Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

Výber dodávateľa služieb kybernetickej bezpečnosti

Návod pre obce a mestá v piatich krokoch

Dosiahnutie súladu so zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti vyžaduje od prevádzkovateľov základných služieb najmä stanovenie a implementáciu bezpečnostných opatrení a výkon ďalších odborných činností.

Kybernetická bezpečnosť je mimoriadne závislá na vedomostiach a zručnostiach a Slovensko sa bude ešte mnoho rokov vysporiadavať s nedostatkom kvalifikovanej pracovnej sily v tejto oblasti. Mnoho organizácií v postavení prevádzkovateľa základnej služby nedisponuje zamestnancami - špecialistami informačnej a kybernetickej bezpečnosti. Častým riešením nedostatku špecialistov je výkon odborných činností dodávateľskou formou.

Výber kvalitného a dôveryhodného dodávateľa môže byť netriviálnou úlohou, najmä pre štatutárov menších organizácií. Toto usmernenie má napomôcť starostom obcí a primátorom miest k úspešnému procesu výberu.

Cieľom opatrení je minimalizovať bezpečnostné riziká, predchádzať kybernetickým bezpečnostným incidentom a predísť ich negatívnemu dopadu na základné služby.

Zodpovednosť štatutára

Plnenie úloh kybernetickej bezpečnosti si vyžaduje odborné spôsobilosti a môže byť vykonávané aj dodávateľským spôsobom. Viaceré zákonom stanovené zodpovednosti však nie je možné zmluvne preniesť na tretiu stranu, ani sa ich vzdať. Bez ohľadu na druh a rozsah dodávaných činností, **zákonná zodpovednosť za strategické riadenie kybernetickej bezpečnosti vždy patrí prevádzkovateľovi základnej služby a jeho štatutárnemu orgánu.** To, či je organizácia prevádzkovateľom základnej služby, sa dá overiť na stránkach nbu.gov.sk

Rozhodnutia o úlohách musí prijímať štatutárny zástupca, alebo ním poverený zamestnanec organizácie.

V zmysle Obchodného zákonníka je štatutárny orgán povinný konať s odbornou starostlivosťou v súlade so záujmami organizácie, pričom v jej mene zodpovedá za porušenie povinností. Obdobne to platí aj pre starostov obcí a primátorov miest, ktorým táto zodpovednosť vyplýva z osobitných právnych predpisov, akým je aj zákon o obecnom zriadení.

Povinnosť štatutárneho orgánu konať s odbornou starostlivosťou vyžaduje, aby si štatutár pri konkrétnom rozhodovaní zaobstaral a vyhodnotil všetky objektívne dostupné informácie. Následne sa má náležite rozhodnúť v kontexte týchto informácií a vlastnej profesionality.

Zmluva s dodávateľom služieb

Služby kybernetickej bezpečnosti je možné obstarať ako služby vykonávané dodávateľským spôsobom na základe zmluvy. Ide však o zmluvnú zodpovednosť, ktorá sa od zákonnej zodpovednosti líši.

Zmluva s dodávateľom nepredstavuje nahradenie zákonných zodpovednostných vzťahov a ich prenos na tretiu osobu.

Zmluva s externým dodávateľom služieb kybernetickej bezpečnosti môže určovať konkrétne sankcie dodávateľa ak poruší zmluvné povinnosti. Porušenie parametrov zmluvy môže byť riešené vopred dohodnutým znížením platieb alebo automatickou zmluvnou pokutou, a to nezávisle od toho, či vznikla škoda.

Typy služieb

Pokrytie roly manažéra kybernetickej bezpečnosti formou externej služby je v malých organizáciách bežné. Úlohy tejto roly vyplývajú zo zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe. Minimálne kvalifikačné požiadavky sú uvedené v prílohe č. 1.

Audit kybernetickej bezpečnosti je posudzovanie zhody, ktoré môže vykonávať len certifikovaný audítor kybernetickej bezpečnosti. Zoznam certifikovaných audítorov kybernetickej bezpečnosti je na nbu.gov.sk

Audit kybernetickej bezpečnosti môže vykonávať výhradne certifikovaný audítor kybernetickej bezpečnosti.

Prevádzkovateľ základnej služby môže v období od 1. augusta 2021 do 31. decembra 2023 pre I. a II. kategóriu sietí a informačných systémov **namiesto auditu vykonať preverenie účinnosti prijatých bezpečnostných opatrení prostredníctvom manažéra kybernetickej bezpečnosti** funkcionalitou jednotného informačného systému kybernetickej bezpečnosti na nbu.gov.sk

1 Prvý kontakt s potenciálnym dodávateľom

V tomto odporúčaní sa sústredíme na základný postup, ako identifikovať dôveryhodného dodávateľa služieb kybernetickej bezpečnosti. Počas celého výberu majte na pamäti fakt, že **výkon úloh v kybernetickej bezpečnosti je kriticky závislý na kvalifikácii potvrdenej profesionálnou praxou.**

Už pri prvom kontakte potenciálny partner „odhalí" svoju dôveryhodnosť, profesionalitu a schopnosť správne naplniť vaše potreby.

