

Zero-trust arhitektura i održivost digitalnih sistema

Zero-trust architecture and sustainability of digital systems

Srdan Mičić, Federalna uprava policije Sarajevo/Directorate of Federal Police Sarajevo

Sažetak – Razvojem informacionih tehnologija, arhitektura korporativnih digitalnih sistema također prolazi kroz duboke promjene, a granice unutar sistema između mrežnih nivoa postaju nedefinisane izazvane pojavom “cloud” tehnologija, mobilnih uređaja i rada na daljinu. Sve više kompanija zbog ekonomičnosti i bržoj dostupnosti svojim podacima, implementira cloud servere, što povećava rizik od kompromitacije podataka između “cloud” servera i interne mreže. Tradicionalni model sigurnosti zasnovan na mrežnom perimetru pokazao se nedovoljnim u navedenom okruženju. Kao odgovor na ove izazove razvijen je koncept Zero-Trust arhitekture (ZTA), koji zasniva na principu „nikada ne vjeruj, uvijek provjeri“, što bi značilo da nijedan korisnik ili uređaj ne treba automatski smatrati pouzdanim. Cilj ovog rada je analizirati osnovne principe Zero-Trust arhitekture i razmotriti njen doprinos održivosti i otpornosti digitalnih sistema. Posebna pažnja posvećena je ulozi kontinuirane autentifikacije, upravljanja korisničkim računima i mikrosegmentacije u očuvanju sigurnosti digitalne infrastrukture.

Ključne riječi – Zero Trust arhitektura, održivost digitalnih Sistema

Abstract - With the development of information technologies, the architecture of corporate digital systems has undergone significant changes, and the boundaries within systems between network layers have become increasingly blurred due to the emergence of cloud technologies, mobile devices, and remote work. An increasing number of companies, driven by cost efficiency and faster access to their data, are implementing cloud servers, which increases the risk of data compromise between cloud servers and internal networks. The traditional security model based on the network perimeter has proven insufficient in such an environment. In response to these challenges, the concept of Zero Trust Architecture (ZTA) has been developed, based on the principle “never trust, always verify,” meaning that no user or device should be automatically considered trustworthy.

The aim of this paper is to analyze the fundamental principles of Zero Trust architecture and examine its contribution to the sustainability and resilience of digital

systems. Special attention is given to the role of continuous authentication, user account management, and micro-segmentation in maintaining the security of digital infrastructure.

Keywords – Zero Trust Architecture, sustainability of digital systems

I. UVOD

Digitalni sistemi savremenog doba karakterišu kompleksne mrežne strukture, mobilni korisnici, “cloud” servisi i “remote” pristup (pristup sa udaljene lokacije). Ovakvo okruženje generiše nove bezbjednosne izazove, uključujući lateralno kretanje napadača, napade na privilegovane korisničkih računa i njihovu kompromitaciju.

Današnje aplikacije, sistemi i računarska mreža kao dio infrastrukture, moraju zadovoljiti funkciju zahtjeva krajnjih korisnika i pružiti svu potrebnu podršku radu sistema, što na prvom mjestu uključuje informacionu bezbjednost. U jednoj od definicija NIST-a (National Institute of Standards and Technology), ona predstavlja skup tehnika i metoda kojima se vrši prevencija oštećenja, informacionih, sistema i usluga uključujući i informacije sadržane u njima kako bi se osigurao njihov integritet, dostupnost i povjerljivost.

Prema izvještajima European Union Agency for Cybersecurity (ENISA), veliki procenat cyber incidenata povezan je s ljudskim faktorom, posebno kroz napade cryptolockera, phishinga i napade socijalnog inženjeringa (što direktno potvrđuje da ljudski faktor ostaje jedan od vodećih uzroka sigurnosnih povreda), cyber napadi sve češće zaobilaze tradicionalne perimetarske sigurnosne kontrole, gdje se ističe “Phishing” kao dominantan vektor upada u system (60%) i razvija se kroz tehnike koje se koriste u kampanjama velikih razmjera[1].

Koncept digitalne otpornosti razvijen je kao odgovor na potrebu organizacija da osiguraju nesmetan kontinuitet poslovanja i funkcionalnost sistema uprkos sigurnosnim incidentima. Zero-Trust pristup ima posebno važnu ulogu u kontekstu održivosti digitalnih sistema, jer omogućava

dugoročnu stabilnost i otpornost infrastrukture na cyber napade, tehničke greške i sistemske ranjivosti.

