Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-011**
Název dokumentu:	**Politika řízení technických zranitelností**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Politika se vztahuje na všechny osoby odpovědné za správu a instalaci programového vybavení na JU, s přesahem na uživatele daného vybavení.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 8, 10, 11, 13
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07.2026**
Platnost do:	odvolání
Počet stran + příloh:	2 + 0
Verze:	1.1
Význam a benefity:	Politika má za cíl zvýšit úroveň zabezpečení a kontroly nad programovým vybavením JU, a to snížením rizik souvisejících s instalací, aktualizací (změnami) a používáním daného programového vybavení.
Uložení:	Sekce kyberbezpečnosti na Wiki JU
Ruší dokumenty:	-
Zpracovatel:	Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

Za zranitelnost je považováno slabé místo aktiva nebo slabé místo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

JU musí chránit integritu programového vybavení zavedením opatření detekce a prevence proti škodlivému kódu. Rovněž musí zajistit, aby byly zavedeny vhodné postupy pro informovanost uživatelů, v souladu s Politikou bezpečnosti lidských zdrojů.

Instalace programového vybavení musí být v souladu s Politikou řízení změn a Politikou ochrany před škodlivým kódem.

a) Pravidla pro omezení instalace programového vybavení

Je zakázáno instalovat jakékoliv programové vybavení z nedůvěryhodných zdrojů na pracovní stanice zaměstnanců. Rovněž je zakázáno instalovat jakékoliv programové vybavení na počítače ve studovnách, bez předešlého souhlasu správců daných počítačů.

Za instalaci důvěryhodného programového vybavení na servery JU jsou odpovědní správci serverů.

b) Pravidla a postupy vyhledávání opravných programových balíčků

U každého programového balíku se JU musí řídit podle důvěryhodného zdroje informací o identifikovaných zranitelnostech (např. https://nvd.nist.gov/) a o vydaných záplatách (obvykle webové stránky dodavatele nebo vhodně nakonfigurovaným serverem pro automatické aktualizace).

c) Pravidla a postupy testování oprav programového vybavení

Pro zajištění správné funkce opravného programového balíčku a zamezení vedlejších účinků na ostatní systémy, zodpovědný pracovník před jeho hromadným nasazením provede jeho otestování a vyhodnocení.

d) Pravidla a postupy nasazení oprav programového vybavení

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

- vypnutí služeb, které jsou zranitelností ovlivněny,
- úprava nastavení firewallů nebo jiných opatření pro řízení přístupu uživatelů,
- zvýšení povědomí uživatelů o detekci a reakci na útoky, nebo
- zvýšené monitorování činnosti za účelem identifikace útoků na zranitelnost.

Za určitých mimořádných okolností umožní správce aktiva instalaci záplaty podle procesu reakce na incident, nikoliv podle procesu řízení změn; o každém takovém rozhodnutí pořizuje správce aktiva záznam.

Nasazení oprav programového vybavení musí být v souladu s Politikou řízení změn[1].

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.

[1] ;Za určitých mimořádných okolností se nasazení oprav programového vybavení řídí podle procesu reakce na incident, nikoliv podle procesu řízení změn.