Dôveryhodný dodávateľ služieb kybernetickej bezpečnosti

- predovšetkým sa zaujíma ako bola riešená u vás kybernetická bezpečnosť doteraz
- vie uviesť svoju overiteľnú profesionálnu históriu a referencie
- vie dokladovať svoju kvalifikáciu a certifikácie
- zrozumiteľne vysvetlí, čo a prečo treba vykonať vo vašej organizácii
- má záujem odovzdať svoje knowhow
- navrhne vám pravidelné návštevy a konzultácie priamo vo vašich priestoroch.

Ponuku služieb dodávateľ vypracuje až na základe informácií, ktoré si od vás vyžiada. Ponúkané služby dodávateľ vysvetlí a objasní, akým spôsobom prispejú k zvýšeniu úrovne kybernetickej bezpečnosti vo vašej obci či meste. Ponuku dodávateľ optimalizuje podľa vašej aktuálnej situácie a špecifík, aby sa napríklad vyhol duplicitnej bezpečnostnej dokumentácii.

Ak váš dodávateľ plánuje použiť aj **subdodávateľa,** zákon o kybernetickej bezpečnosti aj GDPR vyžadujú, aby aj tento bol vami vopred schválený.

Čoho sa vystríhať?

Na trhu sú aj dodávatelia služieb, ktorých prínos je pochybný. Služby ponúkajú aj bez príslušnej kvalifikácie a bez toho, aby mali znalosti o situácii u potenciálneho zákazníka.

Málo kvalifikovaní dodávatelia pri ponuke svojich služieb kladú dôraz na vzory dokumentácie, argumentujú pokutami, nezaujímajú sa o špecifické riziká a prijaté opatrenia, nevedia preukázať svoju odbornosť a prax.

Reálny vplyv týchto dodávateľov na zvýšenie úrovne kybernetickej bezpečnosti v organizácii je mizivý. Dodajú vám iba falošný pocit bezpečia. Paradoxom je, že dôsledkom ich neprofesionality môže byť nakoniec udelenie pokút, ktorými argumentovali na začiatku.

2 Analýza rizík ako súčasť ponuky

Analýza rizík je kľúčová aktivita ktorá by mala byť súčasťou ponuky. Iba na základe analýzy rizík je možné navrhnúť a prijať relevantné bezpečnostné opatrenia. Aj preto je vyžadovaná zákonom. Metodika analýzy rizík je dostupná aj na stránke MIRRI.

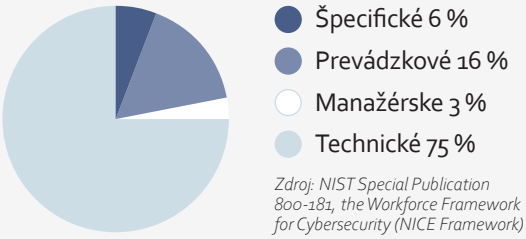
Sieťové a aplikačné infraštruktúry sa mnohokrát zásadne líšia. Preto k analýze patrí aj posúdenie vášho technického prostredia. Bez znalosti IT prostredia organizácie a bez predstavy o jej aktívach a reálnych hrozbách v jej prostredí nie je možné odhadnúť primeranosť opatrení a stanoviť potreby organizácie v oblasti kybernetickej bezpečnosti.

- Zaujímajte sa ako a v akom rozsahu plánuje potenciálny dodávateľ vykonať analýzu rizík
- Nechajte si vysvetliť, čo bude výstupom analýzy a ako bude tento výstup použitý
- Požadujte konkrétne príklady bezpečnostných rizík, ktoré budú v organizácii analyzované
- Pýtajte sa, ako budete následne tieto riziká v organizácii riadiť
- Dodávateľ by mal zdôvodniť primeranosť opatrení a porovnať hodnotu opatrení s hodnotou identifikovaných rizík

A zbystrite pozornosť, ak dodávateľ ako jediné riziko uvedie pokutu! V tom prípade buď vami manipuluje, alebo kybernetickej bezpečnosti jednoducho nerozumie.

