające się o protokoły wrażliwe na opóźnienia, jak Telnet czy SNA;
- Fizyka: sygnał w przewodzie bądź światłowodzie przemieszcza się średnio z prędkością równą 2/3 prędkości światła w próżni;
- W przypadku łączy satelitarnych opóźnienia propagacji wynoszą około 260 ms dla międzykontynentalnych skoków satelitarnych.
- W przypadku przewodów naziemnych opóźnienie propagacji jest równe około 1 ms na 200 km.
- Opóźnienia szeregowe: czas wprowadzenia danych cyfrowych do linii transmisyjnej, który zależy od rozmiaru danych oraz szybkości linii, np. dla pakietu 1014 b i linii T1 o szybkości 1,544 Mb/s zajmuje około 5 ms;

Wydajność sieci – opóźnienia i ich wahania

- Opóźnienia spowodowane komutacją pakietów odnoszą się do czasu oczekiwania występującego podczas przekazywania danych przez routery i przełączniki. Zależy od szybkości obwodów wewnętrznych i CPU oraz architektury przełączania, typu pamięci RAM (DRAM, SRAM);
- Routery zazwyczaj wprowadzają większe opóźnienia niż przełączniki, ale parametr ten zależy od klasy urządzenia;
- Opóźnienia tego typu obejmują również opóźnienia związane z kolejkowaniem. Średnia liczba pakietów w kolejce do urządzenia przełączającego pakiety wzrasta wykładniczo wraz ze wzrostem wykorzystania:
  długość kolejki=wykorzystanie/(1-wykorzystanie)
- Przykład: przełącznik pakietów ma 5 użytkowników, dostarczających pakiety z prędkością 10 pakietów/s. Średnia długość pakietu to 1024 b. Przełącznik przesyła te dane poprzez łącze WAN o przepływności 56 kb/s. Wówczas:
  obciążenie = 5 * 10 * 1024 = 51200 b/s
  wykorzystanie = 51200 / 56000 = 91,4%
  średnia liczba pakietów w kolejce = (0,914)/(1-0,914) = 10,63 pakietów
- Poprawę można uzyskać zmieniając typ łącza WAN, albo bardziej złożony mechanizm kolejkowania;

Wydajność sieci – wahania opóźnień

- Jeżeli jest to tylko możliwe, należy zgromadzić dokładne wymagania klienta dotyczące wahania opóźnień;
- W przypadku klientów, którzy nie są w stanie określić dokładnych celów warto założyć, że wahania powinny być mniejsze niż 1 bądź 2% wartości opóźnienia;
- Technologią najmniej wrażliwą na opóźnienia oraz fluktuacje jest ATM (klasy usług).

Wydajność sieci – czas odpowiedzi

- Użytkownicy dostrzegają czas potrzebny na uzyskanie odpowiedzi od systemu sieciowego. Omówione wcześniej parametry są najczęściej dla klienta niezrozumiałe;
- Użytkownicy stają się nerwowi, kiedy czas odpowiedzi jest dłuższy niż 100 ms bądź 1/10 s;
- Próg 100 ms jest często wykorzystywany jako wartość zegara w przypadku protokołów oferujących niezawodne przesyłanie danych;
- Próg ten odnosi się do aplikacji interaktywnych. Dla aplikacji operujących na dużych ilościach danych, takich jak przesyłanie dużych plików czy graficznych stron internetowych, użytkownicy są skłonni czekać co najmniej 10 do 20 s;
- Jeżeli użytkownicy nie znają się na technice, należy dostarczyć im informacji odnośnie tego, jak długo trzeba czekać w zależności od rozmiarów plików i wykorzystywanych technologii

