

Zero Trust

(Architektúra nulovej dôvery)

Čo je Zero Trust?

Zero Trust (ZT) je stratégia implementácie kybernetickej bezpečnosti.

Pojem „Zero Trust“ pochádza z roku 1994 z akademickej práce „Formalising Trust as a Computational Concept“, autorom je Stephen Paul Marsh z University of Stirling

Zdroj:
<https://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf>

Je ZT koncept důležitý?



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies¹ safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public

Ochrana perimetra

„Tradičný“ prístup k bezpečnosti

Ochrana perimetra je dobrý koncept. Ale ani zďaleka nie postačujúci pre súčasné požiadavky kybernetickej bezpečnosti.

Koncept ochrany perimetra vychádza principiálne z predpokladu, že je postačujúce zabezpečiť ochranu informačných systémov a dát vo vstupnom bode. Po overení vo vstupnom bode sú aktivity (používateľa) pokladané za legitímne.

Dôležitosť ochrany perimetra stále platí. Zmena nastala v tom, že sa to už nedá chápať ako základný koncept bezpečnosti – je to len jedno z opatrení (jeden z prvkov bezpečnosti).

Chápanie ochrany perimetra je nevyhnutné zásadným spôsobom zmeniť – prispôbiť súčasným trendom a požiadavkám kybernetickej bezpečnosti a definovať nový univerzálny koncept.



O čo ide v Zero Trust?

Princípy Zero Trust

- 1 | Never Trust, Always Verify [Explicitné overenie]
- 2 | Implement Least Privilege [Princíp minimálnych privilégií]
- 3 | Assume Breach [Predpokladané narušenie (bezpečnosti)]

Zero Trust Architecture (ZTA) je architektúra kybernetickej bezpečnosti založená na princípoch *Zero Trust (ZT)*.

Never Trust, Always Verify

- “Never Trust, Always Verify” = “Verify Explicitly” = “Continuous Verification”
- Never Trust $\neq$ Don't Trust
- Autentizácia, autorizácia, mikro-segmentácia siete
- Nespoliehať sa len na predošlé overenie alebo vlastnosť subjektu (napr. „VPN používateľ“)
- Používať silné autentizačné mechanizmy
 - Dvojfaktorová autentizácia
 - Ak heslá, tak silné
- Rovnováha medzi bezpečnosťou a „použiteľnosťou“



