**Manažér kybernetickej bezpečnosti – Ako zabezpečiť bezpečnosť v organizácií?**

V dnešnom prepojenom svete čelia firmy čoraz sofistikovanejším kybernetickým hrozbám. Zároveň sa stupňujú legislatívne požiadavky na ochranu dát a infraštruktúry. V tomto dynamickom prostredí sa pozícia **manažéra kybernetickej bezpečnosti** stáva kľúčovou.

Nie každá organizácia si však môže dovoliť alebo potrebuje zamestnávať špecialistu na plný úväzok. Je možnosť zabezpečiť **externého manažéra kybernetickej bezpečnosti (EMKB)**? Aké sú výhody a nevýhody outsourcingu EMKB a čo od nej vyžaduje zákon?

**Kto je externý manažér kybernetickej bezpečnosti?**

Externý manažér kybernetickej bezpečnosti je **odborník alebo tím odborníkov**, ktorý poskytuje služby v oblasti kybernetickej bezpečnosti pre organizáciu na základe zmluvy o externom poskytovaní služieb. Táto osoba alebo tím preberá zodpovednosť za implementáciu, udržiavanie a neustále zlepšovanie bezpečnostných opatrení v súlade s platnou legislatívou best practice . Ich úlohou je chrániť informačné aktíva firmy pred kybernetickými útokmi, zaisťovať súlad s legislatívou a minimalizovať riziká.

**Výhody externého manažéra kybernetickej bezpečnosti**

Rozhodnutie pre EMKB prináša niekoľko kľúčových benefitov:

* **Odborné znalosti a skúsenosti:** Získate prístup k odborníkom a aktuálnym informáciám o najnovších hrozbách a trendoch v kybernetickej bezpečnosti. EMKB sa špecializuje na túto oblasť a jeho vedomosti sú neustále aktualizované potrebnými školeniami.
* **Zníženie nákladov:** Nie všetky organizácie potrebujú alebo si vedia zabezpečiť interného zamestnanca na tejto pozícií. V prípade outsourcingu platíte len za službu, ktorú skutočne potrebujete.
* **Nezávislý a objektívny pohľad:** Externý manažér prináša nezaujatý pohľad na vaše bezpečnostné procesy a systémy, identifikuje slabé miesta, ktoré by interný tím nemusel vidieť, a navrhuje riešenia bez interných predsudkov.
* **Súlad s legislatívou (Compliance):** Kvalitný EMKB zabezpečí, že vaša organizácia bude spĺňať všetky aktuálne a nadchádzajúce požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a súvisiacich predpisov, ako aj smernice **NIS2**. To pomáha predchádzať vysokým pokutám a sankciám.
* **Rýchla implementácia:** Externí špecialisti sú často schopní rýchlejšie implementovať potrebné zmeny a opatrenia, keďže majú už skúsenosti so zavádzaním procesov a metodík.

**Nevýhody externého manažéra kybernetickej bezpečnosti**

Je dôležité zvážiť aj potenciálne nevýhody:

* **Menšia interná kontrola:** Môže dôjsť k pocitu menšej priamej kontroly nad každodennými operáciami kybernetickej bezpečnosti, keďže zodpovednosť je delegovaná externe.
* **Komunikácia a integrácia:** Efektívna komunikácia a bezproblémová integrácia s internými tímami je kľúčová. Nedostatočná komunikácia môže viesť k nedorozumeniam alebo neefektívnosti.
* **Obmedzené znalosti špecifík firmy:** Externý manažér nemusí mať tak hlboké znalosti o špecifických interných procesoch a kultúre firmy ako interný zamestnanec. Dôležitá je otvorená komunikácia a zdieľanie informácií.
* **Dôvera:** Zverenie citlivých informácií a prístupov externému partnerovi si vyžaduje vysokú úroveň dôvery a transparentnosti.

