

VZOR Obsah ohlášení případů porušení zabezpečení osobních údajů

Porušením zabezpečení OÚ je chápána jakákoliv událost, která by mohla mít za následek porušení důvěrnosti, integrity nebo dostupnosti OÚ. Přesněji se dá porušení zabezpečení popsat jako neoprávněné zničení, ztráta, změna, neautorizované odhalení nebo neoprávněný přístup k OÚ. Mezi tyto případy patří **neúmyslné i záměrné** porušení ochrany. Konkrétními příklady porušení zabezpečení OÚ mohou být:

- přístup k OÚ neautorizovanou osobou
- odeslání OÚ nesprávnému adresátu
- ztráta nebo krádež zařízení obsahující OÚ
- ztráta dostupnosti OÚ
- neoprávněná změna OÚ.

Proces reakce na porušení zabezpečení

1. **Detekce a evidence** - odhalení případu porušení zabezpečení OÚ je následně zavedeno pověřencem do evidence incidentů.
 - a) aktivity CVT – odhalení útoků, výsledky penetračních testů
 - b) oznámení realizované řadovým zaměstnancem, studentem anebo jakoukoli fyzickou osobou, která porušení zabezpečení odhalí (ztráta zařízení obsahující OÚ, nesprávná konfigurace použitého systému nebo nezajištění papírových dokumentů s OÚ, apod.)
 - c) oznámení na základě automatizovaných nástrojů za účelem detekce takových případů (automatizovaný monitoring síťového provozu, automatizované sledování pohybu OÚ v cloudovém prostředí.
 - d) oznámení od zpracovatele OÚ – kromě popsanych úkonů mohou být vykonány právní úkony vyplývající z uzavřené smlouvy se zpracovatelem OÚ.

Po nahlášení bezpečnostního incidentu na centrálním místě (pověřenec) je tato událost zaevidovaná v centrální evidenci. Následně by mělo proběhnout vyšetření incidentu, které poskytne odpovědi na základní otázky:

 - Co bylo zdrojem, příčinou porušení zabezpečení?
 - Jaké osobní údaje a fyzické osoby byly tímto porušením dotknuty?
2. **Kategorizace** – posouzení případu porušení zabezpečení ve smyslu určení potenciálních dopadů na dotčené fyzické osoby
3. **Oznámení případu porušení zabezpečení** relevantním subjektům – dozorovému orgánu nebo dotčeným fyzickým osobám.
 - a) V případě, že je nepravděpodobné, že porušení zabezpečení má za následek nějaké riziko pro práva a svobody konkrétních fyzických osob, nemusí UTB tuto skutečnost nikomu oznamovat. Zdůvodnění neoznámení této skutečnosti musí být zdokumentované na centrálním místě.
 - b) V případě, že je pravděpodobné, že porušení zabezpečení má za následek nějaké riziko pro práva a svobody fyzických osob, oznámí UTB tuto skutečnost příslušnému dozorovému orgánu.

- c) V případě, že je pravděpodobné, že porušení zabezpečení má za následek vysoké riziko pro práva a svobody dotčených fyzických osob, oznámí UTB tuto skutečnost dotčeným fyzickým osobám, a to i v případě potenciální možnosti, že daná fyzická osoba byla dotčena. V případě, že UTB nebude mít kontakt na výše uvedené fyzické osoby, může vydat veřejné oznámení týkající se daného případu porušení zabezpečení OÚ.
- d) V případě oznámení události dozorovému úřadu nebo dotčeným fyzickým osobám poskytne UTB tyto údaje:
- Popis povahy porušení zabezpečení OÚ – popis kategorií subjektu údajů, kterých se porušení dotklo, odhadovaný počet těchto fyzických osob a jejich kategorie a počet dotknutých záznamů o minimálním zpracování OÚ.
 - Jméno a kontaktní údaje pověřence.
 - Popis pravděpodobných důsledků porušení zabezpečení
 - Popis plánovaných anebo přijatých opatření včetně předběžných opatření určených ke zmírnění možných nepříznivých dopadů.
4. **Obnova** – pokus o nápravu důsledků způsobených daným případem porušení zabezpečení.
5. **Ponaučení** – přijetí vhodných opatření za účelem prevence před podobnými případy porušení zabezpečení OÚ. Každý výskyt porušení zabezpečení OÚ je potřebné přezkoumat za účelem určení zdroje tohoto porušení. Cílem je, aby bylo následně možné přijat vhodné technické anebo organizační opatření tak, aby se výskyt podobného případu eliminoval. Výsledek přezkoumání i návrh následných organizačních opatření je zdokumentovaný na centrálním místě. Ke každému takovému případu zaujme pověřenec stanovisko a na základě tohoto stanoviska budou učiněné další kroky, například implementace navržených opatření, jejich zpřísnění anebo zmírnění.