Implement least privilege

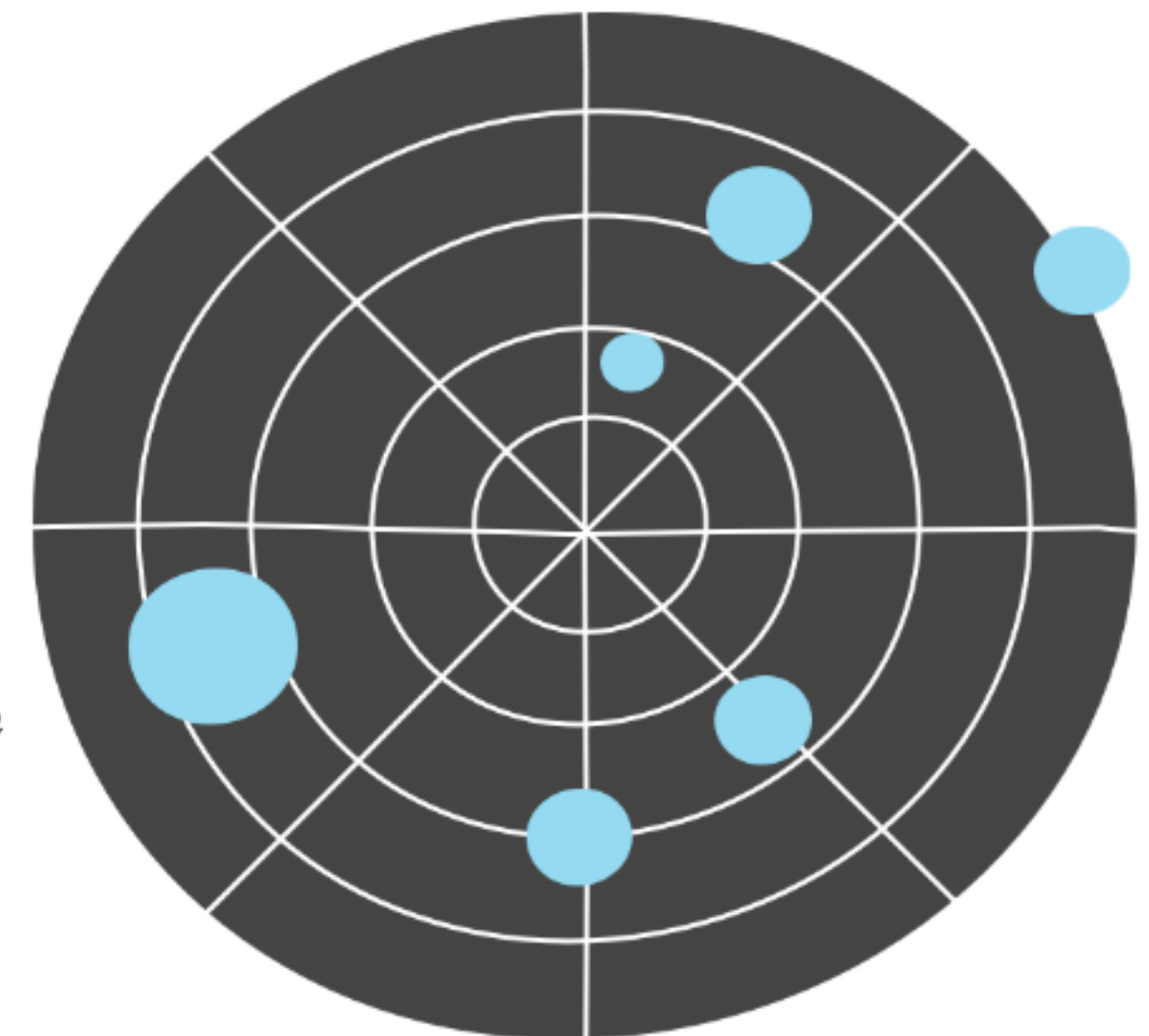
- Princíp minimálnych privilégií (na každej vrstve – používateľ, zariadenie, sw modul, atď.)
- STN EN ISO/IEC 27002: 9.2.3 Riadenie privilégií
- Cieľom je zabezpečiť, aby mohli subjekty pristupovať len k informáciám a prostriedkom, ktoré sú nevyhnutné pre dosiahnutie opodstatneného zámeru
- Podľa štatistík majú používatelia k dispozícii významne viac oprávnení ako v skutočnosti potrebujú
- Rieši sa typicky v rámci IAM projektov (procesne aj technicky)

Who are
your users?

Where is your data and
