VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Úplné znění ke dni: 1. 4. 2025
Zapracovává: dodatek č. 1

ÚPLNÉ ZNĚNÍ
SMĚRNICE Č. 1/2024
ŘÍZENÍ KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI VUT

Článek 1
Předmět a účel úpravy

1. Tato směrnice v souladu s právními předpisy upravujícími zajištění kybernetické bezpečnosti definuje osoby odpovědné za řízení kybernetické a informační bezpečnosti (dále jen kybernetická bezpečnost) na VUT a stanovuje jejich práva a povinnosti.
2. Účelem této směrnice je zajištění kybernetické bezpečnosti a odolnosti dle standardů plynoucích z obecně závazných právních předpisů, a to včetně stanovení objektivních postupů pro nastavení, realizaci a vyhodnocování konkrétních opatření.
3. Realizace konkrétních opatření pro zajištění kybernetické bezpečnosti je pracovněprávní povinností každého zaměstnance. Vedoucí pracovníci v rámci svých povinností odpovídají za implementaci konkrétních opatření a postupů na jimi vedených pracovištích.

Článek 2
Organizace řízení (role)

1. Pro řízení kybernetické bezpečnosti na VUT se zřizují role:
    a. Manažer kybernetické bezpečnosti (dále jen “Manažer KB”),
    b. Architekt kybernetické bezpečnosti (dále jen “Architekt KB”),
    c. Auditor kybernetické bezpečnosti (dále jen “Auditor KB”).
2. Na řízení kybernetické bezpečnosti se v rámci svých kompetencí stanovených vnitřními předpisy a organizačními dokumenty podílí v rozsahu stanoveném článkem 6 této směrnice Garanti aktiv.
3. Zvláštní normou[1] se zřizuje Výbor pro řízení kybernetické bezpečnosti (dále jen “Výbor KB“).
4. Manažer KB a Architekt KB jsou pracovními pozicemi v rámci Centra výpočetních a informačních služeb VUT (dále jen „CVIS“).
5. Roli Auditora KB vykonává pověřený zaměstnanec Odboru Auditu a kontroly rektorátu VUT.

[1] Směrnice č. 5/2021 - Poradní sbory a pracovní skupiny zřizované v souladu se Statutem VUT

Článek 3
Manažer kybernetické bezpečnosti

1. Manažer KB v rámci zajišťování kybernetické bezpečnosti komunikuje s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen "NÚKIB"), a to včetně plnění oznamovací povinnosti při řešení kybernetických bezpečnostních událostí a incidentů
2. Manažer KB zejména:
    a. eviduje jednotlivá aktiva a poskytuje informace a součinnost Garantům aktiv,
    b. koordinuje řešení kybernetických bezpečnostních událostí a incidentů
    c. koordinuje činnosti zajišťující bezpečnost informačních aktiv,
    d. plánuje a řídí projekty kybernetické bezpečnosti schválené Výborem KB,
    e. postupem dle čl. 8a vydává Pravidla pro zajišťování kybernetické a informační bezpečnosti.
    f. spravuje systém řízení bezpečnosti informací,
    g. provádí analýzu rizik pro evidovaná aktiva,
    h. svolává a připravuje podklady pro jednání Výboru KB,
    i. podílí se na přípravě Strategie kybernetické bezpečnosti VUT,
    j. v souladu s platnou legislativou oznamuje NÚKIB bezpečnostní incidenty,
    k. poskytuje podklady pro Auditora KB a orgány VUT.

3. Při výkonu činností dle této směrnice je Manažer KB oprávněn:
    a. požadovat informace a součinnost od Garantů aktiv, a to včetně případného vypracování nezbytných dokumentů pro řízení rizik či realizaci konkrétních opatření
    b. vyžádat si audit od Auditora KB,
    c. požadovat od Výboru KB rozhodnutí o přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení přijatelné míry rizika a finančního limitu na eliminaci nepřijatelných rizik.

