Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

NCC-SK
SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Bezpečnosť dodávateľského reťazca, riadenie súladu, audit a kontrola.

JUDr. Štefan Pilár

18. november 2025

POVINNOSTI PZS A TRETÍCH STRÁN

Povinnosti PZS a tretích strán

- **Tretia strana** = poskytovateľ činností **priamo súvisiacich s dostupnosťou, dôvernosťou a integritou** prevádzky **sietí a informačných systémov** prevádzkovateľa základnej služby

alebo inými slovami

- **Tretia strana** = dodávateľ na výkon činností, ktoré **priamo súvisia s prevádzkou sietí a informačných systémov** prevádzkovateľa základnej služby



Spolufinancovaný Európskou úniou

Povinnosti PZS a tretích strán

- [*PZS*] uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
- [*PZS*] vykonať analýzy rizík pred uzatvorením zmluvy
- [*Tretia strana*] vykonávať a realizovať bezpečnostné opatrenia podľa zmluvy a „tohto" zákona
- [*Tretia strana*] podrobiť sa kontrole plnenia opatrení zo strany PZS
- [*Tretia strana*] dodávatelia kritických PZS sa musia podrobiť kontrole plnenia opatrení zo strany NBÚ
- [*Tretia strana*] dodávatelia kritických PZS majú pri výkone kontroly NBÚ má postavenie PZS
- [*PZS*] kritická PZS musia nahlásiť svoje tretie strany NBÚ

VÝNIMKA Z POVINNOSTI UZATVORIŤ ZMLUVU S TREŤOU STRANOU

Výnimka z povinnosti uzatvoriť zmluvu

- [*§ 19 ods. 3 Zákona*] *Povinnosť uzatvoriť zmluvu podľa odseku 2* ***neplatí****, ak je* ***tretia strana prevádzkovateľom základnej služby****, alebo ak je* ***riziko*** *vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany* ***nízke****.*

Výnimka

- Tretia strana = **PZS**
- Tretia strana = **PDS**
- Riziko činnosti = **nízke**



ANALÝZA RIZÍK TRETEJ STRANY

Analýza rizík tretej strany

Spôsob výkonu:

- Metodika analýzy rizík tretej strany
  - použiť metodiku, ktorú má organizácia osvojenú v procesoch riadenia rizík
  - zabezpečenie opakovateľnosti a porovnateľnosti výsledkov
  - metodika NBÚ, príp. iný štandardizovaný rámec (ISO 27005, NIST SP 800-30)
- Špecifický kontext rizík vyplývajúcich zo vzťahu s treťou stranou (rozsah, aktíva, hrozby, zraniteľnosti, dopady...)

Analýza rizík tretej strany

- **Identifikácia aktív**, na ktoré môže mať zmluva s treťou stranou dopad (služby, informácie, infraštruktúra, ale aj dobré meno organizácie)
- **Identifikácia hrozieb** aplikovateľných pre vzťah s treťou stranou (podmnožina katalógu hrozieb)
- **Identifikácia zraniteľností** zneužiteľných v dôsledku využitia tretej strany (interné aj externé v procesoch a systémoch tretej strany)
- **Zistenie existujúcich bezpečnostných opatrení prijatých u tretej strany** -> kritická aktivita!
- **Identifikácia scenárov rizík** (sled alebo kombinácia udalostí vedúcich od počiatočnej príčiny k nežiaducemu následku)
- **Vyhodnotenie scenárov rizík** v zmysle metodiky (napr. kvalitatívnou, príp. semikvantitatívnou formou)

Spolufinancovaný Európskou úniou

OBSAHOVÉ NÁLEŽITOSTI ZMLUVY S TREŤOU STRANOU

Obsahové náležitosti zmluvy s treťou stranou

- [*§ 7 ods. 2 Vyhlášky č. 227/2025 Z. z.*] **Zmluva podľa § 19 ods. 2 zákona obsahuje <u>najmä</u>**
  - záväzok dodávateľa na výkon činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby
  - vyjadrenie súhlasu tretej strany s uvedenými bezpečnostnými politikami
  - ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u tretej strany
  - ustanovenie o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení



Obsahové náležitosti zmluvy s treťou stranou

VZOR zverejnený NBÚ



Obsahové náležitosti zmluvy s treťou stranou

PLUS

- súčasťou zmluvy podľa § 19 ods. 2 zákona sú **bezpečnostné požiadavky špecifické pre** („*dotknuté*“) **informačné a komunikačné technológie** alebo **operačné technológie**
- **celý dodávateľský reťazec**
- **najmenej raz za dva roky monitorované, preskúmavané, vyhodnocované a riadené zmeny v postupoch a v poskytovaní služieb alebo iných činností tretích strán**



PRECHODNÉ USTANOVENIA

RIADENIE DODÁVATEĽOV PODĽA VYHLÁŠKY č. 227/2025 Z. z.

- [*§ 8 Vyhlášky č. 227/2025 Z. z.*] Zmluva podľa § 19 ods. 2 zákona uzatvorená do 31. augusta 2025 ostáva v platnosti **najneskôr do doby pôvodne v nej dohodnutej**; túto dobu nemožno po 31. auguste 2025 predĺžiť, **ak už uzatvorená zmluva nie je v súlade s bezpečnostnými opatreniam**i podľa § 3 až 7. Týmto ustanovením nie je dotknutý § 34b ods. 5 zákona.



ZÁVER

Ďakujeme za Váš čas

- Nasledujúci webinár na tému „ Fyzická bezpečnosť, bezpečnosť prostredia a správa koncových zariadení. Ochrana proti škodlivému kódu a nežiaducemu obsahu.“ 9.12.2025



NCC-SK

SLOVAKIA CYBERSECURITY COORDINATION CENTRE



Financované Európskou úniou

Vyjadrené názory a postoje sú názormi a vyhláseniami autorov a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za nich nepreberajú žiadnu zodpovednosť.

Ochrana vlastníckych práv

Všetky autorské práva k tomuto dokumentu sú vyhradené pre Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (ďalej len „KCCKB“). Autorské práva k tomuto dokumentu má a autorské práva k tomuto dokumentu vykonáva KCCKB.

Vlastnícke práva tretích strán

Všetky ochranné známky a iné obdobné právne chránené označenia spomenuté v tomto dokumente sú výhradným vlastníctvom ich vlastníkov, ktorí sú, pokiaľ sa nejedná o KCCKB, v dokumente označení vo forme príslušnej citácie.

Akékoľvek kopírovanie či iné neoprávnené použitie celého dokumentu alebo jeho časti, v elektronickej alebo listinnej podobe, bez predchádzajúceho písomného súhlasu jeho autorov, napr. KCCKB, je zakázané. Porušenie vlastníckych a iných súvisiacich práv bude riešené v zmysle právnych predpisov Slovenskej republiky.

Limity informácií

Informácie obsiahnuté v tomto dokumente sú poskytované iba na informačné účely a bez akejkoľvek záruky, výslovnej či implicitnej. Názov KCCKB, logo KCCKB a ďalšie produkty a služby KCCKB sú ochrannými známkami KCCKB. Ostatné názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami, alebo značkami služieb iných organizácií.