Politika zvládání kybernetických bezpečnostních incidentů

I. Úvodní ustanovení

1) Politika zvládání kybernetických bezpečnostních incidentů stanovuje postupy a odpovědnosti osob v případech zvládání kybernetického bezpečnostního incidentu a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 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 (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také *„vyhláška o kybernetické bezpečnosti*") v podmínkách Univerzity Hradec Králové (dále také *„UHK*").
2) Účelem politiky je stanovit postupy vedoucí ke snížení dopadů kybernetických bezpečnostních incidentů a k zastavení jejich šíření a k prevenci před jejich opakováním.
3) Tato politika je závazná pro všechny zaměstnance UHK, při jejichž práci jsou používány prvky informačních a komunikačních technologií.

II. Definování kategorií kybernetického bezpečnostního incidentu

1) Kategorie kybernetického bezpečnostního incidentu jsou stanoveny vyhláškou o kybernetické bezpečnosti.
2) Kategorie kybernetického bezpečnostního incidentu je dána úrovní jejich závažnosti a předpokládaného dopadu na aktiva významného informačního systému (dále také *„VIS*") UHK:
   a) kategorie I – méně závažný incident, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje zásahy garantů aktiv nebo administrátorů k omezení dalšího šíření incidentu včetně minimalizace vzniklých škod,
   b) kategorie II – závažný incident, při kterém je narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy garantů aktiv nebo administrátorů k zabránění dalšího šíření incidentu včetně minimalizace vzniklých škod,
   c) kategorie III – velmi závažný incident, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo aktiv. Jeho řešení vyžaduje neprodlené zásahy garantů aktiv nebo administrátorů k zabránění dalšího šíření incidentu včetně minimalizace vzniklých i potenciálních škod.

III. Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů

1) Na UHK je zaveden nástroj pro detekci kybernetických bezpečnostních incidentů.
2) Na UHK je určen nástroj pro evidenci, správu a řešení provozních a bezpečnostních událostí a incidentů, který je jednotným kontaktním místem.
3) Na UHK jsou stanoveny postupy a role pro analýzu kybernetických bezpečnostních událostí, jejich kategorizaci a posouzení, zda se jedná o kybernetický bezpečnostní incident.
4) Postupy zvládání a kybernetických bezpečnostních incidentů jsou stanoveny v závislosti na hodnocení aktiv a rizik jednotlivých prvků informačních a komunikačních technologií.
5) V rámci klasifikace kybernetických bezpečnostních incidentů jsou posuzovány dopady, nutnost reakce a naléhavost řešení.
6) Forma a náležitosti hlášení kybernetických bezpečnostních incidentů Národnímu úřadu pro kybernetickou a informační bezpečnost (dále také *„NÚKIB"*) jsou stanoveny vyhláškou o kybernetické bezpečnosti.
7) Za nahlášení kybernetických bezpečnostních incidentů NÚKIB je na UHK odpovědný Manažer kybernetické bezpečnosti (dále také *„KB"*).

IV. Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů

1) Testování systému zvládání kybernetických bezpečnostních incidentů je dokumentováno a řízeno.
2) Testování systému zvládání kybernetických bezpečnostních incidentů je prováděno jednou za rok.
3) K testování systému zvládání kybernetických bezpečnostních incidentů jsou použita pouze testovací data.

V. Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti

1) Každý kybernetický bezpečnostní incident je hodnocen z hlediska dopadů na důvěrnost, dostupnost a integritu jednotlivých aktiv.
2) Výsledky hodnocení kybernetického bezpečnostního incidentu jsou podnětem pro zlepšování kybernetické bezpečnosti.
3) Opatření plynoucí z vyhodnocení kybernetického bezpečnostního incidentu jsou podnětem pro aktualizaci *Plánu zvládání rizik*.
4) Každý kybernetický bezpečnostní incident, jeho vyhodnocení včetně návrhu na opatření jsou předkládána k projednání Výboru kybernetické bezpečnosti (dále také *„Výbor KB"*).

VI. Evidence incidentů

1) Evidence kybernetických bezpečnostních incidentů je na UHK centrálně vedena v nástroji pro evidenci, správu a řešení provozních a bezpečnostních událostí a incidentů.

2) Za vedení evidence kybernetických bezpečnostních incidentů je odpovědný Vedoucí oddělení informačních technologií (dále také *„Vedoucí OIT"*).

VII. Závěrečná ustanovení

Politika zvládání kybernetických bezpečnostních incidentů vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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