

Národní politika koordinovaného zveřejňování zranitelností

Vytvořeno Národním úřadem pro kybernetickou a informační bezpečnost.



01 01
0101010
01010101010101
01010101010101010
0 101010101010101010 10101
01010101010101010101010101010
1010101010101010101010101010101
01010101010101010101010101010101
0101010101010101010101010101010
1010101010101010101010101010101
10101010101010101010101010101
10101010101010101010101010101
0101010101010101010101010101
101010 010101
0101

O dokumentu

Národní politika koordinovaného zveřejňování zranitelností (Coordinated Vulnerability Disclosure, dále také „CVD“) představuje ucelený pohled České republiky (dále „ČR“) na problematiku CVD, včetně podpory jeho zavádění napříč subjekty až po nastínění implementace v rámci českého právního řádu.

Tento dokument je určen mimo jiné pro:

Vlastníky, vývojáře, dodavatele a manažery kybernetické bezpečnosti, kteří zvažují zavedení CVD jako nástroje pro navyšování zabezpečení ICT produktů.

Výzkumníky z oblasti nalézání zranitelností v ICT produktech, kteří hledají způsob, jak provádět etický hacking v souladu s právním řádem ČR.

Úvodní slovo ředitele NÚKIB



Ing. Lukáš Kintr

Ředitel Národního úřadu
pro kybernetickou
a informační bezpečnost

Vážené dámy, vážení pánové,

v posledních letech jsme svědky rychlé digitalizace, která proměňuje všechny oblasti naší společnosti a vytváří nové příležitosti pro další rozvoj a inovace. Tento dynamický vývoj nám přináší nespočet výhod, umožňuje zlepšovat procesy, zvyšovat efektivitu a otevírat dveře k novým technologickým možnostem. Avšak jak se stále více spoléháme na technologie, musíme čelit i rostoucím kybernetickým hrozbám a zranitelnostem, které mohou mít závažné dopady nejen na jednotlivé organizace, ale i na celou naši společnost.

Technologie, které nám přinášejí tolik užitku, nejsou bezchybné. Zranitelnosti, jež v nich existují, mohou být snadno zneužity, a to často s nezanedbatelnými následky – ať už se jedná o ekonomické škody, reputační škody, nebo postupnou ztrátu důvěry v tyto technologie. Kybernetické útoky, které využívají tyto zranitelnosti, se stávají stále častějšími a sofistikovanějšími, což klade před všechny organizace, bez ohledu na jejich velikost či zaměření, nové a náročné výzvy.

Hrozba zneužití zranitelností je přirozeným důsledkem nejen rychlého vývoje informačních a komunikačních technologií, ale i jejich rozšiřující se aplikace, každodenního užívání a nezbytných aktualizací. Vzhledem k tomu, že technologie jsou stále složitější a propojenější, je nereálné očekávat, že jejich výrobci, správci či vlastníci budou schopni sami identifikovat a opravit veškeré zranitelnosti, které se mohou objevit. Dlouhodobým problematickým aspektem je rovněž nedostatečná ochrana informací o zranitelnostech, které jsou často zveřejňovány ještě před nalezením jejich nápravy. Tato situace vyžaduje nové přístupy, nabízející efektivnější řešení těchto problémů.

Jedním z klíčových nástrojů, který může pomoci zmírnit tato rizika, je koordinované zveřejňování zranitelností, zkráceně CVD. Tento proces spočívá v systematické spolupráci zejména mezi nálezci zranitelností a vlastníky ICT produktů. CVD má za cíl zajistit širokou možnost testování ICT produktů a zároveň ochránit informaci o zjištěných zranitelnostech tak, aby byly včas sdíleny pouze s těmi, kteří je mohou efektivně řešit, čímž se minimalizuje riziko jejich zneužití, a dojde tak navýšení bezpečnosti informační infrastruktury či citlivých dat.

Tento dokument si klade za cíl vysvětlit principy koordinovaného zveřejňování zranitelností v českém kontextu. Poskytuje i základní rámec, jak CVD efektivně zavést a aplikovat v České republice. Zároveň dokument představuje pohled České republiky na CVD a způsob, jak podpořit jeho zavádění napříč subjekty v České republice. Pevně věřím, že implementace CVD posílí naši schopnost čelit kybernetickým hrozbám a přispěje k posílení kybernetické bezpečnosti v České republice.

Manažerské shrnutí

Koordinované zveřejňování zranitelností (CVD) představuje formalizovaný proces dobrovolného objevování zranitelnosti v produktech informačních a komunikačních technologií (dále „ICT“) třetími osobami (tzv. objeviteli). Nedílnou součástí procesu je též notifikace objevené zranitelnosti vlastníkovi/správci ICT produktu za účelem provedení bezpečnostní opravy a následného zveřejnění zranitelnosti.

Chybějící pohled státu na CVD

Aktuálně neexistuje formalizovaný a ucelený pohled ČR na CVD ani jeho specifická právní úprava.

Role NÚKIB a zřízení Platformy CVD

Národní úřad pro kybernetickou a informační bezpečnost (dále „NÚKIB“) vytvoří pro účely zveřejňování metodických materiálů a usnadnění zavedení CVD pro orgány veřejné moci i soukromý sektor bezpečný prostor (dále také „Platforma CVD“).

Obsah a funkce Platformy CVD

Platforma CVD bude obsahovat pohled státu na CVD, včetně vymezení specifické role koordinátora CVD, a metodické materiály podporující zavádění CVD v ČR.

Výhody dobrovolného zavádění politik CVD

Dobrovolné zavádění politik CVD napříč jednotlivými subjekty v ČR minimalizuje rizika plynoucí z neformálního/neřízeného odhalování zranitelností, jakými jsou riziko právního postihu na straně objevitele zranitelnosti či riziko zneužití objevené zranitelnosti v ICT produktech. Zároveň dojde k posílení kybernetické bezpečnosti v ČR.

Rizika neexistence politiky CVD

Bez zavedení politiky CVD hrozí, že dobrovolní objevitelé zranitelností budou svoji činnost provádět bez jakéhokoli souhlasu či smlouvy s vlastníkem, resp. správcem ICT produktu, čímž se vystavují nebezpečí závažných právních důsledků. Případně z důvodu hrozby možného právního postihu nebudou zranitelnosti aktivně odhalovat, a ty tak budou moci být zneužity potenciálními útočníky.

Obsah

3	O dokumentu
4	Úvodní slovo ředitele NÚKIB
6	Manažerské shrnutí

9 Kybernetické hrozby v éře digitalizace

10	Úvod
11	CVD v kostce
13	Směrnice NIS 2 a CVD
14	Osoby zapojené do procesu CVD

15 Způsoby etického nalézání zranitelností

17	Vztah CVD a Bug Bounty programů
----	---------------------------------

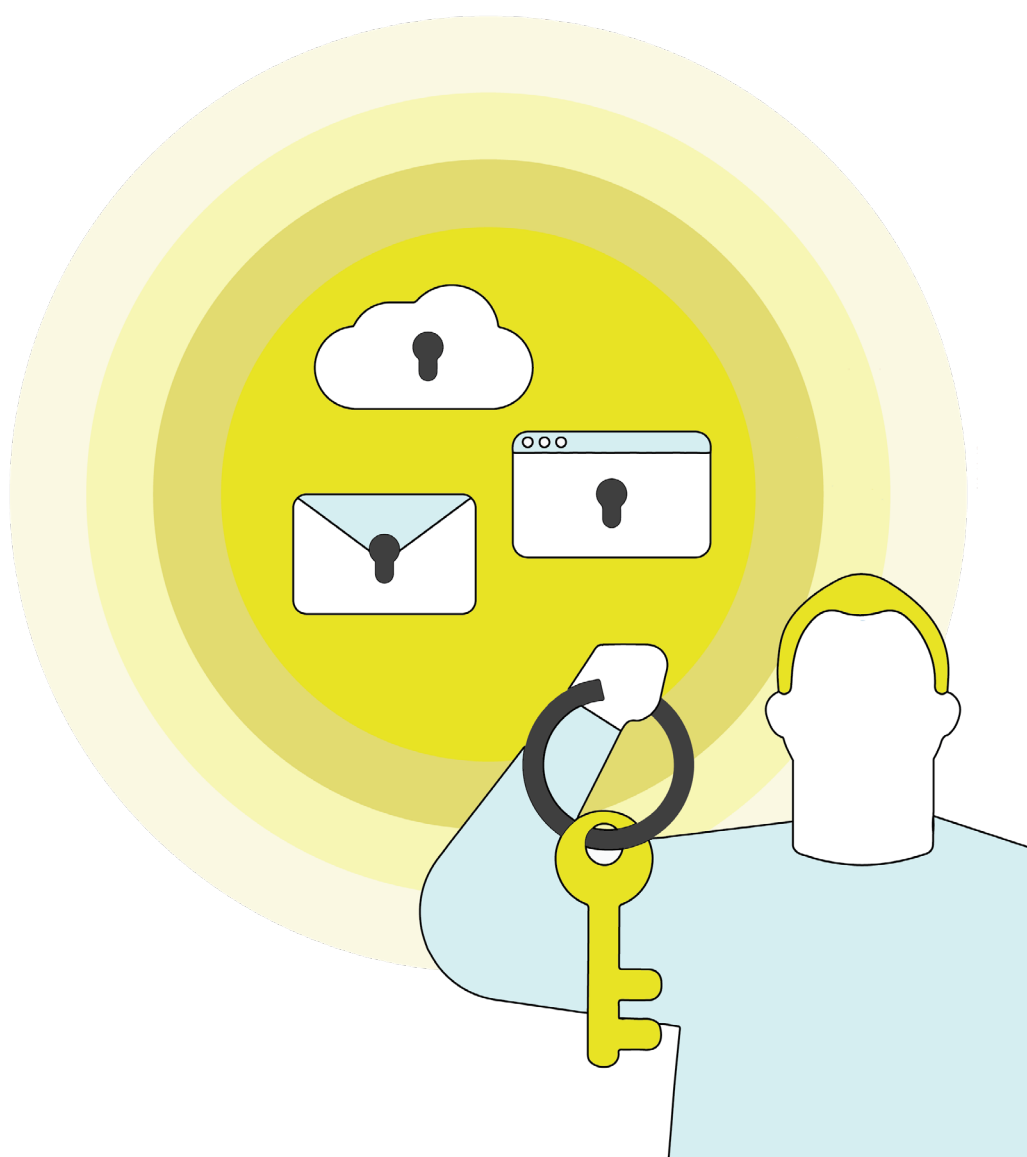
19 Koordinované zveřejňování zranitelností

20	Politika CVD
23	Role koordinátora CVD
24	Důsledky zavedení politiky CVD
25	Doporučení k vytvoření politiky CVD
26	Implementace CVD

38 Národní politika koordinovaného zveřejňování zranitelností

39	Platforma CVD jako nástroj pro snadnější implementaci a propagaci CVD
41	Cíle Platformy CVD
41	Vládní CERT jako koordinátor CVD
45	Spolupráce vládního a národního CERT
46	Zapojení soukromých subjektů do koordinace CVD
46	Nasazení CVD z hlediska právního řádu ČR
47	Základní právní východiska

51 Zdroje



**Kybernetické hrozby
v éře digitalizace:
Jak je zvládat efektivně?**

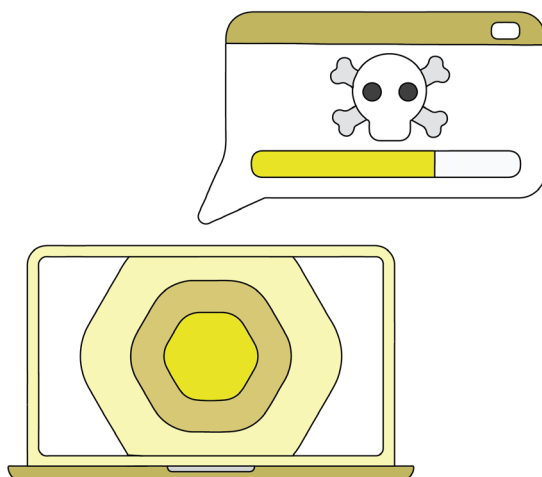
Úvod

Rostoucí digitalizace společnosti představuje příležitost pro růst a rozvoj, ale přináší s sebou i kybernetické hrozby a zranitelnosti, které mohou způsobit závažné škody.

