SBÍRKA ROZHODNUTÍ A OPATŘENÍ JIHOČESKÉ UNIVERZITY V ČESKÝCH BUDĚJOVICÍCH

číslo: R 511 datum: 17. října 2022

Opatření rektora
k zajišťování kybernetické bezpečnosti na Jihočeské univerzitě v Českých Budějovicích

ČÁST PRVNÍ
ÚVODNÍ USTANOVENÍ

Článek 1
Účel úpravy

Toto opatření upravuje naplnění povinností Jihočeské univerzity v Českých Budějovicích (dále jen „JU“) k zajištění kybernetické bezpečnosti (dále též jen „KB“) na JU, k zajištění jednotného Systému řízení bezpečnosti informací a s tím souvisejícího dohledu nad jeho dodržováním v rámci JU při implementaci a plnění požadavků příslušných právních předpisů v oblasti KB[1] nebo v přímé souvislosti s nimi.

Článek 2
Personální zajištění oblasti KB

Za účelem zajištění KB na JU se zřizují:

a) Výbor pro řízení kybernetické bezpečnosti JU (dále jen „Výbor KB“)
b) pozice Manažera kybernetické bezpečnosti JU (dále jen „Manažer KB“)

ČÁST DRUHÁ
VÝBOR KB

Článek 3
Účel zřízení Výboru KB

Výbor KB je zřízen k zajištění řízení kybernetické bezpečnosti ve smyslu zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů.

---

[1] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Článek 4
Činnost Výboru KB

1. Výbor KB zejména:
   a) stanovuje cíle a strategii KB JU na základě návrhů manažera KB,
   b) poskytuje Útvaru kybernetické bezpečnosti rektorátu JU součinnost při koordinaci přípravy, implementace a rozvoje jednotného Systému řízení bezpečnosti informací JU v oblasti KB (dále jen „SŘBI“),
   c) projednává a doporučuje ke schválení rektorem koncepci bezpečnostní politiky a další dokumentaci v oblasti KB a kontroluje její implementaci v rámci JU,
   d) pomáhá vytvářet koncept KB,
   e) vyjadřuje se k návrhům a implementaci bezpečnostních procesů,
   f) podílí se na hodnocení účinnosti bezpečnostních opatření, jejich důsledků i vhodnosti, včetně identifikace odpovídajících alternativ vhodných pro JU,
   g) projednává zprávy z auditu, vydané a schválené Auditorem KB JU,
   h) informuje vedení JU o opatřeních v oblasti KB.

2. Výbor KB dále projednává a předkládá rektorovi:
   a) posouzení přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení přijatelné míry rizika,
   b) návrh rozpočtu na opatření pro oblast KB,
   c) návrh na stanovení pořadí důležitosti realizace jednotlivých bezpečnostních opatření a bezpečnostních projektů navržených Manažerem KB.

3. Výbor KB projednává a předkládá rektorovi bezpečnostní dokumentaci v oblasti KB, a to zejména:
   a) organizaci a související dokumentaci SŘBI,
   b) seznam informačních a komunikačních systémů zahrnutých do SŘBI,
   c) zprávy z přezkoumání SŘBI,
   d) prohlášení o aplikovatelnosti SŘBI.

4. O své činnosti Výbor KB předkládá rektorovi informativní zprávu nejméně 1x ročně.

5. V oblasti ochrany osobních údajů[2] má Výbor KB následující pravomoci a odpovědnosti:
   a) spolupracuje s pověřencem pro ochranu osobních údajů,
   b) vyjadřuje se k návrhům a implementaci bezpečnostních procesů pro ochranu osobních údajů v rozsahu opatření kybernetické bezpečnosti,
   c) informuje vedení JU o opatřeních v oblasti ochrany osobních údajů v rozsahu opatření kybernetické bezpečnosti,
   d) projednává zprávy z auditu a kontrol v oblasti ochrany osobních údajů zasahující do sféry KB, včetně zpráv z testování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

6. Chod výboru KB zajišťuje po administrativní a organizační stránce Centrum informačních technologií JU.

---

[2] Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), zákon č. 110/2019 Sb., o zpracování osobních údajů, aj.

