ARCHITEKTÚRA NULOVEJ DÔVERY

Architektúra nulovej dôvery, čiže Zero Trust Architecture (ZTA) je bezpečnostný koncept postavený na princípe „nikdy dôverovať - vždy overovať".

Zahŕňa overenie identity používateľov a zariadení pred každým poskytnutím prístupu k zdrojom, bez ohľadu na to, či sa nachádzajú na vnútornej alebo vonkajšej strane sieťového perimetra.

Cieľom architektúry nulovej dôvery je lepšie chrániť zdroje pred únikmi, zneužitím a ďalšími kybernetickými bezpečnostnými hrozbami.

Pojem a koncept architektúry nulovej dôvery spopularizoval analytik Forrester Research John Kindervag v roku 2010. Výraznejší rozvoj a nasadenie nastali v ostatných rokoch, kedy vzrástla potreba nových a účinných opatrení kybernetickej bezpečnosti. Zero-trust architektúra nie je jediné izolované opatrenie, ale kombinácia bezpečnostných mechanizmov.Zero-trust architektúra nie je jediné izolované opatrenie, ale kombinácia bezpečnostných mechanizmov.

Dôležitosť nedôvery

Dôvera a dôveryhodnosť, alebo skôr nedôvera a nedôveryhodnosť, sú dnes základnými problémami informačnej a kybernetickej bezpečnosti.

Zmenou prístupu k dôvere je možné uľahčiť budovanie a údržbu sietí, dokonca urobiť ich nákladovo efektívnejšími.

V tejto problematike je základným princípom, že **už neexistujú dôveryhodné a nedôveryhodné**

- rozhrania na IT zariadeniach,
- siete,
- používatelia.

Architektúra nulovej dôvery vyžaduje, aby profesionáli v oblasti informačnej bezpečnosti považovali všetku sieťovú prevádzku zásadne za nedôveryhodnú.

Takto poňatá architektúra implicitne netvrdí, že zamestnanci sú nedôveryhodní, avšak dôveru nepovažuje za vhodný koncept, ktorý by mali bezpečnostní profesionáli uplatňovať na sieťovú prevádzku a na dáta.

Realita si vyžaduje nový prístup

Zmenou modelu dôvery sa znižuje prípadné pokušenie zlomyseľných interných používateľov. Zlepšujú sa tým aj šance na odhalenie kybernetických bezpečnostných incidentov skôr, ako by sa stali úspešné.

Architektúra nulovej dôvery pomáha chrániť organizácie pred rôznymi typmi hrozieb a vektormi útokov. V dôsledku rastu mobility a uplatnenia cloudových služieb, ktoré výrazne rozširujú perimetre sietí, sa koncept stáva čoraz dôležitejším. Umožňuje organizáciám lepšie zvládať riziká súvisiace s kybernetickou bezpečnosťou a zlepšiť si aj plnenie právnych povinností pri ochrane údajov.

Kľúčové komponenty architektúry nulovej dôvery

Správa identít a prístupov

Proces riadenia prístupov osôb k sieti a informačnému systému alebo tiež správa identít a prístupov (Identity and Access Management – IAM) je odbornou disciplínou. Umožňuje oprávneným jednotlivcom prístup k potrebným zdrojom v správny čas a z oprávnených dôvodov. Tento proces umožňuje organizácii spravovať a riadiť prístup k svojim zdrojom na základe identity používateľa. Pomáha organizácii udržiavať aktuálne informácie o používateľoch, ako sú ich roly a oprávnenia. Týmto sa znižuje riziko nedovoleného prístupu k citlivým informáciám.

Všeobecným pravidlom procesu je zásada, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie jeho zverených úloh. Tento princíp sa nazýva zásada najnižších privilégií (Principle of Least Privilege - POLP).

