Spis treści

[1. Przedstawienie i omówienie infrastruktury on-premise. 3](#_Toc137164664)

[1.1 Co to jest infrastruktura on-premise, jakie są jej zalety i wady? 3](#_Toc137164665)

[1.2. Rodzaje infrastruktury on-premise, takie jak serwery, stacje robocze, magazyny danych i urządzenia sieciowe. 4](#_Toc137164666)

[1.3 Wirtualizacja. 5](#_Toc137164667)

[1.4. Bezpieczeństwo w infrastrukturze on-premise, w tym zabezpieczenie sieci, systemów operacyjnych i aplikacji. 7](#_Toc137164668)

[1.5. Zarządzanie i monitorowanie infrastruktury on-premise, w tym narzędzia i praktyki. 8](#_Toc137164669)

[1.6. Przykłady firm i branż, które wykorzystują głównie lokalną infrastrukturę i dlaczego? 9](#_Toc137164670)

# 1. Przedstawienie i omówienie infrastruktury on-premise.

## 1.1 Co to jest infrastruktura on-premise, jakie są jej zalety i wady?

**[miejsce na topologie]**

Infrastruktura on-premise to tradycyjne podejście do zarządzania zasobami IT w organizacji, w którym wszystkie systemy informatyczne, serwery, urządzenia sieciowe, oprogramowanie oraz dane są przechowywane, zarządzane i utrzymywane na własnych serwerach wewnętrznych lub w lokalizacjach fizycznych organizacji. Jest to przeciwieństwo rozwiązań chmurowych, w których zasoby IT są przechowywane i zarządzane przez zewnętrznego dostawcę usług w chmurze.

Zalety:

* Pełna kontrola nad danymi firmy,
* Bezpieczeństwo dostosowane bezpośrednio pod organizację, większa kontrola nad bezpieczeństwem zasobów firmy,
* Infrastruktura on-premise umożliwia pełne dostosowanie systemów i oprogramowania do indywidualnych potrzeb organizacji,
* Brak opóźnień związanych z przesyłem danych przez internet.

Wady:

* Utrzymanie własnej infrastruktury IT wiąże się z większymi kosztami początkowymi oraz bieżącymi, takimi jak zakup sprzętu, oprogramowania, opłaty licencyjne czy koszty utrzymania i energii elektrycznej,
* Skalowalność wymagająca dodatkowych zakupów (w tym czasy oczekiwania na dostawy, licencje i inne tym podobne),
* Utrzymanie i wsparcie w 100% należy do właściciela,
* Odporność na awarie, zazwyczaj niższa niż w Data Center uznanego vendora chmurowego.

Podsumowując, taki rodzaj infrastruktury IT może być korzystnym rozwiązaniem dla organizacji, które wymagają pełnej kontroli nad swoimi danymi i systemami, jednak niesie to ze sobą wyższe koszty oraz posiadanie wykwalifikowanej kadry potrafiącej się odnaleźć w różnych sytuacjach i awariach związanymi z systemami.

## 1.2. Rodzaje infrastruktury on-premise, takie jak serwery, stacje robocze, magazyny danych i urządzenia sieciowe.

Rozwiązania lokalne obejmują różne rodzaje sprzętu i systemów, które umożliwiają działanie środowiska informatycznego w organizacji. Głównie są to:

* Serwery - służące do przechowywania, przetwarzania i zarządzania danymi oraz aplikacjami. Podstawa każdej infrastruktury lokalnej i zwykle są zlokalizowane w dedykowanych pomieszczeniach. Serwery mogą pełnić różne role, takie jak serwery plików, serwery baz danych, serwery aplikacji czy serwery pocztowe.
* Macierze dyskowe - dedykowane systemy przechowywania danych, które są używane do archiwizacji, tworzenia kopii zapasowych i zarządzania dużymi ilościami informacji. Magazyny danych mogą być oparte na technologii HDD, SSD lub taśmowej, a dane mogą być przechowywane w sposób zdecentralizowany lub scentralizowany, w zależności od potrzeb organizacji.
* Urządzenia sieciowe - sprzęt odpowiedzialny za komunikację pomiędzy różnymi elementami infrastruktury on-premise. Do głównych urządzeń sieciowych należą:

1. Switche - odpowiadają za łączenie różnych urządzeń w sieci LAN oraz za przekazywanie danych między nimi.
2. Routery: Routery są odpowiedzialne za kierowanie ruchu sieciowego między różnymi sieciami, w tym między siecią lokalną a Internetem. Pozwalają na łączenie ze sobą różnych urządzeń oraz zarządzanie ruchem danych w sieci.
3. Zapory sieciowe - monitorują ruch sieciowy i chronią sieć organizacji przed nieautoryzowanym dostępem i innymi zagrożeniami. Zapory sieciowe mogą być zarówno sprzętowe, jak i programowe.
4. Access pointy - umożliwiają bezprzewodowe łączenie się z siecią lokalną. Są niezbędne do tworzenia bezprzewodowej infrastruktury sieciowej.

