Politika zvládání Kybernetických Bezpečnostních Incidentů (KBI)

Verze 1.0

Obsah

1. Úvod, cíl a rozsah

1.1 Cíl politiky

Cílem této politiky je zajistit **jednotný, důsledný a efektivní přístup** ke zvládání kybernetických bezpečnostních incidentů (KBI) s cílem minimalizovat jejich dopad na kritické systémy, služby a aktiva Univerzity. Politika stanovuje jasné role, odpovědnosti a postupy pro detekci, analýzu, řešení, hlášení a následné vyhodnocení KBI.

1.2 Rozsah a legislativní rámec

Tato politika je závazná pro všechny zaměstnance, externí dodavatele a aktivní systémy Univerzity, jejichž činnost souvisí s provozem nebo zabezpečením informačních a komunikačních systémů.

Univerzita je **poskytovatel regulované služby s vyššími povinnostmi** dle Zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen ZoKB), souvisejícími vyhláškami a metodickým pokynem NÚKIB k hlášení KBI.

2. Definice a role

2.1 Vysvětlení klíčových pojmů

- **Kybernetická bezpečnostní událost (dále jen KBU):** Stav systému nebo sítě, který signalizuje **možné** narušení bezpečnosti (např. neúspěšné pokusy o přihlášení, vysoká zátěž procesoru).
- **Kybernetický bezpečnostní incident (dále jen KBI):** Potvrzená Událost, která ohrožuje nebo narušuje **Důvěrnost, Integritu nebo Dostupnost (DIA)** informací, systémů nebo služeb.
- **CSIRT:** Zkratka pro **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam, jedná se o specializovaný tým pro reakci na KBU/KBI, který je hlavní operační jednotkou pro technické zvládání a řešení bezpečnostních hrozeb v organizaci. CSIRT je tedy operačním jádrem celého procesu zvládání incidentů, zatímco Manažer KB (MKB) má roli řídící a regulatorní (hlášení na NÚKIB, vyhodnocení, komunikace s vedením).
- **Osobní Údaje:** Jakékoli informace týkající se identifikované nebo identifikovatelné fyzické osoby.
- **Triage:** CSIRT posuzuje 3 otázky: Je to reálná hrozba? (Odrážejí se logy reálnému útoku, nebo jde o falešný poplach/chybu systému?), Jak je to závažné? (Jak velký je dopad, jaká je pravděpodobnost a rychlost šíření?), Kdo to má řešit? (Má se to předat technikům, nebo Manažerovi KB k hlášení NÚKIB?)

2.2 Role a odpovědnosti

Role	Zodpovědnost v procesu KBI
Zaměstnanec/Uživatel	Hlášení KBU/KBI na stanovené kontaktní body.
CSIRT Tým	**Příjem, triage a analýza** KBU. **Vlastní řešení incidentu** (izolace, odstranění, obnova). Předání potvrzených KBI Manažerovi kybernetické bezpečnosti (dál jen MKB) k posouzení hlášení.
Manažer KB (MKB)	**Vyhodnocení** KBI (klasifikace a kategorizace dopadu). **Zodpovědnost za hlášení NÚKIBu** (prvotní hlášení, závěrečná zpráva). Komunikace s vedením UJEP. Post-mortem analýza.
Krizový tým	Svolán MKB v případě KBI - **kategorie III** (Vysoký dopad). Zahrnuje MKB, vedení UJEP (rektor, kvestor), DPO, tiskového mluvčího a zástupce právního oddělení.
Výbor KB	Schvaluje výsledky testování a revizí; bere na vědomí statistiky incidentů.

3. Hlášení a detekce KBU

3.1 Zdroje a způsoby hlášení (CSIRT)

Všechny KB události a potenciální KBI se hlásí a evidují centrálně v RT systému.

Zdroj hlášení	Popis
Automatizované hlášení	Výstupy a alarmy z bezpečnostních nástrojů **SIEM/SPLUNK**. Tyto výstupy jsou primárním a nepřetržitým zdrojem KBU pro CSIRT, které následně CSIRT zpracovává dle metodického pokynu jak přímo v SIEM, tak do RT systému pro účely následné evidence.
E-mailové hlášení	Zaměstnanci hlásí KBU e-mailem na adresu **kb@rt.ujep.cz**. Ticketovací systém RT (Request Tracker) automaticky eviduje hlášení, čímž vzniká záznam o KBU.

Zdroj hlášení	Popis
Telefonické hlášení	Závažné/časově kritické KBU lze hlásit telefonicky členům CSIRT nebo MKB, jejich telefonní čísla jsou dostupná na webu UJEP. Následně je MKB/CSIRT povinen založit záznam v systému RT.

3.2 Klasifikace a kategorizace dopadu KBU

Po detekci a základní analýze provede CSIRT a MKB klasifikaci KBU do jedné z následujících kategorií. Klasifikace se opírá o míru dopadu na **Důvěrnost, Integritu a Dostupnost (DIA)** kritických aktiv Univerzity.