Mikrosegmentácia

Táto technika rozdelí sieť na menšie segmenty, aby sa znížilo riziko laterálneho šírenia incidentu naprieč celou sieťou. Umožňuje to zároveň presnejšie riadiť prístup k dôležitým zdrojom a zlepšuje sa schopnosť identifikovať a riešiť hrozby. Rozdelenie počítačovej siete pomocou adresného plánu na logické segmenty oddelí od seba navzájom dôležité časti siete. Prípadný útok sa tak obmedzí na špecifický segment siete a útočníci majú sťažený prístup do iných častí siete. Podľa všeobecnej zásady by mali mať systémy umožnené len vopred špecifikované služby. Servery so službami priamo prístupnými z externých sietí by mali byť umiestňované v samostatných sieťových segmentoch, pričom v rovnakom segmente sa majú vyskytovať len servery s rovnakými bezpečnostnými požiadavkami a podobným účelom.

Viacfaktorová autentizácia

V tomto prípade sa používajú výrazy autentizácia aj autentifikácia. Ide o overenie tvrdenia používateľa, že je držiteľom konkrétneho jedinečného identifikátora. Tento elektronický proces umožňuje potvrdiť elektronickú identifikáciu fyzickej osoby, inej entity, alebo pôvod a integritu údajov v elektronickej forme.

Každá z metód autentizácie má pri konkrétnom použití výhody aj nevýhody, pričom v praxi sa metódy často kombinujú najmä pri uplatnení viacfaktorovej autentizácie (Multi Factor Authentication - MFA).

Viacfaktorová autentizácia vyžaduje od používateľa, aby sa do systémov prihlasoval pomocou viacerých, zreťazených metód overovania. Môže to byť použitie hesla spolu s jednorazovým kódom poslaným na mobilný telefón používateľa, rôzne typy tokenov alebo biometrických údajov ako je napríklad odtlačok prsta. Týmto sa znižuje riziko útoku na heslá a zlepšuje ochrana zdrojov pred nedovoleným prístupom.

Priebežné monitorovanie a hodnotenie rizika

Kontinuálne sledovanie a hodnotenie rizika je proces, ktorý umožňuje organizácii neustále monitorovať sieť a informačné systémy a hodnotiť potenciálne bezpečnostné riziká ohrozujúce informačné aktíva.

Výhody architektúry nulovej dôvery

Zníženie komplexity

Architektúra nulovej dôvery pomáha znížiť zložitosť bezpečnostných opatrení, pretože poskytuje jednotný prístup k spravovaniu identít a prístupov, mikrosegmentácii a viacfaktorovej autentizácii. Umožňuje to zlúčiť rôzne bezpečnostné opatrenia do jedného celku a uľahčuje ich správu.

Vyššia efektivita

S uplatnením architektúry nulovej dôvery majú organizácie prístup k dôležitým zdrojom bez ohľadu na to, kde sa používatelia nachádzajú. Práca z domu alebo vzdialených lokalít má rovnakú úroveň bezpečnosti ako na pracovisku. Organizácie majú takto prístup aj ku cloudovým službám a iným externým zdrojom s vyššou mierou bezpečnosti, než je možné dosiahnuť tradičnými bezpečnostnými opatreniami.

Zlepšenie bezpečnosti

Ak sa vždy overuje identita používateľov a zariadení pred poskytnutím prístupu k zdrojom, je zaručená vyššia úroveň bezpečnosti. Týmto sa znižuje riziko úniku dát a kybernetických útokov, pretože sa zabraňuje neoprávnenému prístupu k dôležitým zdrojom.

Zvýšenie viditeľnosti a kontroly nad prístupom k zdrojom

Organizácie môžu lepšie sledovať a kontrolovať prístup k dôležitým zdrojom, čo umožňuje rýchlejšie identifikovať a pokrývať potenciálne hrozby.