* Systemy zasilania awaryjnego (UPS) i chłodzenia
* Narzędzia zarządzania i monitorowania
* Stacje robocze

Urządzenia te tworzą sieć lokalną (LAN, czyli kluczowy element, łączący wszystkie urządzenia, takie jak serwery, stacje robocze i urządzenia sieciowe. Typowe sieci LAN oparte są na kablu Ethernet lub bezprzewodowej technologii Wi-Fi. Architektura sieci może obejmować różne warstwy i podsegmenty, takie jak sieci VLAN, aby zwiększyć bezpieczeństwo i wydajność. Ważnym aspektem sieci jest również łącze internetowe, które umożliwia dostęp do zasobów online oraz zdalne zarządzanie infrastrukturą.

Wszystkie te elementy tworzą kompleksową infrastrukturę, która umożliwia organizacjom przechowywanie, przetwarzanie, zarządzanie i wymianę informacji oraz zasobów w sposób kontrolowany i bezpieczny. W zależności od potrzeb i wymagań organizacji, konfiguracja i skala infrastruktury on-premise może się różnić, jednak wymienione powyżej komponenty są kluczowe dla zapewnienia efektywnego środowiska IT.

## 1.3 Wirtualizacja.



(opis źródła)

Wirtualizacja jest technologią, która pozwala na tworzenie wirtualnych instancji serwerów na jednym fizycznym urządzeniu. Proces ten polega na wykorzystaniu oprogramowania zwanego Hypervisorem (Wirtualizatorem) do tworzenia, zarządzania i izolowania wirtualnych środowisk serwerowych na jednym fizycznym serwerze. Prościej mówiąc, wirtualizator dzieli serwer na małe części, z których każda wykorzystuje ustaloną wartość jego zasobów. Każde z tych wirtualnych środowisk, zwanych maszynami wirtualnymi, działa niezależnie od siebie, jakby były oddzielnymi serwerami fizycznymi. Obecnie na rynku najpopularniejsze są rozwiązania firm VMware oraz Microsoft (Hyper-V).

Zalety wirtualizacji serwerów:

* Konsolidacja serwerów: Dzięki wirtualizacji możliwe jest skupienie wielu serwerów na jednym sprzęcie. To pozwala na redukcję liczby fizycznych urządzeń w serwerowniach bądź centrach danych, co prowadzi do oszczędności kosztów związanych z zakupem, zarządzaniem i utrzymaniem sprzętu.
* Elastyczność i skalowalność. Wirtualne maszyny mogą być łatwo tworzone, uruchamiane, zatrzymywane i skalowane w zależności od aktualnych potrzeb. To zapewnia elastyczność w zarządzaniu zasobami i umożliwia łatwe dostosowanie się do zmieniających się wymagań biznesowych.
* Izolacja i bezpieczeństwo. W przypadku awarii jednej z maszyn, pozostałe mogą nadal działać niezakłócone. Izolacja ta pomaga również w zwiększaniu bezpieczeństwa, ponieważ atak na jedną maszynę wirtualną nie wpływa na inne.
* Łatwość tworzenia kopii zapasowych i przywracania. Wirtualizacja upraszcza proces tworzenia kopii zapasowych i przywracania staje się bardziej elastyczny i wydajny. Można łatwo wykonać obrazy maszyn wirtualnych i przywrócić je w razie potrzeby, co ułatwia proces zarządzania danymi i ochrony przed utratą danych.