Přestože technologie přináší velké množství výhod a nabízí spousty příležitostí pokroku, nemůže zůstat opomenuta problematika jejich zranitelností. Zneužití těchto zranitelností mnohdy vede k nezanedbatelným škodám (ekonomickým, reputačním a jiným).

Hrozba zneužití zranitelností je spojena jak s vývojem ICT, tak s jejich aplikací, užíváním a aktualizacemi. S ohledem na šíři využití technologií, jejich složitost, vzájemnou provázanost a kompetitivní prostředí je nereálné, aby jejich výrobci nebo správci byli schopni vždy sami odhalit a vyřešit veškeré zranitelnosti.

Zranitelnost v informatice představuje označení pro programátorskou nebo jinou technickou chybu, která může v ICT produktech způsobit bezpečnostní problém a která může být zneužita jednou nebo více hrozbami.



Případnou zranitelnost lze objevit jak zcela náhodně¹ (např. uživatelem při užívání produktu), tak záměrně, ať už s dobrým úmyslem (typicky v rámci testování produktu), nebo s úmyslem zranitelnost zneužít.

Specifickým způsobem nalézání zranitelností je proces CVD. Na jeho základě mohou být tyto zranitelnosti vyhledávány a ohlašovány standardizovaným procesem. V případě širšího využití může CVD představovat významný nástroj pro mitigaci zranitelností a celkové posílení kybernetické bezpečnosti.

¹ Náhodné objevení představuje např. takovou situaci, kdy zkušený či nezkušený objevitel v ICT produktu nahodile nalezne zranitelnosti bez toho, aniž by pro její nalezení vyvíjel činnost s cílem tuto zranitelnost nalézt.

CVD v kostce

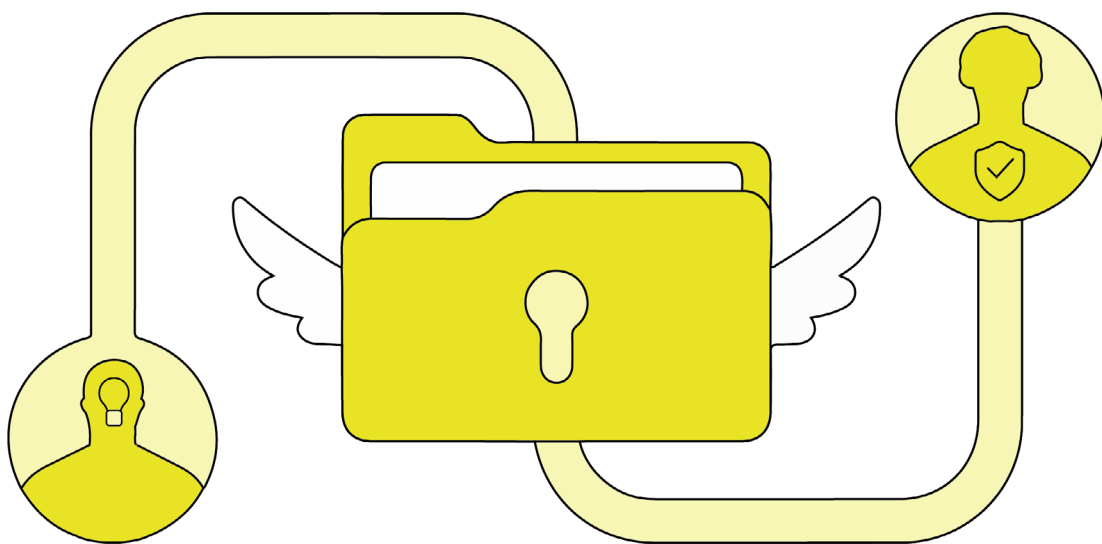
Koordinované zveřejňování zranitelností (*angl. Coordinated Vulnerability Disclosure*) představuje formalizovaný proces, při kterém nálezci zranitelností spolupracují a sdílejí informace s příslušnými zúčastněnými stranami, jako jsou dodavatelé a vlastníci infrastruktury ICT. CVD má za cíl zajistit, aby byly zranitelnosti zveřejněny, jakmile se dodavatelé podaří vyvinout opravu, záplatu nebo najít jiné řešení k jejich mitigaci. Součástí procesu je typicky nalezení zranitelnosti, její nahlášení a následné odstraňování takto objevených zranitelností.

Oproti neřízenému procesu odhalování a nakládání se zranitelnostmi, kdy žádný ze subjektů zapojených do tohoto procesu nemá záruku, že ostatní zapojené subjekty nenaloží s informací o zranitelnosti v jeho neprospěch, je v případě CVD celý proces upraven tzv. politikou CVD, která usiluje o poskytnutí takové záruky. CVD je zpravidla otevřeno pro jakéhokoli objevitele zranitelností, pakliže se bude řídit politikou CVD.

Právě z důvodu celkového posílení kybernetické bezpečnosti je zavádění CVD tématem jak na tuzemské, tak mezinárodní úrovni.

I proto NÚKIB vytváří celonárodní politiku CVD, ve které bude jasně a srozumitelně vymezen přístup k CVD, a současně vymezí způsoby metodické pomoci při zavádění procesu CVD napříč subjekty.

Národní politika je založena na principu dobrovolnosti v zavedení CVD. Odpovědné osoby si tak samy mohou zvolit, zda a jak implementují CVD v rámci své organizace, včetně vymezení podmínek, za jakých mohou objevitelé zranitelnosti v ICT produktech nalézat. Tento přístup akcentuje ochranu odpovědných osob a jejich ICT produktů. Vzhledem k tomu, že právní řád ČR tento přístup umožňuje, nepředpokládá Národní politika CVD v současné době změnu legislativy. Výjimkou je pouze určení koordinátora pro účely CVD, jakožto povinnost vyplývající ze směrnice NIS 2, případně existence povinnosti implementovat CVD vyplývající z jiných právních předpisů². To nevylučuje, že v budoucnu dojde ke specifické úpravě právního řádu v souvislosti s CVD.



² Viz nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti).

Směrnice NIS 2 a CVD

Na evropské úrovni dne 16. ledna 2023 vstoupila v platnost tzv. směrnice NIS 2*.

Cílem směrnice NIS 2 je prohloubení kyberbezpečnosti v členských státech, přičemž je v ní explicitně zmíněna povinnost členských států zavést národní strategii kybernetické bezpečnosti, včetně vymezení politiky dobrovolného koordinovaného zveřejňování zranitelností. Současně by každý stát měl pověřit jednoho ze svých týmů CSIRT jako koordinátora pro účely koordinovaného zveřejňování zranitelností.

**[Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148]*

Osoby zapojené do procesu CVD

Odpovědná osoba

je fyzická nebo právnická osoba, případně orgán veřejné moci, který vlastní, užívá, vyrábí, prodává či spravuje ICT produkty.

Objevitel zranitelnosti

(dále „objevitel“) je zpravidla fyzická osoba, která záměrně nebo náhodně, avšak s dobrým úmyslem* identifikuje potenciální zranitelnost v ICT produktech, včetně jejich implementace a konfigurace, a nahlásí ji odpovědné osobě nebo koordinátorovi.

**Dobrým úmyslem se v tomto případě rozumí, že činnost objevitele úmyslně směřuje primárně k nalezení a ohlášení zranitelností za účelem navýšení kybernetického zabezpečení ICT produktu a prevence využití zranitelnosti ze strany potenciálních útočníků.*

2

Způsoby etického nalézání zranitelností

Existuje více způsobů nalézání zranitelností v ICT produktech s dobrým úmyslem. Ty se odlišují jednak právním titulem opravňujícím k nalézání zranitelností, jednak i finanční nákladností či časovou náročností.

Formy hackingu s dobrým úmyslem

Nalézání zranitelností výrobcem / dodavatelem v rámci interních procesů

Finančně relativně nákladný způsob, vyžadující vyčlenění dostatečných kapacit na nalézání zranitelností.

Nalézání zranitelností bez právního titulu

Objevitel se vystavuje reálnému nebezpečí v podobě negativních právních důsledků.

Nejedná se pouze o odpovědnost za způsobení škody, ale zejména trestněprávní postihy, neboť neoprávněný přístup do ICT systémů může naplňovat znaky trestného činu.

Bug Bounty programy / CVD

Legální možnost, jak nalézat zranitelnosti v ICT produktech bez nutnosti předchozí specifické domluvy s odpovědnou osobou.

Je založeno na obecném svolení odpovědné osoby k testování ICT produktů. Bug Bounty programy motivují objevitele vyplacením odměny za nalezení specifických zranitelností.

CVD akcentuje komunikaci objevitele s odpovědnou osobou a koordinátorem a je založeno na ochraně informace o zranitelnosti, aby nebyla zveřejněna dříve, než odpovědná osoba provede její nápravu.

Penetrační testování

Nalézání zranitelností profesionálními etickými hackery na základě smlouvy s odpovědnou osobou a za odměnu. Standardně využívaný způsob umožňující jednoduchý screening zranitelností i hloubkový test celé ICT infrastruktury.

Součástí mohou být i fingované phishingové kampaně, test fyzického zabezpečení apod. Stejně jako v případě interního nalézání zranitelností se nicméně jedná o nákladnou službu, navíc prováděnou jednorázově v omezeném časovém rozsahu (typicky jednoho měsíce).

Vztah CVD a Bug Bounty programů

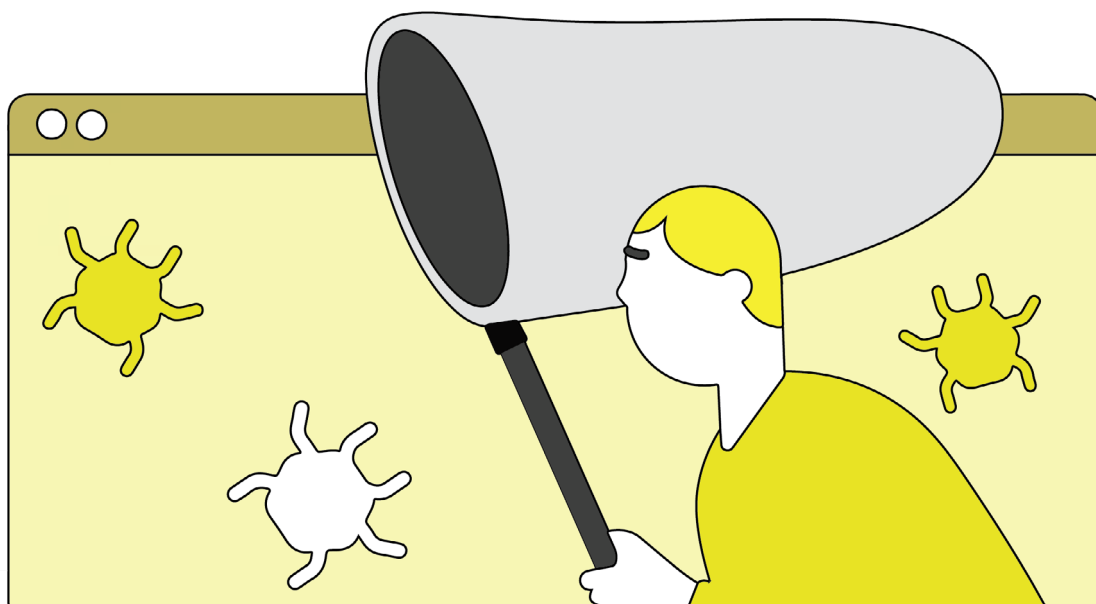
Oproti dalším variantám etického hackingu Bug Bounty a CVD umožňují nalézání zranitelností po dlouhou dobu a velkým množstvím objevitelů, kterým pro tuto činnost nehrozí negativní právní důsledky, pokud dodržují podmínky odpovědné osoby.