4. Manažera KB jmenuje a odvolává na návrh ředitele CVIS rektor.

Článek 4
Architekt kybernetické bezpečnosti

1. Architekt KB navrhuje vhodné postupy a opatření kybernetické bezpečnosti, jejich design a postup implementace, tak aby jejich realizace byla dosažitelná v rámci dostupných technických a finančních prostředků.
2. Architekt KB zejména:
    a. udržuje veškerou jím vytvářenou dokumentaci dle odst. 1 v aktuální podobě,
    b. identifikuje rizika a navrhuje opatření na jejich snížení,
    c. přiravuje podklady pro Manažera KB a Auditora KB,
    d. podílí se na přípravě strategie kybernetické bezpečnosti,
    e. navrhuje preventivní opatření, která vedou k udržování systému řízení bezpečnosti informací a obecně kybernetické bezpečnosti na VUT..
3. Při výkonu činností dle této směrnice je Architekt KB oprávněn:
    a. požadovat od Manažera KB informace a součinnost při vypracování dokumentů,
    b. vyžádat si podklady pro zpracování dokumentace od Garantů aktiv.

4. V rámci své činnosti pak Architekt KB vyhotovuje zejména:
    a. definici systému řízení bezpečností informací,

b. analýzu vývoje a metodiku hodnocení rizik,
c. model architektury kybernetické a informační bezpečnosti organizace,
d. model procesů pro řízení kybernetické bezpečnosti,
e. plán implementace bezpečnostních opatření,
f. definici testů pro verifikaci bezpečnostních opatření.

Architekt KB odpovídá za účinnost jím navržených opatření, není však zodpovědný za implementaci konkrétních jím navržených opatření.

6. Architekta KB jmenuje a odvolává na návrh ředitele CVIS rektor.

Článek 5
Auditor kybernetické bezpečnosti

1. Auditor KB vykonává dohled nad implementací modelů a opatření navržených Architektem KB, zejména tím, že provádí verifikaci souladu implementace s navrženým řešením a náhodné kontroly systémů, zda nedošlo k nedokumentovaným odchylkám, které by zvyšovaly riziko kybernetické hrozby.
2. Kromě průběžných činností definovaných v předchozím odstavci Auditor KB:
   a. vypracovává závěrečnou zprávu o implementaci opatření,
   b. vypracovává průběžnou zprávu o plnění strategie kybernetické bezpečnosti
   c. provádí audit na žádost Manažera KB a seznamuje jej o jeho výsledku,
   d. provádí audit aktiva, na žádost Garanta aktiva a seznamuje jej o jeho výsledku,
   e. informuje Výbor KB o výsledcích auditu.
3. V rámci své činnosti je Auditor KB oprávněn:
   a. vyžádat si dokumenty od Manažera KB a Garantů aktiv,
   b. seznámit s výsledkem auditu Výbor KB,
   c. žádat doplňující informace od Architekta KB.
4. Auditora KB jmenuje a odvolává na návrh vedoucího Odboru auditu a kontroly rektor.

Článek 6
Garant aktiva

1. Aktivem, resp. informačním aktivem se v souladu s obecně závaznými právními předpisy[2] rozumí jakákoliv data, informace, znalosti, procesy, software, hardware, služby, či zařízení, která mají pro VUT hodnotu a jejichž důvěrnost, integrita a dostupnost, ztráta, , odcizení nebo zneužití by VUT ztížilo činnost či způsobilo jakoukoli újmu.
2. Garantem aktiva je osoba odpovědná za konkrétní aktivum a vykonávající veškerá rozhodnutí s ním spojená.
3. Garant aktiva je zejména povinen:
   a. poskytovat osobám uvedeným v čl. 2 odst. 1 nezbytné informace pro hodnocení rizik,
   b. aplikovat jednotlivá opatření a povinnosti vyplývající ze schválených dokumentů,
   c. spolupracovat s Manažerem KB a Auditorem KB.
4. Garant aktiva může v rámci výkonu svých povinností ve vztahu ke kybernetické bezpečnosti:
   a. požádat Manažera KB o výjimku z pravidel kybernetické bezpečnosti,
   b. požádat Auditora KB o mimořádný audit.