Wady wirtualizacji serwerów:

* Wydajność. W przypadku wymagających aplikacji, które potrzebują dużej ilości zasobów, może być konieczne dokładne dostosowanie i optymalizacja wirtualizatora.
* Awaryjność. W przypadku awarii fizycznego serwera, wszystkie maszyny wirtualne działające na tym serwerze mogą zostać dotknięte. Dlatego ważne jest odpowiednie planowanie i zastosowanie wysokiej dostępności, takiej jak klastry lub replikacja, aby minimalizować ryzyko przerw w działaniu systemów.
* Konieczne jest zapewnienie odpowiedniego monitorowania, konfiguracji, skalowania i zabezpieczenia wirtualnych maszyn.
* Zależność od sprzętu. Serwery, które są wirtualizatorami wymagają odpowiednich podzespołów i infrastruktury do obsługi obciążenia. Aby uzyskać optymalne wyniki, konieczne jest zainwestowanie w odpowiednio wydajne serwery, pamięć masową i sieciowe oraz dbanie o ich zwiększanie ich wydajności w razie wzrostu ilości wirtualnych maszyn.

## 1.4. Bezpieczeństwo w infrastrukturze on-premise, w tym zabezpieczenie sieci, systemów operacyjnych i aplikacji.

Bezpieczeństwo obejmuje wiele aspektów, w tym zabezpieczanie sieci, systemów operacyjnych i aplikacji. Za zabezpieczenie sieci odpowiedzialnych jest wiele czynników, ale najważniejszymi z nich są:

* Zapory sieciowe monitorujące ruch sieciowy i chroniące sieć przed nieautoryzowanym dostępem oraz innymi zagrożeniami. Zapory sieciowe powinny być konfigurowane zgodnie z zasadą „Zero Trust”,
* Wirtualne sieci prywatne (VPN): VPN pozwala na bezpieczne łączenie się z siecią firmową przez Internet, chroniąc dane przesyłane między zdalnymi użytkownikami a siecią przed przechwytywaniem i manipulacją,
* Segmentacja sieci: Podział sieci na mniejsze segmenty (np. za pomocą sieci VLAN) może zwiększyć bezpieczeństwo, izolując różne części sieci przed potencjalnymi zagrożeniami i atakami,
* Kontrola dostępu.

Do tego dochodzą zabezpieczenia systemów operacyjnych, które wprowadzane są poprzez regularne aktualizacje (a czasami cofanie aktualizacji) wpływające na poprawę luk w systemie, oprogramowanie antywirusowe pomagające chronić system przed znanymi wirusami bądź innymi rodzajami złośliwego oprogramowania. Oprócz tego ważna jest ochrona systemów przed działaniem błędu ludzkiego. To znaczy, że dział IT odpowiedzialny za daną organizację wprowadza zasady bezpieczeństwa ograniczające uprawnienia użytkowników, wymaganie uwierzytelnień i blokadę części akcji jakie użytkownik może podjąć.

W przypadku infrastruktury lokalnej, odpowiedzialność za bezpieczeństwo sieci, systemów operacyjnych i aplikacji spoczywa głównie na organizacji. Dlatego ważne jest, aby wdrożyć odpowiednie strategie i narzędzia zabezpieczające oraz regularnie monitorować i aktualizować środowisko, aby zapewnić jego bezpieczeństwo i zgodność z obowiązującymi regulacjami. Istotnymi czynnościami jest audytowanie i monitorowanie rozwiązań IT, zabezpieczenie danych fizycznie (zabezpieczenie serwerowni w całości spada na organizacje, która dane zasoby posiada) oraz zapewnienie ciągłości działania poprzez zatrudnienie odpowiednich specjalistów potrafiących szybko reagować na incydenty związane z bezpieczeństwem, minimalizując ryzyko utraty danych, przestoju i uszkodzeń reputacji. Do czynności związanych dochodzą również dodatkowe zadania mające na celu wdrożenie polityk i procedur bezpieczeństwa związanych z urządzeniami znajdującymi się w budynku, a także zarządzanie dostępem, szyfrowanie danych i ich utylizacja.

## 1.5. Zarządzanie i monitorowanie infrastruktury on-premise, w tym narzędzia i praktyki.

Zarządzanie i monitorowanie infrastruktury IT to proces, który obejmuje kompleksowe nadzorowanie wszystkich elementów infrastruktury IT znajdującej się na terenie przedsiębiorstwa. W skład tej infrastruktury mogą wchodzić serwery, stacje robocze, urządzenia sieciowe, systemy operacyjne, aplikacje biznesowe, bazy danych i wiele innych. W jego skład wchodzą:

