Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-019**
Název dokumentu:	**Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí (KBU)**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Vztahuje se na všechny detekční nástroje schopné poskytnout informaci o bezpečnostních událostech.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 14, 23, 24
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 zajistit kontinuální detekci bezpečnostních událostí, zachycení nových trendů hrozeb i povinností organizace, a udržení komplexního přehledu o existujících hrozbách.
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

Pro trvalou funkčnost nasazených nástrojů pro detekci kybernetických bezpečnostních událostí je nutné zajistit jejich dlouhodobou funkčnost a správné nastavení.

a) Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí

Existuje seznam, jakým způsobem jsou bezpečnostní události evidovány, např. oznámení zaměstnanců a dodavatelů v Servicedesk, události detekované SW nástrojem atp.

Je stanoven způsob, jak se má událost vyhodnotit a zařadit do klasifikačních stupňů podle jejího významu (typ události, velikost možného dopadu).

Události klasifikované jako bezpečnostní incident musí být eskalovány k manažerovi kybernetické bezpečnosti.

MKB má postup, jakým způsobem má být incident vyhodnocen a jak má být klasifikován. Pro každý klasifikační stupeň musí být určeny způsoby jeho eskalace a vypořádání.

b) Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí

Manažer KB pravidelně kontroluje:

1. úspěšnost označení událostí za bezpečnostní incident a jejich závažnost,
2. shodu nastavených detekčních parametrů se závažností incidentu,
3. komplexnost nástrojů pro detekci událostí vůči zákonným povinnostem organizace,
4. parametry detekovaných událostí:
    - záznam (událost je detekována, evidována, sebrána, uložena, povšimnuta=zviditelněna),
    - nástroj, kde byla detekována – správce (jeho existenci, nastavení přístupových práv) - způsob vyhodnocení (automaticky/manuálně z reportu),
    - funkčnost eskalace události do incidentu,
    - úspěšnost využití získané informace.

Dle výsledků provádí návrhy změn do seznamu SW nástrojů sloužících k detekci bezpečnostních událostí.

c) Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Manažer kybernetické bezpečnosti dle seznamu všech nástrojů sloužících k detekci bezpečnostních událostí určuje:

- parametry detekce rozhodující k posouzení závažnosti bezpečnostních událostí,
- způsob sběru informací o bezpečnostních událostech.

Správce nástroje sloužícího k detekci bezpečnostních událostí provádí nastavení požadovaných funkcionalit tak, aby detekované události poskytovaly potřebnou informaci nebo přispívaly k celkovému posouzení události a jejich korelaci s jinými nástroji.

4. Historie revizí

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