Politika ochrany před škodlivým kódem

I. Úvodní ustanovení

1) Politika ochrany před škodlivým kódem stanovuje pravidla a postupy pro minimalizaci rizik spojených s průnikem škodlivého kódu nebo jiného nežádoucího škodlivého programového prostředku do informačních systémů 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) Tato politika je závazná pro všechny zaměstnance UHK odpovědné za zajištění ochrany před škodlivým kódem v rámci UHK.

II. Pravidla a postupy pro ochranu síťové komunikace

1) Ochrana síťové komunikace je systémově zajištěna a průběžně aktualizována souborem technologických prostředků v celé síti UHK.
2) Nastavení a procesy změn nástroje pro ochranu síťové komunikace jsou dokumentovány a řízeny.
3) Kontrola komunikace mezi jednotlivými segmenty sítě je realizována nástrojem pro ochranu před škodlivým kódem a jsou aplikována opatření pro prevenci a detekování škodlivých programových kódů.
4) Záznamy událostí z nástroje pro ochranu síťové komunikace jsou centrálně ukládány.
5) Správce IKT na Úseku serverové a síťové infrastruktury odpovídá za realizaci ochrany síťové komunikace před škodlivým kódem.

III. Pravidla a postupy pro ochranu serverů a sdílených datových úložišť

1) Ochrana serverů a sdílených datových úložišť je zajištěna centrálním nástrojem pro ochranu před škodlivým kódem a jsou aplikována opatření pro prevenci a detekování škodlivých programových kódů.
2) Nastavení a procesy změn nástroje pro ochranu serverů a sdílených datových úložišť jsou dokumentovány a řízeny.
3) Jsou nastavena opatření pro detekci, prevenci a obnovu infikovaných dat, s upřednostněním smazání zavirovaného souboru před jeho léčbou.
4) Záznamy událostí (detekce škodlivého kódu) z nástrojů pro ochranu serverů a sdílených datových úložišť jsou centrálně ukládány.
5) Správce IKT na Úseku serverové a síťové infrastruktury odpovídá za realizaci ochrany serverů a sdílených datových úložišť před škodlivým kódem.

IV. Pravidla a postupy pro ochranu pracovních stanic

1) Nástroj pro ochranu před škodlivým kódem je součástí programového vybavení každé pracovní stanice a je pravidelně a centrálně aktualizován.
2) Jsou nastavena opatření pro detekci, prevenci a obnovu infikovaných dat s upřednostněním smazání zavirovaného souboru před jeho léčbou.
3) Záznamy událostí (detekce škodlivého kódu) z nástroje pro ochranu pracovních stanic jsou centrálně ukládány.
4) Uživatelům je zakázáno měnit na pracovní stanici konfiguraci nástroje pro ochranu před škodlivým kódem.
5) Zásady ochrany před škodlivým kódem jsou součástí zvyšování bezpečnostního povědomí uživatelů.
6) Správce IKT na Úseku serverové a síťové infrastruktury odpovídá za centrální distribuci a aktualizaci nástroje pro ochranu pracovních stanic před škodlivým kódem.

V. Závěrečná ustanovení

Politika ochrany před škodlivým kódem vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

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