Riadenie súladu

Architektúra nulovej dôvery vytvára predpoklady, aby si organizácie plnili zákonné povinnosti v oblasti informačnej a kybernetickej bezpečnosti, predovšetkým požiadaviek GDPR a Zákona o kybernetickej bezpečnosti. Lepšia kontrola nad prístupom k dôležitým zdrojom a schopnosť identifikovať a riešiť hrozby pomáha organizácii splniť požiadavky v oblasti ochrany údajov a elektronických služieb.

Ako implementovať architektúru nulovej dôvery

1. Identifikovať kritické zdroje a používateľov

Pred samotnou implementáciou je potrebné identifikovať kritické zdroje a používateľov, ktorí budú mať prístup k týmto zdrojom. Zahŕňa to určenie dôležitých aplikácií, systémov a dát, ktoré musia byť chránené, aj používateľov, ktorí budú mať prístup k týmto zdrojom.

2. Implementovať správu identít a prístupov

S úspešnou implementáciou organizácie spravujú a kontrolujú prístup k zdrojom na základe identity a príslušnej roly používateľa. Môže zahŕňať použitie centrálneho autoritatívneho zdroja používateľských údajov a oprávnení, ako aj použitie jednotného prístupu k autentifikácii a autorizácii (Single Sign-On).

3. Rozdeliť sieť na segmenty

Mikrosegmentácia je dôležitou súčasťou architektúry nulovej dôvery, pretože umožňuje organizáciám rozdeliť sieť na menšie segmenty. V tomto je zahrnuté aj použitie firewallov, virtualizácie a iných nástrojov a prvkov na ochranu siete.

4. Implementovať viacfaktorové overenie

Viacfaktorové overenie zvyšuje úroveň zabezpečenia tým, že vyžaduje od používateľa overenie identity prostredníctvom viacerých metód.

5. Priebežne monitorovať a hodnotiť riziko

Neustály monitoring siete a systémov a hodnotenie potenciálnych rizík aj použitím nástrojov na automatické detegovanie útokov sú v súčasnosti už nevyhnutné. S tým súvisí aj proces na analýzu a riadenie rizík, ktorý umožňuje organizácii zvážiť a reagovať na potenciálne hrozby v reálnom čase.

6. Testovať a validovať

Implementácia architektúry nulovej dôvery sa riebežne validuje, aby sa zabezpečilo jej správne fungovanie a aby sa zaručila ochrana dôležitých zdrojov. Preto sú nevyhnutné testovania konfigurácie siete, rôznych scenárov pre prístup k zdrojom či odolnosti voči hrozbám.

Udržiavanie a aktualizácia architektúry nulovej dôvery

Pravidelné kontroly

Pravidelné kontroly sa týkajú nastavenia siete, oprávnení používateľov a zabezpečenia zdrojov.

Aktualizácia

Aktualizácia bezpečnostných opatrení v architektúre nulovej dôvery zabezpečí, že budú stále účinné proti aktuálnym hrozbám. Či už ide softvér, firewally, sieťové segmentácie a iné nástroje na ochranu siete.

