Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

I. Úvodní ustanovení

1) Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí stanovuje pravidla využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí 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 této politiky je zajistit kontinuální detekci bezpečnostních událostí, zachycení nových trendů hrozeb i povinností UHK, a udržení komplexního přehledu o existujících hrozbách. Pro trvalou funkčnost nasazených nástrojů pro detekci kybernetických bezpečnostních událostí je nutné zajistit jejich dlouhodobou funkčnost a správné nastavení.

3) Tato politika je závazná pro všechny zaměstnance UHK odpovědné za využití a údržbu nástroje pro detekci kybernetických bezpečnostních událostí v rámci UHK.

II. Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí

1) Pro evidenci a vyhodnocení je využíván nástroj pro správu a řešení provozních a bezpečnostních událostí, který je současně jednotným kontaktním místem.

2) Nástroj pro správu a řešení provozních a bezpečnostních událostí poskytuje informace pro určené bezpečnostní role, uživatele a dodavatele. Přístup k těmto informacím je řízen na základě přístupových oprávnění.

3) V případě vyhodnocení neopodstatněné reakce nástroje na událost, která není bezpečnostně relevantní, jsou upravena detekční pravidla nástroje pro detekci kybernetických bezpečnostních událostí.

4) V případě vyhodnocení, že událost není indikována jako chyba, ale de facto se o chybu jedná a musí být reagováno, jsou upravena detekční pravidla nástroje pro detekci kybernetických bezpečnostních událostí.

5) Za evidenci a vyhodnocení kybernetických bezpečnostních událostí je odpovědný Vedoucí oddělení informačních technologií (dále také *„OIT"*) ve spolupráci s

Manažerem kybernetické bezpečnosti (dále také *„Manažer KB"*) a Garanty příslušných aktiv.

III. Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí

1) Pravidla a postupy určené k řešení kybernetických bezpečnostních jsou řízeny, dokumentovány a pravidelně analyzovány, revidovány a aktualizovány, včetně definice, klasifikace a kategorizace.

2) Aktualizace pravidel a postupů vyhodnocování kybernetických bezpečnostních událostí je prováděna nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí nebo na základě analýzy rizik jednotlivých aktiv.

3) Za aktualizaci nastavení bezpečnostních pravidel pro vyhodnocení kybernetických bezpečnostních událostí je odpovědný Vedoucí OIT ve spolupráci s Manažerem KB a Garanty příslušných aktiv.

IV. Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

1) Pravidla a postupy pro optimalizaci bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí jsou dokumentovány a řízeny a jsou v souladu s aktuálním nastavením aktiv zaznamenaných v evidenci aktiv.

2) Optimalizace nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí je prováděna pro všechny prvky informačních a komunikačních technologií s cílem předcházení kybernetických bezpečnostních událostí.

3) Za optimalizaci nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí je odpovědný Vedoucí OIT ve spolupráci s Manažerem KB a Garanty příslušných aktiv.

V. Závěrečná ustanovení

Politika využití a údržby nástroje pro sběr a vyhodnocení 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