Bezpieczeństwo

- Projekt zabezpieczeń jest jednym z najważniejszych aspektów projektowania sieci przedsiębiorstwa;głównym celem wielu przedsiębiorstw jest to, aby problemy związane z bezpieczeństwem nie wpływały na zdolność firmy do prowadzenia interesów;
- Klienci zamawiający projekt sieci chcą być pewni, że ochroni on przed zniszczeniem oraz niewłaściwym wykorzystaniem danych handlowych, bądź innej własności firmy;
- Na etapie planowania należy zidentyfikować sieciowe aktywa informatyczne, które muszą być chronione, należy dokonać analizy ryzyka oraz określić wymagania dotyczące rozwoju;
- Wprowadzanie zabezpieczeń może zwiększyć koszty tworzenia i eksploatacji sieci;
- Ścisła polityka bezpieczeństwa może również wpływać na wydajność pracy użytkowników, zwłaszcza gdy konieczne jest poświęcenie łatwości obsługi na rzecz ochrony zasobów i danych;
- Źle opracowane zabezpieczenia mogą denerwować użytkowników powodując, że będą próbowali wymyślić sposoby na ich ominięcie;
- Bezpieczeństwo może mieć wpływ na rozwiązania związane z nadmiarowością sieci, jeżeli np. ruch sieciowy musi przejść przez urządzenie szyfrujące;
- Praktycznym celem jest zapewnienie takiego stanu, aby koszt poniesiony na implementację zabezpieczeń nie przewyższał kosztu powrotu do normalnego stanu w przypadkach naruszenia bezpieczeństwa;

Bezpieczeństwo – aktywa informatyczne

- Należy określić aktywa informatyczne które muszą być chronione, ich wartość oraz szacunkowe koszty powiązane ze stratą tych aktywów w przypadku naruszenia bezpieczeństwa;
- Sieciowe aktywa informatyczne obejmują: sprzęt komputerowy, oprogramowanie, aplikacje oraz dane;
- Mniej oczywista, ale równie istotna, jest własność intelektualna, sekrety handlowe oraz reputacja przedsiębiorstwa;
- Dane mogą obejmować: projekty techniczne, dokumenty planowania finansowego, informacje dotyczące stosunków z klientami, dokumenty analizujące konkurencję, informacje dotyczące konfiguracji sprzętu komputerowego oraz oprogramowania itd.;
- Urządzenia sieciowe: serwery, przełączniki, routery, firewall-e, systemy wykrywania włamań. Są one atrakcyjnym celem dla hakerów;
- Zwiększenie odporności urządzeń sieciowych wiąże się z wykonywaniem minimalnej liczby niezbędnych usług, obdarzaniem zaufaniem tylko autoryzowanych partnerów, stosowaniem bezpiecznych kanałów do zarządzania urządzeniami oraz wstawianiem łat w oprogramowaniu urządzeń;
- Aktywem może być również czas użytkownika (ataki wirusów i czas potrzebny na ich usunięcie);
- Aktywem może być również zdolność do oferowania usług klientom;
- Projektant musi współpracować z menadżerami handlowymi oraz technicznymi, aby określić, które aktywa są krytyczne dla działania firmy;

Bezpieczeństwo – analiza potencjalnych zagrożeń

- Analizowanie potencjalnych zagrożeń oraz gromadzenie informacji na temat ich prawdopodobieństwa wystąpienia oraz dotkliwości;
- Jest to proces ciągły, np. klucze szyfrujące i możliwość ich złamania;
- Analiza niebezpieczeństwa wynikającego z niepodejmowania żadnej akcji;
- Jak poufne są dane klienta?
- Jaki byłby koszt finansowy, jeżeli ktoś zdołałby uzyskać dostęp do danych i wykradł tajemnice handlowe?
- Jaki byłby koszt finansowy, gdyby ktoś zmienił dane?
- Jaki byłby koszt finansowy związany z unieruchomieniem sieci na skutek naruszenia bezpieczeństwa, co uniemożliwiłoby pracownikom wykonanie ich pracy?
- W przypadku, gdy nastąpi zachwianie przez hakera bezpieczeństwa urządzenia sieciowego, mogą nastąpić następujące zagrożenia:
  - Dane przepływające przez sieć mogą zostać przechwycone, przeanalizowane, zmienione bądź usunięte, co zagraża integralności i poufności;
  - Dodatkowe pokrewne usługi sieciowe, które opierają się na zaufaniu pomiędzy urządzeniami sieciowymi, mogą zostać narażone na niebezpieczeństwo (przekierowanie routingu);

