Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-018**
Název dokumentu:	**Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí (KBU)**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Bezpečnostní událost je každá událost, která má nebo by mohla mít dopad na bezpečnost informací, tzn. jejich důvěrnost, dostupnost, nebo integritu. Může to být i událost, která je nahlášena fyzickými nebo právnickými osobami. Příklady událostí jsou vypsány v úvodu informačního vyhlášení.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 22, 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:	Bez přehledu o bezpečnostních událostech, nemůže dojít k jejich posouzení. Jejich detekce, záznam, evidence, sběr, vyhodnocení jsou podkladem pro řízení bezpečného provozu. Musí být stanoveny nástroje pro detekci bezpečnostních událostí a určen způsob a rozsah jejich nastavení a použití.
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

JU musí zajistit detekci kybernetických bezpečnostních událostí přiměřeně s ohledem na důležitost aktiv v rámci:

- koncových stanic,
- mobilních zařízení,
- serverů,
- datových úložišť a výměnných datových nosičů,
- síťových aktivních prvků a
- obdobných aktiv.

V potaz bezpečnostní události se jedná např. o:

- detekovaný nepovedený pokus o přístup do systému / k informacím (např. zapomenuté heslo),
- plánovanou (avizovanou) nedostupnost např. z důvodu údržby nebo jakoukoliv událost, jejíž opakovaný/mnohonásobný výskyt by mohl narušit dostupnost,
- škodlivý kód detekovaný a zachycený antivirovou ochranou dříve, než byly napáchány jakékoliv škody,
- detekovaný pokus o překonání technického opatření,
- snahu zaměstnance o kopírování velkého množství dat, která přímo nesouvisejí s jeho každodenní pracovní náplní, ale ke kterým potřebuje mít přístup a tato aktivita byla speciálním nástrojem detekována a zamítnuta atp.

Událost přímo nezpůsobí incident, ale její výskyt je významný a jejím ignorováním může v budoucnu dojít k incidentu.

a) Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí

JU kombinuje manuální a automatizované způsoby detekce, zjištění a záznamu událostí. Tyto postupy zahrnují oznámení zaměstnanců a zainteresovaných stran (včetně dodavatelů a NÚKIB), která jsou integrovaná s výstupy všech aplikovaných elektronických a SW nástrojů, zejména SIEM, EZS atp.

V rámci komunikační sítě, jejíž součástí je informační a komunikační systém, JU používá nástroj pro detekci kybernetických bezpečnostních událostí, který zajišťuje:

- ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi,
- ověření a kontrolu přenášených dat na perimetru komunikační sítě a
- blokování nežádoucí komunikace.

Rozsah záznamů striktně splňuje požadavek na komplexitu souvisejících informací o vzájemně souvisejících aktivitách, na poskytování informací pro určené bezpečnostní role a na uchování důkazů.

- Kompletní pravidla a postupy jsou k dispozici ve směrnici pro řízení KBU JU.

b) Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události

JU uplatňuje standardizované způsoby, jak na zjištěné události reagovat. Události klasifikované jako incident se bezodkladně eskalují k MKB.

Technické a provozní postupy zahrnují seskupování záznamů a dohledání kompletního řetězce potřebných informací, identifikačních parametrů (jako jsou ID osoby, čas, IP adresa, MAC adresa či použitý protokol) a využitých služeb. Cílem těchto kroků je spolehlivá identifikace incidentů a zajištění průkazného uchování důkazů.

Do těchto procesů spadají také postupy včasného varování správců systémů, nasazení okamžitých restriktivních opatření a poskytování zpětné vazby, která slouží pro správné nastavení a rekonfiguraci technologických bezpečnostních opatření infrastruktury.

- Kompletní metodika a postupy jsou k dispozici ve směrnici pro řízení KBU JU.

c) Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí

Existuje seznam všech SW nástrojů sloužících k detekci bezpečnostních událostí.

Pro každý SW nástroj sloužící k detekci bezpečnostních událostí musí být stanoveno

1. k čemu nástroj slouží a v jakém rozsahu je používán,
2. kdo odpovídá za jeho správu a monitoring, reporting bezpečnostních událostí,
3. jak jsou evidovány a zálohovány detekované bezpečnostní události,
4. jak je nástroj aktualizován a pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje.

Historie revizí

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