CVD a Bug Bounty mají mnoho společného a v praxi jsou tyto pojmy často zaměňovány či se obsahově překrývají. Rozdíl je v akcentu na specifické prvky procesu nalézání zranitelností.

CVD zahrnuje zejména povinnou mlčenlivost objevitele o nalezené zranitelnosti, ochranu komunikace s objevitelem a možnost obrátit se na koordinátora určeného státem.

CVD nutně nemusí zahrnovat odměňování objevitelů (byť je doporučováno) a klade důraz na proces nahlášení, koordinaci a způsob zveřejnění zranitelnosti až po její nápravě.

Bug Bounty programy mohou tyto aspekty rovněž zahrnovat, zpravidla však kladnou výrazný důraz na odměňování dle závažnosti nalezené zranitelnosti a soutěž mezi objeviteli.



Vztah CVD a Bug Bounty

CVD



Bug Bounty

3

**Koordinované
zveřejňování zranitelností**

3.1 Politika CVD

Základním nástrojem koordinovaného zveřejňování zranitelností je politika CVD. Jedná se o odpovědnou osobou zveřejněné podmínky, za jakých mohou potenciální objevitelé nalézat zranitelnosti v ICT produktech, či jejich implementaci u odpovědné osoby.

V rámci CVD politiky odpovědná osoba vymezí i požadovanou formu smlouvy s objevitelem, ve které mu udělí oprávnění nalézat zranitelnosti; typicky se bude jednat o odsouhlasení podmínek nalézání takových zranitelností na webových stránkách odpovědné osoby.

Bez existence politiky CVD, resp. zmíněného odsouhlasení a dodržování podmínek, může být objevitelovo jednání za určitých okolností považováno za zásah do práv a svobod jiné osoby. Takové jednání s sebou může nést občanskoprávní i trestněprávní důsledky, které mohou být pro objevitele velmi závažné (např. povinnost nahradit škodu vzniklou tímto jednáním či dokonce možnost uložení trestu odnětí svobody pro spáchání jednoho z tzv. kybernetických trestných činů³).

Účinná politika CVD upravuje nakládání s objevenou zranitelností od okamžiku samotného objevení zranitelnosti přes její vyhodnocení až k samotnému řešení/nápravě a případnému zveřejnění zranitelnosti.

Vydáním politiky CVD dává odpovědná osoba souhlas s objevováním zranitelností v ICT produktech, pouze však k těm produktům, ke kterým má toto oprávnění souhlas udělit⁴. Případnému objeviteli umožní jím objevené zranitelnosti bezpečně a s minimalizovanou hrozbou právního postihu ohlásit.

³ Jedná se o množinu trestných činů, z nichž nejpodstatnější je trestný čin podle § 230 odst. 1 a 2 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

⁴ V tomto ohledu je třeba, aby oprávněná osoba identifikovala ICT produkty, k nimž nemůže oprávnění udělit, např. z licenčních důvodů.

Zmíněnou cestou v praxi dochází u konkrétní odpovědné osoby k nastavení formalizovaného procesu, který upravuje postup, co dělat v případě objevení zranitelnosti, jak informaci o zranitelnosti bezpečně přijmout, vyhodnotit, opravit a jak informovat uživatele o existenci a způsobu nápravy dané zranitelnosti.

Nastavená politika CVD umožní efektivní a relativně nenákladné objevování a nápravu zranitelností, přičemž v širším kontextu dojde ke zvýšení důvěry v ICT produkty odpovědné osoby a celkové posílení kybernetické bezpečnosti.

Z právního hlediska musí každá odpovědná osoba při tvorbě a definování konkrétních práv a povinností uvedených v CVD postupovat v intencích zákona, přičemž platí, že objevitel zranitelnosti není ani v rámci fungujícího CVD zbaven případné právní odpovědnosti.

Odpovědnost objevitele může být kvalitně nastavenou politikou CVD značně omezena. Při dobře nastavené politice CVD by objevitel měl být chráněn před trestněprávními důsledky spojenými s neoprávněným nalézáním zranitelností v ICT produktech, před odpovědností za škodu či autorskoprávními postihy (v rozsahu podmínek politiky CVD), a to v případě, že se bude držet pravidel politiky CVD.

I při existenci politiky CVD by si měl objevitel počínat takovým způsobem, aby svým jednáním nezpůsobil neoprávněný zásah do ICT produktů, ke kterému může dojít v případě, že překročí meze stanovené politikou CVD. Zároveň by měl postupovat velmi obezřetně a volit co nejméně invazivní prostředky k vyhledávání zranitelností. Odpovědná osoba by pro tyto účely měla v politice CVD negativně vymezit, které nástroje a způsoby nalézání zranitelností nejsou v rámci CVD povoleny, případně pozitivně vymezit ty, které povoleny jsou⁵.

Pro efektivní spolupráci v rámci CVD, zajištění bezpečné komunikace a koordinace je nezbytné, aby politika CVD poskytovala pochopitelný a jednoznačný návod, jak se má objevitel chovat, aby se na něj vztahovala její ochrana.

⁵ Jako příklady nalézání zranitelností ke zvážení zákazu lze uvést: odepření služby (angl. DoS, DDoS), útoky hrubou silou (angl. brute force), prolamování hesel (angl. password cracking), kopírování, pozměňování či mazání osobních údajů, testování fyzického přístupu do zařízení nebo jeho krádež, instalování škodlivého kódu (trojský kůň, počítačový červ apod.) do ICT produktu, sociální inženýrství včetně útoků kategorie phishing, vishing, smishing, baiting, tailgating a bait and switch a jiné netechnické testování zranitelností (sniffing, dumpster diving či shoulder surfing). Naopak jako příklady povolených prostředků nalézání zranitelností ve webových aplikacích lze uvést: obcházení ověřovacích mechanismů, cross-site scripting (XSS), cross-site request forgery (CSRF), injektování SQL či LDAP kódu, clickjacking, porušení autentifikace a managementu relací, porušení přímého odkazu na objekt apod.

ICT produkt

je jakýkoli prostředek sloužící přímo k provozu ICT, včetně softwarového a hardwarového řešení informačních a komunikačních systémů, jejich implementace a konfigurace. Pod tento pojem lze zařadit celé sestavy softwarových či hardwarových komponent ICT, ale i jednotlivé komponenty, jejich konfigurace a nastavení.

Koordinátor

je jedním z týmů CSIRT členského státu Evropské unie. V případě objevení zranitelnosti a notifikace koordinátora je koordinátor schopen:

propojit zúčastněné strany, koordinovat další postup k nápravě zranitelnosti, informovat další koordinátory či relevantní subjekty, v krajních případech poskytnout i technickou či odbornou pomoc.

V ČR tuto roli bude zastávat vládní CERT, který je součástí NÚKIB.

3.2 Role koordinátora CVD

Co do komunikace mezi objevitelem a odpovědnou osobou je nutné zajistit jednak srozumitelnost a určitost, jednak ochranu před možným nezamýšleným zveřejněním. Po nahlášení zranitelnosti by měli zůstat objevitel a odpovědná osoba v kontaktu a dohodnout další postup.

Pro případy, kdy jedna ze stran dostatečně nekomunikuje, nechce poskytnout relevantní informace či se jedná o zranitelnost dopadající na vysoký počet odpovědných osob, lze kontaktovat koordinátora CVD, jenž je k této činnosti určen státem nebo mu byla role koordinátora svěřena.

Do procesu CVD vstupuje koordinátor zpravidla až v případě, že jej jedna ze stran procesu sama osloví. Nejčastěji se tak děje v případě nedostatečné komunikace odpovědné osoby (např. když tato osoba nereaguje na oznámení zranitelnosti). Koordinátor do CVD vstupuje též v případě nalezení významné zranitelnosti, o čemž jej může notifikovat jak odpovědná osoba, tak samotný objevitel.

Díky svým odborným kapacitám může následně koordinátor vyhodnotit, zda je skutečně zranitelnost významná, například pro intenzitu dopadu na množství jiných subjektů, přeshraniční aspekty⁶, případně pokud odpovědná osoba poskytuje služby významné pro chod státu a zranitelnost může narušit poskytování těchto služeb.⁷

Úkolem koordinátora je následně podpora součinnosti obou stran a případně poskytování metodické či v krajních případech i technické pomoci při opravě zranitelnosti. Koordinátor současně může posoudit významnost zranitelnosti a provést další kroky ke zmírnění jejího dopadu napříč více subjekty.

Je nicméně třeba zdůraznit, že koordinátor nemá v rámci CVD možnost ukládat povinnosti a jeho role primárně spočívá v koordinaci procesu a metodické pomoci. To však nevylučuje možnost koordinátora využít informaci o zranitelnosti v rámci výkonu své případné působnosti dle zákona.⁸

⁶ Např. pokud zranitelnost má aspekt, který je třeba dále komunikovat, typicky u ICT produktu, který využívá množství dalších subjektů globálně. Koordinátor má navíc v takovém případě povinnost spolupracovat s koordinátory z jiných členských zemí Evropské unie dle čl. 12 odst. 1 směrnice NIS 2.

⁷ Příkladem těchto služeb mohou být služby uvedené ve vyhlášce č. 408/2025 Sb., vyhláška o regulovaných službách

⁸ Typicky se může jednat o vydání protiopatření dle § 20 a násl. zákona č. 264/2025 Sb., zákon o kybernetické bezpečnosti.

3.3 Důsledky zavedení politiky CVD

Politika CVD stanoví postup, při jehož dodržování je riziko právního postihu pro objevitele minimalizováno.

Odměny a příležitosti

Odborníkům z oblasti kybernetické bezpečnosti (např. penetračním testerům) se tak vytvoří prostor, ve kterém mohou využít svoji odbornost k hledání zranitelnosti, a v případě dobře nastavené politiky CVD mohou za objevení zranitelnosti získat kupříkladu i veřejné ocenění či finanční odměnu.

Rizika bez politiky CVD

Při absenci politiky CVD (či jiného souhlasu odpovědné osoby) objevitelé zpravidla nemají možnost, jak zranitelnosti legálně externě objevovat.⁹ Není-li politika CVD zveřejněna, hrozí, že na objevení a zveřejnění zranitelností bude nahlíženo jako na trestnou činnost spočívající v neoprávněném přístupu nebo zásahu do počítačového systému či nosiče informací. Objeviteli rovněž hrozí sankce v podobě vznesených nároků na náhradu škody, postihy za porušení ochrany osobních údajů nebo porušení práva autorského.

Výhody zavedení CVD

Pro odpovědnou osobu zavedení politiky CVD může představovat způsob, jak účinně a levně zjišťovat informace o zranitelnostech v ICT produktech dříve, než je zneužijí potenciální útočníci. Prostřednictvím CVD může dále odpovědná osoba demonstrovat, že dává důraz na zabezpečení svých ICT produktů, což může zvýšit její důvěryhodnost ve společnosti.

Náklady a výzvy CVD

Na druhou stranu zavedení CVD bude znamenat náklady pro odpovědnou osobu ve smyslu vyčlenění provozních, technických a personálních kapacit. Tím se zvýší i zátěž dotčených ICT produktů, které budou vystaveny zvýšenému počtu útočných technik. Pro odpovědnou osobu může být komplikovaná rovněž detekce, zda je osoba útočící na ICT produkt objevitelem nebo útočníkem.

