ZKB ALEFNULA

Příloha — detail kurzů

Manager kybernetické bezpečnosti

Znalost ZKB: **1-denní kurz Zákon o kybernetické bezpečnosti**
Odborná znalost: **5-denní kurz Manager kybernetické bezpečnosti** na úrovni auditorských znalostí ISMS, možnost certifikace auditor ISMS

Architekt kybernetické bezpečnosti

Znalost ZKB: **1-denní kurz Zákon o kybernetické bezpečnosti**
Odborná znalost: **5-denní kurz Architekt kybernetické bezpečnosti**, s velkým rozsahem a intensivním obsahem technických opatření

Auditor kybernetické bezpečnosti:

Znalost ZKB: **1-denní kurz Zákon o kybernetické bezpečnosti**
Odborná znalost: **5-denní kurz Auditor kybernetické bezpečnosti** na úrovni auditorských znalostí ISMS, certifikace auditor ISMS

Garant aktiva:

Znalost ZKB: **1-denní kurz Zákon o kybernetické bezpečnosti**
Odborná znalost: běžné technické kurzy z nabídky Training Centre ALEF NULA nebo u jiných dodavatelů

Administrátor:

Znalost ZKB: **1-denní kurz Zákon o kybernetické bezpečnosti**
Odborná znalost: běžné technické kurzy z nabídky Training Centre ALEF NULA nebo u jiných dodavatelů

Uživatel:

Bezpečnostní povědomí: **120min. eLearning kurz Uživatel – obecné bezpečnostní povědomí**

Dodavatel:

Znalost řízení bezpečnosti: speciální kurzy na míru

ALEF NULA, a.s.
U plynárny 1002/97, Praha 10
Česká republika
tel: +420 225 090 200
www.alef.com
cz-sales@alef.com

Gold Partner

ALEFNULA Trust the Strong

ZKB | Úroveň znalostí bezpečnostních rolí podle Zákona o kybernetické bezpečnosti

MANAŽERSKÉ SHRNUTÍ

Zákon o kybernetické bezpečnosti (dále jen „ZKB“) klade na celou řadu organizací – správců kritické informační infrastruktury (dále jen „KII“) a významných informačních systémů (dále jen „VIS“) nové povinnosti z oblasti informační bezpečnosti.

V rámci bezpečnostních opatření, která zákon nařizuje, se správce musí potýkat s celkovým rozdělením lidských zdrojů v organizaci zejména díky následujícím požadavkům:

- **§6 Organizační bezpečnost**
- **§9 Bezpečnost lidských zdrojů.**

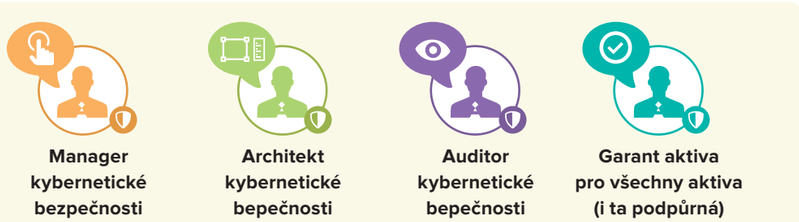
Pro všechny zaměstnance nebo i externí osoby musí být zaveden plán rozvoje bezpečnostního povědomí – tedy způsob, jak budou všichni zaměstnanci i externí osoby vzděláváni. §6 určuje lidské zdroje potřebné k řízení informační bezpečnosti. U všech organizací platí, že musí zavést výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti.

§6 ORGANIZAČNÍ BEZPEČNOST

Rozdělení rolí podle ZKB

Pro správce KII platí povinnost zavedení následujících specifických skupin a rolí:

A) Výbor pro řízení kybernetické bezpečnosti



B) Dodavatelé.

Pro správce VIS platí povinnost zavedení následujících specifických skupin a rolí:

A) Výbor pro řízení kybernetické bezpečnosti

B) Dodavatelé

Aby byl správce VIS schopen efektivně řídit bezpečnost informací, měl by vedle garantů aktiv zavést minimálně roli Managera kybernetické bezpečnosti. Ideálně i Architekta a Auditora. Role, které jsou povinně určené pro správce KII, jsou v podstatě nepostradatelné i pro správce VIS, i když k jejich určení u správců VIS není legislativní povinnost. Relativně je možné snížit úroveň zpětné vazby v podobě auditora. Nižší úrovní rozdělení bezpečnostních rolí správce VIS těžko dosáhne výsledku v podobně zabezpečeného prostředí v souladu se ZKB.

§

VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI
§ 6 Organizační bezpečnost
(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona splní povinnost podle § 4 odst. 2 zákona tím, že zavede organizaci řízení bezpečnosti informací (dále jen „organizační bezpečnost"), v rámci které určí výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s informačním systémem kritické informační infrastruktury, komunikačním systémem kritické informační infrastruktury nebo významným informačním systémem. ¶ (2) Orgán a osoba uvedená v § 3 písm. c) a d) zákona určí bezpečnostní role a) manažer kybernetické bezpečnosti, b) architekt kybernetické bezpečnosti, c) auditor kybernetické bezpečnosti a d) garant aktiva podle § 2 písm. m). ¶ (3) Manažer kybernetické bezpečnosti je osoba odpovědná za systém řízení bezpečnosti informací, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s řízením bezpečnosti informací po dobu nejméně tří let. ¶ (4) Architekt kybernetické bezpečnosti je osoba odpovědná za návrh a implementaci bezpečnostních opatření, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s navrhováním bezpečnostní architektury po dobu nejméně tří let. ¶ (5) Auditor kybernetické bezpečnosti je osoba odpovědná za provádění auditu kybernetické bezpečnosti, která je pro tuto činnost řádně vyškolena a prokáže odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti po dobu nejméně tří let. Auditor kybernetické bezpečnosti vykonává svoji roli nestranně a výkon jeho role je oddělen od výkonu rolí uvedených v odstavci 2 písm. a), b) nebo d). ¶ (6) Orgán a osoba uvedená v § 3 písm. c) až e) zákona splní povinnost podle § 4 odst. 2 zákona tím, že zajistí odborné školení osob, které zastávají bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí podle § 9 odst. 1 písm. b).