who has access to it?

Where are your
workloads running?

What endpoints and hosts are
connected to your networks?



Assume Breach

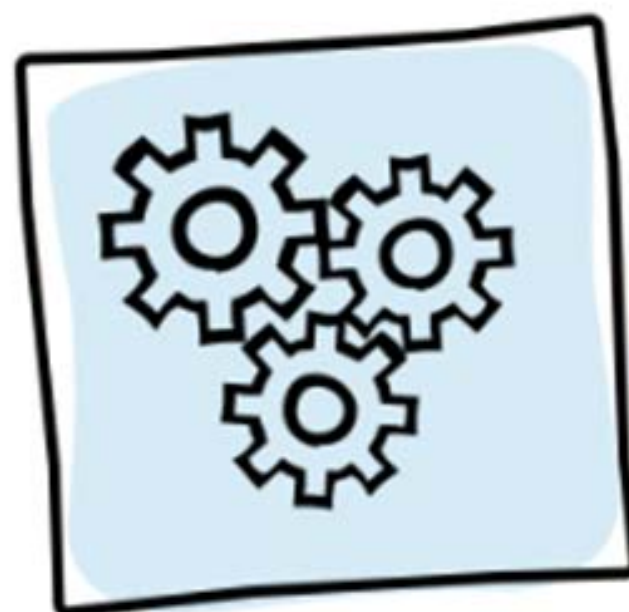
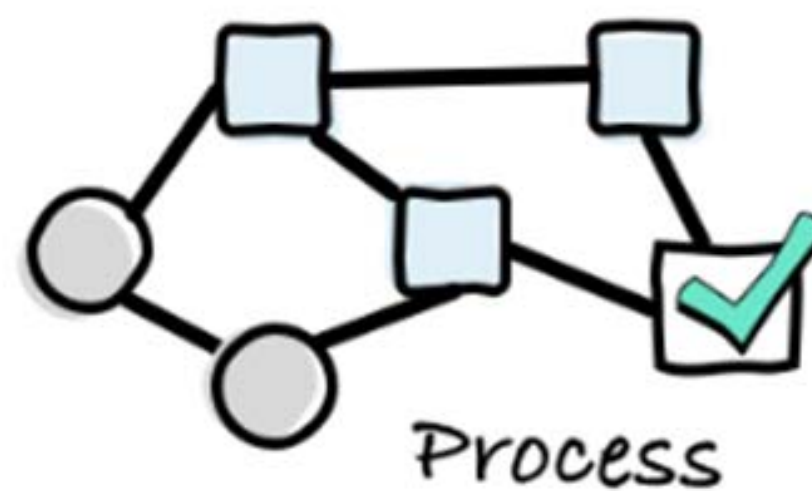
- Zmena myslenia → nepredpokladať narušenie bezpečnosti (breach) by bolo naivné
- Predpokladá, že útok môže prebehnúť, prebieha alebo prebehne
- “Prevent Breach” → “Assume Breach”
- Existencia preventívnych opatrení nie je dostačujúca
- Implementácia, kontrola a vyhodnotenie mechanizmov:
 - Protect
 - Detect
 - Response
 - Recover