U radu će se analizirati naučna i stručna literaturea iz oblasti cyber sigurnosti, digitalne otpornosti i upravljanja informacionim sistemima. Analizirani su relevantni međunarodni standardi, istraživački radovi i izvještaji međunarodnih organizacija, uključujući dokumente koje objavljuje National Institute of Standards and Technology u vezi sa Zero-Trust arhitekturom. Pored toga, primijenjena je komparativna analiza tradicionalnog sigurnosnog modela zasnovanog na mrežnom perimetru i savremenog Zero-Trust pristupa. Analiza obuhvata ključne komponente sigurnosne arhitekture kao što su autentifikacija korisnika, upravljanje identitetom, kontrola pristupa i segmentacija mreže.

II. KONCEPT ZERO-TRUST ARHITEKTURE

Zero-Trust arhitektura predstavlja sigurnosni model koji se temelji na principu kontinuirane provjere identiteta i pristupa resursima. Za razliku od tradicionalnih modela Savremeni digitalni sistemi suočavaju se sa sve složenijim sigurnosnim izazovima koji proizlaze iz ubrzanog razvoja informacionih tehnologija, širenja cloud infrastrukture, mobilnih uređaja i rada na daljinu. U takvom okruženju tradicionalni sigurnosni modeli zasnovani na zaštiti mrežnog perimetra više ne pružaju dovoljan nivo zaštite. Zbog toga se sve veća pažnja posvećuje implementaciji koncepta Zero Trust Architecture, koji polazi od pretpostavke da nijedan korisnik, uređaj ili aplikacija ne smije biti automatski smatran pouzdanim bez prethodne provjere.

Analiza osnovnih principa Zero-Trust arhitekture pokazuje da kontinuirana autentifikacija, stroga kontrola pristupa, princip minimalnih privilegija i mikrosegmentacija mreže značajno doprinose smanjenju rizika od neovlaštenog pristupa i kompromitacije podataka. Primjenom ovih mehanizama organizacije mogu efikasnije kontrolisati pristup digitalnim resursima i pravovremeno otkriti potencijalne sigurnosne incidente.

Takođe, implementacija Zero-Trust modela ima važnu ulogu u jačanju održivosti i otpornosti digitalnih sistema. Kada gledamo na digitalnu otpornost ona podrazumijeva sposobnost sistema da:

1. Spriječi napad
2. Detektuje prijetnju
3. Odgovori na incident
4. Obnovi funkcionalnost
5. Prilagodi se budućim rizicima[2]

ZTA kroz stalni nadzor, verifikaciju identiteta i segmentaciju mrežnih resursa, organizacije postaju sposobnije da spriječe širenje napada, zaštite kritične podatke i osiguraju kontinuitet poslovanja čak i u uslovima povećanih cyber prijetnji.

Može se zaključiti da Zero-Trust arhitektura predstavlja jedan od ključnih pravaca razvoja savremene cyber

sigurnosti. Njena primjena ne samo da povećava nivo zaštite digitalne infrastrukture, već doprinosi i dugoročnoj stabilnosti, pouzdanosti i održivosti digitalnih sistema u savremenom tehnološkom okruženju koji pretpostavljaju da su korisnici unutar mreže pouzdani, Zero-Trust pristup pretpostavlja da potencijalna prijetnja može postojati bilo gdje u sistemu.

Zero-Trust nije isključivo tehnički model i njegova efikasnost zavisi od pravilne klasifikacije podataka, upravljanja identitetima, multifaktorske autentifikacije, ponašajnog nadzora korisnika, kulture odgovornosti zaposlenih. Bez razvijene sigurnosne kulture, zaposlenici mogu zaobići MFA, dijeliti lozinke ili koristiti nesigurne kanale komunikacije, čime se narušava integritet ZTA.

Prema modelu definisanom od strane National Institute of Standards and Technology, Zero-Trust arhitektura podrazumijeva sigurnosni pristup u kojem nijedan korisnik ili uređaj ne dobija implicitno povjerenje, već se svaki zahtjev za pristup resursima mora autentificirati i autorizirati[3]. Glavni principi Zero-Trust modela uključuju:

1. Verifikaciju identiteta korisnika i uređaja
2. Princip najmanjih privilegija (least privilege)
3. Kontinuirani nadzor i analizu pristupa
4. Mikrosegmentaciju mreže
5. Korištenje višefaktorske autentifikacije

Ovi principi omogućavaju kompanijama da značajno smanje prostor za napad i ograniče potencijalnu štetu u slučaju kompromitacije sistema.

