Universitatea Politehnica Timișoara
Facultatea de Automatică și Calculatoare

Arhitectura Zero-Trust

Securitatea sistemelor de calcul

An universitar 2024-2025

GRIGORI DMITRII

Anul 3, secția TI
E-mail: dmitrii.grigori@student.upt.ro

Arhitectura

Definiția arhitecturii Zero-Trust

Arhitectura Zero Trust este un model de securitate cibernetică bazat pe principiul „nu avea încredere în nimeni, verifică totul”. Accesul la resursele unei organizații nu este acordat implicit nici utilizatorilor, nici dispozitivelor, indiferent dacă se află în interiorul sau în afara rețelei.

Fiecare cerere este verificată, autentificată și autorizată în mod continuu, folosind politici stricte de control al accesului și monitorizare constantă. Scopul arhitecturii este de a reduce riscul de breșe de securitate prin eliminarea presupunerii de încredere implicită.

Evoluția și necesitatea Zero-Trust

Inițial, securitatea rețelelor se baza pe perimetre clare, precum "Castle-and-moat", când accesul deplin au device-uri numai din interiorul rețelei și considerate de încredere. Odată cu creșterea mobilității, a muncii de distanță, a utilizării cloud-ului și a dispozitivelor personale (BYOD), perimetrul este dificil de protejat. Atacuri cibernetice au devenit mai sofisticate, exploatând încrederea implicită din interiorul rețelei.

Zero Trust răspunde acestor provocări eliminând încrederea implicită și tratând fiecare acces ca potențial pericol. Aceasta asigură protecție sporită împotrivă atacurilor interne și externe, reducând suprafața de atac. Este esențial pentru organizațiile moderne care folosesc servicii de cloud cu angajați mobili sau colaborează cu parteneri externi.

Compararea cu modelele tradiționale de securitate

Modele tradiționale, precum Castle and Moat, presupun următoarele:

- Existența unui perimetru de rețea clar delimitat
- Acces din exterior este restricționat, iar utilizatorii și dispozitivele din interior sunt considerați de încredere.
- Odată ce cineva a trecut de perimetru, are acces larg la resurse.
- Se bazeaza pe firewall, VPN și segmentarea rețelei

Modelul Zero-Trust presupune:

- Lipsește perimetru, fiecare cerere de acces este verificată, indiferent de locație.
- Lipsește încredere implicită pentru utilizatori sau dispozitivi, fie că este intern sau extern
- Accesul la resurse se acordă pe baza principiului „cel mai mic privilegiu” și este monitorizat continuu.

- Folosește autentificare multifactor, politici stricte de control al accesului de monitorizare permanentă.

Principii

Principiul „Nu aveți încredere, verificați întotdeauna”

„Never trust, always verify”, stă la baza arhitecturii Zero Trust. Acest principiu presupune că niciun utilizator, dispozitiv sau aplicație nu este considerat de încredere în mod implicit, indiferent dacă se află în interiorul sau în afara rețelei organizației. Fiecare cerere de acces este verificată riguros prin autentificare, autorizare și monitorizare continuă, pentru a preveni accesul neautorizat și a reduce riscul de atacuri cibernetice.

Controlul strict al accesului

„Strict access control”, este un principiu esențial în arhitectură, presupunând accesul la resurse prin acordarea doar utilizatorilor, dispozitivelor sau aplicațiilor care au nevoie, pe baza principiului „cel mai mic privilegiu”. Fiecare cerere de acces este evaluată în funcție de identitate, context și nivelul de risc, iar permisiunile sunt revizuite și actualizate constant pentru a preveni accesul neautorizat.

Monitorizarea și auditarea continuă

„Continuous monitoring and auditing”, implică supravegherea permanentă a activităților utilizatorilor, dispozitivelor și aplicațiilor pentru a detecta comportamente anormale sau potențiale amenințări de securitate. Toate acțiunile sunt înregistrate și analizate, iar alertele generate permit intervenția rapidă în cazul unor incidente. Astfel, organizația poate răspunde eficient la riscuri și poate asigura conformitatea cu politicile de securitate.

Cei 5 piloni ai arhitecturii

Identitate și acces

Se concentrează pe verificarea și gestionarea identității utilizatorilor, dispozitivelor și serviciilor care solicită acces la resursele organizației, principale aspecte fiind:

- Autentificarea puternică (multifactor) pentru a confirma identitatea fiecărui utilizator sau dispozitiv
- Autorizare granulară, acordând acces doar la resurse strict necesare
- Gestionarea identităților, prin soluții centralizate, precum IAM (Identity and Access Management de la AWS), care permit controlul și monitorizarea accesului în timp real.
- Verificarea continuă, nu doar la autentificarea ci și pe parcusul sesiunii.