Čoho sa týka Zero Trust?



People



Technology

Zero Trust nie čiernobiely

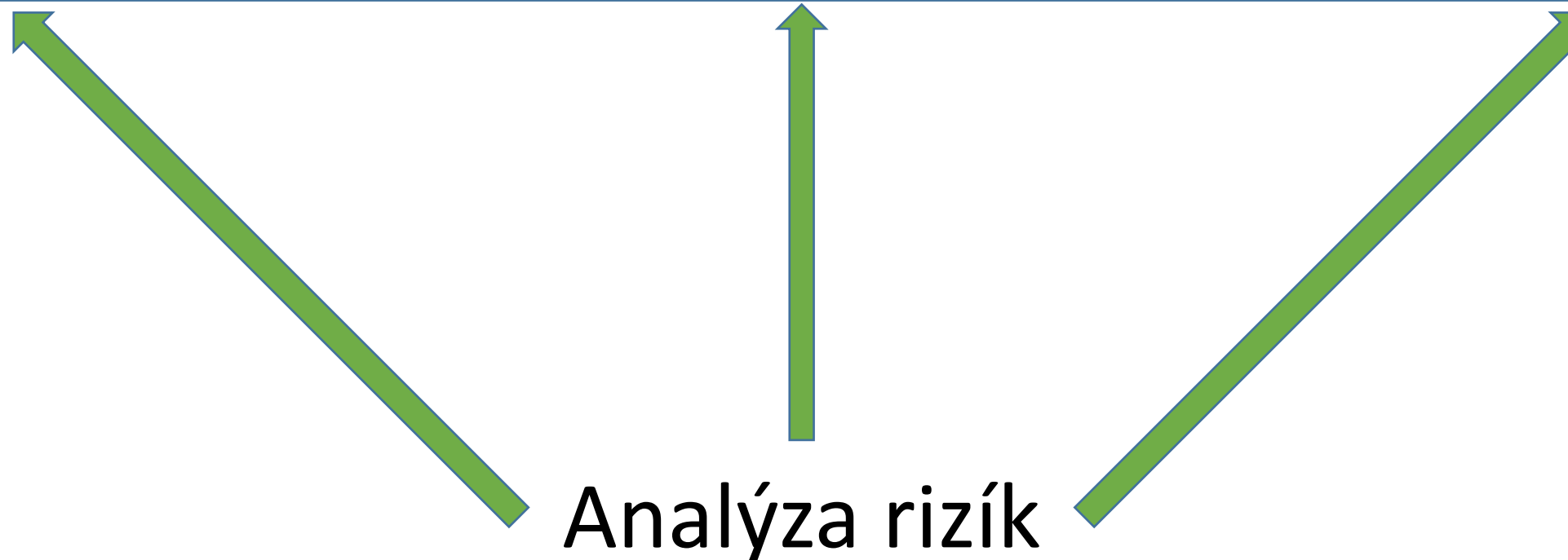
—

Implicit Trust
Trust Everything, Verify Nothing



Graded Trust

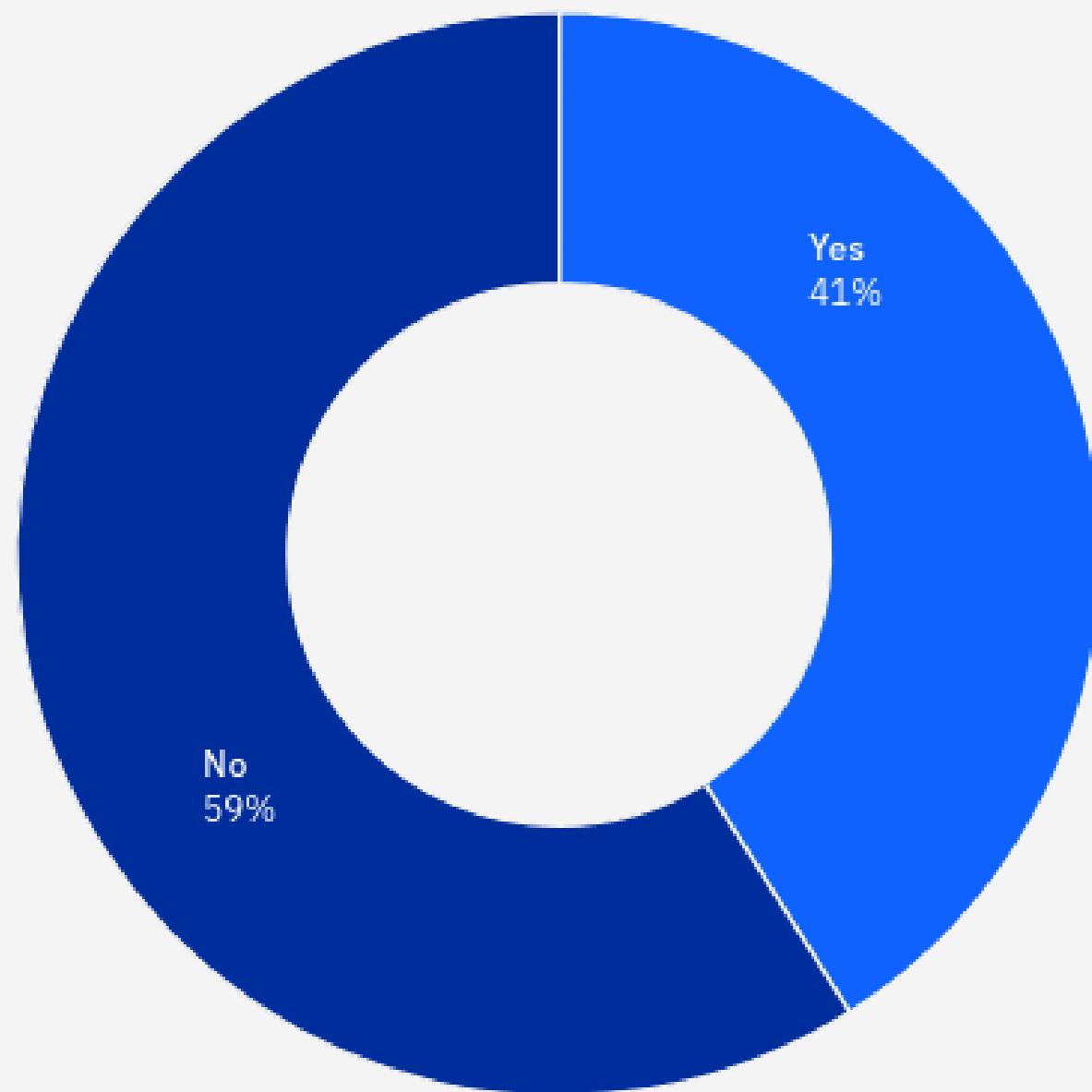
Zero Trust
Trust Nothing, Verify Everything



Analýza rizík

Vplyv ZT na náklady incidentu

Has your organization deployed a zero trust security architecture?