Článek 5
Složení Výboru KB

1. Výbor KB má nejméně tři členy. Členy Výboru KB jmenuje a odvolává rektor.

2. Členy Výboru KB musí být minimálně:
   a) prorektor nebo člen kolegia rektora, do jehož působnosti spadá oblast informačních technologií a KB, jako předseda Výboru KB,
   b) manažer KB,
   c) ředitel CIT JU.

3. Výbor KB může na své schůze zvát další relevantní osoby.

Článek 6
Práva a povinnosti členů Výboru KB

1. Členové Výboru KB mají právo podílet se aktivně na činnosti Výboru KB, vznášet dotazy, náměty, připomínky k projednávaným zprávám a návrhům, uplatňovat svá stanoviska k řešení problémů.

2. Členové Výboru KB jsou povinni účastnit se jeho schůzí a plnit úkoly, kterými je Výbor KB pověřil.

3. Předseda Výboru KB zejména:
   a) řídí a organizuje činnost Výboru KB, řídí jeho schůze,
   b) vydává stanoviska, doporučení a další dokumenty Výboru KB,
   c) dbá na plnění usnesení přijatých Výborem KB,
   d) ukládá, na základě rozhodnutí Výboru KB, úkoly v oblasti KB a koordinuje jejich plnění za účelem dosažení souladu informačních a komunikačních systémů JU s požadavky právních předpisů a interními normativními akty.

4. Na základě jednání Výboru KB předkládá předseda rektorovi schválené návrhy dokumentů, či požadavků na uskutečnění výdajů z finančních zdrojů JU na zabezpečení nutné míry KB dle článku 4 odst. 2 a 3.

5. V nepřítomnosti předsedy Výboru KB plní jeho úkoly jím určený jiný člen Výboru KB.

Článek 7
Schůze Výboru KB

1. Schůze Výboru KB jsou svolávány podle potřeby, nejméně však jednou za 6 měsíců.

2. Schůzi svolává předseda Výboru KB spolu s manažerem KB, případně alespoň jeden z nich. V době jejich nepřítomnosti svolá schůzi člen Výboru KB určený dle čl. 6 odst. 5.

3. Program schůze Výboru KB navrhuje člen Výboru KB, který svolal schůzi. Vychází přitom z materiálů předložených k projednání, z návrhů členů Výboru KB a úkolů uložených na jeho

schůzích. Členové Výboru KB mohou navrhovat změnu programu před samotnou schůzí i po jejím zahájení.

4. Odborné podklady pro jednání Výboru KB připravují zejména členové Výboru KB.

5. Schůze Výboru KB se může konat prezenčně, distančně s využitím prostředků komunikace na dálku nebo hybridní formou, kdy je část členů Výboru KB přítomna fyzicky a část členů je přítomna distančně s využitím prostředků komunikace na dálku. Formu schůze určí člen Výboru KB, který ji svolal.

6. Výbor KB projevuje svou vůli formou usnesení, která jsou přijímána na základě hlasování zpravidla v rámci schůze Výboru KB.

7. Výbor KB je usnášeníschopný při účasti nadpoloviční většiny všech jeho členů.

8. Ke schválení návrhu je potřeba nadpoloviční většina hlasů všech členů Výboru KB.

9. Jestliže by, s ohledem na význam záležitosti či časové možnosti členů Výboru KB, bylo svolání schůze neúčelné, může předseda Výboru KB rozhodnout o projednání záležitosti a přijetí usnesení mimo schůzi (per rollam), a to pomocí prostředků umožňujících komunikaci na dálku. Toto hlasování se realizuje tak, že předseda Výboru KB rozešle jeho členům přesný text návrhu usnesení a současně stanoví lhůtu, ve které je potřeba provést hlasování. Návrh projednaný mimo schůzi (per rollam) je přijat, pokud pro něj hlasovala nadpoloviční většina všech členů Výboru KB. Po skončení lhůty pro hlasování předseda Výboru KB neprodleně informuje členy Výboru KB o výsledku hlasování.