Dispozitive și securitate endpoint

Se concentrează pe identificarea, monitorizarea și protejarea tuturor dispozitivelor care accesează resursele organizației, indiferent dacă sunt laptopuri, telefoane mobile sau alte echipamente. Principale aspecte includ:

- Inventarierea și gestionarea dispozitivelor – organizarea și monitorizarea tuturor dispozitivelor conectate la rețea.
- Verificarea stării de securitate – evaluarea conformității dispozitivelor cu politicile de securitatea (updates, antivirus, criptare)
- Controlul accesului pe bază de dispozitiv – permisiunea de acces la resurse doar pentru dispozitivele care respectă standardele de securitate.
- Monitorizarea și răspuns la incidente – detectarea rapidă a comportamentelor suspecte sau a amenințărilor la nivel de endpoint și reacție promptă pentru a limita impactul.

Aplicații și sarcini de lucru

Se referă la protejarea aplicațiilor, serviciilor și proceselor care rulează în infrastructura organizației, fie găzduite local, în cloud sau hibrid. Aspectele sunt:

- Controlul accesului la aplicații - permisiunea de acces doar pentru utilizatori și dispozitive autorizate.
- Segmentarea aplicațiilor și a sarcinilor de lucru – limitarea comunicării între aplicații și procese pentru a reduce riscul de propagare a unui atac.
- Monitorizarea comportamentului aplicațiilor - supravegherea continuă pentru a detecta activități neobișnuite sau potențial periculoase.
- Actualizarea și securizarea aplicațiilor - implementarea rapidă a patch-urilor de securitate pentru reducerea vulnerabilităților

Date și protecție informațională

Acest pilon se concentrează pe identificarea, clasificarea, protejarea și monitorizarea datelor organizației, indiferent unde sunt stocate sau procesate. Principale aspecte sunt:

- Clasificarea datelor – identificarea și etichetarea datelor sensibile sau critice
- Criptarea datelor – protejarea datelor atât în tranzit, cât și în repaus, pentru a preveni accesul neautorizat
- Controlul accesului la date – permisiunea de acces doar pentru utilizatorii și aplicațiile autorizate, pe baza principiului cel mai mic privelegiu
- Monitorizarea și auditarea accessului la date – supravegherea continuă a modului în care sunt accesate și utilizate datele, pentru a detecta activități suspecte sau neconforme
- Prevenirea pierderii datelor („Data Loss Prevention” – DLP), implementarea de politici și tehnologii care împedică scurgerea sau furtul de informații.

Rețea și segmentare

Se concentrează pe protejarea infrastructurii de rețea prin împărțirea acestea în segmente mai mici și controlarea strictă a traficului dintre ele. Aspectele includ:

- Segmentarea rețelei - împărțirea rețelei în zone izolate pentru a limita mișcarea laterală a atacatorilor în cazul unui incident
- Controlul traficului – aplicarea de politici stricte de acces și filtrare a traficului între segmente, pe baza identității și contextului
- Monitorizarea traficului de rețea - supravegherea continuă a comunicațiilor pentru a detecta activități neobișnuite sau potențial periculoase
- Criptarea comunicațiilor - asigurarea confidențialității și integrității datelor transmise prin rețea

Micro segmentare

Conceptul de micro-segmentare

Micro-segmentare în arhitectura Zero Trust reprezintă procesul de împărțire a rețelei în segmente foarte mici și izolate, până la nivel de aplicație, sarcina de lucru sau chiar utilizator. Fiecare segment are propriile politici stricte de acces și securitate.

Avantajele micro-segmentării în securitate

Prin utilizarea a micro-segmentării, aceasta limitează suprafața de atac, fiecare segment având politici stricte, ceea ce face mai dificilă exploatarea vulnerabilităților. Accesul este

granular, se permite definirea de reguli specifice pentru fiecare aplicație. Este posibilă izolarea rapidă a amenințărilor în cazul unui incident, precum și detectarea acestora.

Implementarea micro-segmentării în rețele complexe

Implementarea micro-segmentării presupune mai mulți pași esențiali:

- Inventarierea resurselor – identificarea tuturor aplicațiilor, dispozitivelor și fluxuri de date din rețea
- Clasificarea și gruparea – gruparea resurselor cu funcționalități sau niveluri de risc similare în segmente mici și bine definite
- Definirea politicilor de acces – stabilirea regulilor stricte de acces între segmente, pe baza principiului cel mai mic privilegiu
- Utilizarea tehnologiilor de virtualizare și SDN – folosirea a SDN (Software-defined networking), firewall-urilor de tip next-generation sau a soluțiilor de securitate la nivel de hypervisor pentru a aplica politicile de segmentare
- Monitorizare și ajustare continuă - supravegherea traficului între segmente, identificarea anomaliilor și ajustarea regulilor de acces pe măsură ce infrastructura evoluează
- Automatizare – implementarea unor instrumente de automatizare pentru gestionarea eficientă a politicilor și a segmentelor în medii mari și dinamice.