III. KOMPONENTE ZERO-TRUST SISTEMA

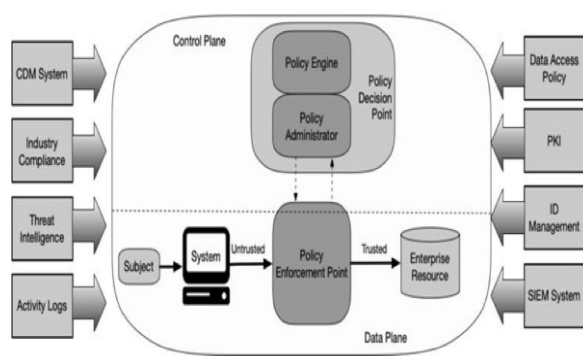
Zero-Trust predstavlja bezbjednosni model zasnovan na principu da se povjerenje ne dodjeljuje unaprijed nijednom entitetu u mreži, već se svaki zahtjev za pristup resursima mora kontinuirano verifikovati na osnovu identiteta i konteksta. U okviru Zero-Trust modela poseban naglasak stavlja se na granularniju kontrolu pristupa, autentifikaciju i autorizacijusvakog zahtjeva i transakcije, princip najmanjih privilegija i kontinuiran monitoring sistema.

Zero-Trust arhitektura sastoji se od više ključnih komponenti koje zajedno osiguravaju kontrolu pristupa i sigurnost digitalnih resursa. Najvažnije komponente uključuju logički model[4]:

1. Generator politika "Policy Engine" (komponenta koja donosi odluku o pristupu određenom resursu. Ona analizira različite informacije kao što su identitet korisnika, sigurnosne politike organizacije, stanje uređaja i druge sigurnosne signale kako bi odlučila da li će pristup biti odobren ili odbijen);
2. Administrator politika "Policy Administrator" (provodi odluku koju je donio Policy Engine.

Njegova funkcija je da uspostavi ili prekine komunikaciju između korisnika i resursa, te generiše autentifikacione tokene ili kredencijale potrebne za pristup sistemu);

3. Tačka upisivanja politika “Policy Enforcement Point” (komponenta koja tehnički sprovodi sigurnosne odluke. Ona omogućava, nadgleda i po potrebi prekida vezu između korisnika i digitalnih resursa kako bi se osiguralo da se pristup odvija u skladu sa sigurnosnim pravilima).



Slika 1. Logički model ZTA [5].

Takva arhitektura omogućava fleksibilnu i skalabilnu zaštitu digitalne infrastrukture, posebno u cloud okruženjima i distribuiranim mrežama.

IV. ZERO-TRUST I ODRŽIVOST DIGITALNIH SISTEMA

Zero-Trust i održivost digitalnih sistema je savremeni koncept u oblasti cyber sigurnosti i upravljanja digitalnom infrastrukturom. Kombinuje sigurnosni model „nultog povjerenja“ sa ciljem dugoročne stabilnosti i otpornosti digitalnih sistema. Digitalna otpornost podrazumijeva sposobnost sistema da spriječi napad, detektuje prijetnju, odgovori na incident, obnovi funkcionalnost sistema. Održivi digitalni sistemi moraju biti sposobni da funkcionišu čak i u uslovima cyber napada ili tehničkih kvarova. Zero-Trust arhitektura doprinosi digitalnoj otpornosti kroz smanjenje mogućnosti neovlaštenog pristupa, ograničavanje širenja napada unutar mreže i bržu detekciju sigurnosnih incidenata [6].

Implementacija Zero-Trust principa ima značajan doprinos i održivosti digitalnih sistema, jer omogućava veću otpornost na sigurnosne incidente, bržu detekciju prijetnji i efikasniji oporavak nakon napada. Time Zero-Trust arhitektura postaje jedan od ključnih koncepata savremene cyber sigurnosti i važan element u izgradnji stabilnih i dugoročno održivih digitalnih infrastrukture.

Istraživanja pokazuju da implementacija Zero-Trust modela može značajno smanjiti troškove sigurnosnih

incidenata i poboljšati sposobnost organizacija da odgovore na cyber prijetnje. [7]

Regulatorni okvir Evropske unije dodatno naglašava značaj otpornosti kroz Digital Operational Resilience Act (DORA), koji zahtijeva kontinuirano upravljanje ICT rizicima i testiranje operativne otpornosti.[8] Digitalna infrastruktura danas sve više zavisi od “cloud” tehnologija i distribuiranih servisa. U takvom okruženju tradicionalna sigurnosna rješenja postaju neefikasna jer se mrežni perimetar praktično gubi.

V. ODRŽIVOST DIGITALNIH SISTEMA KROZ ZERO-TRUST PRISTUP

Primjena Zero-Trust modela doprinosi održivosti sistema kroz modularnu i adaptivnu arhitekturu koja omogućava lakšu integraciju novih tehnologija i servisa. Za razliku od tradicionalnih sigurnosnih modela zasnovanih na zaštiti mrežnog perimetra, Zero-Trust pristup podrazumijeva kontinuiranu verifikaciju korisnika, uređaja i aplikacija prije odobravanja pristupa digitalnim resursima. Ovakav pristup smanjuje mogućnost neovlaštenog pristupa i povećava otpornost sistema na savremene cyber prijetnje. Prema preporukama koje je objavio National Institute of Standards and Technology, Zero-Trust arhitektura pomjera fokus zaštite sa mrežnog perimetra na identitet korisnika, uređaje i digitalne resurse, uz pretpostavku da mreža može biti kompromitovana u bilo kojem trenutku. [9]

