Politechnika Wrocławska

# Zero Trust Architecture

Ochrona Centrów Danych

Krzysztof Bocian,
Anna Płecha,
Aneta Prządka

HR EXCELLENCE IN RESEARCH

# Wprowadzenie

Terminy Zero Trust, Zero Trust Network lub Zero Trust Architecture, wymyślone przez analityka ds. bezpieczeństwa z firmy Forrester Research, odnoszą się do koncepcji bezpieczeństwa sieciowego opartego o 3 reguły:

- Nigdy nie ufaj.
- Zawsze weryfikuj.
- Ciągle monitoruj.

Zakładają one, że należy weryfikować wszystkich i wszystko nawiązujące próbę połączenia do Twoich systemów przed udzieleniem dostępu. Istnieje kilka głównych sposobów implementacji podejścia zero-trust w sieci firmowej, by umożliwić dostęp do usług i aplikacji dla wewnętrznych i zewnętrznych użytkowników – z zachowaniem kilku warstw bezpieczeństwa.



https://stinet.pl/roznorodne-koncepcje-wdrozeniowe-zero-trust-network/

# Porady/zasady modelu

- Jawna weryfikacja
- Korzystanie z dostępu z najniższym poziomem uprawnień
- Podejście “zakładanego naruszenia bezpieczeństwa”

https://www.microsoft.com/pl-pl/security/business/zero-trust

Politechnika Wrocławska

# Obszary ochrony Zero Trust

- Tożsamości
- Punkty końcowe
- Aplikacje
- Dane
- Infrastruktura
- Sieć

https://www.microsoft.com/pl-pl/security/business/zero-trust

Politechnika Wrocławska

# Przykłady

- Tradycyjne VPN
- Udostępnianie aplikacji internetowych za pośrednictwem Web Application Firewall (WAF)
- Virtual Desktop Infrastructure (VDI)
- Remote Browser Isolation (RBI)
- DMZ – Demilitarized Zones
- Content Delivery Network (CDN)
- API Gateway

https://stinet.pl/roznorodne-koncepcje-wdrozeniowe-zero-trust-network/

Politechnika Wrocławska

# Przykłady

Zgodnie z zasadą “nigdy nie ufaj, zawsze sprawdzaj” działa coraz więcej firm. Możemy ją znaleźć w takich aspektach, jak na przykład zarządzanie tożsamościami i dostępem, szacuje się także, że w ciągu najbliższych kilku lat większość firm zamiast tradycyjnego VPNa będzie korzystać z takiego opartego o zasadę Zero Trust.

Zarządzanie tożsamościami zgodnie z zasadami Zero Trust mogą odbywać się na przykład z wykorzystaniem usługi Azure AD.

Politechnika Wrocławska

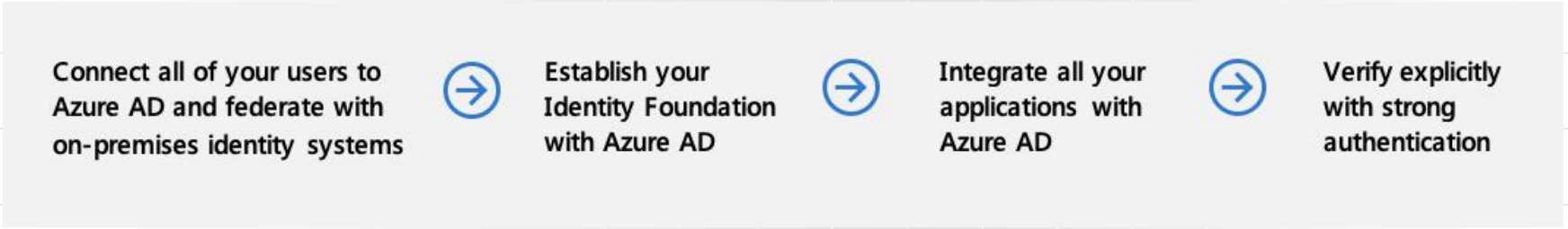
# Przykłady - Azure AD

Azure Active Directory (Azure AD) to oparta na chmurze usługa do zarządzania tożsamością i dostępem, co ułatwia pracownikom logowanie się i uzyskiwanie dostępu do zasobów:

- zasoby zewnętrzne jak usługi Microsoft 365 lub inne SaaS
- zasoby wewnętrzne firmy - aplikacje w sieci firmowej lub aplikacje chmurowe opracowane przez daną organizację.

Usługi Azure AD można użyć do wymagania uwierzytelniania wieloskładnikowego, ponadto ułatwia ochronę tożsamości i poświadczeń zgodnie z wymaganiami nadzoru nad dostępem.

# Przykłady Azure AD




https://docs.microsoft.com/en-us/security/zero-trust/deploy/identity

Politechnika Wrocławska

# Przykłady Azure AD

1. **Connect all of your users to Azure AD and federate with on-premises identity systems** - wybór opcji uwierzytelniania dostosowany do potrzeb firmy oraz przeniesienie wyłącznie tych tożsamości, które są konieczne.

2. **Establish your Identity Foundation with Azure AD** - strategia Zero Trust wymaga ciągłej weryfikacji opartej o zasadę najmniejszych uprawnień, dlatego Azure AD powinno stać na każdej ścieżce żądania dostępu i nadzorować ją.

3. **Integrate all your applications with Azure AD** - należy zintegrować wszelkie aplikacje, do których dostęp powinien być chroniony z usługą Azure AD.

4. **Verify explicitly with strong authentication** - wdrożenie Azure AD MFA oraz blokowanie starszych i mniej bezpiecznych form uwierzytelniania jako wektora potencjalnego ataku.

Politechnika Wrocławska

# Przykłady Azure AD

Ponadto możliwe jest:

- zarządzanie politykami dostępu warunkowego
- rejestrowanie urządzeń, by ograniczyć dostęp z niepożądanych źródeł
- zarządzanie tożsamościami oraz ich dostępem
- weryfikacja użytkownika, urządzenia, lokalizacji w czasie rzeczywistym w celu określenia ryzyka.

Politechnika Wrocławska

# Zalety ZTA

- Redukcja możliwych zagrożeń
- Ograniczenie ruchu atakującego pomiędzy urządzeniami w organizacji
- Ograniczenie wycieku danych
- Zwiększona kontrola dostępu
- Zwiększone bezpieczeństwo danych
- Możliwość głębokiego monitorowania

https://cybersecurity.att.com/blogs/security-essentials/what-is-a-zero-trust-architecture

Politechnika Wrocławska

# Wady ZTA

- Złożone zarządzanie użytkownikami
- Trudniejsze wdrażanie oprogramowania
- Skomplikowane wdrażanie ZTA
- Większe koszta implementacji ZTA
- Wolniejsze przetwarzanie danych
- Utrudniony dostęp do zasobów
- Model nie jest całkowicie odporny na zagrożenia z wewnątrz

Politechnika Wrocławska

# Możliwość implementacji ZTA

- Mała skala - aplikacja, jedno urządzenie
- Średnia skala - firma
- Duża skala - sieć firm lub oddziałów

Politechnika Wrocławska

# Dziękujemy za uwagę