3 Technické znalosti dodávateľa

Pri poskytovaní služieb kybernetickej bezpečnosti alebo v službách podpory pri riešení kybernetických bezpečnostných incidentov sú typicky požadované najmä technické znalosti a zručnosti. Medzinárodné normy požadujú v informačnej a kybernetickej bezpečnosti ťažiskovo technickú kvalifikáciu, následne prevádzkovú, špecifickú a manažérsku.



Zdroj: NIST Special Publication 800-181, the Workforce Framework for Cybersecurity (NICE Framework)

4 Preukázateľná odbornosť tímu dodávateľa

Spôsob, ako si môžete overiť kvalifikáciu potenciálneho dodávateľa, je najmä vyžadovanie odborných certifikátov. V informačnej a kybernetickej bezpečnosti sú odborné certifikáty uznávaným spôsobom preukázania spôsobilostí. Skratky najznámejších a najčastejšie vyžadovaných certifikátov pre služby kybernetickej bezpečnosti sú CISA, CISM, CRISC, CISSP. Rozšírený zoznam certifikátov a vysvetlenie skratiek je v prílohe č.2.

Tím potenciálneho dodávateľa by mali tvoriť zamestnanci alebo kontrahované fyzické osoby, ktorí

- majú spôsobilosť na právne úkony v plnom rozsahu,
- odbornosť je preukázateľne overiteľná podľa stanovených kritérií (viď prílohy)
- vedia poskytnúť profesionálny životopis a zoznam projektov, na ktorých sa podieľali

5 Prax v odbore

Národný bezpečnostný úrad vydáva certifikačnú schému overovania odbornej spôsobilosti manažéra kybernetickej bezpečnosti, ktorá je zverejnená aj na webovej stránke. V časti všeobecných požiadaviek na spôsobilosť sú uvedené **minimálne kvalifikačné požiadavky** na úroveň vzdelania a prax profesionála, ktorý poskytuje služby manažéra kybernetickej bezpečnosti (príloha č.1)

- **Uplatnite** analogické požiadavky aj pri výbere dodávateľa služieb kybernetickej bezpečnosti.
- **Overte si,** do akej miery potenciálny dodávateľ spĺňa tieto požiadavky a získate tak ďalšiu predstavu o jeho praxi a kompetentnosti.

Dokumentáciou sa bezpečnostné opatrenia nekončia

Kedy je potrebné spozornieť?

Ak potenciálny dodávateľ tvrdí, že dodaním sady dokumentov bude zaručený súlad so zákonom, zjavne hodlá zneužiť vašu neinformovanosť. A našiel si obchodnú príležitosť bez ohľadu na vaše reálne potreby.

Pred kybernetickým bezpečnostným incidentom vás neochráni žiadny dokument.

Kybernetická bezpečnosť je náročná na konkrétne **opatrenia v technologickej aj procesnej rovine.** Potrebné sú nielen „papierové" opatrenia, ale najmä tie implementované do praxe.

Všeobecne napísaná bezpečnostná dokumentácia alebo neprispôsobený vzor dokumentácie nikdy nesplnia všetky špecifické požiadavky a opatrenia v kybernetickej bezpečnosti.

Príloha č. 1 - Kvalifikačné požiadavky

Minimálne požiadavky na úroveň vzdelania a prax profesionála, ktorý poskytuje služby manažéra kybernetickej bezpečnosti

Vzdelanie a požadovaný doklad	Prax a spôsob jej preukázania (alternatívy predložených dokumentov)
Úplné stredné všeobecné vzdelanie a úplné stredné odborné vzdelanie (doklad o získanom stupni vzdelania a o získanej kvalifikácii)	• skúsenosti v oblasti informačných technológií - najmenej **10 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **7 rokov praxe** • medzinárodný certifikát z oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT sa považuje za započítateľnú odbornú prax
Vysokoškolské vzdelanie prvého stupňa (doklady o absolvovaní štúdia)	• skúsenosti v oblasti informačných technológií - najmenej **7 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **5 rokov praxe** • medzinárodný certifikát z oblasti riadenia informačnej bezpečnosti sa považuje započítateľnú odbornú prax
Vysokoškolské vzdelanie druhého stupňa (doklady o absolvovaní štúdia)	• skúsenosti v oblasti informačných technológií - najmenej **5 rokov praxe** (životopis s uvedením kontaktu na overiteľnú referenciu), • skúsenosti v oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT - najmenej **3 roky praxe** • medzinárodný certifikát z oblasti riadenia IT služieb, riadenia informačnej bezpečnosti, riadenia rizík, alebo architektúry IT sa považuje za započítateľnú odbornú prax

Príloha č. 2 - Zoznam odborných certifikátov

Výber certifikátov, ktorými tím dodávateľa preukazuje odbornú spôsobilosť. Ak tím deklaruje, že je odborne spôsobilý vykonávať služby v oblasti informačnej a kybernetickej bezpečnosti, členovia by mali disponovať aspoň niektorými z týchto certifikátov. V praxi postačuje, aby aspoň jeden člen tímu mal niektorý z certifikátov ISACA, (ISC)², GIAC, alebo CompTIA.