⁹ Vyjma nalézání zranitelností na základě smlouvy o penetračním testování, která nicméně na rozdíl od CVD předpokládá konkrétní domluvu s odpovědnou osobou na rozsahu a způsobu nalézání zranitelností.

Zvýšené bezpečnostní požadavky

Zároveň je vhodné, aby odpovědná osoba měla například aktivní a odladěné systémy pro odhalení průniku (IDS) a systémy pro prevenci průniku (IPS) a aby firewall / web application firewall blokoval nechtěné aktivity.

Vyvážení nákladů a přínosů CVD

Uvedená pozitiva by nicméně měla tyto zvýšené náklady a další negativa v důsledku minimálně vyrovnat, zejména z důvodu prevence případných kybernetických útoků, které mohou způsobit značnou majetkovou či reputační škodu.

3.4 Doporučení k vytvoření politiky CVD

Pro transparentní a funkční nastavení CVD je vhodné, aby politika CVD splňovala tyto parametry:

Veřejná dostupnost

Měla by být **VEŘEJNĚ PŘÍSTUPNÁ**, viditelná a snadno dohledatelná. Ideálním řešením je politiku CVD zveřejnit na internetových stránkách dané odpovědné osoby.

Vymezení podmínek politiky

Měla by vymezit **OBECNÉ PODMÍNKY** stanovující, jaké ICT produkty spadají do rozsahu politiky CVD, které techniky objevení zranitelností jsou zakázány a jaké informace má objevitel ve zprávě o objevené zranitelnosti poskytnout. V podmínkách by neměl chybět souhlas s vyhledáváním zranitelností a zmínka o tom, že při dodržení podmínek politiky CVD nebude odpovědná osoba pro jednání objevitele uplatňovat soukromoprávní nároky a dává svolení s jednáním, které by jinak mohlo být považováno za kybernetický trestný čin.

Srozumitelnost a jasnost podmínek

Podmínky by měly být sepsány **SROZUMITELNĚ, STRUČNĚ a JASNĚ** tak, aby strany pochopily vzájemná práva a povinnosti. Důraz by měl být kladen rovněž na negativní právní dopady v případě nedodržení postupů definovaných v podmínkách.

Bezpečný kontaktní kanál

Měla by zavést **KONTAKTNÍ MECHANISMUS**, umožňující objeviteli oznámit odpovědné osobě zabezpečeným způsobem informace o zranitelnosti (např. kontaktní formulář, e-mailová adresa, telefonní číslo či zákaznický servis). Pro jeho správnou funkci se doporučuje vytvořit způsob potvrzení přijetí zprávy o zranitelnosti (např. skrz automatické odesílání e-mailových zpráv), což vytvoří komunikační kanál pro další postup. Současně tím může objevitel prokazovat, že k nalezení zranitelnosti došlo v rámci politiky CVD.

Odměňování objevitelů

Měla by zavést **SYSTÉM ODMĚŇOVÁNÍ OBJEVITELŮ** za účelem motivace dalších objevitelů k vyhledávání zranitelností. Absence odměňování nemá vliv na funkčnost politiky CVD, ale zvýší atraktivnost nalézání zranitelností u daných ICT produktů. Odměňování nutně nemusí znamenat finanční odměnu, ale i nabídnutí veřejného uznání či materiální odměnu v podobě symbolických a drobných dárků.

3.5 Implementace CVD

Implementace a provádění koordinovaného zveřejňování zranitelnosti sestává z několika fází:

Nastavení politiky CVD

1. fáze

Příprava a zpřístupnění kapacit

2. fáze

Zveřejnění politiky CVD

3. fáze

Nalézání zranitelností

4. fáze

Notifikace odpovědné osoby

5. fáze

Klasifikace zranitelností

6. fáze

Náprava zranitelností

7. fáze

Způsob a rozsah zveřejnění

8. fáze

Odměňování objevitele

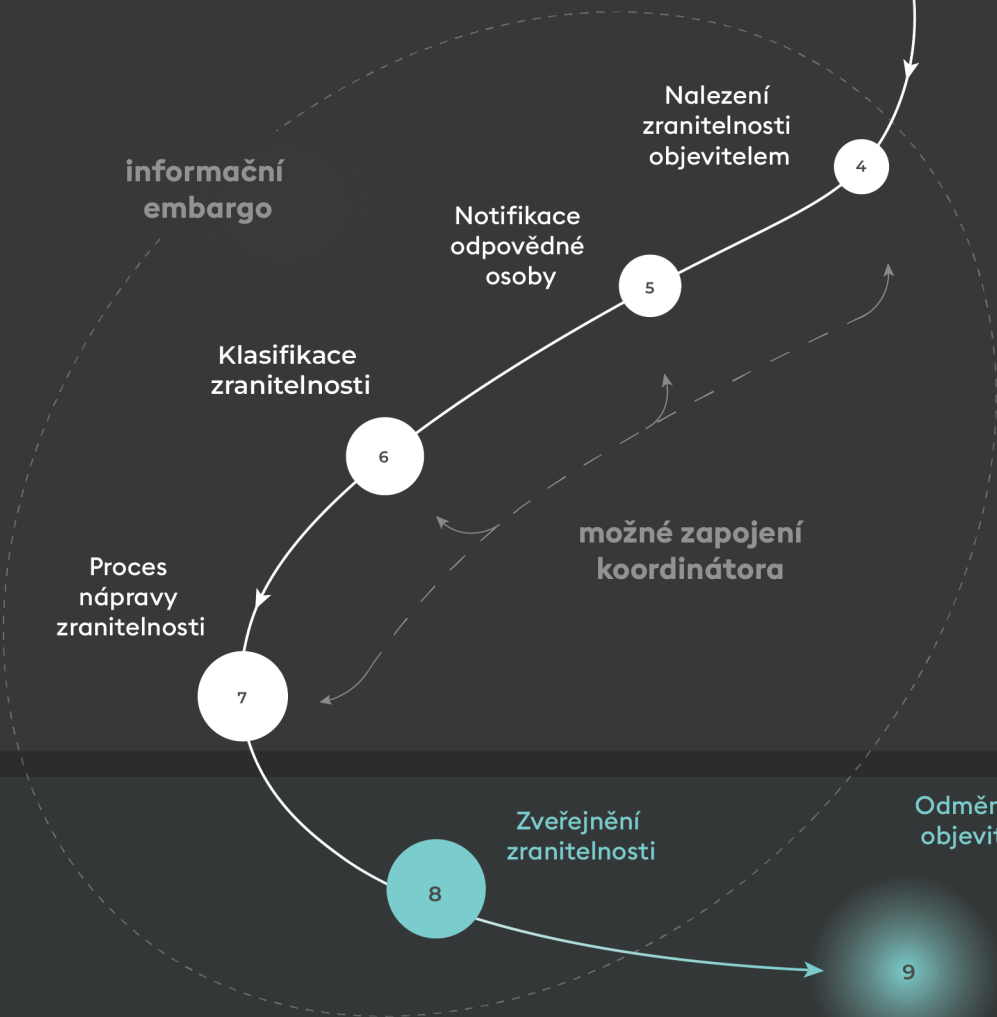
9. fáze

Implementace a provádění koordinovaného zveřejňování zranitelnosti

fáze zavedení CVD



fáze od nalezení zranitelnosti po její nápravu



fáze po nápravě zranitelnosti

1 Fáze nastavení politiky CVD

Odpovědná osoba by prvně měla zhodnotit, zda a do jaké míry CVD zavést. V této fázi je nezbytné vymezit rozsah konkrétních ICT produktů (lze tak vypsát např. seznam webových stránek spravovaných odpovědnou osobou), ve kterých mohou být zranitelnosti nalézány, a metod, které může objevitel k nalézání zranitelností pro dodržení pravidel politiky CVD využít.¹¹ Dále by měla odpovědná osoba určit způsob notifikace o zranitelnostech (tzn. zda bude využíván kontaktní formulář, e-mailová komunikace nebo jiný nástroj).

S tím souvisí rozhodnutí, zda přijímat i anonymní hlášení či nikoli. Pro zajištění vyšší důvěrnosti je vhodnější požadovat po objevitelích pravdivé kontaktní údaje, ač lze předpokládat, že někteří objevitelé mohou být od hlášení odrazeni. Anonymní podání na druhou stranu významně ztěžuje případné vymáhání škody na objeviteli, pakliže překročí podmínky politiky CVD.

Je proto na odpovědné osobě, aby zvážila výhody a nevýhody umožnění anonymního nahlášení zranitelností, tj. zda upřednostní vyšší pravděpodobnost nahlášení zranitelnosti oproti efektivitě případného vymáhání škody.

V politice by mělo být mimo jiné zdůrazněno, že svolení k objevování zranitelností se neuplatňuje na produkty a systémy třetích stran, vyjma těch, u kterých je odpovědná osoba oprávněna takové svolení dát a skutečně jej udělí. Jedná se o podstatný limit při implementaci CVD, kdy odpovědná osoba musí sama identifikovat ICT produkty třetích osob, které může zahrnout do rozsahu politiky CVD. Obecně odpovědná osoba nemůže dát souhlas s nalézáním zranitelností u ICT produktů třetích osob, vyjma vlastní implementace takových produktů a jejich konfigurace (takto lze například testovat vlastní síťové připojení ke cloudovému úložišti třetí osoby).

V ostatních případech musí mít sama odpovědná osoba svolení od třetí osoby k tomu, aby mohla ICT produkt do rozsahu politiky CVD zahrnout. Pokud odpovědná osoba udělí souhlas k nalézání zranitelností v ICT produktu, aniž by k tomu měla oprávnění, nemusí politika CVD poskytovat bezpečný přístav pro objevitele a mohou vzniknout negativní právní či jiné důsledky i pro odpovědnou osobu.

Velmi důležitou součástí politiky CVD by měla být mlčenlivost objevitele, tzv. informační embargo, které zajistí důvěrnost celého procesu.

¹¹ Rozsah udělených oprávnění lze definovat jako písemně specifikovaný rozsah systémů, IP adres (odkazující např. na aplikace, webové servery, databáze či operační systémy) a dalších případných aktiv organizace, které mohou být součástí objevování zranitelností.

Informační embargo

Po objevení zranitelnosti nesmí objevitel s informacemi o zranitelnosti ~~jakkoli~~ nakládat, vyjma komunikace s odpovědnou osobou či koordinátorem. Důvodem existence informačního embarga je potřeba odpovědné osoby získat dostatečný čas k nápravě objevené zranitelnosti. Informační embargo zabraňuje potenciálním útočníkům získat informace o objevené zranitelnosti předtím, než bude zranitelnost odstraněna.

CVD je pokryto informačním embargem od fáze objevení, až po fázi možného zveřejnění zranitelnosti.

Délka informačního embarga může být ovlivněna různými faktory, zohledněna by měla být zejména závažnost a složitost objevené zranitelnosti a technické možnosti odpovědné osoby vytvořit nápravné opatření. Porušení informačního embarga znamená překročení podmínek politiky CVD, tj. porušení smlouvy. V takovém případě objevitel musí zpravidla nahradit vzniklou škodu odpovědné osobě. Neoprávněné zveřejnění informace o zranitelnosti nicméně není spojeno se specifickou trestní rovinou nalézání zranitelností v ICT produktech, resp. nezakládá trestní odpovědnost pro neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému a nosiče informací.

Kromě informačního embarga je také na zvážení odpovědné osoby, zda v rámci své politiky CVD bude vyžadovat mlčenlivost objevitelů ohledně skutečností, se kterými se v rámci procesu zveřejňování zranitelností seznámí. Tato povinnost pak může trvat i po zveřejnění zranitelnosti a chránit informace o infrastruktuře odpovědné osoby.

