Rektorský výnos č. 09/2024

Bezpečnostní politika kybernetické bezpečnosti

I. Úvodní ustanovení

1) Bezpečnostní politika kybernetické bezpečnosti stanovuje a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále také *„zákon o kybernetické bezpečnosti“*) a vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále také *„vyhláška o kybernetické bezpečnosti“*) v podmínkách Univerzity Hradec Králové (dále také *„UHK“*).
2) Účelem tohoto rektorského výnosu je deklarovat a schválit základní principy bezpečnosti pro provoz významných informačních systémů (dále také *„VIS“*) na UHK. Bezpečnostní politika kybernetické bezpečnosti je výchozím dokumentem pro bezpečnostní politiky a bezpečnostní dokumentaci realizující kybernetickou bezpečnost VIS na UHK.

II. Závaznost

1) Povinnost řídit se zákonem o kybernetické bezpečnosti má orgán nebo osoba uvedená v § 3 zákona o kybernetické bezpečnosti. Tento orgán nebo osoba spolupracuje a postupuje alespoň v rozsahu stanoveném v zákoně o kybernetické bezpečnosti. UHK je v souladu s ustanovením § 3 písm. e) zákona o kybernetické bezpečnosti určena jako správce a provozovatel VIS.
2) UHK jako správce a provozovatel VIS implementuje a provádí bezpečnostní opatření, hlásí kontaktní údaje a kybernetické bezpečnostní události a incidenty alespoň v rozsahu stanoveném v zákoně o kybernetické bezpečnosti. Národní úřad pro kybernetickou a informační bezpečnost (dále také *„NÚKIB“*) kontroluje soulad se zákonem o kybernetické bezpečnosti a prováděcími vyhláškami.
3) Tento výnos a navazující bezpečnostní politiky jsou závazné pro všechny zaměstnance a studenty UHK.

III. Rozsah působnosti

1) K zajištění a podpoře kybernetické bezpečnosti se UHK řídí tímto rektorským výnosem, který:
   a) popisuje a vysvětluje zajištění bezpečnosti VIS UHK,
   b) popisuje role a kompetence k zajištění a výkonu agendy kybernetické bezpečnosti na UHK,
   c) stanovuje bezpečnostní strategii,
   d) stanovuje cíle a postupy bezpečnostní strategie,
   e) uvádí strukturu bezpečnostních politik a bezpečnostní dokumentace,
   f) zahrnuje způsoby revize tohoto rektorského výnosu.
2) Problematika kybernetické bezpečnosti pokrývá celou strukturu UHK ve všech lokalitách jejího působení, včetně spolupracujících organizací, které přichází do styku s VIS UHK.
3) Kybernetická bezpečnost se dotýká všech identifikovaných aktiv UHK, a to v míře a rozsahu odpovídajícím významu daného aktiva.

IV. Role a kompetence

1) K zajištění a výkonu agendy kybernetické bezpečnosti na UHK je zřízena role Manažera kybernetické bezpečnosti (dále také *„Manažer KB“*) a poradní sbor Výbor kybernetické bezpečnosti (dále také *„Výbor KB“*).
2) Manažer KB zajišťuje úkony vyplývající z povinností role manažera kybernetické bezpečnosti dle zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. Veškeré činnosti Manažera KB jsou popsány v rektorském výnose upravujícím postavení *Manažera kybernetické bezpečnosti UHK*.[1]
3) Výbor KB je zřízen rektorem UHK k zajištění řízení kybernetické bezpečnosti na UHK ve smyslu zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti. Veškeré činnosti Výboru KB jsou popsány v rektorském výnose upravující postavení *Výboru kybernetické bezpečnosti UHK*[2].

[1] V době vydání tohoto výnosu je interním řídicím aktem upravujícím postavení manažera kybernetické bezpečnosti rektorský výnos č. 17/2023.
[2] V době vydání tohoto výnosu je interním řídicím aktem upravujícím postavení výboru kybernetické bezpečnosti rektorský výnos č. 16/2023.

V. Bezpečnostní strategie

1) Pro bezpečnost VIS UHK se zavádí strategie řízení bezpečnosti. Realizace strategie řízení bezpečnosti vychází z identifikace a hodnocení rizik jednotlivých aktiv využívaných pro provozování VIS.

2) Realizace strategie řízení bezpečnosti je dle zákona o kybernetické bezpečnosti zajišťována těmito bezpečnostními opatřeními:

   a) organizační opatření,

   b) technická opatření.

3) Organizačními opatřeními se dle zákona o kybernetické bezpečnosti rozumí:

   a) systém řízení bezpečnosti informací,

   b) řízení rizik,

   c) bezpečnostní politika,

   d) organizační bezpečnost,

   e) stanovení bezpečnostních požadavků pro dodavatele,

   f) řízení aktiv,

   g) bezpečnost lidských zdrojů,

   h) řízení provozu a komunikací kritické informační infrastruktury nebo významného

   i) informačního systému,

   j) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,

   k) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,

   l) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

   m) řízení kontinuity činností,

   n) kontrola a audit kritické informační infrastruktury a významných informačních systémů.

4) Technickými opatřeními se dle zákona o kybernetické bezpečnosti rozumí:

   a) fyzická bezpečnost,

   b) nástroj pro ochranu integrity komunikačních sítí,

   c) nástroj pro ověřování identity uživatelů,

   d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací,

l) bezpečnost průmyslových a řídících systémů.

