Ako zvýšiť kybernetickú odolnosť pomocou riadenia prístupu?

Roman Varga,CISO

November 2023

DÔVERA ZDRAVOTNÁ POISŤOVŇA

Riadenie prístupu vs Zero Trust Architektúra(ZTA)

- Riadenie prístupu je založené na princípoch nulovej dôveryhodnosti
- Je navrhnuté tak, aby zabránila prípadnému kyber útočníkovi posun hlbšie do siete pri hľadaní citlivých údajov a iných aktív vysokej hodnoty. získavaním zvýšených privilégií pomocou rôznych nástrojov. tzv. lateral movement

DÔVERA ZDRAVOTNÁ POISŤOVŇA

Kyber odolnosť = riadenie prístupu v prevádzke

Riadenie prístupu je:

- jednou z opatrení na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti
- znamená kontrolovanie a monitorovanie toho, kto a ako môže pristupovať k informačným systémom a sieťam

Cieľom riadenia prístupu:

- je zabrániť neoprávnenému alebo nezákonnému prístupu k dôležitým údajom alebo službám

Riadenie prístupu v prevádzke pomáha zvýšiť kybernetickú odolnosť tým, že:

- zabraňuje útokom na informačné systémy a siete napr. pomocou šifrovania, politík hesiel, certifikátov
- zabezpečuje dostatočnú kontrolu nad totožnosťou a oprávnením používateľov pri prihlásení alebo autentifikácii
- umožňuje rýchle a efektívne reakcie na incidenty alebo krízy kybernetického charakteru

Pravidlá – rámec pre riadenie prístupov

8:57

Aké pravidlá platia pre riadenie prístupov?

Četbot 8:58

V spoločnosti Dôvera zdravotná poisťovňa, a.s. platia pravidlá pre riadenie prístupov, ktoré sú súčasťou bezpečnostnej politiky ICT [1][2][5]. Niektoré z týchto pravidiel sú:

1. Riadenie a správa rizík: Proces analýzy a manažmentu rizík, ktoré môžu mať vplyv na prostredie ICT, s vynaložením akceptovateľných nákladov [1].
2. Prístupové práva: Pravidlá pre priraďovanie, správu a odobratie prístupových práv pre dodávateľov a interných zamestnancov [2].
3. Kybernetická bezpečnosť: Riadenie a pravidlá týkajúce sa kybernetickej bezpečnosti, vrátane riešenia bezpečnostných incidentov a riadenia bezpečnostných rizík [3][5].
4. Bezpečnostná architektúra: Riadenie bezpečnostnej architektúry v súlade so stratégiou kybernetickej bezpečnosti [3].
5. Riadenie identít a prístupových práv: Pravidlá pre riadenie identít, prístupových práv a privilegovaných prístupov, vrátane nezlúčiteľnosti funkcií .
6. Bezpečnostný monitoring a správa záznamov: Pravidlá pre monitorovanie bezpečnosti a správu bezpečnostných záznamov .
7. Fyzická bezpečnosť a bezpečnosť prostredia: Pravidlá týkajúce sa fyzickej bezpečnosti a bezpečnosti prostredia, ako je ochrana aktív a chránených priestorov [3].
8. Pravidlá správania a dobrej praxe: Pravidlá pre správanie sa zamestnancov a dodávateľov v súvislosti s kybernetickou bezpečnosťou [5].

Interný zamestnanci – proces riadenia prístupu.

Security stratégia - Bezpečnostná politika ICT - Školenia o kyber bezpečnosti - Testy

- Prax: v prípade nových zamestnancov títo majú pridelený PC len s prístupom na intranet a mail a do doby úspešného ☺ vykonania e-learningu kyber bezpečnosti **nebudú mať sprístupnené IS**. Proces je naviazaný na IDM (naviazané na AD).
- V prípade ostatných zamestnancov: v prípade nevykonania vzdelávania, budú im prístupy do IS odobrané.
- Zodpovednosť za „tlak“ na zamestnancov majú aj ich manažéri, service desk a manažér kyber bezpečnosti ako aj kontrolný systém pridelených prístupov počas životného cyklu.
- Samozrejme ak zamestnanec končí v pracovnom pomere tak sa mu okamžite po ukončení odoberú prístupy. Všetko je riadené cez service desk a interný IS (Proces nástup-výstup zamestnanca plus Audit).
- Privilegované účty majú svoje pravidlá v bezpečnostnej politike a sú pod auditom. SIEM, security operation tím ako aj architekti v návrhu riešení tvoria pomyselný dáždnik, ktorý sa stále ladí. Končí to penetračnými testami.

Dodávateľské vzťahy - – proces riadenia prístupu.

- Prístupy pre používateľov dodávateľských spoločností je možné zriadiť len v prípade ak existuje medzi spoločnosťou a príslušným dodávateľom písomná zmluva o spolupráci (o ochrane dôverných informácií, o dielo, o službách a atď.) s príslušnými ustanoveniami o mlčanlivosti, ochrane osobných údajov a povinnosti dodržiavať BP ICT dodávateľom.

- Žiadosti o prístupy osôb do ICT/IS spoločnosti v mene dodávateľských subjektov sú posudzované individuálne a schvaľuje ich riaditeľ úseku IT a CISO.

- Prístupy tretích strán sú prideľované iba v nevyhnutnom rozsahu a čase pre plnenie zmluvných záväzkov. Všetky tieto prístupové práva sú evidované a monitorované. Prístup je riadení cez Jump server.

- Dodávatelia (sprostredkovatelia podľa GDPR) prechádzajú prísnym auditom ISO/IEC 27k – vlastná metodika, kde spolupracuje DPO a CISO

https://www.linkedin.com/in/varga-roman-55815539/

Q & A

Zdroj informácií

(1) Gartner Predicts 10% of Large Enterprises Will Have a Mature and .... https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026.

(2) How to Get Started with Zero Trust Security - Gartner. https://www.gartner.com/smarterwithgartner/new-to-zero-trust-security-start-here.

(3) 2023 Strategic Roadmap for Zero Trust Security Program ... - Gartner. https://www.gartner.com/en/documents/4268799.

(4) Gartner Predicts Big Zero Trust Uptake, but Most Won't Benefit. https://virtualizationreview.com/articles/2022/06/23/gartner-predictions.aspx.

(5) Zero Trust Security Gartner - Security Service Edge. https://www.security-service-edge.org/zero-trust-security-gartner/.

https://is.muni.cz/th/rrj0o/ParadigmInPsychology.doc

https://www.linkedin.com/feed/update/urn:li:activity:7111675687324819456/

StrategiaKybernetickejBezpecnosti2021g.indd (gov.sk)

Odborne-stanovisko-IT-Asociacie-Slovenska-k-vladnemu-navrhu-zakona-o-kybernetickej-bezpecnosti.pdf (itas.sk)

Novela zákona o kybernetickej bezpečnosti | isamosprava.sk

https://www.cloudflare.com/

Chat GPT