Současně by měla odpovědná osoba specifikovat metody a techniky, které v rámci CVD nepovoluje, případně vymezí ty, které jsou jediné povolené. Zejména by měla zvážit zakázání způsobů nalézání zranitelností, u kterých lze předpokládat způsobení závažného výpadku funkčnosti či služeb, zásahy do osobních údajů, fyzické testování apod.¹² Doporučeno je ponechat možnost nalézat zranitelnosti způsoby, které nebudou znamenat významný problém pro odpovědnou osobu, typicky ve webových aplikacích.¹³

Zmíněné vymezení hranic CVD je kritické pro zabránění negativních důsledků objevování zranitelností jak pro objevitele, tak pro odpovědnou osobu.

S ohledem na účel CVD se nedoporučuje do podmínek politiky CVD zavádět smluvní pokuty pro porušení povinnosti ze strany objevitele, například informačního embarga. Jakkoli mohou být smluvní pokuty pro odpovědnou osobu pojistkou v případě způsobení škody, lze předpokládat, že objevitele bude smluvní pokuta odrazovat od nalézání zranitelností u dané odpovědné osoby, případně budou motivováni anonymně zveřejnit informaci o nalezené zranitelnosti.

2.

Fáze přípravy a zpřístupnění kapacit

Je zaměřena na budování kapacit a nastavování vnitřních procesů odpovědné osoby tak, aby se zajistila schopnost adekvátní reakce na nahlášené zranitelnosti. K tomu by odpovědná osoba měla vyhradit zaměstnance či případně vytvořit speciální útvar, který se bude problematikou CVD zabývat. Do gesce těchto pracovníků by mělo spadat vše od nastavení procesu CVD až po samotné zkoumání a odstraňování zranitelností.

3.

Fáze zveřejnění politiky CVD

Po pečlivé přípravě nastavení interních procesů nakládání s objevenou zranitelností odpovědná osoba zveřejní například na svých internetových stránkách politiku CVD, aby případní objevitelé mohli v mezích této politiky začít s vyhledáváním zranitelností v ICT produktech odpovědné osoby.

¹² Jako příklady nalézání zranitelností ke zvážení zákazu lze uvést: odepření služby (angl. DoS, DDoS), útoky hrubou silou (angl. brute force), prolamování hesel (angl. password cracking) a další, jak jsou popsány v odkazu na str. 21.

¹³ Jako příklady nalézání zranitelností ve webových aplikacích lze uvést: obcházení ověřovacích mechanismů, cross-site scripting (XSS), cross-site request forgery (CSRF), injektování SQL či LDAP kódu a další.

4.

Fáze nalézání zranitelností

Je těžištěm celého procesu. Zahrnuje již aktivní roli objevitele a vytvoření jeho vztahu s odpovědnou osobou. V případě cíleného nalézání zranitelností v rámci CVD musí objevitel porozumět dané politice CVD a postupovat dle pravidel stanovených odpovědnou osobou (včetně např. aktivního odsouhlasení podmínek, vyplnění kontaktního formuláře, registrace apod.). Není-li si objevitel jistý, jak si zveřejněné podmínky politiky CVD vyložit, měl by ještě před samotným zahájením objevování zranitelností danou odpovědnou osobu kontaktovat.

Pokud objevitel nalezne zranitelnost bez znalosti podmínek politiky CVD, bude záležet na tom, zda je jeho jednání dovoleno odpovědnou osobou. Pokud ano, je chráněn politikou CVD. V případě, že svolení v politice CVD chybí, či jednání překročilo podmínky politiky CVD, budou aplikovány obecné podmínky vzniku trestní odpovědnosti a odpovědnosti za škodu. Z tohoto důvodu by si objevitel měl vždy dopředu zjistit, zda odpovědná osoba svolila s nalézáním zranitelností a za jakých podmínek.

5.

Fáze notifikace odpovědné osoby

Následně může objevitel zahájit nalézání zranitelností dle pravidel politiky CVD. V případě cíleného nalézání zranitelností je nicméně nezbytné očekávat, že k jejich objevení vůbec nemusí dojít, ať už z důvodu dostatečného zabezpečení testovaného ICT produktu, či z důvodu omezených znalostí nebo technické kapacity na straně objevitele.

V případech nalezení zranitelnosti by však měl objevitel využít kontaktu dle politiky CVD a poskytnout odpovědné osobě informace obsahující:

- *objevitelovy pravdivé kontaktní údaje (pakliže tento krok daná politika CVD vyžaduje),*
- *nalezený typ zranitelnosti a její podrobný popis, včetně případného popisu významnosti zranitelnosti z pohledu objevitele,*
- *popis nástrojů a postupů použitých objevitelem k nalezení zranitelnosti.*

Poté, co je notifikace o zranitelnosti doručena odpovědné osobě, měla by tato osoba informovat objevitele o přijetí notifikace, sdělit mu další postup a zdůraznit existenci informačního embarga. V tomto ohledu je zejména vhodné uvést předpokládaný časový rámec, ve kterém odpovědná osoba zašle objeviteli zpětnou vazbu k nahlášené zranitelnosti.

Objevitel má možnost o zranitelnosti notifikovat rovněž koordinátora, což je vhodné zejména v případě významné zranitelnosti; tato notifikace může či nemusí být anonymní.

Doporučený časový průběh CVD po nalezení zranitelnosti

Dle barvy:

→ kdo činí jednání

● koho se jednání týká

— povinné jednání

- - - - - nepovinné jednání

objevitel

Nalezení
zranitelnosti

odpovědná osoba

koordinátor

Časová osa

T + 0 hod.

T + 24 hod.

T + 29 dnů

(v případě složitosti T + 89 dnů)

T + 30 dnů

(v případě složitosti T + 90 dnů)

další subjekty

Informování dodavatelů/správ-
ců/majitelů ICT produktů
dotčených zranitelností
o zranitelnosti

Přijetí
notifikace
o zranitelnosti

Přijetí notifikace
o zranitelnosti

Informování
odpovědné
osoby o přijetí
notifikace

Informování
objevitele
o přijetí
notifikace

Informování
koordinátora
o přijetí
notifikace

Klasifikace
zranitelnosti

Možné
poskytnutí
informací

Možné
poskytnutí
metodické podpory

Náprava
zranitelnosti

Informování
veřejnosti/uživatelů
o zranitelnosti a její
nápravě

Informování dodavate-
lů/správců/majitelů ICT
produktů dotčených zraní-
telností o její nápravě

Informování
o nápravě
a poskytnutí
odměny

Informování o nápravě
(pouze v případě,
že koordinátor vstoupil
do procesu CVD)



Fáze klasifikace zranitelností

Po obdržení notifikace ze strany objevitele by měla odpovědná osoba nejprve posoudit povahu a závažnost notifikované zranitelnosti. Takto lze určité zranitelnosti prioritizovat, případně vyřadit falešně pozitivní nálezy či zanedbatelné zranitelnosti, jejichž využití nepředstavuje hrozbu.

V tomto ohledu je možné využít Common Vulnerability Scoring System¹⁴, což je mezinárodně používaný klasifikační systém zranitelností. V případě, že odpovědná osoba nebude schopna sama dle svých kapacit zranitelnost dostatečně klasifikovat, může kontaktovat za účelem metodické pomoci koordinátora.

V tomto kroku je rovněž žádoucí, aby odpovědná osoba informovala o zranitelnosti jí známé dodavatele, správce nebo majitele ICT produktů dotčených nalezenou zranitelností. Ti se pak mohou podílet na nápravě zranitelnosti v další fázi CVD. Pokud do procesu CVD vstoupil koordinátor, má díky svému odbornému zázemí kapacity posoudit, kterých ICT produktů a subjektů se může zranitelnost podstatným způsobem dotknout, a tyto pak z vlastní iniciativy kontaktovat.



Fáze nápravy zranitelností

Odpovědná osoba vyčlení kapacity na nápravu zranitelnosti. Vzhledem k jedinečnému charakteru každé zranitelnosti nelze přesně stanovit okamžik, do kterého by mělo k nápravě dojít¹⁵. Obecně platí, že řádně otestovaná oprava s pozdějším datem zveřejnění je považována za lepší řešení, než urychlený a neucelený způsob nápravy. Z tohoto důvodu by mělo platit výše popsané informační embargo, aby odpovědná osoba měla jistotu, že nemusí nápravu zranitelnosti uspěchat.

¹⁴ Jedná se o systém standardizované metodiky hodnocení objevených zranitelností často užívaný pod zkratkou CVSS. Více informací o CVSS např. na internetové adrese <https://www.first.org/cvss>.

¹⁵ Náprava by však neměla překročit přiměřeně předvídatelnou dobu. Obecně lze doporučit, aby k nápravě zranitelnosti došlo do 30 dní, v případě zranitelnosti, která je technicky složitá na nápravu, do 90 dní.

Fázi nápravy zranitelnosti lze rozdělit na dva kroky:

I. Izolování problému

Notifikace zaslaná objevitelem bude zpravidla popisovat jednu cestu ke zneužití zranitelnosti. Avšak velmi často existují i další cesty a způsoby, jak zranitelnostizneužít. Proto je žádoucí, aby specialisté odpovědné osoby potenciálně zranitelnou část ICT produktu dočasně izolovali a provedli analýzu dalších možných cest a způsobů zneužití zranitelnosti.

II. Odstranění problému

V tomto kroku je velmi důležitá komunikace mezi objevitelem a odpovědnou osobou, a to nejen ohledně jejích časových potřeb, ale také ohledně poskytování dalších informací odpovědné osobě (např. výpis použitých nástrojů či doplnění chybějících informací v původní notifikaci zranitelnosti) nebo odpovědí na dotazy objevitele.

Přestane-li jedna ze stran komunikovat, lze se obrátit na koordinátora, který v takovém případě může do procesu vstoupit jako prostředník a pokusit se zajistit spolupráci obou stran.

Na základě podnětu ze strany odpovědné osoby může koordinátor vstoupit do procesu i v případě nemožnosti danou zranitelnost napravit z důvodu významných objektivních skutečností.¹⁶ Koordinátor pak může poskytnout nejen metodickou, ale v kritických případech i technickou pomoc s řešením problému. To nicméně nezbavuje odpovědnou osobu povinnosti konstantně vyvíjet snahu daný problém v rámci svých kapacit řešit. Nutno dodat, že koordinátor není ze zákona povinen technickou pomoc poskytnout. Pokud mu jeho kapacity nedovolí se nahlášené zranitelnosti po technické stránce věnovat, je oprávněn technickou pomoc neposkytnout.

Ukončení této fáze nastává v ideálním případě ve chvíli, kdy odpovědná osoba nalezne způsob nápravy zranitelnosti a vytvoří a rozešle bezpečnostní aktualizaci uživatelům. O tomto by měla odpovědná osoba rovněž informovat objevitele a koordinátora, pokud byl do procesu zapojen.

Nelze vyloučit, že zranitelnost nebude odpovědná osoba schopna napravit, a to ani ve lhůtě domluvené s koordinátorem.

V takovém případě by měla o této skutečnosti informovat objevitele i koordinátora a domluvit se s nimi na dalším postupu a zejména dodržování informačního embarga. Nemožnost napravit zranitelnost by nicméně neměla bránit poskytnutí případné odměny, pokud objevitel dodržel podmínky politiky CVD.

¹⁶ Mezi tyto skutečnosti se řadí např. nepředvídatelná vnější událost či příliš komplikovaný problém, jehož bezprostřední náprava zdaleka přesahuje finanční nebo technické možnosti odpovědné osoby.

