Politika řízení technických zranitelností

I. Úvodní ustanovení

1) Politika řízení technických zranitelností stanovuje pravidla pro řízení technických zranitelností 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:

   - identifikovat zranitelnosti, které by mohly omezit funkčnost nebo bezpečnost provozu prvků informačních a komunikačních technologií,
   - stanovit způsob přijetí opatření k řešení a eliminaci zranitelností,
   - stanovit pravidla pro omezení instalace programového vybavení,
   - stanovit pravidla a postupy vyhledávání opravných programových balíčků,
   - stanovit pravidla a postupy testování oprav programového vybavení,
   - stanovit pravidla a postupy nasazení oprav programového vybavení.

3) Tato politika je závazná pro všechny osoby odpovědné za správu a instalaci programového vybavení v UHK, s přesahem na uživatele daného vybavení.

II. Technické zranitelnosti informačních a komunikačních technologií

1) Technické zranitelnosti informačních a komunikačních technologií se dělí na:

   a) chyby v programovém kódu, které vznikly během vývoje produktů nebo při jejich aktualizacích a opravách,

   b) chyby v instalaci a konfiguraci technických prostředků a instalovaného programového vybavení.

2) Proces řízení technických zranitelností prvků informačních a komunikačních technologií je dokumentovaný a je založen na:

   a) identifikaci zranitelností,

   b) stanovení priorit řešení zranitelností,

   c) řešení zranitelností dle priorit,

   d) implementace náhradního opatření, není-li oprava dostupná,

   e) kontrole aplikovaných opatření.

3) Pro všechny provozované a spravované systémy musí být vypracována metodika nasazení technických zranitelností (patch management), v které je uveden zdroj oprav, plán nasazení, a způsob testování a nasazení.

4) Nasazení oprav zranitelností musí probíhat v souladu s *Politikou řízení změn*.

III. Pravidla pro omezení instalace programového vybavení

1) UHK vede evidenci podpůrných aktiv v *Registru aktiv*.

2) U programového vybavení evidence obsahuje alespoň následující informace:

   a) dodavatele a výrobce programového vybavení,

   b) aktuální nasazenou verzi,

   c) umístění programového vybavení.

3) Je zakázáno instalovat neschválené programové vybavení, smí být instalováno pouze programové vybavení nezbytné pro správnou funkcionalitu a pro jeho správu.

4) Instalace nového programového vybavení musí probíhat v souladu s *Politikou řízení změn*.

5) Aplikační správce VIS je odpovědný za provedení řádné instalace programového vybavení.

IV. Pravidla a postupy vyhledávání opravných programových balíčků

1) Aplikační správce VIS v součinnosti s Garantem podpůrného aktiva pravidelně monitoruje informace o technických zranitelnostech z dostupných zdrojů, identifikuje rizika a navrhuje Vedoucímu oddělení informačních technologií (dále také *„OIT"*) metody řešení.

2) Vedoucí OIT spolu s příslušnými Garanty aktiv posuzuje rizika a stanovuje postup řešení.

3) Po odsouhlasení Vedoucím OIT aplikační správce VIS zajistí instalaci opravných programových balíčků.

V. Pravidla a postupy testování oprav programového vybavení

1) Testování oprav a nového programového vybavení je realizováno v prostředí odděleném od produkčního prostředí.

2) Testy musí prokázat správnost úprav programového vybavení.

3) Nasazení do produkčního prostředí je realizováno po úspěšném vyhodnocení testů a schválením Garantem příslušného aktiva.

4) Pokud není možné realizovat testování programového vybavení z důvodu zvýšených nákladů nebo nedostatku zdrojů, je nutno vyhodnotit všechna související rizika nasazení oprav programového vybavení.

VI. Pravidla a postupy nasazení oprav programového vybavení

1) Pro každý prvek informační a komunikační technologie je řízen a dokumentován proces nasazení oprav programového vybavení.

2) V rámci nasazení oprav programového vybavení do produkčního prostředí jsou vytvořeny body návratu (RPO) a zálohy dat.

3) V případě nasazení oprav programového vybavení jsou zálohovány předchozí verze programového vybavení.

4) Za okolností, kdy záplata na identifikovanou zranitelnost ještě není k dispozici nebo vedlejší účinky jejího zavedení nejsou přijatelné, musí zodpovědný zaměstnanec přijmout alternativní kontrolní opatření jako jsou:

   a) vypnutí služeb, které jsou zranitelností ovlivněny,

   b) úprava nastavení firewallů nebo jiných opatření pro řízení přístupu uživatelů,

   c) zvýšení povědomí uživatelů o detekci a reakci na útoky nebo

   d) zvýšené monitorování činnosti za účelem identifikace útoků na zranitelnost.

5) Za určitých mimořádných okolností umožní aplikační správce VIS instalaci záplaty podle procesu reakce na incident, nikoliv podle procesu řízení změn. každém takovém rozhodnutí pořizuje aplikační správce VIS záznam.

6) Nasazení oprav programového vybavení musí být v souladu s *Politikou řízení změn*.

VII. Závěrečná ustanovení

Politika řízení technických zranitelností vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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