§9 BEZPEČNOST LIDSKÝCH ZDROJŮ

Vzdělávání lidských zdrojů je požadováno v takovém formátu, že pro většinu rolí je potřeba zavést 2 směry:

- **Znalost ZKB**
- **Odborná znalost vztažená k roli nebo obecné bezpečnostní povědomí pro běžného uživatele**

Vedle rolí stanovených v rámci §6 Organizační bezpečnosti, je potřeba stanovit vzdělávací úroveň pro další role: Administrátor, Uživatel a Dodavatel.

Reálné rozdělení rolí podle ZKB a jejich znalost ZKB

Reálné rozdělení rolí KII i VIS podle ZKB nebo praxe a reálná požadovaná úroveň teoretických znalostí ZKB:

A) Výbor pro řízení kybernetické bezpečnosti
- — **Manager kybernetické bezpečnosti** – vysoká úroveň
- — **Architekt kybernetické bezpečnosti** – vysoká úroveň
- — **Auditor Kybernetické bezpečnosti** – vysoká úroveň
- — **Garant aktiva (KII všech/VIS primárních)** – povědomí

B) Administrátor – povědomí
C) Uživatel – žádná
D) Dodavatelé – žádná

Základem úspěšného řízení informační bezpečnosti je komunikace mezi lidmi. Pokud je pro nějakou roli dostačující povědomí, musí tato role vědět, že všechny záležitosti s dopadem do informační bezpečnosti musí konzultovat s Managerem kybernetické bezpečnosti. Takový proces je řešitelný na úrovni bezpečnostní politiky.

§9 BEZPEČNOST LIDSKÝCH ZDROJŮ

Reálné rozdělení rolí podle ZKB a jejich odborná znalost.

Současně se znalostí ZKB je vyžadována jako druhá větev odborná znalost vzhledem k roli, kterou zaměstnanec nebo externí osoba zastává:

A) Výbor pro řízení kybernetické bezpečnosti
- — **Manager kybernetické bezpečnosti** – obecné principy řízení bezpečnosti, fyzická bezpečnost, procesní (organizační) bezpečnost, managerská schopnost, technologická bezpečnost
- — **Architekt kybernetické bezpečnosti** – technologická bezpečnost – síťová bezpečnost, aplikační bezpečnost, kryptografie, technické nástroje kontinuity…
- — **Auditor Kybernetické bezpečnosti** – auditorský certifikát ISMS, technol. bezpečnost
- — **Garant aktiva (KII všech/VIS primárních)** – znalost svěřeného aktiva

B) Administrátor – znalost svěřeného technického aktiva/technického opatření
C) Uživatel – znalost bezpečnostních politik správce KII/VIS a obecné bezpečnostní povědomí
D) Dodavatelé – znalost systému řízení informační bezpečnosti správce KII/VIS

§

VYHLÁŠKA O KYBERNETICKÉ BEZPEČNOSTI
§ 9 Bezpečnost lidských zdrojů
(1) Orgán a osoba uvedená v § 3 písm. c) až e) zákona splní povinnost podle § 4 odst. 2 zákona tím, že a) stanoví plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a určí osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny, b) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení, c) zajistí kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a d) zajistí vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role. ¶ (2) Orgán a osoba uvedená v § 3 písm. c) až e) zákona vede o školení podle odstavce 1 přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly. ¶ (3) Orgán a osoba uvedená v § 3 písm. c) a d) zákona splní povinnost podle § 4 odst. 2 zákona dále tím, že a) stanoví pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů, b) hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí, c) určí pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a d) zajistí změnu přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.

Požadavky na vzdělání rolí podle ZKB

Národní bezpečnostní úřad bohužel neurčil přesný systém vzdělávání potřebný k naplnění role. Uchazeči o roli Manager kybernetické bezpečnosti tak stačí získat jakékoliv osvědčení o absolvování téměř čehokoliv — tím je osoba vyškolena, mít 3 roky praxe a splňuje podmínky pro tuto roli. Naše společnost nabízí vzdělávací systém pro všechny role lidem, kteří myslí chování podle ZKB vážně. Náš certifikát nemá žádnou hodnotu opravňující jeho držitele k plnění rolí podle ZKB, ale jsou za ním kurzy, které účastníka vybaví znalostmi k plnění činnosti v rámci svěřené role. A pokud Národní bezpečnostní úřad certifikační program (doufejme) jednou dodatečně určí, neměl by být problém ho díky znalostem získaným v Training Centre ALEF NULA úspěšně zvládnout.

Více informací zde: http://training.alef.com/cz/