Skratka	Názov	Vydavateľ
CISA	Certified Information Systems Auditor	ISACA
CISM	Certified Information Security Manager	
CRISC	Certified In Risk and Information Systems Control	
CDPSE	Certified Data Privacy Security Engineer	
CISSP	Certified Information Systems Security Professional	(ISC)²
CSSLP	Certified Secure Software Lifecycle Professional	
CCSP	Certified Cloud Security Professional	
SSCP	Systems Security Certified Practitioner	
CCFP	Certified Cyber Forensics Professional	
CASP	CompTIA Advanced Security Practitioner	CompTIA
CSA+	CompTIA Cyber Security Analyst	
Security+	CompTIA Security+	
Pentest+	CompTIA Pentest+	
OSCP	Offensive Security Certified Professional	Offensive Security
OSWP	Offensive Security Wireless Professional	
OSCE	Offensive Security Certified Expert	
OSEE	Offensive Security Exploitation Expert	
OSWE	Offensive Security Web Expert	

Skratka	Názov	Vydavateľ
GISF	GIAC Information Security Fundamentals	GIAC
GSEC	GIAC Security Essentials Certification	
GISP	GIAC Information Security Professional	
GPPA	GIAC Certified Perimeter Protection Analyst	
GCIA	GIAC Certified Intrusion Analyst	
GCED	GIAC Certified Enterprise Defender	
GPEN	GIAC Certified Penetration Tester	
GWAPT	GIAC Certified Web Application Penetration Tester	
GSTRT	GIAC Strategic Planning, Policy, and Leadership	
GSNA	GIAC Systems and Network Auditor	
GCFA	GIAC Certified Forensic Analyst	
GLEG	GIAC Law of Data Security & Investigations	
GSE	GIAC Security Expert	
CEH	Certified Ethical Hacker	EC-Council
CHFI	Certified Hacking Forensic Investigator	
ECIH	EC-Council Certified Incident Handler	
ENSA	EC-Council Network Security Administrator	
CCISO	Certified Chief Information Security Officer	
EDRP	EC-Council Disaster Recovery Professional	
LA27k	ISO/IEC 27001 Lead Auditor	ISO

Zoznam certifikátov uvedených vyššie v prehľadovej tabuľke je len informatívny a nie je vyčerpávajúci. Nie je preto vylúčené, že odborná spôsobilosť pre kvalifikovaný výkon služieb v oblasti informačnej a kybernetickej bezpečnosti môže byť daná aj na základe iného, v prehľadovej tabuľke neuvedeného certifikátu.

Ak máte akékoľvek otázky týkajúce sa praxe kybernetickej bezpečnosti alebo implementácie technických, či organizačných opatrení, poradíme vám. Stačí, ak napíšete vašu otázku alebo opis konkrétneho problému na adresu poradna@cybercompetence.sk. **Zabezpečíme, aby na vašu otázku odpovedal niektorý zo špičkových slovenských odborníkov.** Vybrané odpovede budeme v anonymizovanom tvare uvádzať aj na našej webovej stránke, v sekcii Často kladené otázky.

Odborné stanoviská NBÚ nájdete na web stránke Úradu v časti „Úrad – Informácie – Odborné stanoviská – Kybernetická bezpečnosť". Metodiky ku tvorbe bezpečnostnej dokumentácie pre sektor verejnej správy sú dostupné na webovom sídle MIRRI v časti „Kybernetická bezpečnosť - Bezpečnostná dokumentácia - metodiky".

Tu uvedený informačný obsah vychádza z verejne dostupných a nám známych informácií a slúži na získanie všeobecného obrazu vo veciach, ktorých sa týka. Preto ho nemožno považovať za univerzálny, súhrnný alebo komplexný. Nezodpovedáme za skutočnosti, ku ktorým nemáme dostatočné informácie alebo ktoré majú základ v nepresných alebo nesprávnych informáciách alebo informáciách, ktoré nám nie sú známe. Informačný obsah ďalej nie je možné považovať za právne záväzný výklad právnych predpisov, ako ani za normatívny, individuálny alebo hybridný správny akt.

Kompetečné a certifikačné centrum kybernetickej bezpečnosti

poradna@cybercompetence.sk www.cybercompetence.sk FAQ www.cybercompetence.sk/casto-kladene-otazky-riadenie-kb/

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 978-80-69011-22-9

Verzia V.1