Održivost digitalnih sistema ne zavisi isključivo od tehnoloških rješenja, već i od organizacionih i regulatornih faktora. Integracija Zero-Trust pristupa sa međunarodnim sigurnosnim standardima, kao što je ISO/IEC 27001, omogućava sistematsko upravljanje sigurnošću informacija i kontinuirano unapređenje sigurnosnih kontrola.[10] Takođe, usklađenost sa savremenim regulatornim okvirima, poput Digital Operational Resilience Act (DORA), doprinosi jačanju digitalne otpornosti organizacija i smanjenju sistemskih rizika u digitalnom okruženju[11].

Pored tehnoloških i regulatornih aspekata, važnu ulogu u implementaciji Zero-Trust modela imaju organizacione mjere kao što su upravljanje identitetima i pristupom, kontinuirana procjena rizika i edukacija zaposlenih. Kombinacija ovih elemenata omogućava organizacijama da izgrade sigurnu i održivu digitalnu infrastrukturu koja je sposobna da odgovori na savremene sigurnosne izazove i osigura dugoročnu stabilnost informacionih sistema.

VI. ZAKLJUČAK

Savremeni digitalni sistemi suočavaju se sa sve složenijim sigurnosnim izazovima koji proizlaze iz ubranog razvoja informacionih tehnologija, širenja cloud infrastrukture, mobilnih uređaja i rada na daljinu. U takvom okruženju tradicionalni sigurnosni modeli zasnovani na zaštiti mrežnog perimetra više ne pružaju dovoljan nivo zaštite. Zbog toga se sve veća pažnja posvećuje implementaciji koncepta Zero Trust Architecture, koji polazi od pretpostavke da nijedan

korisnik, uređaj ili aplikacija ne smije biti automatski smatran pouzdanim bez prethodne provjere.

Analiza osnovnih principa Zero-Trust arhitekture pokazuje da kontinuirana autentifikacija, stroga kontrola pristupa, princip minimalnih privilegija i mikrosegmentacija mreže značajno doprinose smanjenju rizika od neovlaštenog pristupa i kompromitacije podataka. Primjenom ovih mehanizama organizacije mogu efikasnije kontrolisati pristup digitalnim resursima i pravovremeno otkriti potencijalne sigurnosne incidente.

Takođe, implementacija Zero-Trust modela ima važnu ulogu u jačanju održivosti i otpornosti digitalnih sistema. Kroz stalni nadzor, verifikaciju identiteta i segmentaciju mrežnih resursa, organizacije postaju sposobnije da spriječe širenje napada, zaštite kritične podatke i osiguraju kontinuitet poslovanja čak i u uslovima povećanih cyber prijetnji.

Može se zaključiti da Zero-Trust arhitektura predstavlja jedan od ključnih pravaca razvoja savremene cyber sigurnosti. Njena primjena ne samo da povećava nivo zaštite digitalne infrastrukture, već doprinosi i dugoročnoj stabilnosti, pouzdanosti i održivosti digitalnih sistema u savremenom tehnološkom okruženju.

LITERATURA

- [1] <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- [2] ISO/IEC 27001:2022 – Information security management systems Requirements
<https://km.thainsw.net/kmdcs/images/File/ISO%2027001-2022%20rm.pdf>
- [3] Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST Special Publication 800-160, Volume 2, National Institute of Standards and Technology, Gaithersburg, 2021, <https://www.solvitursystems.com/post/understanding-nist-special-publication-800-207-the-roadmap-to-zero-trust-architecture?utm>
- [4] National Institute of Standards and Technology, Implementing a Zero Trust Architecture. (NIST Computer Security Resource Center), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-35.pdf>
- [5] S. Rose, S. Mitchell, S. Connelly, „Zero Trust Architecture“, NIST SP 800-207, 2020.
- [6] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207)*. National Institute of Standards and Technology.
- [7] Yusuf, A. M. i dr., Zero Trust Architecture as a New Paradigm in Cyber Security, Journal of Embedded Systems, Security and Intelligent Systems(https://www.researchgate.net/publication/395708909_Zero_Trust_Architecture_as_a_New_Paradigm_in_Cyber_Security)
- [8] Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA), <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>
- [9] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and TechnologyZero Trust Architecture – Principles and Implementation.
- [10] International Organization for Standardization (2022). ISO/IEC 27001: Information Security Management Systems. <https://km.thainsw.net/kmdcs/images/File/ISO%2027001-2022%20rm.pdf>
- [11] European Union (2022). Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA). <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>