# Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

## I. Úvodní ustanovení

1) Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí stanovuje postupy a odpovědnosti osob v případech zjištění kybernetické bezpečnostní události 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 pravidla nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí a systém bezpečnostních opatření.
3) Tato politika je závazná pro všechny zaměstnance UHK odpovědné za nasazení nástroje pro detekci kybernetických bezpečnostních událostí v rámci UHK.

## II. Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí

1) Pro detekci kybernetických bezpečnostních událostí jsou stanovena pravidla pro zaznamenávání událostí, která jsou dokumentována a řízena.
2) Nástroj pro detekci kybernetických bezpečnostních událostí zajišťuje sběr informací o provozních a bezpečnostních událostech a ochranu získaných informací před neoprávněným využitím nebo jejich změnou.
3) Nástroj pro detekci kybernetických bezpečnostních událostí umožňuje poskytování informací pro určené bezpečnostní role o detekovaných bezpečnostních událostech.
4) Nástroj pro detekci kybernetických bezpečnostních incidentů umožňuje automatickou detekci známých zranitelností včetně pravidelné aktualizace.
5) Nástroj je nastaven ke sběru a zaznamenání bezpečnostních a provozních událostí alespoň v rozsahu:
    a) datum a čas vzniku události,
    b) typ činnosti provedené v prvku informační a komunikační technologie,
    c) identifikace prvku informačního aktiva, které činnost zaznamenalo,
    d) identifikace účtu, pod kterým byla činnost provedena,

e) síťová identifikace zařízení původce události,

f) úspěšnost nebo neúspěšnost provedené činnosti v prvku informační a komunikační technologie,

g) přihlášení a odhlášení ke všem účtům včetně neúspěšných pokusů,

h) činnosti provedené administrátory,

i) manipulace s účty, včetně autentizace nebo autorizace,

j) neprovedení činností v prvku informační a komunikační technologie, v důsledku nedostatku přístupových oprávnění,

k) zahájení a ukončení činností technických aktiv,

l) chybová hlášení technických aktiv,

m) přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a

n) změny nastavení nástroje pro zaznamenávání událostí.

6) Záznamy událostí prvků informačních a komunikačních technologií se povinně u významných informačních systémů (dále také *„VIS"*) uchovávají nejméně po dobu 12 měsíců v souladu s vyhláškou o kybernetické bezpečnosti.

7) Přístupy a pokusy o přístup musí být automaticky zaznamenávány a monitorovány. Záznamy musí být uchovány po dobu minimálně 18 měsíců u systémů provozovaných jako VIS a po dobu minimálně 12 měsíců u ostatních informačních systémů.

8) Rozsah záznamů musí splňovat požadavek na komplexitu souvisejících informací o vzájemně souvisejících aktivitách, na poskytování informací pro určené bezpečnostní role a na uchování důkazů.

9) Všechny prvky informačních a komunikačních technologií jsou napojeny na určený zdroj přesného času a jsou alespoň jednou za den synchronizovány.

10) Správce IKT na Úseku serverové a síťové infrastruktury je odpovědný za využití nástroje pro detekci kybernetických bezpečnostních událostí na UHK.

## III. Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události

1) Na UHK je používán nástroj pro sběr a vyhodnocování kybernetické bezpečnostní události s cílem identifikovat kybernetické bezpečnostní události.

2) Nástroj pro správu a řešení provozních událostí a kybernetických bezpečnostních událostí je jednotným kontaktním místem.

3) Nástroje uvedené v odst. 1 a 2 poskytují informace pro určené provozní a bezpečnostní role o detekovaných kybernetických bezpečnostních událostech, včetně včasného varování.

4) Proces řešení kybernetických bezpečnostních událostí je dokumentován a řízen.

5) Správce IKT na Úseku serverové a síťové infrastruktury je odpovědný za provoz nástroje pro detekci kybernetických bezpečnostních událostí a nástroje pro správu a řešení provozních událostí a kybernetických bezpečnostních událostí.

## IV. Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí

1) Potenciální hrozby jsou v nástroji pro detekci kybernetických bezpečnostních událostí zpracovávány a vyhodnocovány.

2) V případě zjištění neopodstatněné reakce nástroje pro detekci kybernetických bezpečnostních událostí na událost, která není bezpečnostně relevantní, je nutno detekční pravidla nástroje pro detekci kybernetických bezpečnostních událostí upravit.

3) V případě zjištění, že událost není indikována jako chyba, přestože se o chybu jedná a je nutno na ni reagovat jsou upravena detekční pravidla nástroje pro detekci kybernetických bezpečnostních událostí.

4) Za optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí je odpovědný Správce IKT na Úseku serverové a síťové infrastruktury ve spolupráci s Vedoucím OIT.

# V. Závěrečná ustanovení

Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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