8



Fáze zaměřená na způsoby a rozsah zveřejnění zranitelností

Nastává poté, co odpovědná osoba již opravila zranitelnost a vydala bezpečnostní aktualizaci pro zabezpečení ICT produktu. Zveřejnění zranitelnosti může proběhnout na internetových stránkách a sociálních sítích odpovědné osoby a v rámci notifikace klientům užívajícím její ICT produkt.

Je však třeba zdůraznit, že zveřejnění zranitelnosti není povinné a je zcela na vůli odpovědné osoby, zda a v jakém rozsahu k tomuto kroku přistoupí. Odpovědná osoba by si při této volbě nicméně měla být vědoma, že pokud se jedná o zranitelnost, kterou lze klasifikovat jako vysokou či dokonce kritickou, může být objevitel sám motivován k jejímu zveřejnění (být v rozporu s informačním embargem).

V případech, kdy do procesu vstupuje koordinátor, má v rámci svých zákonných pravomocí a povinností možnost s informací o zranitelnosti dále nakládat.¹⁷

Ještě před samotným zveřejněním se odpovědné osobě doporučuje rozeslat návrh informace o zranitelnosti všem zainteresovaným stranám, které se tak budou moci k obsahu a formě zveřejňovaných informací vyjádřit. Bude se typicky jednat o samotného objevitele a koordinátora (pokud do procesu CVD vstoupil), ale i dodavatele, správce nebo majitele ICT produktů, kteří jsou dotčeni nalezenou zranitelností.

V rámci politiky CVD je možné stanovit podmínky, za jakých bude moci zranitelnost zveřejnit i objevitel včetně například svého kontaktu, aniž by porušil informační embargo. V takovém případě se pro objevitele zvýší atraktivita CVD dané odpovědné osoby, neboť mohou zveřejnit svůj úspěch a kontaktní údaje. V tomto ohledu by odpovědná osoba měla přesně určit, kdy a v jakém rozsahu informační embargo zaniká, tak aby objevitel již nebyl vázán mlčenlivostí o informaci týkající se existence zranitelnosti.

S ohledem na účel CVD je ale vhodné, aby informační embargo trvalo až do doby, než je zranitelnost opravena a rozeslána bezpečnostní aktualizace.

¹⁷ Např. NÚKIB, jehož součástí je vládní CERT, tedy koordinátor CVD pro ČR, je oprávněn vydat varování dle § 22 odst. 1 zákona č. 264/2025 Sb., zákon o kybernetické bezpečnosti.



Fáze odměňování objevitele

Pokud objevitel dodržel veškerý postup daný politikou CVD, doporučuje se jej za jeho úsilí odměnit. Vhodnou formou může být veřejné poděkování a vyzdvižení objevitele za jeho příspěvek ke zlepšení bezpečnosti ICT produktu či finanční nebo jiná hmotná odměna (např. poukazy, symbolické dárky, trička). Forma a výše odměny by každopádně měla záviset na kvalitě nahlášení a významu dané zranitelnosti.

Odměna by ideálně měla být objeviteli poskytnuta do 15 až 30 dní od nahlášení zranitelnosti, což by mělo být specifikováno v politice CVD. V této lhůtě by odpovědná osoba již měla mít dostatek informací, zda nahlášená zranitelnost splňuje nárok na odměnu (dle podmínek politiky CVD). Poskytnutí odměny nebrání ani skutečnost, že zranitelnost nelze ve lhůtě 15 dní napravit, například z důvodu její složitosti. Nastavení lhůt pro poskytnutí odměny rovněž zvyšuje důvěryhodnost CVD odpovědné osoby a zvyšuje jeho atraktivitu pro objevitele.¹⁸ Vyplacením odměny před napravením zranitelnosti, které může trvat delší dobu navíc sníží riziko, že objevitelé zranitelnost zveřejní sami.

Odměňování je velmi důležité z hlediska vytváření pozitivního vztahu mezi potenciálními objeviteli a odpovědnou osobou. Vytváří se motivace pokračovat ve spolupráci a nalézat další zranitelnosti.

¹⁸ V takovém případě se odměna vyplácí zpravidla tomu objeviteli, který jako první zranitelnost nahlásí.

Proč podporovat CVD?

01

Česká republika skrze NÚKIB bude aktivně podporovat zavádění CVD v soukromé i veřejné sféře pomocí metodických materiálů, pilotních projektů, vzdělávání a dalších nástrojů.

02

Široké zavedení CVD posílí kybernetickou bezpečnost napříč subjekty v České republice a navýší povědomí ve společnosti o důležitosti zabezpečení ICT produktů.

03

CVD umožní objevitelům nalézat zranitelnosti v ICT produktech v souladu s právními předpisy za podmínek odpovědné osoby a současně ochrání informaci zranitelnosti.

4

Národní politika koordinovaného zveřejňování zranitelností

Pro úspěšné rozšíření CVD jako nástroje pro posilování zabezpečení ICT produktů je nezbytné, aby ČR aktivně CVD propagovala a poskytla nástroje pro snadnou implementaci CVD napříč subjekty v ČR. Současně musí být připraveny kapacity státu pro zajištění role koordinátora.

4.1 Platforma CVD jako nástroj pro snadnější implementaci a propagaci CVD

Svým charakterem CVD umožňuje nalézání zranitelností v ICT produktech napříč celou společností, s minimálními náklady pro odpovědné osoby, které si politiku CVD v rámci své organizace zavedou.

Popsaný proces však může u mnoha odpovědných osob budit představu složitého mechanismu, který může navíc v případě nalezení zranitelnosti poškodit jejich reputaci či reputaci jejich ICT produktů. Reputační, provozní a finanční rizika spojená se zneužitím neodhalené zranitelnosti jsou však téměř vždy daleko vyšší než v dobré víře odhalená a napravená zranitelnost.

Z hlediska bezpečnosti ČR je proto na místě prosazovat koordinované zveřejňování zranitelností jako nedílnou součást zajišťování kybernetické bezpečnosti, jež má pozitivní dopad na stát i na samotné odpovědné osoby. Současně je potřeba, aby stát pomohl jak soukromým, tak veřejnoprávním subjektům se zaváděním vlastní politiky CVD a odstraňoval bariéry, které by tomu mohly bránit.

Pro co nejširší zavedení funkčních politik CVD napříč jednotlivými subjekty v ČR je nutno vytvořit právně-technickou metodiku koordinovaného zveřejňování zranitelností zohledňující zákonné požadavky ČR a tu zveřejnit přístupnou formou široké veřejnosti na tzv. Platformě CVD. Gestorem jejího vytvoření by byl NÚKIB jakožto gestor kybernetické bezpečnosti v ČR.

Na Platformě CVD by měl být v obecné i konkrétní rovině popsán právní rámec pro aplikaci politiky CVD odpovědnými osobami a konkrétní doporučení k obsahu politiky CVD, jež by eliminovala nebo alespoň zmírňovala právní postihy hrozící objeviteli při nalézání a ohlašování zranitelností. Dále by měla Platforma CVD obsahovat popis vztahů mezi všemi aktéry procesu koordinovaného zveřejňování zranitelností, tzn. vztahů mezi objevitelem, odpovědnou osobou a koordinátorem.

Kroky k implementaci Národní politiky CVD v ČR

1.

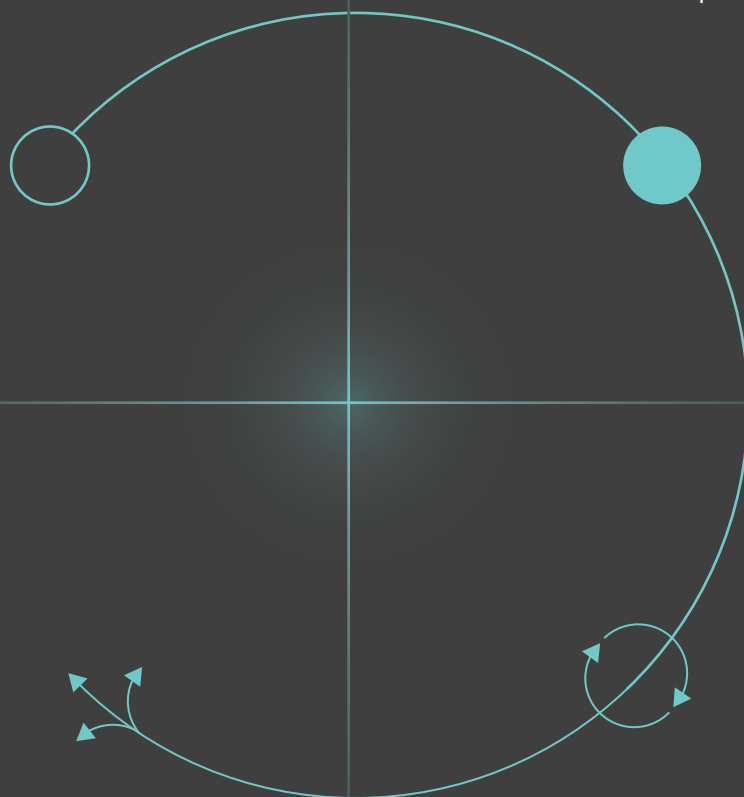
Zavedení koordinátora CVD na vládním CERT

Spolupráce napříč koordinátory
CVD v Evropské unii

2.

Vytvoření platformy CVD

Sdílení materiálů usnadňujících
implementaci CVD



4.

Postupné zavádění CVD napříč subjekty v ČR

Podpora pilotních projektů

3.

Zveřejnění metodických materiálů pro implementaci CVD

Propagace CVD jako efektivního
způsobu navyšování zabezpečení
ICT produktů

4.2 Cíle Platformy CVD

Návod

Bude obsahovat soubor materiálů k inspiraci či přímé implementaci CVD. Národní politika CVD, popřípadě obdobné publikace mezinárodních organizací, mohou sloužit jako inspirace pro zavádění CVD.

Přístup ČR

Potenciálním objevitelům představí pohled ČR na problematiku CVD a umožnit jim vyvarovat se jednání, které by pro ně mělo negativní právní důsledky. Tím bude posílena jejich právní jistota a motivace objevovat zranitelnosti u osob působících v ČR, které přijaly vlastní politiku CVD, resp. poskytly oprávnění vyhledávat zranitelnosti jinak.

Osvěta

Pomůže k osvětě o koncepci CVD jako státem podporovaného procesu, majícího za cíl posílení kyberbezpečnosti ČR. V některých státech došlo k zavedení politik CVD ve státní správě právě za účelem motivování jednotlivých osob k zavedení vlastních politik CVD a posílení celkové kybernetické bezpečnosti státu.¹⁹

4.3 Vládní CERT jako koordinátor CVD

Primárním gestorem kybernetické bezpečnosti v České republice je NÚKIB, jehož součástí je i vládní CERT, který plní roli týmu CSIRT²⁰. Je proto vhodné, aby roli koordinátora zastával právě vládní CERT, mezi jehož působnost patří i přijímání hlášení o kybernetických bezpečnostních incidentech, jejich vyhodnocování a hodnocení zranitelností. Jakožto koordinátorovi budou vládnímu CERT příslušet pravomoci:

Přijímání hlášení o zranitelnostech a jejich vyhodnocení

Jakákoli osoba bude moci vládnímu CERT nahlásit objevenou zranitelnost (i anonymně), ať už z důvodu nedostatečné komunikace ze strany odpovědné osoby, závažnosti zranitelnosti, či jiného důvodu.

¹⁹ Jedná se např. o Nizozemsko, Belgii či Francii.

²⁰ Týmy pro reakce na počítačové bezpečnostní incidenty zřízené členskými státy dle čl. 10 směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2). V ČR tuto úlohu zastává vládní CERT a národní CERT dle § 42 odst. 5 písm. j) a § 43 odst. 1 písm. h) zákona č. 264/2025 Sb., zákon o kybernetické bezpečnosti.

