					Sem vložte název registrované právnické osoby						
Číslo dokumentu: P39					Název dokumentu: **Politika koordinovaného oznamování zranitelností**						
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:						
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
GDPR	čl. 32 odst. 1 písm. d)	
směrnice NIS2	čl. 21 odst. 2 písm. e)	
nařízení DORA	čl. 11 odst. 1 písm. d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Účel

1.1 Stanovit formální proces pro přijímání, zpracování a zveřejňování informací o zranitelnostech týkajících se systémů nebo služeb organizace v souladu s požadavky čl. 21 odst. 2 písm. e) směrnice NIS2 na řízení zranitelností a jejich oznamování.

1.2 Podporovat externí bezpečnostní výzkumníky, partnery a uživatele v odpovědném hlášení zranitelností (Coordinated Vulnerability Disclosure, CVD) a vymezit způsob, jakým organizace komunikuje informace o zranitelnostech zainteresovaným stranám.

2. Rozsah

2.1 Tato politika se vztahuje na všechny síťové a informační systémy vlastněné nebo provozované organizací a na všechny zjištěné zranitelnosti v těchto systémech.

2.2 Zahrnuje interní týmy (bezpečnost, IT, vývoj) i všechny externí strany oznamující zranitelnosti (např. výzkumníky, zákazníky, dodavatele). Upravuje také komunikaci s výrobci produktů nebo poskytovateli služeb, pokud se zranitelnost týká jejich komponent.

3. Cíle

3.1 Včas identifikovat a odstraňovat bezpečnostní zranitelnosti s využitím interních posouzení i externích oznámení.

3.2 Poskytnout externím oznamovatelům jasné pokyny pro bezpečné a zákonné předávání informací o zranitelnostech a zajistit, aby organizace účinně reagovala a přijímala nápravná opatření.

3.3 Zajistit soulad s požadavky směrnice NIS2 a osvědčenými postupy v odvětví (ISO/IEC 29147 a ISO/IEC 30111) pro koordinované oznamování zranitelností a tím posilovat celkovou bezpečnost ekosystému.

4. Role a odpovědnosti

4.1 Tým pro reakci na zranitelnosti (VRT): určený tým vedený ředitelem informační bezpečnosti (CISO) nebo vedoucím řízení zranitelností, který přijímá hlášení zranitelností, provádí triáž, posuzuje riziko a dopad a koordinuje nápravu i veřejné zveřejnění.

4.2 Týmy IT a vývoje: spolupracují s VRT při validaci nahlášených zranitelností, vývoji a testování záplat nebo zmírňujících opatření a při nasazení oprav. V případě potřeby poskytují technické podklady pro bezpečnostní oznámení.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Monitorování a audit

9.1 VRT bude vést evidenci oznámených zranitelností, ve které bude sledovat každé hlášení od jeho přijetí až po uzavření. Tato evidence bude měsíčně přezkoumávána, aby byl zajištěn včasný postup u otevřených položek. Položky po termínu budou eskalovány.

9.2 Interní audit nebo nezávislý bezpečnostní hodnotitel bude každoročně přezkoumávat účinnost procesu řízení zranitelností, například kontrolou, zda byly vzorky případů zranitelností zpracovány v souladu s politikou (potvrzeny, opraveny a zveřejněny včas). Ověří také funkčnost veřejně dostupného kanálu pro oznámení (např. zda jsou testovací e-maily přijímány a zpracovávány).

9.3 Metriky týkající se zranitelností (objem podle závažnosti, doby nápravy apod.) budou čtvrtletně sestavovány a předkládány výboru pro správu a řízení kybernetické bezpečnosti za účelem aktualizace hodnocení rizik.

10. Přezkum a údržba

10.1 Tato politika bude přezkoumávána nejméně jednou ročně. Mimořádný přezkum vyvolá také jakákoli významná změna našeho IT prostředí (např. spuštění nové služby dostupné z internetu) nebo relevantní vývoj právních předpisů (např. nové právní předpisy EU o oznamování zranitelností produktů).

10.2 Aktualizace politiky budou zohledňovat zpětnou vazbu od externích oznamovatelů a poznatky z interních analýz po incidentech. Významné změny schvaluje ředitel informační bezpečnosti (CISO) a jsou komunikovány všem zaměstnancům a zveřejněny v našem online úložišti bezpečnostních politik za účelem transparentnosti.

11. Související politiky a vazby

11.1 P01 – P01 Politika informační bezpečnosti. Stanoví mandát vedení pro řízení zranitelností a jejich oznamování.

11.2 P19 – Politika řízení zranitelností a záplat. Upravuje interní proces nápravy navazující na příjem hlášení CVD.

11.3 P24 – Politika bezpečného vývoje. Zajišťuje opravy a posilování SDLC na základě nahlášených problémů.

11.4 P25 – Politika požadavků na zabezpečení aplikací. Zajišťuje, aby produkty obsahovaly požadavky umožňující připravenost na oznamování zranitelností.

11.5 P30 – Politika reakce na incidenty (P30). Řeší aktivní zneužívání oznámených zranitelností.

11.6 P31 – Politika sběru důkazů a forenzního šetření. Zajišťuje uchování artefaktů souvisejících s nahlášenými nebo zneužitými chybami.

11.7 P26 – Bezpečnostní politika dodavatelů a poskytovatelů služeb třetích stran. Koordinuje oznámení týkající se komponent dodavatelů.

11.8 P37 – Politika právního a regulačního souladu. Upravuje oznamování, znění bezpečného právního rámce a zveřejňování.

12. Reference

12.1 směrnice NIS2 (EU 2022/2555), čl. 21 odst. 2 písm. e) (bezpečnost ve vývoji a řízení zranitelností a jejich oznamování)

12.2 prováděcí nařízení Komise (EU) 2024/2690, příloha, oddíl 6.10 (technické požadavky na procesy řízení zranitelností a jejich oznamování)

12.3 Technické pokyny ENISA k opatřením pro řízení rizik kybernetické bezpečnosti – část věnovaná řízení zranitelností a jejich oznamování

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (opatření A.5.7 k informacím o hrozbách a oznamování zranitelností; opatření A.8.28 k bezpečnému vývoji)

12.5 ISO/IEC 29147:2018 (pokyny pro oznamování zranitelností) a ISO/IEC 30111:2019 (pokyny pro procesy řízení zranitelností)