Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-022**
Název dokumentu:	**Politika zvládání kybernetických bezpečnostních incidentů**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Tato politika je závazná pro všechny pracovníky, jejichž působnost souvisí se zvládáním kybernetických bezpečnostních incidentů (KBI). Definované postupy lze v případě potřeby využít také pro ostatní oblasti kybernetické bezpečnosti (KB).
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 14, 22, 23, 24
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	4 + 3
Verze:	1.1
Význam a benefity:	Norma ISO 27002: Cílem je zajistit důsledný a efektivní přístup k řízení incidentů bezpečnosti informací, včetně komunikace ohledně bezpečnostních událostí a slabých míst. Pro praxi je nejdůležitějším přínosem minimalizace dopadů incidentů.
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

Politika obsahuje proces sledování, zaznamenávání a vyhodnocování bezpečnostních událostí a řízení efektivního řešení incidentů s cílem umožnit pokračování nebo obnovení kritických funkcí a procesů v případě jejich reálného nebo teoretického narušení pomocí přijetí vhodných nápravných opatření (omezení opakovaného vzniku) a účinných plánů interní komunikace. Systémy musí být nastavené tak, aby bylo možné, po stanovený čas, analyzovat důkazy o činnostech vedoucích k incidentům.

a) Definování kategorií kybernetického bezpečnostního incidentu

Určujícím měřítkem stupně událostí/incidentů je velikost jejich dopadu.

Stupně dopadu

- Kybernetická bezpečnostní událost – není incidentem, nikam se nehlásí
- Interní kybernetický bezpečnostní incident – interní klasifikace organizace, zvážit nahlášení CERT týmu
- Kybernetický bezpečnostní incident – Méně závažný (Kategorie I), nízký dopad, hlásit CERT týmu
- Kybernetický bezpečnostní incident – Závažný (Kategorie II), střední dopad, hlásit CERT týmu
- Kybernetický bezpečnostní incident – Velmi závažný (Kategorie III), vysoký dopad, hlásit CERT týmu

Kategorie incidentů (typy) jsou implementovány v systému evidence incidentů

- Sociální inženýrství, podezřelá emailová komunikace (phishing, pharming, atp.)
- Ztráta či modifikace dat (souborů, osobních údajů)
- Zneužití autorských práv
- Ztráta/krádež ICT techniky (mobilní zařízení, notebook, tablet, USB, externí harddisk)
- Prolomení hesel, neoprávněný přístup do systému / k informacím (zneužití přihlášení osob, aplikací)
- škodlivý kód, SW, napadená ICT technika (vir, malware, trojský kůň, spyware, ransomware, adware)
- Omezení dostupnosti systému / IT služeb (DoS, DDoS, hacking, botnet)
- Porucha hardware (monitor, klávesnice, tiskárny, příslušenství ICT)
- Porucha software (operační systém, aplikace, programy)
- Překonání technických opatření (včetně neoprávněného přístupu do chráněných prostor)
- Porušení organizačních opatření
- Jiný bezpečnostní incident

b) Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů

Každý zaměstnanec je povinen ohlásit/zaznamenat jakoukoliv událost, která má nebo by mohla mít vliv na bezpečnost informací do kontaktního formuláře nebo aplikace, popřípadě přímému nadřízenému. Hlášení může podat i veřejnost.

Evidence hlášení (podoba záznamu) musí obsahovat:

- autora (jméno a příjmení, ideálně i uživatelské jméno),
- čas (kdy byla bezpečnostní událost detekována),
- popis,
- kontakt.

Událost posoudí (identifikuje) určená osoba (defaultně Manažer KB) a přidá atributy:

- kdo ji posoudil,
- reakce na podání, poděkování, upřesňující dotaz, informace o stavu,
- klasifikace událost/incident,
- stav (registrován, planý poplach, přidělen, přijat, řešen, vyřešen, uzavřen).[1]

K incidentu je potřeba přiřadit záznamy:

- stanovená opatření 1, 2, 3, atd. a workflow pro kontrolu splnění opatření (kdo, co, kde, kdy nastavil, příloha souboru, LOGu),
- stupeň incidentu, jaký je jeho dopad (textový popis různých typů dopadů a jejich výše),
- kategorie (textový popis nebo výběr ze seznamu),
- příčina (textový popis),
- dokumentace a důkazní materiály související se vznikem incidentu,
- eskalace (textový popis kdo byl informován, řeší, atd.),
- důkazy (přiložit soubory XLSX, DOCX, MSG, JPG, TXT, atd.).
- účinnost opatření (textový popis),
- poznámka (textový popis),
- po realizaci všech opatření datum ukončení řešení incidentu,
- výsledek (textový popis),
- případně odpověď autorovi hlášení.