Beneficii

Reducerea suprafeței de atac

Utilizarea arhitecturii Zero Trust duce la reducerea suprafeței de atac prin aplicarea unor controale stricte de acces și verificare continuă a tuturor entităților care solicită acces la resurse deoarece nu există încredere implicită a utilizatorilor din rețea, accesul fiind acordat doar la resursele strict necesare. Rețeaua este împărțită în segmente mici și izolate, astfel încât compromiterea unui segment nu permite acces la celălalt, iar monitorizarea și auditare continuă beneficiază la detecția rapidă la comportamente anormale sau tentative de atac.

Creșterea vizibilității și controlului

Fiecare acces și acțiune este înregistrată, facilitând răspunsul rapid la incidente, iar fluxul de date poate fi urmărit pentru identificarea actorului la accesul la date.

Implementare

Pașii esențiali în adoptarea Zero-Trust

Pentru adoptarea arhitecturii Zero Trust este esențial implementarea practicilor și pilonilor descriși de mai sus, precum:

- Evaluarea infrastructurii existente
- Definirea suprafeței de protejat
- Implementarea autentificării puternice
- Aplicarea principiului cel mai mic privilegiu
- Micro-segmentarea rețelei
- Monitorizarea și auditare continuă
- Automatizarea și actualizarea politicilor

Tehnologii și instrumente necesare

Tehnologiile moderne și instrumente sunt opțiunile destul de vaste în lumea digitală cotidiană și diferențiază în scopul utilizării, precum și costul acestora. Totuși produsele importante pentru adoptarea arhitecturii Zero-Trust sunt următoarele:

- Identity and Access Management (IAM) - soluții pentru gestionarea identităților și controlul accesului (Azure, AWS, Okta)
- Autentificare multifactor (MFA)
- Single Sign-On (SSO) - simplifică și securizează accesului la aplicații multiple
- Network Access Control (NAC) - controlează accesul dispozitivelor la rețea
- Soluții de monitorizare și analiză (SIEM – Security Information and Event Management, EDR – Endpoint detection and Response) pentru vizibilitate și răspuns la incidente

Provocări în implementare și soluții

Este posibilă apariția a multitudine de provocări în implementarea acestor tehnologii, precum complexitatea infrastructurii existente, soluția fiind adoptarea treptată a Zero Trust, începând cu zone critice și automatizarea politicilor. Pentru integrația cu sisteme vechi (legacy), este posibil de folosire a gateway-uri, proxy-uri, fiind wrapper-i pentru adăugarea controale de securitate la sisteme care nu pot fi modificate.

Pentru utilizatori este important instruirea personalului și comunicarea clară a beneficiilor în utilizarea soluțiilor de autentificare precum SSO sau MFA.

Prin abordarea soluțiilor adecvate, este posibil de implementarea treptată a zonelor critice din sistem, ceea ce aduce un impact considerabil la securitatea produsului și funcționarea întregului sistem.

Exemple de implementare

Studiu de caz: implementarea Zero-Trust într-o corporație

OPSWAT este companie specializată în soluții de securitate cibernetică, recunoscută pentru produsele sale care ajută organizațiile să adopte principiile Zero Trust. Compania oferă tehnologii avansate pentru protecția infrastructurii critice, concentrându-se pe controlul accesului, inspecția fișierelor și a dispozitivelor, precum și prevenirea amenințărilor. Produsele importante care implementează o arhitectură Zero Trust, sunt următoarele:

- MetaDefender Core – permite scanarea și decontaminarea fișierelor cu peste 30 de antiviruși
- MetaAccess – verifică conformitatea dispozitivelor înainte de a permite accesul la resursele interne, prin integrare cu soluții de Single Sign-On (SSO) și Identity Providers, precum și blocare automată în cazul în care un dispozitiv devine neconform.
- MetaDefender Vault - gestionează și monitorizează transferul de fișiere între zonele de securitate, depozitarea securizată fișierelor, precum și trasabilitate crescută, prin faptul că fiecare acțiune de fișiere este înregistrată pentru audit și conformitate.

Implementarea arhitecturii Zero Trust prin produsele OPSWAT permite unei corporații să controleze riguros accesul la resurse, să prevină amenințările avansate și să asigure continuitatea operațională într-un mediu digital complex.

Bibliografie

https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-architecture

https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/zero-trust-architecture/

https://www.ibm.com/think/topics/zero-trust

https://www.cloudflare.com/learning/access-management/castle-and-moat-network-security/

https://www.microsoft.com/ro-ro/security/business/zero-trust#tabs-ocfc66_tab0

https://www.microsoft.com/ro-ro/security/business/security-101/what-is-zero-trust-architecture

https://www.opswat.com/solutions/zero-trust-access