**Požiadavky na pozíciu zo zákona**

Slovenská legislatíva, najmä **zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti** a jeho vykonávacie predpisy, stanovuje jasné požiadavky na pozíciu manažéra kybernetickej bezpečnosti. Hoci zákon nešpecifikuje, či má byť táto pozícia interná alebo externá, popisuje jej funkciu a zodpovednosti, ktoré musí spĺňať:

* **Vymenovanie manažéra:** Každý **prevádzkovateľ základnej služby** a **poskytovateľ digitálnej služby** má povinnosť **vymenovať manažéra kybernetickej bezpečnosti** (§ 21 zákona č. 69/2018 Z. z.). Táto povinnosť sa v kontexte **NIS2** rozšíri na podstatne širšie spektrum subjektov.
* **Úlohy a zodpovednosti:** Manažér kybernetickej bezpečnosti je zodpovedný za **riadenie kybernetickej bezpečnosti organizácie**. Medzi jeho kľúčové úlohy patrí:
  + **Vypracovanie a udržiavanie bezpečnostnej dokumentácie** (politiky, smernice, postupy).
  + **Identifikácia a riadenie rizík** kybernetickej bezpečnosti.
  + **Dohľad nad implementáciou bezpečnostných opatrení** (§ 20 a vyhláška NBÚ č. 362/2018 Z. z.).
  + **Riadenie kybernetických incidentov** vrátane ich hlásenia Národnému bezpečnostnému úradu (NBÚ) (§ 19).
  + **Zvyšovanie povedomia a školenie zamestnancov** v oblasti kybernetickej bezpečnosti.
  + **Monitorovanie a hodnotenie efektívnosti** zavedených bezpečnostných opatrení (§ 22).
* **Odborná spôsobilosť:** Hoci zákon priamo nešpecifikuje konkrétne certifikácie, vyžaduje sa **odborná spôsobilosť a praktické skúsenosti** v oblasti kybernetickej bezpečnosti. Kvalitný externý manažér by mal preukázať relevantné certifikácie (napr. CISSP, CISM) a bohaté skúsenosti s riadením bezpečnosti.

**Ktoré firmy potrebujú manažéra kybernetickej bezpečnosti?**

Služba manažéra kybernetickej bezpečnosti je potrebná pre:

* **Subjekty spadajúce pod zákon č. 69/2018 Z. z. a smernicu NIS2:** Ak ste už teraz prevádzkovateľom základnej služby, poskytovateľom digitálnej služby, alebo ak vaša organizácia pôsobí v jednom z mnohých odvetví, ktoré budú regulované podľa novej smernice **NIS2** (napríklad energetika, doprava, bankovníctvo, zdravotníctvo, digitálna infraštruktúra, verejná správa, a mnohé ďalšie, ktoré NIS2 novo pokrýva ako "základné" alebo "kritické" subjekty), je pre vás manažér KB kľúčový pre dosiahnutie a udržanie súladu.
* **Stredné a väčšie podniky:** Aj keď možno nie sú priamo pod reguláciou, spracovávajú citlivé dáta, majú rozsiahlu IT infraštruktúru a čelia významným kybernetickým rizikám.
* **Spoločnosti hľadajúce proaktívny prístup k bezpečnosti:** Pre tých, ktorí chcú nielen reagovať na hrozby, ale im aj predchádzať a neustále zlepšovať svoju kybernetickú odolnosť.
* **Organizácie pripravujúce sa na certifikáciu alebo audit:** Manažér KB môže poskytnúť cennú pomoc pri príprave na certifikácie podľa noriem ako ISO/IEC 27001, čím zjednoduší a zefektívni proces.

**Záver**

Externý manažér kybernetickej bezpečnosti predstavuje flexibilné a efektívne riešenie pre organizácie, ktoré sa snažia navigovať v zložitom prostredí kybernetických hrozieb a regulačných požiadaviek. Správne zvolený EMKB môže byť neoceniteľným partnerom, ktorý chráni vaše aktíva a zabezpečuje súlad s legislatívou.

CeMS je certifikovaným audítorom kybernetickej bezpečnosti a má dostatočný počet manažérov kybernetickej bezpečnosti, ktorí môžu pomôcť aj vašej organizácií.

Ak máte záujem vyškoliť si interného manažéra kybernetickej bezpečnosti neváhajte si absolvovať školenia v oblasti informačnej bezpečnosti.