**Žiadosť o vykonanie auditu**

kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z.



Dátum: 18. 11. 2021 **|** Služba: Audit kybernetickej bezpečnosti **|** Verzia 1.0

Černyševského 10 **|** 851 01 Bratislava **|** info@istrosec.com **|** www.istrosec.com

|  |  |
| --- | --- |
| **Identifikácia prevádzkovateľa základnej služby** | |
| **Názov organizácie:** |  |
| **IČO:** |  |
| **Sektor:** |  |
| **Podsektor:** |  |
| **Certifikát ISO 27001:** | áno/nie |
| **Je k dispozícií správa z predchádzajúceho auditu kybernetickej bezpečnosti?** | áno/nie |
| **Vyskytol sa od posledného auditu kybernetický bezpečnostný incident?** | áno/nie |
| **Bola vám uložená pokuta za porušenie povinností podľa zákona č. 69/2018 Z. z.?** | áno/nie |
| **Počet zamestnancov:** |  |
| **Adresa:** |  |
| **Kontaktná osoba:** |  |
| **email:** |  |
| **telefón:** |  |
| **Identifikácia (zoznam) základných služieb podporených auditovanými informačnými systémami a sieťami** | |
|  | |
|  |
|  |
| **Zoznam informačných systémov** | |  |
| **(V prípade viacerých IS nakopírujte tento blok viackrát)** | |  |
| **Názov IS:** |  |  |
| **Klasifikácia IS podľa Prílohy č. 2 k vyhláške č. 362/2018 Z. z.:** |  |  |
| **Identifikácia organizačných útvarov:** |  |  |
| **Počet zamestnancov zodpovedných za prevádzku IS:** |  |  |
| **Rozsah pri externom zabezpečovaní činností správy v ČD:** |  |  |
| **Identifikácia kľúčových dodávateľov:** |  |  |
| **Názov základnej služby, ktorá je závislá od informačného systému:** |  |  |
| **Vplyv výpadku informačného systému na základnú službu:** |  |  |
| **Počet používateľov základnej služby:** |  |  |
| **Teritoriálne rozloženie:** |  |  |
| **Dôsledky výpadku na používateľov:** |  |  |
| **Prílohy:** | |  |
| a) identifikácia kľúčových dodávateľov a zmlúv a dohôd o úrovni poskytovaných služieb | |  |
| b) schéma sieťovej architektúry s uvedením miest prepojení sietí a pripojenia voči externým sieťam | |  |
| c) zoznam aktív a používaných technológií so závislosťami od iných informačných systémov a služieb dodávateľov s uvedením vlastníkov týchto aktív a identifikáciou citlivosti podľa osobitného predpisu | |  |
| d) organizačné útvary a počty zamestnancov prevádzkujúcich informačné systémy a siete vrátane počtu dodávateľov; pri prítomnosti zamestnancov dodávateľa na pracovisku prevádzkovateľa počas auditu sa lokality dodávateľov nezapočítavajú, | |  |
| e) správa z posledného penetračného testovania informačného systému, použitá metodika a rozsah testovania a doloženie kvalifikácie zamestnancov vykonávajúcich penetračné testy, ak sú penetračné testy vykonané | |  |
| f) evidencia záznamov o kybernetických bezpečnostných incidentoch s vplyvom na poskytovanie základných služieb od doby vykonania posledného auditu alebo za posledné dva roky pri prvom audite | |  |
| g) rozhodnutie o uložení pokuty na úseku kybernetickej bezpečnosti, ak bola uložená, a ďalšie prípady porušenia povinností podľa zákona, ak k porušeniam došlo | |  |
| h) bezpečnostná dokumentácia podľa § 20 ods. 5 zákona alebo osobitného predpisu | |  |
| i) číslo platného potvrdenia o priemyselnej bezpečnosti, ak je vydané | |  |

**O spoločnosti ISTROSEC**

IstroSec je etickou spoločnosťou, ktorá vykonáva svoje podnikateľské aktivity čestne, apoliticky, priamo a spravodlivo voči všetkým zúčastneným stranám.

**Vízia IstroSec**

Byť medzinárodným lídrom v oblasti výskumu, vývoja a služieb kybernetickej bezpečnosti a poskytovať inovatívne a účinné bezpečnostné riešenia.

**Ciele IstroSec**

Našim cieľom je ponúkať kvalitné a odborné služby našim zákazníkom za primeranú cenu a prostredníctvom nich kontinuálne zvyšovať ich odolnosť voči bezpečnostným hrozbám.

**Skúsenosti IstroSec**

Máme za sebou stovky vyriešených bezpečnostných incidentov, vrátane skupín APT. Máme tiež vlastné CVE a vykonali sme tisíce penetračných testov, analýz škodlivého softvéru a školení.

**Klienti IstroSec**

Našimi zákazníkmi sú malé a stredné podniky, korporácie, spoločnosti z rebríčka Fortune 500 a vládne subjekty vo všetkých priemyselných odvetviach, ktoré berú kybernetickú bezpečnosť veľmi vážne.