Bezpieczeństwo – analiza potencjalnych zagrożeń

- W przypadku, gdy nastąpi zachwianie przez hakera bezpieczeństwa urządzenia sieciowego, mogą nastąpić następujące zagrożenia:
  - Hasło użytkownika może zostać ujawnione i wykorzystane do dalszych włamań, a nawet do ataków na inne sieci;
  - Konfiguracja urządzenia może zostać zmieniona tak, aby umożliwić połączenia, które nie powinny być dozwolone i uniemożliwić te, które powinny być dozwolone.
- Uniemożliwienie dostępu do łącza osobom trzecim;
- Przedsiębiorstwa powinny również rozważyć problemy powodowane przez nieporadnych bądź złośliwych użytkowników wewnętrznych (ściąganie oprogramowania z niesprawdzonych stron);
- Organizacje powinny przeprowadzać szkolenia dotyczące bezpieczeństwa oraz programy podnoszące świadomość pracowników, aby zminimalizować zagrożenie wystąpienia ataków wewnętrznych;

Bezpieczeństwo – ataki rozpoznawcze

- Ataki rozpoznawcze dostarczają informacji o potencjalnych celach oraz ich słabych punktach;
- Są najczęściej przygotowaniem do bardziej ukierunkowanych ataków na pewien wyznaczony cel;
- Napastnicy dokonujący ataków rozpoznawczych używają narzędzi służących do ustalenia osiągalności hostów, podsieci, usług i aplikacji;
- Czasami narzędzia te są bardzo wyrafinowane i mogą przebić się przez ściany ogniowe;
- W celu zdobycia informacji dotyczących sieci, napastnik może spróbować kilku metod ataku:
  - Zgromadzić informacje o konfiguracji oraz zarządzaniu siecią z rejestrów DNS;
  - Odkryć możliwości dostępu do sieci wykorzystując „war dialing” (podłączenie do komutowanych punktów dostępowych) lub „war driving” (podłączenie do bezprzewodowych punktów dostępowych);
  - Zgromadzić informacje o topologii oraz adresowaniu sieci wykorzystując narzędzie do mapowania sieci;
  - Określić osiągalność hostów, usług i aplikacji poprzez wykorzystanie skanowania za pomocą narzędzia ping oraz skanowania portów;
  - Rozpoznać system operacyjny oraz wersje aplikacji i starać się odkryć znane luki w oprogramowaniu;
  - Rozpoznać chwilowe luki utworzone w trakcie uaktualniania systemów, konfiguracji oraz wersji oprogramowania.

Bezpieczeństwo – ataki odmowy usług

- Ataki DoS wybierają jako swój cel dostępność sieci, hosta bądź aplikacji, uniemożliwiając dostęp uprawnionym użytkownikom;
- Mogą w łatwy sposób zakłócić działania biznesowe i są stosunkowo proste do przeprowadzenia;
- Obejmują: zalewanie serwerów publicznych ogromnymi ilościami żądań połączeń, co powoduje, że serwer nie reaguje na działania uprawnionych użytkowników, oraz zalewanie połączeń sieciowych ruchem losowym, czego celem jest maksymalne możliwe zajęcie szerokości pasma;
- Z uwagi na możliwość spowodowania znacznego czasu przestoju, trzeba zbadać dokładnie projektowaną sieć pod kątem odporności na tego typu ataki.

Bezpieczeństwo – wymagania dotyczące bezpieczeństwa

- Podstawowe wymagania sprowadzają się do potrzeby wypracowania i wybrania procedur oraz technologii, które zapewnią:
  - Poufność danych;
  - Integralność danych;
  - Dostępność zasobów systemowych oraz danych;
- Bardziej szczegółowe wymagania mogą obejmować jeden bądź więcej z poniższych celów:
  - Zezwolenie osobom z zewnątrz na dostęp do danych umieszczonych w sieci publicznej bądź na serwerach FTP, ale nie na dostęp do danych wewnętrznych;
  - Autoryzowanie oraz uwierzytelnianie pracowników filii przedsiębiorstwa, użytkowników mobilnych oraz telepracowników;
  - Wykrywanie intruzów i określenie stopnia dokonanych przez nich zniszczeń;
  - Uwierzytelnianie uaktualnień tablic routingu otrzymanych od wewnętrznych i zewnętrznych routerów;
  - Ochrona danych przesyłanych przez VPN do zdalnych lokalizacji;
  - Fizyczne zabezpieczenie hostów oraz urządzeń sieciowych;
  - Logiczne zabezpieczenie hostów oraz urządzeń sieciowych poprzez zastosowanie kont użytkownika z hasłem i praw dostępu do plików i katalogów;
  - Zabezpieczenie aplikacji oraz danych przed wirusami;
  - Szkolenie użytkowników i menedżerów sieci w zakresie potencjalnych zagrożeń oraz sposobów ich unikania;
  - Stosowanie praw autorskich oraz innych prawnych metod ochrony wyrobów oraz własności intelektualnej.