Kategorie	Dopad	Kritéria pro Posouzení
Kategorie I	**Nízký**	Krátkodobý lokální výpadek nekritické služby (< 8h); únik/modifikace nekritických dat. Omezený výpadek **nekritické služby**, lokální napadení (jedna stanice), minimální únik dat. Nezasahuje do chodu univerzity. Postačí interní evidence a řešení.
Kategorie II	**Střední**	Výpadek klíčové služby (8h-24h), např. studijního systému. Únik malého množství citlivých osobních údajů, vyžaduje nasazení více zdrojů (např. napadení diskového pole). Nutné hlášení KBI na NÚKIB, kde je nutné řešit i dopad na osobní údaje.
Kategorie III	**Vysoký/Krizový**	Výpadek kritických služeb (> 24h); masivní únik citlivých osobních údajů, kompromitace administrátorských účtů nebo kritického IS, ohrožení činnosti univerzity. Nutná aktivizace Krizového týmu a plné externí hlášení na NÚKIB.

4. Fáze zvládání KBI (metodika pro CSIRT)

Proces zvládání incidentu se řídí modelem, který zahrnuje pět hlavních fází:

4.1 Příprava

Zajištění dokumentace (tato Politika), školení zaměstnanců, existence funkčních nástrojů (SIEM/SPLUNK, RT, zálohování) a definování komunikačních kanálů.

4.2 Detekce a analýza

- Příjem hlášení KBU (SIEM, RT, telefon).
- **Triage:** Posouzení hlášení KBU
- **Analýza a Ověření:** Potvrzení KBU jako KBI. Určení rozsahu a původce.
- **Kategorizace:** Přiřazení kategorie I, II nebo III (viz bod 3.2).
- **Hlášení MKB:** Informování MKB pro rozhodnutí o hlášení na NÚKIB.

4.3 Zvládání

Tato fáze je primární zodpovědností CSIRT.

- **Izolace:** Okamžitá akce k zastavení šíření incidentu (odpojení sítí, blokování účtů, zastavení služeb).
- **Odstranění:** Identifikace a odstranění **příčiny** incidentu (odstranění malwaru, oprava zranitelnosti, zneplatnění kompromitovaných údajů).
- **Obnova:** Obnovení postižených systémů a dat do normálního stavu (např. z čistých záloh) a nasazení preventivních opatření.

4.4 Vyhodnocení

Po uzavření incidentu provede MKB detailní post-mortem analýzu. Cílem je zjistit, co se stalo, jaká byla reakce a co je potřeba zlepšit. Výsledky vedou k revizi analýzy rizika další bezpečnostní dokumentace včetně této politiky.

5. Eskalace a povinnosti Hlášení

5.1 Povinnost hlášení na NÚKIB

Jako subjekt s **vyššími povinnostmi** je MKB povinen hlásit na NÚKIB **všechny KBI**, u nichž **nelze bez zbytečného odkladu vyloučit úmyslné zavinění**.

Lhůta Hlášení (ZKB)	**Zodpovědnost**
Prvotní hlášení: Bez zbytečného odkladu, **nejpozději do 24 hodin** od okamžiku, kdy MKB KBI identifikoval.	MKB
Závěrečná zpráva: Do 30 dnů od oznámení/vyřešení incidentu.	MKB

5.2 Eskalační politika (Univerzita)

Subjekt/Role	Kategorie I (Nízký dopad)	Kategorie II (Střední dopad)	Kategorie III (Vysoký dopad)
Vedení UJEP	**Ne**	**ANO -** Rektor/Kvestor informováni prostřednictvím MKB **e-mailem**.	**ANO - okamžitá telefonická eskalace**. Svolání Krizového týmu.
DPO (GDPR)	**Ne**	**ANO** – informování DPO. Posouzení hlášení ÚOOÚ (do 72h), pokud došlo k úniku osobních údajů.	**ANO** – Okamžité zapojení DPO. Hlášení ÚOOÚ a subjektům údajů (je-li vyžadováno).
Tiskový mluvčí	**Ne**	**Ne**	**ANO - aktivní komunikace:** Tiskový mluvčí připravuje a spravuje oficiální prohlášení.
Právní Oddělení	Ne	**Ne**	**ANO** – Posouzení hlášení **Policii ČR** (podezření na trestný čin).

6. Vyhodnocení, testování a evidence

6.1 Evidence KBI

Veškerá evidence KBI je vedena v centralizovaném nástroji **RT (Request Tracker)** a obsahuje minimálně: číslo, datum hlášení, zdroj hlášení, typ, dopad, klasifikaci (I, II, III), stav, opatření a datum uzavření.

6.2 Testování a revize

- **Revize Politiky a plánů:** MKB provádí revizi této politiky a plánů zvládání incidentů **1x ročně**

Ing. Jan Povolný

Digitálně podepsal Ing. Jan Povolný
Datum: 2025.11.18 18:02:34 +01'00'