Poskytnutí asistence při řešení zranitelnosti

Nahlášenou zranitelnost vládní CERT vyhodnotí a případně sám upozorní odpovědnou osobu ohledně nalezené zranitelnosti a poskytne metodickou podporu. Odbornou technickou pomoc s řešením zranitelnosti poskytne dle svých kapacit, zejména v případě závažné zranitelnosti.

Dojednávání lhůt pro řešení a zveřejnění zranitelností

Mezi úkoly vládního CERT bude náležet komunikace s odpovědnou osobou ohledně dalšího nakládání s informací o nahlášené zranitelnosti, včetně nastavování lhůt pro její nápravu a zveřejnění. Zpravidla tak bude činit po dohodě s odpovědnou osobou a objevitelem, tak aby lhůta reflektovala kapacity vyčleněné na nápravu zranitelnosti a její následné zveřejnění. S ohledem na charakter zranitelností tato lhůta nemůže být stanovena paušálně pro každý případ, protože doba potřebná pro analýzu zranitelnosti a její nápravu se může případ od případu značně lišit. Přesto by však neměla přesahovat určitou přiměřenou dobu, neboť s průběhem času narůstá riziko objevení a zneužití zranitelnosti jinou osobou.²¹

Jedním ze stěžejních úkolů koordinátora bude podnítit činnost odpovědné osoby pro případ, kdy například nereaguje na zranitelnost zaslané objevitelem nebo odmítá zranitelnost napravit či zveřejnit. V takových situacích bude moci koordinátor určit lhůtu k nápravě či zveřejnění zranitelnosti. Odpovědná osoba sice nemá povinnost takto určenou lhůtu dodržet, jedná se však o způsob, jakým koordinátor může podporovat proces nápravy zranitelnosti a motivovat odpovědnou osobu k činnosti.

Jestliže odpovědná osoba lhůtu není schopna dodržet, měla by v průběhu lhůty informovat koordinátora a případně i objevitele. Za takové situace může být vhodné dojednat novou lhůtu, dle konkrétní situace.

²¹ Lze doporučit, aby byl celý proces CVD dokončen do 30 dní od objevení zranitelnosti, v případě složitější nápravy zranitelnosti do 90 dní (viz schéma na straně 32).

Využití informace o zranitelnosti v rámci působnosti NÚKIB

NÚKIB, jehož je vládní CERT součástí, bude moci informaci o zranitelnosti využít v rámci své působnosti, jako je například vydání varování nebo jiného protiopatření dle zákona č. 264/2025 Sb., zákon o kybernetické bezpečnosti.

Spolupráce s dalšími koordinátory CVD

S ohledem na své ostatní činnosti bude vládní CERT rovněž schopen kvalifikovaně posoudit závažnost objevené zranitelnosti, včetně jejího případného přeshraničního dopadu. V takových případech bude nezbytné, aby vládní CERT kontaktoval příslušné orgány či subjekty v daných zemích a notifikoval je o existenci zranitelnosti, případně s nimi spolupracoval za účelem nápravy zranitelnosti a dalšího postupu.

Současně bude vládní CERT působit jako kontakt pro koordinátory z jiných členských států Evropské unie v případě zranitelnosti nalezené v jiném členském státě, mající dopad na Českou republiku.

Nedodržení lhůt

Vzhledem k tomu, že CVD je dobrovolný proces, koordinátor nebude mít možnost například z důvodu nečinnosti při nápravě zranitelnosti ukládat pokuty a jiné sankce nebo užívat donucovací prostředky, kterými by vynucoval nápravu a zveřejnění zranitelnosti.

Tato skutečnost nicméně nebrání zveřejnění zranitelnosti ze strany koordinátora v případě, že odpovědná osoba bez závažných důvodů nedodrží dohodnuté či určené lhůty, případně nebude vůbec komunikovat.

Působnost vládního CERT jako koordinátora CVD



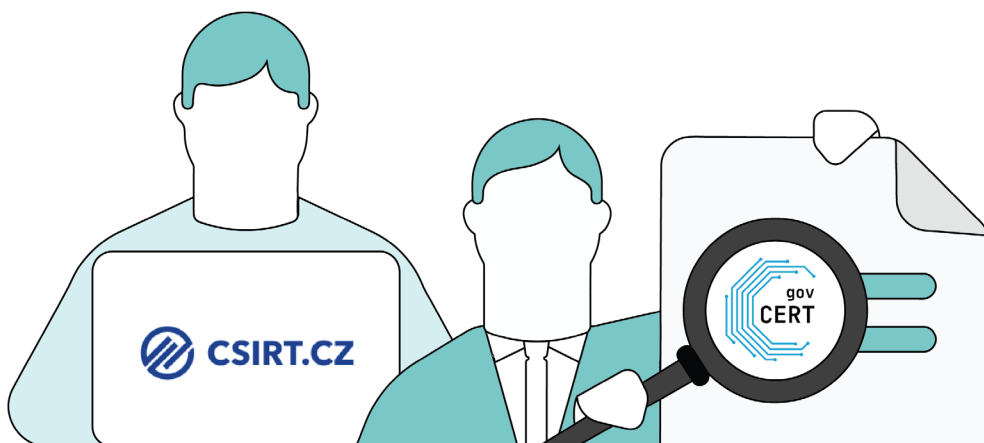
4.4 Spolupráce vládního a národního CERT

ČR vykazuje v rámci organizace týmů CSIRT specifikum v podobě existence dvou týmů typu CERT/CSIRT s celostátní působností.

Kromě vládního CERT působí v ČR též národní CERT, jehož úlohu zastává na základě veřejnoprávní smlouvy soukromý subjekt²². Dané rozdělení kompetencí mezi vládní CERT a národní CERT reflektuje mimo jiné poptávku po centralizovaném soukromoprávním subjektu, který by shromažďoval informace o kybernetických incidentech a poskytoval metodickou a technickou podporu subjektům, u nichž není nezbytné, aby tuto roli zastával orgán veřejné moci. Mnohé osoby totiž nechtějí státu poskytovat informace o kybernetickém zabezpečení či zranitelnostech svých systémů a namísto toho preferují důvěryhodnou soukromou osobu, působící v oblasti kybernetické bezpečnosti po dlouhou dobu.

Potenciál tohoto specifika bude využit i v rámci možnosti nahlašovat zranitelnosti koordinátorovi. Objevitelé v rámci CVD budou moci notifikovat o zranitelnosti anonymně i národní CERT, který by následně koordinoval komunikaci s odpovědnou osobou a dojednávat a určovat lhůty pro nápravu a zveřejnění zranitelnosti.

Tato činnost bude doplňovat obecnou působnost národního CERT, jenž provádí mimo jiné hodnocení zranitelností a zveřejňuje či předává NÚKIB údaje o kybernetických bezpečnostních incidentech. Pokud se zranitelnost bude týkat poskytovatele regulované služby v režimu vyšších povinností²³, případně bude obdobně významná nebo se zahraničním přesahem, bude koordinaci obstarávat výhradně vládní CERT.



²² Aktuálně CZ.NIC, z. s. p. o.

²³ § 8 odst. 1 zákona č. 264/2025 Sb., zákon o kybernetické bezpečnosti.

4.5 Zapojení soukromých subjektů do koordinace CVD

Výše uvedené vymezení koordinátora nebrání tomu, aby obdobnou pomocnou roli zastával i soukromý subjekt nabízející například asistenci s řešením objevených zranitelností. Typicky se jedná o provozatele portálů, které shromažďují zveřejněné CVD politiky a pro odpovědné osoby umožňují předběžně klasifikovat nahlášení zranitelnosti.

Před nahlášením zranitelnosti takovému subjektu by nicméně objevitel měl mít ad hoc svolení odpovědné osoby, případně by mělo být upraveno již v rámci CVD politiky. V opačném případě se vystavuje nebezpečí porušení informačního embarga.

Tyto soukromé subjekty nejsou koordinátory ve výše uvedeném smyslu, byť se jejich činnost může v mnohém překrývat. Koordinátor je určen státem dle požadavků směrnice NIS 2, s čímž je spojeno právo každé osoby nahlásit mu zranitelnost a současně povinnost koordinátora se danou zranitelností zabývat. Soukromý subjekt tak činí na základě vlastní poskytované služby.

4.6 Nasazení CVD z hlediska právního řádu ČR

Má-li být CVD správně nastaveno a aplikováno, je zapotřebí minimalizovat hrozbu právního postihu pro objevitele.

Byť CVD je z pohledu právních aspektů specifické, je nezbytné nacházet jejich řešení v rámci právního řádu ČR, které ochrání jak objevitele, tak odpovědnou osobu. V rámci konkrétní politiky CVD musí být vytvořena ochranná opatření, aby se objevitel nemusel obávat negativních právních důsledků a politika CVD tak mohla účinně fungovat.

Na Platformě CVD bude zveřejněn dokument o právních aspektech CVD. V něm budou jednotlivé právní aspekty relevantní pro CVD detailně analyzovány²⁴, a to včetně doporučení pro nastavení konkrétní politiky CVD, aby byly odstraněny nebo alespoň zmírněny rizika negativních právních důsledků pro objevitele.

²⁴ Jedná se zejména o oblasti trestního práva, náhrady škody a nemajetkové újmy, ochrany osobních údajů a práva duševního vlastnictví.

4.7 Základní právní východiska

V kontextu právního řádu ČR se pro implementaci CVD u jednotlivých odpovědných osob jeví jako nejvhodnější uzavírání smluv mezi odpovědnými osobami a objeviteli.

Takové smlouvy by obsahovaly svolení s vyhledáváním zranitelností, aby se tak předešlo kriminalizaci nalézání zranitelností, vzdání se práva na náhradu škody v případě dodržování ujednání politiky CVD či povinnost nahlásit seznámení se s osobními údaji skrz objevitelskou činnost.

Je na odpovědné osobě, jak způsob uzavření smlouvy sama upraví, kdy například může požadovat po objevitelích uvedení kontaktních údajů, přímé odsouhlasení podmínek politiky CVD²⁵ apod.

Odpovědná osoba by nicméně v takových případech měla brát v potaz, že obdobné požadavky mohou odradit množství potenciálních objevitelů, a politika CVD tak nemusí být v praxi využívána.

²⁵ Např. tzv. click-to-wrap způsob uzavření smlouvy, tedy uzavření smlouvy kliknutím na příslušné tlačítko na internetových stránkách odpovědné osoby.

Ilustrativní příklad

Objevitel na dané webové stránce odpovědné osoby nalezne v sekci „koordinované zveřejňování zranitelností“ politiku CVD, ve které by byly obsaženy podmínky smlouvy. V případě, že objevitel začne objevovat zranitelnosti, svým jednáním konkludentně vyjádří souhlas s podmínkami politiky CVD.

Mezi objevitelem a odpovědnou osobou vznikla smlouva o koordinovaném zveřejňování zranitelností, čímž bude docíleno ochrany objevitele, za předpokladu, že se bude řídit politikou CVD.

