

Kód:	SR/1/2025	
Číslo jednací:	UTB/25/000183	
Klasifikace dokumentu:	INTERNÍ	
Druh:	SMĚRNICE REKTORA	
Název:	Politika řízení technických zranitelností	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	08.01.2025	Verze: 01
Účinnost:	13.01.2025	
Vydává:	Rektor	
Zpracoval:	Manažer kybernetické bezpečnosti	
Spolupracoval:	Centrum výpočetní techniky, Právní oddělení, pověřenec OOÚ	
Počet stran:	4	
Počet příloh:	0	
Rozdělovník:	zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D., v.r.	

Článek 1 Úvodní ustanovení

- (1) Politika řízení technických zranitelností jako součást *Deklarace kybernetické bezpečnosti Univerzity Tomáše Bati ve Zlíně* stanovuje postupy a protokoly podporující účinnou správu aktiv dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „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 (dále jen „vyhláška o kybernetické bezpečnosti“) v podmínkách Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“).
- (2) Účelem této politiky je identifikovat slabá místa, kde by mohlo dojít k omezení funkčnosti nebo bezpečnosti provozu (dále jen „technická zranitelnost“) významného informačního systému (dále jen „VIS“), 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 v podmínkách UTB.
- (3) Tato politika se vztahuje na všechny zaměstnance UTB, informační aktiva vytvořená nebo používaná v rámci VIS, a na uživatele těchto aktiv.
- (4) Jednotlivé pojmy používané v této směrnici jsou vymezeny zejména zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti. Přehled jednotlivých pojmů je uveden v dokumentu *Pojmy kybernetické bezpečnosti*, který je dostupný na webu UTB v sekci *Kybernetická bezpečnost*.

Článek 2

Technické zranitelnosti aktiv

- (1) Aktivy pro stanovení technických zranitelností se rozumí všechna primární aktiva a vybraná podpůrná aktiva v kategorii programového vybavení podle katalogu primárních a podpůrných aktiv v chráněném dokumentu *Hodnocení aktiv a rizik*.
- (2) Technické zranitelnosti aktiv podle odstavce 1 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.
- (3) Proces řízení zranitelností programového vybavení 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.
- (4) Pro odstranění technických zranitelností aktiv podle odstavce 1 musí být zpracována metodika obsahující minimálně identifikaci zdroje oprav, způsob testování a plán nasazení.

Článek 3

Pravidla pro omezení instalace programového vybavení

- (1) Katalog primárních a podpůrných aktiv v chráněném dokumentu *Hodnocení aktiv a rizik* obsahuje u programového vybavení alespoň následující informace:
 - a) dodavatele a výrobce programového vybavení,
 - b) aktuální nasazenou verzi,
 - c) umístění programového vybavení.
- (2) Smí být instalováno pouze takové programové vybavení, které je nezbytné pro správnou funkcionalitu a pro jeho správu a které doporučil dodavatel příslušného programového vybavení.
- (3) Je zakázáno instalovat neschválené programové vybavení, verze programového vybavení se známou zranitelností, příp. bezpečnostní hrozbou hlášenou nadřízenými organizacemi (např. Národní úřad pro kybernetickou a informační bezpečnost) a organizací CESNET, zájmovým sdružením právnických osob, založeným podle občanského zákoníku veřejnými vysokými školami v České republice a Akademií věd České republiky.
- (4) Instalace nového programového vybavení podléhá procesu evidence a sledování změn, za provedení řádné instalace programového vybavení odpovídá garant příslušného aktiva.

Článek 4

Pravidla a postupy vyhledávání opravných programových balíčků

- (1) Garant příslušného aktiva pravidelně monitoruje informace o technických zranitelnostech z dostupných zdrojů, identifikuje rizika a navrhuje řediteli Centra výpočetní techniky UTB (dále jen „CVT“) metody řešení.
- (2) Ředitel CVT spolu s příslušnými Garanty posuzuje rizika a stanovuje postup řešení.
- (3) Po odsouhlasení ředitelem CVT zajistí Garant příslušného aktiva instalaci opravných programových balíčků.
- (4) Ředitel CVT je povinen o postupu podle odstavců 1 až 3 informovat Manažera KB.

Článek 5

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.

Článek 6

Pravidla a postupy nasazení oprav programového vybavení

- (1) Pro každé aktivum je proces nasazení oprav programového vybavení řízen a dokumentován v souladu s *Přílohou č. 1b Politiky řízení aktiv – Zacházení s aktivy*.
- (2) V rámci nasazení oprav programového vybavení do produkčního prostředí jsou vytvořeny body obnovy dat (Recovery Point Objective) a zálohy dat.
- (3) V případě nasazení oprav programového vybavení jsou zálohovány předchozí verze programového vybavení.
- (4) Pokud oprava identifikované zranitelnosti není k dispozici nebo vedlejší účinky jejího nasazení nejsou přijatelné, musí Garant příslušného aktiva 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, kdy by mohlo dojít k bezprostřednímu ohrožení důvěrnosti, dostupnosti a integrity dat, umožní Garant příslušného aktiva instalaci opravy podle procesu reakce na kybernetický bezpečnostní incident, nikoliv podle procesu řízení změn. O každém takovém rozhodnutí, které musí schválit ředitel CVT, pořizuje Garant příslušného aktiva záznam a informuje Manažera KB a pověřence OOÚ.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
08.01.2025	01	Manažer KB	Vytvoření dokumentu