Łatwość zarządzania

- Klienci mają różne wymagania dotyczące łatwości zarządzania siecią. Jedni chcą wykorzystywać protokół SNTP, inni nie chcą;
- Jeżeli klient ma określone wymagania, należy je udokumentować w celu późniejszego doboru sprzętu sieciowego;
- Zarządzanie siecią powinno być upraszczane, gdyż wówczas funkcje zarządzania są łatwiejsze do zrozumienia i wykorzystania przez menadżerów sieci;
- Terminologia:
  - **Zarządzanie wydajnością.** Analizowanie ruchu i zachowania aplikacji, aby zoptymalizować sieć, wypełnić zobowiązania dotyczące poziomu obsługi i zaplanować rozszerzenia sieci;
  - **Zarządzanie uszkodzeniami.** Wykrywanie, wyodrębnianie i naprawianie problemów, zgłaszanie uszkodzeń użytkownikom końcowym oraz menadżerom, śledzenie trendów związanych z problemami;
  - **Zarządzanie konfiguracją.** Kontrolowanie, przetwarzanie, identyfikowanie i zbieranie danych pochodzących z zarządzanych urządzeń;
  - **Zarządzanie bezpieczeństwem.** Monitorowanie i testowanie polityki dotyczącej bezpieczeństwa i ochrony, utrzymywanie i przydział haseł oraz innych informacji dotyczących autoryzacji i identyfikacji, zarządzanie kluczami szyfrującymi, kontrolowanie przestrzegania zasad bezpieczeństwa;
  - **Zarządzanie rozliczaniem.** Rozliczanie wykorzystania sieci, aby rozdzielić koszty użytkowników sieci oraz zaplanować zmiany dotyczące wymagań pojemności.

Użyteczność

- Odnosi się do łatwości obsługi, z jaką użytkownicy mają dostęp do sieci i usług;
- Można zaplanować maksymalizację użyteczności poprzez zastosowanie przyjaznych użytkownikom schematów nazywania hostów oraz łatwych metod konfiguracji (DHCP), oraz dobrze dobranej polityce dotyczącej bezpieczeństwa;
- Ważny jest odpowiedni dobór rozwiązań bezprzewodowych oraz VPN w przypadku użytkowników mobilnych.

Adaptacyjność

- Na etapie projektu należy unikać przyłączania elementów sieci, które mogą w przyszłości utrudniać wdrażanie nowych technologii;
- Dobry projekt sieci może przystosować się do nowych technologii oraz zmian (nowe protokoły, nowe praktyki biznesowe, nowe cele fiskalne, nowe ustawodawstwo, i inne);
- Zdolność sieci do adaptacji wpływa na jej dostępność;
- Elastyczny projekt sieci może również dostosować się do zmiennych wzorców ruchu oraz wymagań dotyczących jakości obsługi (QoS);
- Wybrana technologia sieci LAN i WAN musi być w stanie przystosować się do nowych, rzadko podłączających się do sieci użytkowników, którzy używają aplikacji wymagających stałych prędkości bitowych;
- Kolejnym problemem jest szybkość dostosowywania się urządzeń sieciowych (przełączniki, routery) w przypadku uszkodzeń sieci, włączania się do topologii nowych sieci, reakcja na uszkodzenia łączy.