Schéma CVD od politiky státu
po smlouvu s objevitelem

ÚROVEŇ STÁTU

Politika a přístup
státu k CVD

Metodika pro subjekty
v soukromé i veřejné sféře

Zavedení koordináta

ÚROVEŇ
ODPOVĚDNÉ OSOBY

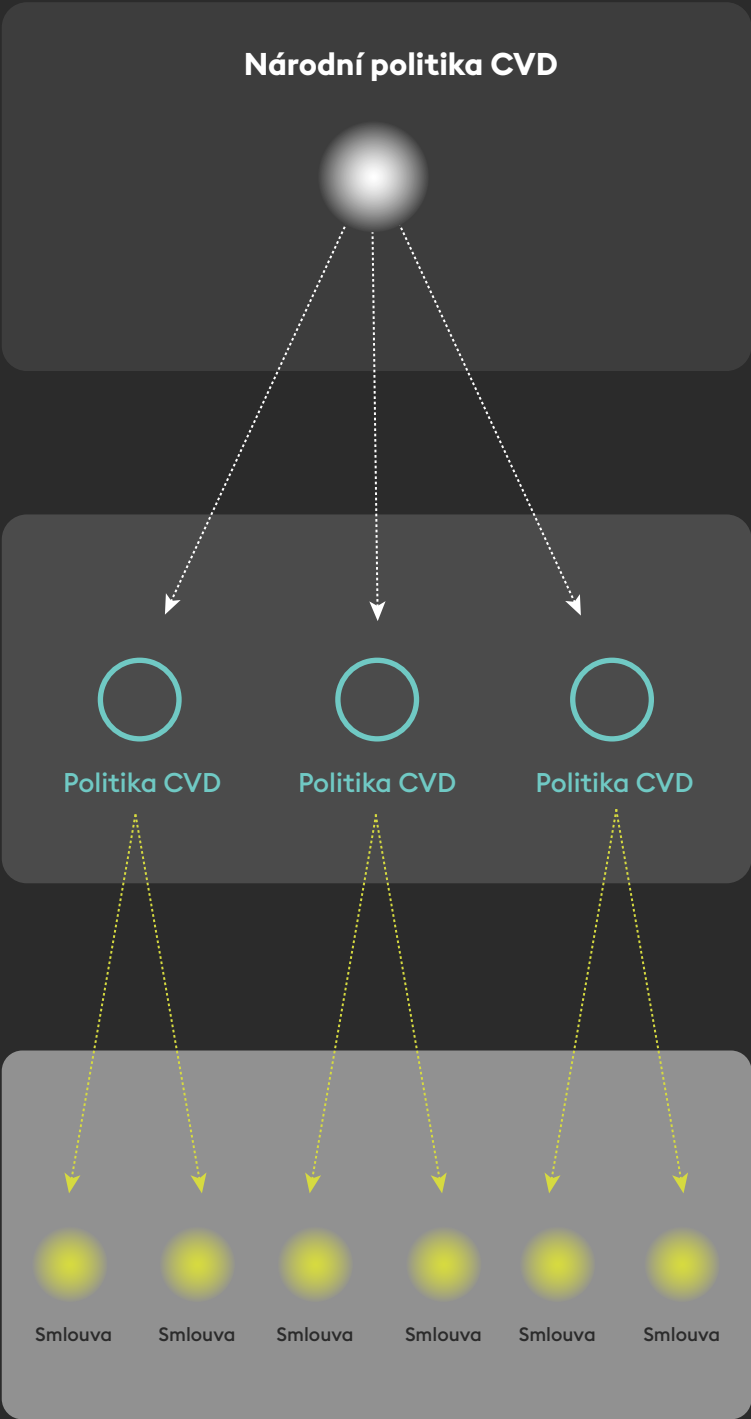
Veřejná politika CVD
konkrétních subjektů
(soukromých osob
a orgánů veřejné moci)

Shrnutí základních
parametrů CVD procesu
konkrétního subjektu

ÚROVEŇ VZTAHU
OBJEVITELE
A ODPOVĚDNÉ
OSOBY

Soukromoprávní smlouvy
s konkrétními objeviteli

Podrobné vymezení práv
a povinností



Praktická ukázka politiky CVD

Níže je praktická ukázka politiky koordinovaného zveřejňování zranitelností, kterou využívá nizozemská vláda jako návod na vytvoření politiky CVD pro soukromý sektor.

Lze si povšimnout velmi stručné, srozumitelné a výstižné formy.

Responsible Disclosure

At the Acme Corporation, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- E-mail your findings to cert@example.com. Encrypt your findings using our [PGP key](#) to prevent this critical information from falling into the wrong hands,
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,
- Do not reveal the problem to others until it has been resolved,
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

What we promise:

- We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date,
- If you have followed the instructions above, we will not take any legal action against you in regard to the report,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,
- We will keep you informed of the progress towards resolving the problem,
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and
- As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

Přehled zavádění CVD V Evropské unii

**Mapa stavu zavedení národní politiky CVD
v jednotlivých členských státech Evropské unie.**

Stav ke dni 13. dubna 2022.

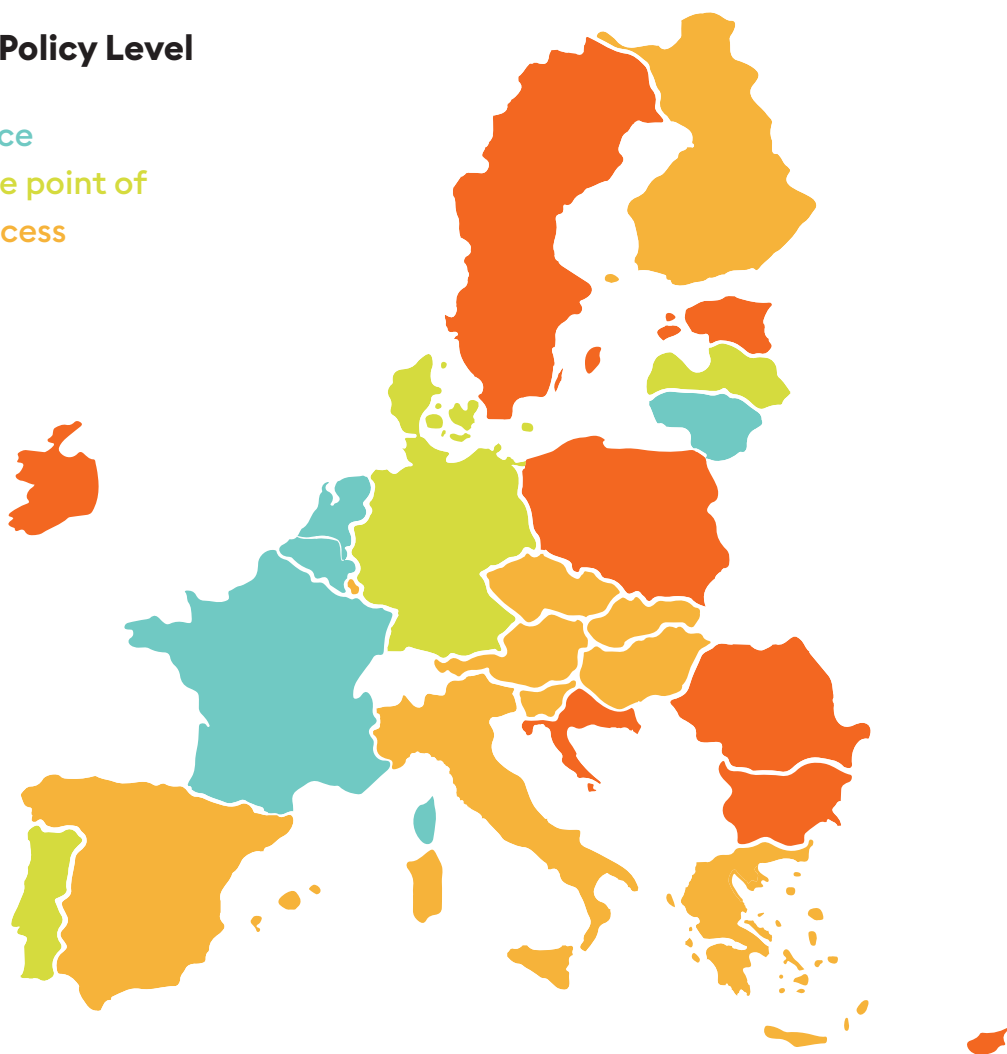
CVD Policy Level

In Place

On the point of

In process

No



Zdroj: ENISA, COORDINATED VULNERABILITY DISCLOSURE POLICIES IN THE EU

Zdroje

- 1) European Union Agency for Cybersecurity, Coordinated Vulnerability Disclosure policies in the EU. European Union Agency for Cybersecurity, duben 2022, ISBN 978-92-9204-574-6, dostupné z: <https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu>
- 2) Centre for European Policy Studies, Software Vulnerability Disclosure in Europe Technology, Policies and Legal Challenges. In: CEPS, červen 2018, ISBN 978-94-6138-687-8. Dostupné z: https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf
- 3) National Cyber Security Centre, Reporting a vulnerability (CVD). In: Ministry of Justice and Security, National Cyber Security Centre [online], [cit. 12.10.2025]. Dostupné z: <https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd>
- 4) National Cyber Security Centre, Preparing a CVD policy. In: Ministry of Justice and Security, National Cyber Security Centre [online], [cit. 12.10.2025]. Dostupné z: <https://english.ncsc.nl/get-to-work/implement-a-cvd-policy/preparing-a-cvd-policy>
- 5) National Cyber Security Centre, CVD-report form. In: Ministry of Justice and Security, National Cyber Security Centre [online], [cit. 12.10.2025]. Dostupné z: <https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd/cvd-report-form>
- 6) National Cyber Security Centre, Coordinated Vulnerability Disclosure: the Guideline, říjen 2018. In: Ministry of Justice and Security, National Cyber Security Centre [online], [cit. 12.10.2025]. Dostupné z: <https://english.ncsc.nl/get-to-work/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline>
- 7) Centre for cyber security Belgium, CCB Coordinated vulnerability disclosure policy. In: Centre for cyber security Belgium [online], [cit. 12.10.2025], dostupné z: https://ccb.belgium.be/sites/default/files/2024-12/Brochure_CVDP_UK_A5_DP2.pdf
- 8) HackerOne, Software Vulnerability Disclosure in Europe: Summary and Key Highlights of the European Parliament CEPS Task Force Report. In: HackerOne [online]. HackerOne Inc., [cit. 12.10.2022], dostupné z: <https://www.hackerone.com/vulnerability-management/software-vulnerability-disclosure-europe-summary-and-key-highlights>
- 9) Národné centrum kybernetickej bezpečnosti SK-CERT, Návod na oznamovanie zraniteľností. In: Národný bezpečnostný úrad, Národné centrum kybernetickej bezpečnosti SK-CERT [online], [cit. 12.10.2025], dostupné z: <https://www.sk-cert.sk/sk/oznamovanie-zranitelnosti/index.html>

- 10) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2), In: Úřední věstník. L 333, 27. 12. 2022, s. 80–152, Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:32022L2555&qid=1761579054825>
- 12) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), In: Úřední věstník. L 119, 4.5.2016, s. 1–88, Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex%3A32016R0679>
- 13) Zákon č. 264/2025 Sb., zákon o kybernetické bezpečnosti. In: Zákony pro lidi [online]. AION CS, 2010–2022, [cit. 1. 11. 2025]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2025-264>
- 14) Zákon č. 89/2012 Sb., občanský zákoník. In: Zákony pro lidi [online]. AION CS, 2010–2022, [cit. 12. 10. 2025]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-89>
- 15) Zákon č. 40/2009, trestní zákoník. In: Zákony pro lidi [online]. AION CS, 2010–2022, [cit. 12. 10. 2025]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40>
- 16) Národní strategie kybernetické bezpečnosti České republiky. Národní úřad pro kybernetickou a informační bezpečnost; dostupné z: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni--plan>
- 17) Akční plán k národní strategii kybernetické bezpečnosti České republiky. Národní úřad pro kybernetickou a informační bezpečnost; Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/>
- 18) Penetrační testování. Národní úřad pro kybernetickou a informační bezpečnost; dostupné z: https://nukib.gov.cz/download/publikace/podperne_materialy/2022-03-07_Penetracni-testovani_v1.2.pdf
- 19) Penetrační testy a exploatace. Selecký. 2012. Brno: Computer Press