ČÁST TŘETÍ
MANAŽER KB

Článek 8
Působnost Manažera KB

1. Manažer KB je přímo podřízen rektorovi a je vždy členem Výboru KB. V rámci organizační struktury rektorátu je zařazen do Úseku rektora, do Útvaru kybernetické bezpečnosti.

2. Manažer KB je pověřen komunikací s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“), včetně případů řešení kybernetických bezpečnostních událostí a incidentů.

3. Manažer KB zejména:
   a) odpovídá za plánování a řízení realizace kybernetických bezpečnostních projektů schválených Výborem KB tak, aby informační a komunikační infrastruktura JU poskytovala služby v této oblasti v souladu s právní úpravou v oblasti KB[3],

[3] Např. zákon o kybernetické bezpečnosti, Vyhláška o kybernetické bezpečnosti, příslušné evropské předpisy aj.

b) odpovídá za vytvoření a chod SŘBI od průzkumů a analýz, průběžného testování prevence až po eliminaci následků a vyhodnocení závažných kybernetických incidentů na JU,
c) odpovídá za zajištění schopnosti JU implementovat opatření ukládaná právními předpisy a za včasnou a hospodárnou implementaci těchto opatření,
d) průběžně analyzuje vývoj SŘBI a vyhodnocuje identifikovaná kybernetická rizika, detekované kybernetické bezpečnostní události a odhalené kybernetické bezpečnostní incidenty a předkládá o tom zprávu, jejímž obsahem jsou i návrhy na zmírnění nepřijatelných rizik a návrhy na změnu priorit bezpečnostních projektů, a to pravidelně každé pololetí Výboru KB,
e) v případě identifikace kybernetického bezpečnostního incidentu podá zprávu rektorovi,
f) je oprávněn stanovit:
    i. rozsah a hranice SŘBI (s ohledem na aktiva a organizační bezpečnost), přičemž určí, kterých organizačních částí a technických prvků se SŘBI týká,
    ii. jednotnou metodiku pro identifikaci a hodnocení aktiv a metodiku pro stanovení kritérií pro přijatelnost rizik,
    iii. cíle kontinuity činností a strategii (plán) řízení kontinuity další činnosti pro oblast KB,
    iv. provozní pravidla a postupy SŘBI,
    v. plán zvládání rizik, který obsahuje cíle a přínosy bezpečnostních opatření pro zvládání rizik včetně určení osoby zajišťující prosazování bezpečnostních opatření,
g) podílí se na schvalování závazných norem pro výběr, unifikaci a systemizaci technických a programových prostředků informačních technologií JU,
h) v případě projektů týkajících se informačních systémů se podílí se na přípravě a organizaci akceptačního řízení, včetně bezpečnostního testování,
i) kontroluje po věcné stránce formulaci zadávacích požadavků veřejných zakázek (včetně veřejných zakázek malého rozsahu) na výstavbu a modernizaci informačních a komunikačních systémů JU, či na pořízení dodávek či služeb, jejichž komponenty mohou mít vliv na KB JU, z hlediska standardů KB a poskytuje součinnost v zadávacích řízeních týkající se vyřešení otázek souvisejících s KB,
j) řídí proces řešení kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu a rozhoduje o způsobu řešení,
k) rozhoduje o realizaci bezpečnostního opatření na základě informací z monitorovacích a dohledových systémů, rozhodnutí Výboru KB, nebo NÚKIB,
l) zajišťuje:
    i. detekci kybernetických bezpečnostních událostí a incidentů,
    ii. zpracovávání zpráv o hodnocení aktiv a rizik a prohlášení o aplikovatelnosti, které obsahuje přehled zavedených bezpečnostních opatření,
    iii. u dodavatelů pravidelné hodnocení rizik, provádění kontrol zavedených bezpečnostních opatření u poskytovaných služeb a odstraňování zjištěných nedostatků,
    iv. aktualizaci SŘBI a příslušné dokumentace dle výsledků auditů nebo významných změn a vyhodnocení účinnosti bezpečnostních opatření,
    v. aktualizaci zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí,
    vi. realizaci reaktivních opatření vydaných NÚKIB,
    vii. součinnost při provádění kontrolních auditů prováděných NÚKIB,
m) navrhuje změny strategie KB JU a bezpečnostní politiky SŘBI,
n) vypracovává plán rozvoje bezpečnostního povědomí a s tímto plánem seznamuje Výbor KB,