* Systemy monitoringu: To narzędzia, które umożliwiają śledzenie stanu poszczególnych elementów infrastruktury. Systemy te umożliwiają wykrycie problemów z wydajnością, awarii czy ataków na system. Narzędzia te analizują również wydajność poszczególnych elementów infrastruktury i pozwalają na przewidywanie potencjalnych problemów związanych z ich pracą.
* Systemy zarządzania konfiguracją: Są to narzędzia, które umożliwiają kontrolowanie i zarządzanie konfiguracją urządzeń i aplikacji, takie jak serwery, routery, czy bazy danych. Systemy te pozwalają na automatyzację procesów związanych z wdrażaniem i aktualizacją oprogramowania, co pomaga w zapewnieniu ciągłości działania systemów.
* Narzędzia do zdalnego zarządzania: To narzędzia, które umożliwiają zdalne zarządzanie i monitorowanie infrastruktury bez konieczności fizycznej obecności w biurze. Narzędzia te umożliwiają wykonywanie zadań administracyjnych, takich jak aktualizacje, tworzenie kopii zapasowych czy rozwiązywanie problemów z wydajnością.
* Narzędzia do automatyzacji procesów: To narzędzia, które umożliwiają automatyzację procesów biznesowych, takich jak tworzenie raportów, procesów sprzedaży czy wdrażania aktualizacji systemów. Narzędzia te pozwalają na zwiększenie wydajności i skuteczności procesów, a jednocześnie zmniejszenie ryzyka ludzkich błędów.

## 1.6. Przykłady firm i branż, które wykorzystują głównie lokalną infrastrukturę i dlaczego?

W dzisiejszych czasach wiele firm korzysta z różnych form infrastruktury IT, w tym zarówno lokalnych, jak i chmurowych. Jednak istnieją branże, w których infrastruktura on-premise jest nadal szeroko stosowana. Taki kierunek zostaje obrany głównie dla bezpieczeństwa i utrzymania większej prywatności danych znajdujących się na urządzeniach firmy (na przykład know-how produktu). Oto kilka przykładów branż oraz firm, które głównie wykorzystują lokalną infrastrukturę IT:

* Branża finansowa: Banki, instytucje ubezpieczeniowe i firmy inwestycyjne często mają rozległe systemy informatyczne zbudowane na infrastrukturze lokalnej. W związku z wysokimi wymogami dotyczącymi bezpieczeństwa i poufności danych, wiele z tych firm preferuje utrzymanie swojej infrastruktury wewnętrznie. Na przykład Allianz (Ubezpieczenia).
* Opieka zdrowotna: Szpitale, kliniki i firmy farmaceutyczne często wykorzystują infrastrukturę lokalną ze względu na wrażliwość danych medycznych i potrzebę szybkiego dostępu do nich. W przypadku ochrony prywatności pacjentów, wiele z tych organizacji preferuje przechowywanie danych w swoich własnych centrach danych. Na przykład Pfizer.
* Przemysł produkcyjny: Firmy z sektora produkcyjnego, takie jak producenci samochodów, elektroniki czy inne duże fabryki, często mają złożone systemy informatyczne związane z zarządzaniem łańcuchem dostaw, śledzeniem produkcji i optymalizacją procesów. Wiele z nich preferuje infrastrukturę lokalną ze względu na kontrolę nad danymi i wydajność działania systemów. Na przykład Toyota.
* Organizacje rządowe: Wiele rządowych instytucji i agencji preferuje utrzymanie infrastruktury IT wewnętrznie ze względu na bezpieczeństwo danych i kontrolę nad systemami. Dotyczy to takich dziedzin jak obrona narodowa, służby wywiadowcze, podatki czy obszar zdrowia publicznego. Na przykład placówki rządowe USA.
* Edukacja: Szkoły, uniwersytety i inne instytucje edukacyjne często wykorzystują lokalną infrastrukturę do zarządzania danymi uczniów, kadry naukowej i infrastrukturą e-learningową. Z uwagi na ochronę danych osobowych uczniów i pracowników, wielu z tych uczelni preferuje utrzymanie infrastruktury wewnętrznie. Dla przykładu WSB Merito.

Warto jednak zauważyć, że trendem ostatnich lat jest również migracja wielu firm do chmury ze względu na elastyczność, skalowalność i koszty. Dlatego w dzisiejszych tak naprawdę najpopularniejszym rozwiązaniem jest hybryda świata chmurowego z światem urządzeń on-premise, nawet tylko poprzez korzystanie z pakietu Microsoft 365 w przedsiębiorstwie (to też rozwiązanie chmurowe gdzie chociażby nie musimy utrzymywać serwera poczty lokalnie).