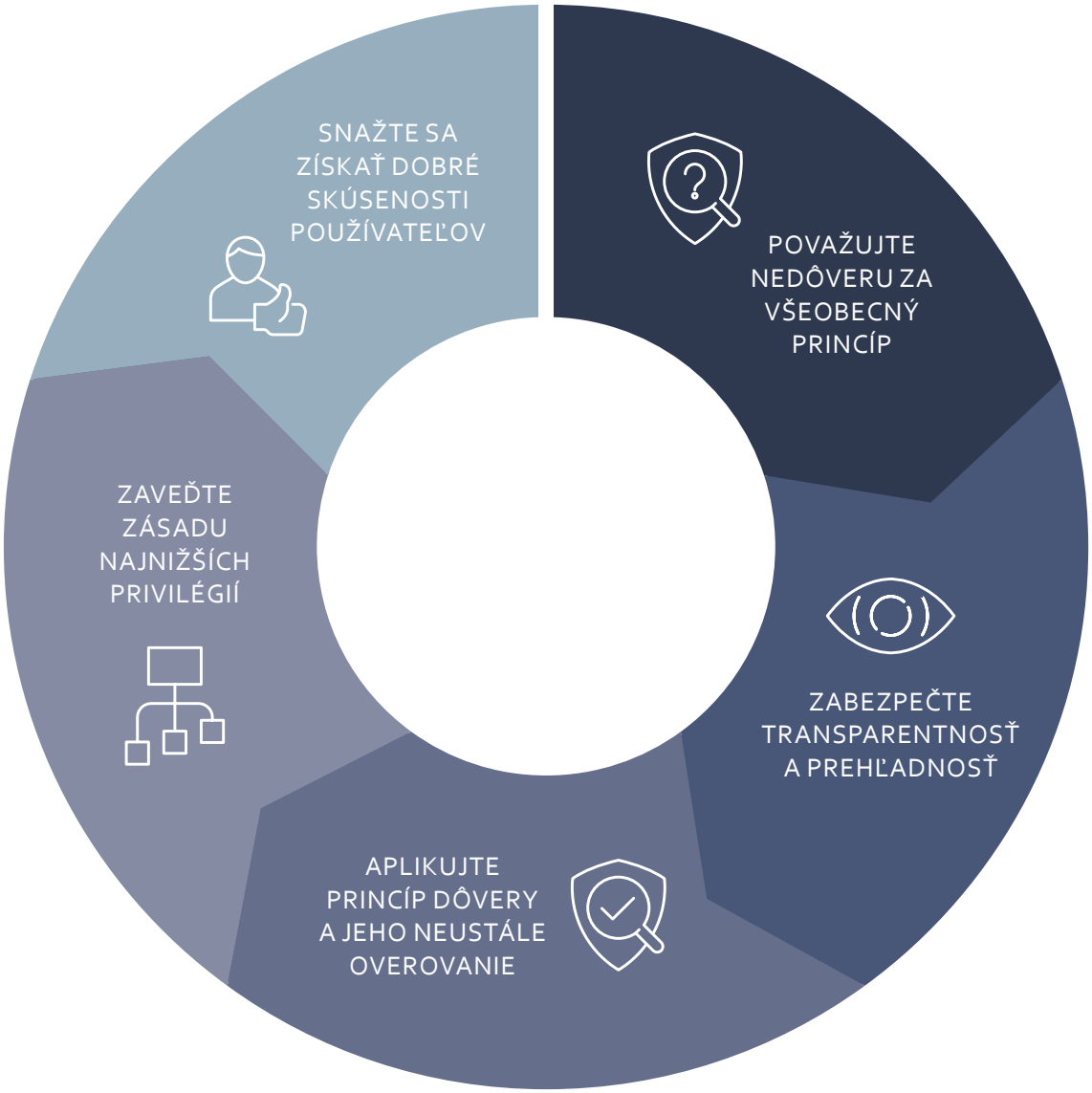
Monitorovanie

Monitoring fungovania architektúry nulovej dôvery je neoddeliteľne spojený s reakciami na akékoľvek nezrovnalosti alebo hrozby. Patrí sem monitorovanie siete na príznaky a signatúry útokov, sledovanie správy identít a prístupov, ako aj sledovanie zmien v konfigurácii siete a oprávneniach používateľov.

Školenia

Pre úspešnú implementáciu a udržanie architektúry nulovej dôvery je nevyhnutné, aby boli používatelia i administrátori dostatočne kvalifikovaní a informovaní o princípoch a postupoch v rozsahu svojich zodpovedností. Tak aby mohli využívať, podporovať a dodržiavať bezpečnostné opatrenia konceptu ako celku.

Graficky sa dá implementácia a udržiavanie konceptu ZTA v organizácii zobraziť nasledovne:



Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ISBN 978-80-69011-00-7
Verzia V.1

www.cybercompetence.sk