VI. Cíle a postupy bezpečnostní strategie

1) Cílem bezpečnostní strategie je zajistit, aby byla kybernetická bezpečnost na UHK řádně vykonávána a nebyl prostřednictvím narušení dostupnosti, důvěrnosti nebo integrity, jakkoliv omezen nebo narušen provoz VIS. Interními opatřeními a postupy pro splnění základních cílů bezpečnostní strategie jsou na UHK prevence, detekce a reakce.

2) Prevencí se rozumí preventivní opatření snižující identifikovaná rizika v závislosti na možnosti jejich technické a ekonomické realizovatelnosti. *Analýza rizik* včetně návrhu *Plánu zvládaní rizik* jsou zpracovávány pravidelně jedenkrát ročně Manažerem KB a nepravidelně v případě podstatných změn v nastavení a konfiguraci VIS UHK. Prioritně jsou využívána technická opatření, organizační opatření jsou zvolena pouze v případě, že ekvivalentní technické opatření neexistuje nebo ho nelze za daných konfiguračních nebo ekonomických podmínek použít.

3) Detekce spočívá v zavedení organizačních a technických opatření pro zajištění včasného odhalení bezpečnostních událostí a bezpečnostních incidentů VIS UHK. Všechny systémy musí zaznamenávat důležitou činnost uživatelů, funkčnost vlastních SW a HW prostředků. Přijatelné riziko, které není ošetřeno příslušnými preventivními opatřeními, musí být zajištěno kvalitní soustavou opatření pro detekci bezpečnostních událostí a incidentů.

4) Reakcí se rozumí specifický postup pro šetření, řešení a případně obnovy VIS UHK, primárně s využitím organizačních opatření s určitou mírou využití technických prostředků.

5) Postupy k zajištění bezpečnostní strategie jsou následující:

   a) zajištění souladu s právními předpisy,

   b) zajištění jednotné ochrany VIS podle požadavků legislativy,

   c) zajištění odpovídajících zdrojů (personálních, technických i finančních) pro oblast kybernetické bezpečnosti,

   d) implementaci bezpečnostních technologií a jejich průběžnou aktualizaci a modernizaci,

   e) zajištění schopnosti zvládání bezpečnostních událostí a incidentů,

   f) zajištění adekvátní úrovně důvěrnosti, integrity a dostupnosti,

   g) formalizaci procesů a postupů,

   h) stanovení odpovědností,

   i) zvýšení úrovně bezpečnostního povědomí zaměstnanců.

6) UHK podporuje stanovené cíle a postupy bezpečnostní strategie a považuje strategii trvalého zajišťování kybernetické bezpečnosti jako nedílnou součást vlastních řídících procesů.

VII. Struktura bezpečnostní dokumentace

1) V rámci řízení kybernetické bezpečnosti udržuje UHK následující systém dokumentace upravující jednotlivé aspekty kybernetické bezpečnosti na UHK:

   a) bezpečnostní politiky,

   b) bezpečnostní dokumentace.

2) Bezpečnostní politiky jsou dostupné na https://www.uhk.cz/kyberbezpecnost-politiky a jsou vydávány v následujícím povinném rozsahu:

   a) Politika systému řízení bezpečnosti informací,

   b) Politika řízení aktiv,

   c) Politika organizační bezpečnosti,

   d) Politik řízení dodavatelů,

   e) Politika bezpečnosti lidských zdrojů,

   f) Politika řízení provozu a komunikací,

   g) Politika řízení přístupu,

   h) Politika bezpečného chování uživatelů,

   i) Politika zálohování a obnovy a dlouhodobého ukládání,

j) Politika bezpečného předávání a výměny informací,

k) Politika řízení technických zranitelností,

l) Politika bezpečného používání mobilních zařízení,

m) Politika akvizice, vývoje a údržby,

n) Politika ochrany osobních údajů,

o) Politika fyzické bezpečnosti,

p) Politika bezpečnosti komunikační sítě,

q) Politika ochrany před škodlivým kódem,

r) Politika nasazení a používání nástrojů pro detekci kybernetických bezpečnostních událostí

s) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

t) Politika bezpečného používání kryptografické ochrany,

u) Politika řízení změn,

v) Politika zvládání kybernetických bezpečnostních incidentů,

w) Politika řízení kontinuity činností.

3) Bezpečnostní dokumentace je vedena v následujícím povinném rozsahu:

a) Zpráva z auditu kybernetické bezpečnosti,

b) Zpráva z přezkoumání systému řízení bezpečnosti informací,

c) Metodiku pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik,

d) Zpráva o hodnocení aktiv a rizik,

e) Prohlášení o aplikovatelnosti,

f) Plán zvládání rizik,

g) Plán rozvoje bezpečnostního povědomí,

h) Evidence změn,

i) Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků.

VIII. Revize bezpečnostní politiky

1) Revize Bezpečnostní politiky kybernetické bezpečnosti se provádí nejméně jednou ročně. Za provedení revize tohoto výnosu rektora odpovídá Manažer KB, finální verzi dokumentu schvaluje Výbor KB.
2) Revize Bezpečnostní politiky kybernetické bezpečnosti:
   a) je zaměřena na bezpečnostní politiky a bezpečnostní dokumentaci,
   b) je zaměřena na zajištění souladu technických a organizačních opatření s bezpečnostními politikami a bezpečnostní dokumentací,
   c) zahrnuje návrhy možností ke zlepšení kybernetické bezpečnosti na UHK,
   d) zahrnuje návrhy změn v provozovaném VIS na UHK.

IX. Závěrečná ustanovení

Tento rektorský výnos vstupuje v platnost i účinnost dnem jeho podpisu.

V Hradci Králové dne 13. 06. 2024

prof. Ing. Kamil Kuča, Ph.D., v. r.
rektor