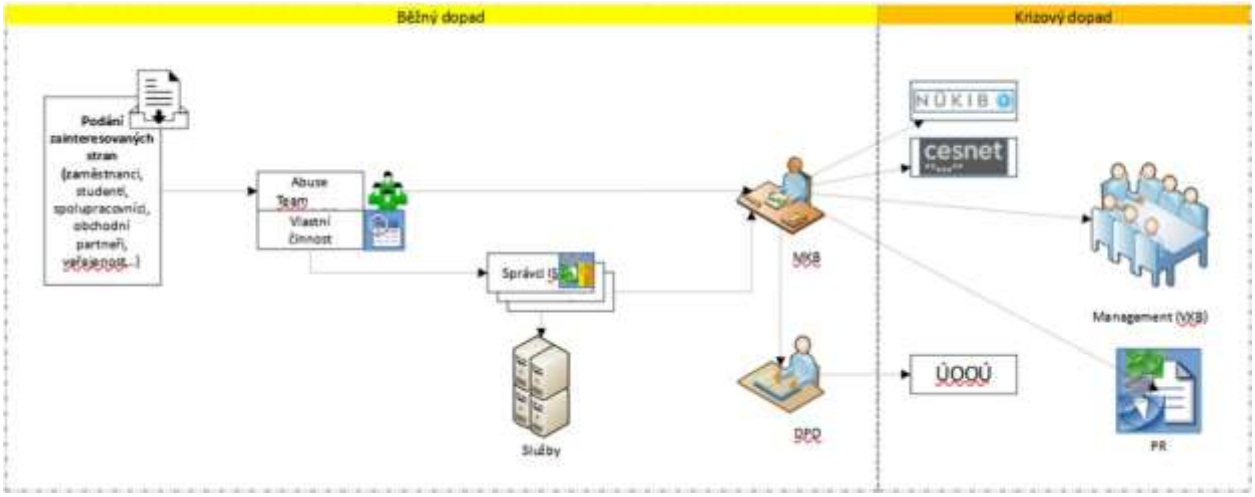
Pro každou kategorii incidentů existuje stručný Plán postupu jeho řešení a Eskalační politika, zohledňující jeho eskalaci na další subjekty, jejich informovanost a spolupráci dle stupně incidentu.

Eskalace méně závažných incidentů zahrnuje hlášení dalším CERT týmům, NÚKIBu, nebo zapojení pověřence pro ochranu osobních údajů (DPO).

Eskalace od závažných incidentů počínaje, zahrnuje povinnost nebo zvážení dalších kroků: zapojení dalších nadřízených, členů výboru KB, tiskového mluvčího, externích subjektů a zákazníků, vypnutí části nebo celé infrastruktury.

Při podezření na trestný čin je nutné hlásit incident Polici ČR prostřednictvím vedení.

[1] Příloha č. 1: Zvládání KBI



Formulář a metodika pro hlášení incidentů na NÚKIB

c) Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů

Revizi platnosti plánů zvládání jednotlivých kategorií incidentů provádí manažer KB nejméně jedenkrát ročně.

Testování plánů kontinuity provozu nebo obnovy aktiv po havárii a míru detailu jejich provedení ukládá a výsledky schvaluje výbor KB jedenkrát ročně.

O všech proběhlých revizích a testech pořizuje manažer KB záznam do deníku.

d) Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti

Vždy po ukončení řešení incidentu, resp. obnovení provozu dotčeného aktiva nebo systému, v termínu do 10 pracovních provede manažer KB vyhodnocení míry všech dopadů a uzavře evidenci incidentu.

V reakci na proběhlé incidenty a výsledky všech výše uvedených uskutečněných testů provede 1x ročně přehodnocení rizik, která se k dotčeným aktivům vztahují a upraví

- plány zvládání jednotlivých kategorií incidentů,
- plány kontinuity,
- postupy obnovy aktiv po havárii a
- analýzu rizik doplněním aktuálních rizik

e) Evidence incidentů

Evidence je podobně jako systém vedení provozních záznamů udržována v centralizovaném nástroji nebo ručně v evidenci (deníku) incidentů, která obsahuje minimálně pole: číslo, datum hlášení, zdroj hlášení, typ incidentu (kategorie), možné ohrožení, závažnost, popis, výsledek, popř. důkazy související se vznikem incidentu.

Statistiku incidentů bere na vědomí při každém zasedání výbor KB.

Historie revizí

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