Average cost of a data breach by the stage of zero trust deployment

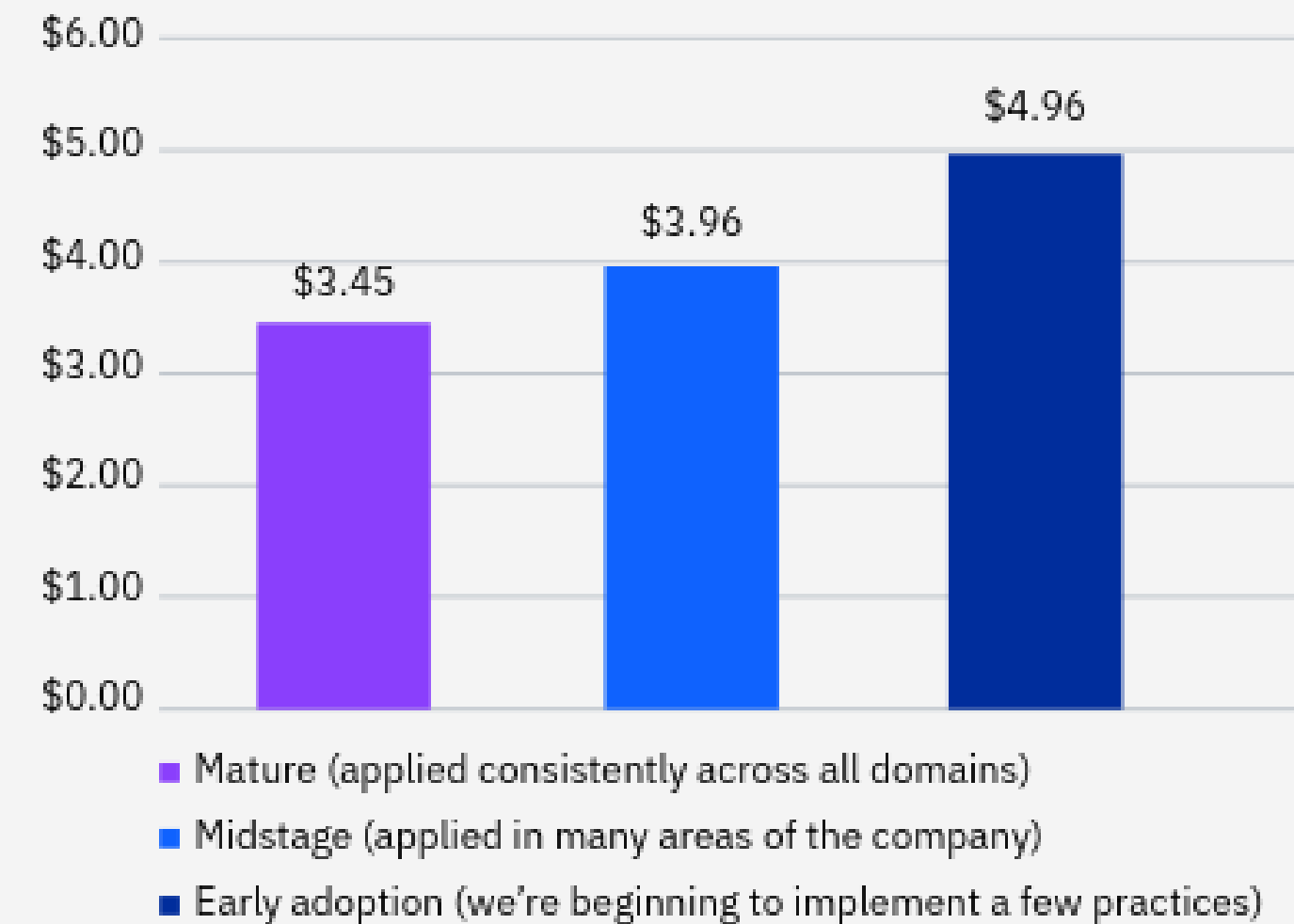


Figure 28: Measured in USD millions

Zaujímavé čítanie

NIST – Zero Trust Architecture (NIST SP 800-207)

<https://www.nist.gov/publications/zero-trust-architecture>

Zero Trust Security: An Enterprise Guide (Published by Apress)

<https://www.amazon.com/Zero-Trust-Security-Enterprise-Guide/dp/148426701X>

IBM Zero Trust Field Guide

<https://www.ibm.com/cloud/architecture/content/field-guide/zero-trust-field-guide/>

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (EXECUTIVE OFFICE OF THE PRESIDENT)

<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

Zero trust architecture design principles (UK National Cyber Security Centre)

<https://www.ncsc.gov.uk/collection/zero-trust-architecture>

Cost of a Data Breach, Report 2022

<https://www.ibm.com/security/data-breach>



Ďakujem za pozornosť

viktor_homolya@sk.ibm.com