[2] Z.č. 181/2014 Sb. o kybernetické bezpečnosti

Článek 7
Výbor kybernetické bezpečnosti

1. Výbor KB je stálý kolektivní orgán, jehož činnost a složení je upraveno zvláštní normou.
2. Výbor KB zejména:
    a. Na návrh Manažera KB schvaluje Strategii kybernetické bezpečnosti VUT,
    b. schvaluje dokumenty připravené Architektem KB,
    c. vyhodnocuje stav kybernetické bezpečnosti VUT.

Článek 8
Kybernetické bezpečnostní události a incidenty

1. V případě zjištění kybernetické bezpečnostní události (dále jen „Událost“) nebo kybernetického bezpečnostního incidentu (dále jen „Incident“) je povinen každý zaměstnanec učinit nezbytné kroky vedoucí k eliminaci případné újmy.
2. O Události či Incidentu je vedoucí zaměstnanec pracoviště, na kterém k jeho vzniku došlo, povinen neprodleně informovat Manažera KB.
3. Manažer KB v případě Incidentu zajistí v zákonných lhůtách informování NÚKIB a v přiměřeném čase i Výboru KB.
4. V případě zjištění závažného Incidentu Manažer KB vždy postupem dle čl. 5 odst. 2 písm c) požádá Auditora o provedení auditu. V případě Události postupuje stejným způsobem, rozhodne-li tak Výbor KB.

Článek 8a
Zajišťování kybernetické a informační bezpečnosti

1. Manažer KB v rámci svých činností dle čl. 3 této směrnice vydává po odsouhlasení Výborem KB závazná Pravidla pro zajišťování kybernetické a informační bezpečnosti (dále jen „Pravidla KB“), a to tak, aby tato Pravidla společně vytvořila základní rámec povinností všech osob využívajících kybernetický prostor VUT.
2. Pravidla KB dle předchozího odstavce zahrnují zejména nastavení systému řízení bezpečností informací (dále jen „SŘBI“), návazné postupy a pravidla, které z konkrétních nastavení SŘBI vyplývají, a dále zákonné požadavky na SŘBI, tak jak jsou definovány obecně závaznými právními předpisy.
3. Manažer KB zajišťuje zveřejnění Pravidel KB na webových stránkách https://vut.cz/kybez a prostřednictvím rektora o nich informuje děkany, ředitele vysokoškolských ústavů a ředitele dalších součástí. Každý uživatel kybernetického prostoru VUT je pak povinen seznámit se s takto zveřejněnými Pravidly KB.
4. Všichni vlastníci aktiv jsou povinni v rámci jimi spravovaných aktiv provádět pravidelná hodnocení.

5. Děkani, ředitelé vysokoškolských ústavů a ředitelé dalších součástí jsou povinni za účelem řádného nastavení určit osoby odpovědné za realizaci činností definovaných v Pravidlech KB a sdělit tuto informaci manažerovi KB.

6. Manažer KB:
    - vede seznam osob definovaných v odst. 5,
    - vyhodnocuje a případně aktualizuje znění Pravidel KB.
    - provádí hodnocení dodržování Pravidel KB a případné nedodržování oznamuje Výboru KB.

Článek 9

Závěrečná ustanovení

1. Rektor do 30 dnů od nabytí účinnosti této směrnice jmenuje Manažera KB, Architekta KB, Auditora KB a členy Výboru KB.
2. Tato vnitřní norma nabývá účinnosti v den uvedený v jejím záhlaví.

doc. Ing. Ladislav Janíček, Ph.D., MBA, LL.M.
rektor