Dostępność finansowa

- Nazywana jest czasem *opłacalnością*;
- Aby projekt sieci był dostępny finansowo, powinien przenosić maksymalną ilość ruchu przy zadanych kosztach;
- Koszty obejmują jednorazowe koszty zakupu wyposażenia oraz powtarzalne koszty związane z operacjami sieciowymi;Niski koszt jest często celem w sieciach kampusowych (niski koszt przełączników w przeliczeniu na jeden port, minimalne koszty okablowania, opłaty dla dostawców usług znikome lub nieistniejące, niedrogie karty NIC dla systemów i serwerów końcowych). Niski koszt jest często ważniejszy od dostępności czy wydajności;
- W sieciach przedsiębiorstwa dostępność jest zazwyczaj ważniejsza niż niski koszt.
- Aby obniżyć koszty operacyjne sieci WAN klienci wytyczają często jeden lub kilka celów technicznych:
  - Wykorzystanie protokołów routingu, które minimalizują ruch sieci WAN;
  - Skonsolidowane równoległe łącza dzierżawione, które sprawiają, że jest mniejszy ruch na magistralach WAN;
  - Wybieranie technologii, które dynamicznie przydzielają szerokość pasma w sieciach WAN (ATM zamiast TDM);
  - Poprawianie sprawności obwodów sieci WAN poprzez wykorzystanie takich rozwiązań jak kompresja;
  - Eliminowanie słabo wykorzystywanych magistrali intersieci oraz oszczędzanie pieniędzy poprzez likwidację kosztów związanych z utrzymywaniem obwodów oraz sprzętu komputerowego obsługującego magistralę;
  - Wykorzystywanie technologii obsługujących przeciążanie sieci.

Dostępność finansowa

- Ze względu na zatłoczoną naturę ruchu opartego o ramki, suma szybkości portów dostępowych może być, w granicach rozsądku, większa niż szybkość sieci podstawowej;
- Kolejna grupa kosztów to koszt zatrudnienia, przeszkolenia i utrzymania personelu obsługującego i zarządzającego siecią. Klienci mogą oczekiwać, że na etapie projektu:
  - Zostanie wybrane wyposażenie współdziałania międzysieciowego, które będzie łatwe w konfiguracji, obsłudze, utrzymaniu i zarządzaniu;
  - Zostanie wybrany projekt sieci, który będzie prosty do zrozumienia oraz będzie zapewniał możliwość łatwej naprawy usterek;
  - Powstanie dobra dokumentacja sieci, która pomoże obniżyć czas potrzebny na naprawę usterek;
  - Zostaną wybrane aplikacje oraz protokoły sieciowe, które są łatwe w obsłudze, dzięki czemu użytkownicy będą mogli, przynajmniej do pewnego stopnia, być samowystarczalni.

Kompromisy przy projektowaniu

- Aby spełnić wysokie wymagania dotyczące dostępności, często potrzebne są nadmiarowe komponenty podnoszące koszt implementacji sieci;
- Aby spełnić rygorystyczne wymagania dotyczące wydajności, niezbędne są kosztowne obwody oraz wyposażenie;
- Ścisła polityka bezpieczeństwa wymaga zastosowania kosztownego monitoringu, a użytkownicy muszą zrezygnować z łatwości obsługi;
- Przy budowie skalowalnej sieci ucierpi dostępność;
- Zaimplementowanie dobrej zdolności przepustowej dla jednej lokalizacji może spowodować opóźnienia dla innej;
- Brak wykwalifikowanego personelu tworzy konieczność kosztownych szkoleń lub niewykorzystanie pewnych możliwości;
- Aby ułatwić analizę kompromisów, klient powinien określić jeden, główny, cel projektu sieci;
- Dodatkowo klient powinien określić priorytety dla reszty celów.

Kompromisy przy projektowaniu

- Na przykład:
  - Skalowalność 20
  - Dostępność 30
  - Wydajność sieci 15
  - Bezpieczeństwo 5
  - Łatwość zarządzania 5
  - Użyteczność 5
  - Łatwość przystosowania się 5
  - Dostępność finansowa 15
  - SUMA 100
- Sytuacja komplikuje się w sytuacji, gdy cele różnią się dla różnych części sieci przedsiębiorstwa.