o) koordinuje opatření ke zvýšení bezpečnostního povědomí v organizaci včetně školení a cvičení KB,
p) odpovídá za stanovení pravidel pro dodavatele, která zohledňují potřeby SŘBI.

4. Manažer KB je oprávněn vyžadovat:
   a) od rektora určení osob pro výkon rolí garantů aktiv a provedení základní identifikace aktiv,
   b) od Výboru KB rozhodnutí o přijatelnosti či nepřijatelnosti identifikovaných kybernetických bezpečnostních rizik včetně stanovení přijatelné míry rizika a stanovení limitu finančních prostředků určených na eliminaci nepřijatelných rizik a o prioritách realizace bezpečnostních opatření a navržených bezpečnostních projektů,
   c) od garantů primárních aktiv zpracování a předložení:
      i. účelu systému a podmínek jeho provozování,
      ii. identifikovaných primárních aktiv a jejich rizik,
      iii. ohodnocení přijatelnosti těchto rizik,
      iv. stanovení bezpečnostních parametrů (úrovní) systémem poskytovaných služeb SLA (Service Level Agreement),
   d) od garantů podpůrných aktiv a administrátorů (tzv. power users):
      i. identifikování podpůrných aktiv a jejich rizik,
      ii. ohodnocení přijatelnosti těchto rizik včetně možnosti přenesení rizik,
      iii. vyhodnocení účinnosti kybernetických bezpečnostních opatření.

ČÁST ČTVRTÁ
Bezpečnost lidských zdrojů

Článek 9
Povinnosti Manažera KB

1. Manažer KB s ohledem na stav a potřeby SŘBI zpracuje plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí, který bude mít náležitosti dle ustanovení § 9 odst. 1 vyhlášky o KB.
2. Manažer KB v souladu s plánem rozvoje bezpečnostního povědomí zajistí:
   a) poučení uživatelů (tj. zaměstnanců, studentů, účastníků kurzů celoživotního vzdělávání a dalších osob využívajících aktiva JU), administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,
   b) pravidelná odborná školení pro osoby zastávající bezpečnostní role, přičemž vychází z aktuálních potřeb JU v oblasti KB,
   c) pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.
3. Manažer KB plní další povinnosti vyplývající z ustanovení § 9 odst. 1 vyhlášky o KB.

Článek 10
Povinnosti uživatelů, administrátorů a osob zastávajících bezpečnostní role

Uživatelé, administrátoři a osoby zastávajících bezpečnostní role jsou povinni:
a) důsledně dodržovat bezpečnostní politiku JU,

b) absolvovat školení dle čl. 9 odst. 2 tohoto opatření,
c) neprodleně oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti.

ČÁST PÁTÁ
ZÁVĚREČNÁ USTANOVENÍ

Článek 11

1. Výbor KB, který byl zřízen již před účinností tohoto opatření, se považuje za Výbor KB zřízený podle tohoto opatření, podle něhož vykonává svou působnost. Totéž obdobně platí i pro členy Výboru KB.
2. Toto opatření nabývá platnosti a účinnosti dnem zveřejnění ve veřejné části webových stránek JU.

prof. PhDr. Bohumil Jiroušek, Dr., v. r.
rektor

Zpracoval: Útvar kybernetické bezpečnosti rektorátu JU
Rozdělovník: Vedení JU, děkani a ředitelé všech součástí JU