					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P39					Názov dokumentu: **Politika koordinovaného zverejňovania zraniteľností**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a právnymi predpismi

Norma/predpis	Kapitola/článok	Poznámka
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	
Nariadenie EÚ GDPR	Čl. 32(1)(d)	
Smernica EÚ NIS2	Čl. 21(2)(e)	
Nariadenie EÚ DORA	Čl. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Účel

1.1 Zaviesť formálny proces prijímania, riešenia a zverejňovania informácií o zraniteľnostiach, ktoré ovplyvňujú systémy alebo služby organizácie, v súlade s článkom 21 ods. 2 písm. e) smernice EÚ NIS2 v oblasti riešenia zraniteľností a ich zverejňovania.

1.2 Podporovať externých bezpečnostných výskumníkov, partnerov a používateľov v zodpovednom nahlasovaní zraniteľností (Coordinated Vulnerability Disclosure – CVD) a určiť spôsob, akým organizácia komunikuje informácie o zraniteľnostiach zainteresovaným stranám.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky sieťové a informačné systémy vo vlastníctve organizácie alebo prevádzkované organizáciou, ako aj na všetky identifikované zraniteľnosti v týchto systémoch.

2.2 Vzťahuje sa na interné tímy (bezpečnostné, IT, vývojové) a na všetky externé strany nahlasujúce zraniteľnosti (napr. výskumníkov, zákazníkov, dodávateľov). Upravuje aj komunikáciu s dodávateľmi produktov alebo poskytovateľmi služieb, ak sa zraniteľnosť týka ich komponentov.

3. Ciele

3.1 Včas identifikovať a odstraňovať bezpečnostné zraniteľnosti s využitím interných posúdení aj externých oznámení.

3.2 Poskytnúť externým oznamovateľom jasné usmernenia na bezpečné a zákonné oznamovanie zraniteľností a organizácii umožniť účinnú reakciu a nápravu.

3.3 Zabezpečiť súlad s požiadavkami smernice EÚ NIS2 a s osvedčenými postupmi v odvetví (ISO/IEC 29147 a ISO/IEC 30111) pre koordinované zverejňovanie zraniteľností a tým posilňovať celkovú bezpečnosť ekosystému.

4. Roly a zodpovednosti

4.1 Tím pre riešenie zraniteľností (VRT): určený tím (vedený CISO alebo manažérom riadenia zraniteľností), ktorý prijíma hlásenia zraniteľností, vykonáva ich triáž, posudzuje riziko a dopad a koordinuje nápravné opatrenia a verejné zverejnenie.

4.2 IT a vývojové tímy: spolupracujú s VRT pri validácii nahlásených zraniteľností, vývoji a testovaní záplat alebo zmierňujúcich opatrení a pri nasadzovaní opráv. V prípade potreby poskytujú technické podklady pre bezpečnostné upozornenia.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Monitorovanie a audit

9.1 VRT vedie register zverejňovania zraniteľností, v ktorom sleduje každé hlásenie od prijatia až po uzavretie. Tento register sa mesačne preskúmava s cieľom zabezpečiť včasný postup pri otvorených položkách. Položky po lehote sa eskalujú.

9.2 Funkcia vnútorného auditu a compliance alebo nezávislý bezpečnostný posudzovateľ každoročne preskúmava účinnosť procesu riešenia zraniteľností, napríklad overením, že vzorky prípadov zraniteľností boli spracované v súlade s politikou (potvrdené, opravené a zverejnené včas). Zároveň overí, že verejne dostupný kanál na nahlasovanie zraniteľností funguje (napr. že testovacie e-maily sú prijaté a riešené).

9.3 Metriky týkajúce sa zraniteľností (objem podľa závažnosti, časy nápravy a pod.) sa budú štvrťročne zostavovať a predkladať výboru pre riadenie kybernetickej bezpečnosti na účely aktualizácie posúdenia rizík.

10. Preskúmanie a údržba

10.1 Táto politika sa preskúmava najmenej raz ročne. Mimoriadne preskúmanie sa vykoná aj pri akejkoľvek významnej zmene nášho IT prostredia (napr. spustenie novej služby prístupnej z internetu) alebo pri relevantnom regulačnom vývoji (napr. nové právne predpisy EÚ o zverejňovaní zraniteľností produktov).

10.2 Aktualizácie politiky musia zohľadniť spätnú väzbu od externých oznamovateľov a poznatky z interných poincidentných analýz. Významné zmeny schvaľuje CISO a oznamujú sa všetkým zamestnancom; zároveň sa zverejnia v našom online úložisku bezpečnostných politík v záujme transparentnosti.

11. Súvisiace politiky a väzby

11.1 P01 – Politika informačnej bezpečnosti. Manažérsky mandát pre riešenie a zverejňovanie zraniteľností.

11.2 P19 – Politika riadenia zraniteľností a záplat. Interný proces nápravy nadväzujúci na prijímanie hlásení CVD.

11.3 P24 – Politika bezpečného vývoja. Zabezpečuje opravy a posilnenie SDLC na základe nahlásených problémov.

11.4 P25 – Politika požiadaviek na bezpečnosť aplikácií. Zabezpečuje, aby produkty obsahovali požiadavky pripravené na proces zverejňovania.

11.5 P30 – Politika reakcie na incidenty. Rieši aktívne zneužívanie zverejnených zraniteľností.

11.6 P31 – Politika zberu dôkazov a forenznej analýzy. Uchováva artefakty zo zraniteľností, ktoré boli nahlásené alebo zneužité.

11.7 P26 – Politika bezpečnosti tretích strán a dodávateľov. Koordinuje zverejnenia týkajúce sa komponentov dodávateľov.

11.8 P37 – Politika právneho a regulačného súladu. Upravuje notifikácie, znenie safe harbor a zverejnenie.

12. Referencie

12.1 Smernica NIS2 (EÚ 2022/2555), článok 21 ods. 2 písm. e) (bezpečnosť pri vývoji a riešenie zraniteľností a ich zverejňovanie)

12.2 Vykonávacie nariadenie Komisie (EÚ) 2024/2690, príloha, oddiel 6.10 (technické požiadavky na procesy riešenia zraniteľností a ich zverejňovania)

12.3 Technické usmernenie ENISA k opatreniam riadenia rizík kybernetickej bezpečnosti – časť o riešení zraniteľností a ich zverejňovaní

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontrola A.5.7 o spravodajstve o hrozbách a zverejňovaní zraniteľností; kontrola A.8.28 o bezpečnom vývoji)

12.5 ISO/IEC 29147:2018 (usmernenia pre zverejňovanie zraniteľností) a ISO/IEC 30111:2019 (usmernenia pre procesy riešenia zraniteľností)