CISCO
SECURE

CISCO The bridge to possible

Nový normál práce

Bezpečný prístup k dátam a službám na základe identity

Karol Piling, Cisco Slovensko

ITAPA 29.11 – 1.12.2022

Posun v IT prostredí

Používatelia, zariadenia a aplikácie odkiaľkoľvek

VPN používatelia
Dodávatelia
Tretie strany

Súkromné aj mobilné zariadenia

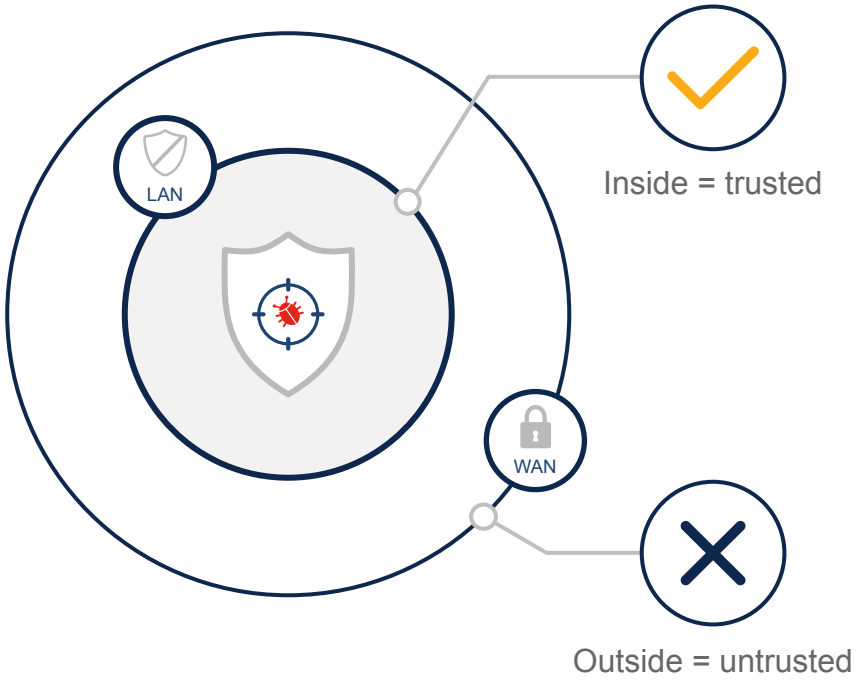
IoT zariadenia

SaaS & Cloud aplikácie

Hybridná Infraštruktúra

Cloud Infraštruktúra

Ako vyzerá bezpečnostný perimeter?



Prístup na princípe ochrany perimetru

Tento prístup k zabezpečeniu podnikových sietí predpokladal, že:

- Overenie iba na vstupe z externého prostredia je postačujúce.
- Každé koncové zariadenie je vlastnené, vydávané a spravované podnikom.
- Všetky zariadenia a aplikácie sú na známych a predvídateľných miestach, najčastejšie za firewallom.
- Zariadenia v sieti si môžu navzájom dôverovať.

Výzvy pre organizácie

Neautorizovaný prístup, identifikácia zraniteľností a medzery vo viditeľnosti

Ako vieme, že používatelia sú tie osoby, za ktoré ich naozaj pokladáme?

Sú ich zariadenia zabezpečené a aktualizované ?

Čo je pripojené do siete? Ako sa to pripojilo?

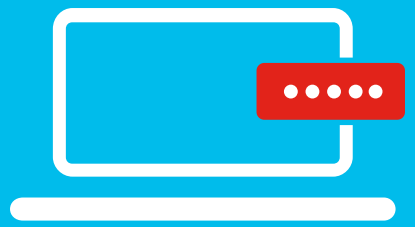
Aké dáta sú v cloud-e? Kto/čo má k dátam prístup?

Ako zabezpečiť a auditovať všetky pripojenia?

Čo existuje v cloude? Ako sa to pripája?

Dnešné hrozby ako výsledok prílišnej dôvery

Potrebujeme iný uhol pohľadu na implementáciu bezpečnosti – “dôveruj, ale preveruj”



Cieľ: Identita

81% úspešných útokov využíva kompromitované účty

Cieľ: Aplikácia

54% zraniteľností web aplikácií má verejne dostupný exploit

Cieľ: Zariadenie

300% nárast rôznych verzií malvéru cieleného na IoT

Päť základných princípov Zero Trust

- Sieť sa považuje vždy za nepriateľskú
- Hrozby existujú v rovnakej miere v internej a aj externej sieti
- O dôvernosti siete sa nemôžeme rozhodovať iba na základe lokality
- Všetky zariadenia, užívatelia a dátové toky musia byť overené a autorizované
- Bezpečnostné politiky musia byť dynamické a vzniknúť z čo najväčšieho počtu zdrojov

https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

Zero Trust

Jeden produkt

Základné piliere v architektúre Zero Trust

Všadeprítomný **least-privilege** prístup k IT aktívam spoločnosti

Potvrdenie získame overením:

- identity používateľa viacfaktorovou autentifikáciou
- identity pripájaného zariadenia jeho bezpečnostnou previerkou
- lokality pripojenia spolu s ďalšími relevantnými atribútmi

Presadzujeme prístup “least-privilege”:

- do počítačových sietí
- k špecifickým zariadeniam
- k aplikáciám
- k dátam
- bez ohľadu na fyzickú lokalitu

Neustále verifikujeme, že:

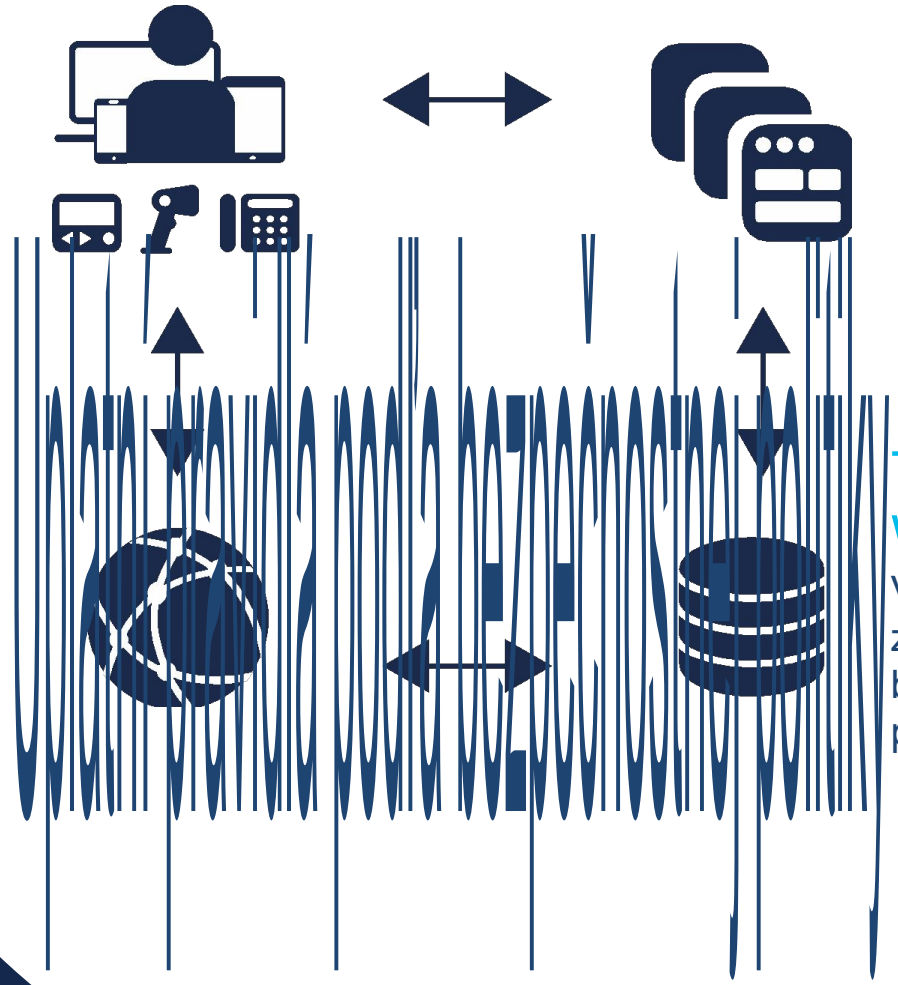
- pôvodne určujúce faktory sú stále pravdivé
- v dátových tokoch sa hrozby nenachádzajú
- neobvyklé správanie nepresahuje únosnú mieru rizika
- v prípade kompromitácie sú prístupové práva odňaté

Cisco Zero Trust

Dôveryhodný a bezpečný prístup používateľov k aplikáciám a dátam, kedykoľvek a z akéhokoľvek miesta.

Duo pre Workforce

Len dôveryhodné zariadenia a oprávnení používateľia môžu pristúpiť k IT aktívam.



SD-Access pre Workplace

Uplatní “least-privilege” prístup pre všetkých používateľov a všetky pripojené zariadenia.

Tetration pre Workload

V prístupe k aplikáciám zohľadní riziká vs. potreby biznisu, aj v amulti-cloud prostredí.

Sumár: Cisco Zero Trust a benefity pre Vás

Používateľom a zariadeniam:

- DUO pre oprávnených používateľov
- Kategorizácia zariadení pomocou DPI
- **Benefit: Viditeľnosť do IT infraštruktúry.**

Na základe úrovne dôvery:

- Pre všetkých používateľov, zariadenia aj aplikácie
- Vrátane bezpečnej segmentácie
- **Benefit: Zamedzenie neautorizovaného prístupu.**

Úroveň dôvery nie je vždy tá istá:

- Identifikácia indikácií kompromitácie a posúdenie zraniteľností
- Odňatie prístupových práv
- **Benefit: Automatická obrana proti plošnému šíreniu malvéru.**

SECURE

Ďakujem za pozornosť