KOORDINOVANÉ ZVEŘEJŇOVÁNÍ ZRANITELNOSTÍ (CVD)

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

CVD team
Oddělení národních strategií a politik
Sekce strategických agend a spolupráce

CVD:

Koordinované zveřejňování zranitelností *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 dodavateli podaří vyvinout opravu, záplatu nebo najít jiné řešení. 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.*

Vymezení CVD

1. Užší - specifický proces nalézání, oznamování a zveřejňování zranitelností

2. Širší vymezení - forma etického hackingu

Etické nalézání zranitelností v ICT produktech

1. Prostřednictvím interních kapacit
   - *subjekt sám na své náklady a dle svých kapacit nalézá zranitelnosti v jím spravovaných ICT produktech*

2. Penetrační testování
   - *profesionální tým hackerů nalézá zranitelnosti na základě jednorázové smlouvy*

3. Bug bounty
   - *vypsání krátkodobého programu k nalézání zranitelností za odměnu*

4. Neformalizovaný etický hacking
   - *dobrovolná aktivita etických hackerů bez souhlasu správce testovaných ICT produktů*

5. **Koordinované zveřejňování zranitelností (Coordinated vulnerability disclosure - „CVD“):**
   - *dlouhodobá politika subjektu umožňující nalézání zranitelností dobrovolnými etickými hackery*

Osoby zúčastněné na CVD

Odpovědná organizace	Objevitel zranitelnosti	Koordinátor
Fyzická nebo právnická osoba, případně i orgán veřejné moci, která vlastní, vyrábí, prodává či spravuje ICT produkty.	**Zpravidla fyzická osoba, která záměrně nebo náhodně, avšak s dobrým úmyslem, identifikuje potencionální zranitelnost v ICT produktech a nahlásí ji odpovědné organizaci či koordinátorovi.**	**Organizace typu CSIRT. V případě objevení zranitelnosti je koordinátor schopen propojit zúčastněné strany a koordinovat další postup k nápravě zranitelnosti, která ohrožuje více odpovědných organizací. Koordinátor může v krajních případech poskytnout i technickou či odbornou pomoc.**

Principy CVD:

- Dobrovolnost zavedení CVD
  je na odpovědné osobě, zda vyhodnotí CVD ve své organizaci jako užitečné pro navýšení kyberbezpečnosti

- Nastavení pravidel odpovědnou osobou
  odpovědná osoba si může přesně nastavit hranice CVD (zejména rozsah toho, co může objevitel testovat - scope)

- Spolupráce mezi objevitelem x odpovědnou osobou x koordinátorem
  CVD je založeno na sdílení informací mezi objevitelem a odpovědnou osobou, za případné pomoci koordinátora

- Ochrana informace o zranitelnosti
  po objevení zranitelnosti je objevitel vázán mlčenlivostí – informačním embargem

- Zveřejnění zranitelnosti primárně v rukou odpovědné osoby
  odpovědná osoba je zodpovědná za nápravu zranitelnosti a neměla by se bránit jejímu zveřejnění

Výhody zavedení CVD pro konkrétní organizaci

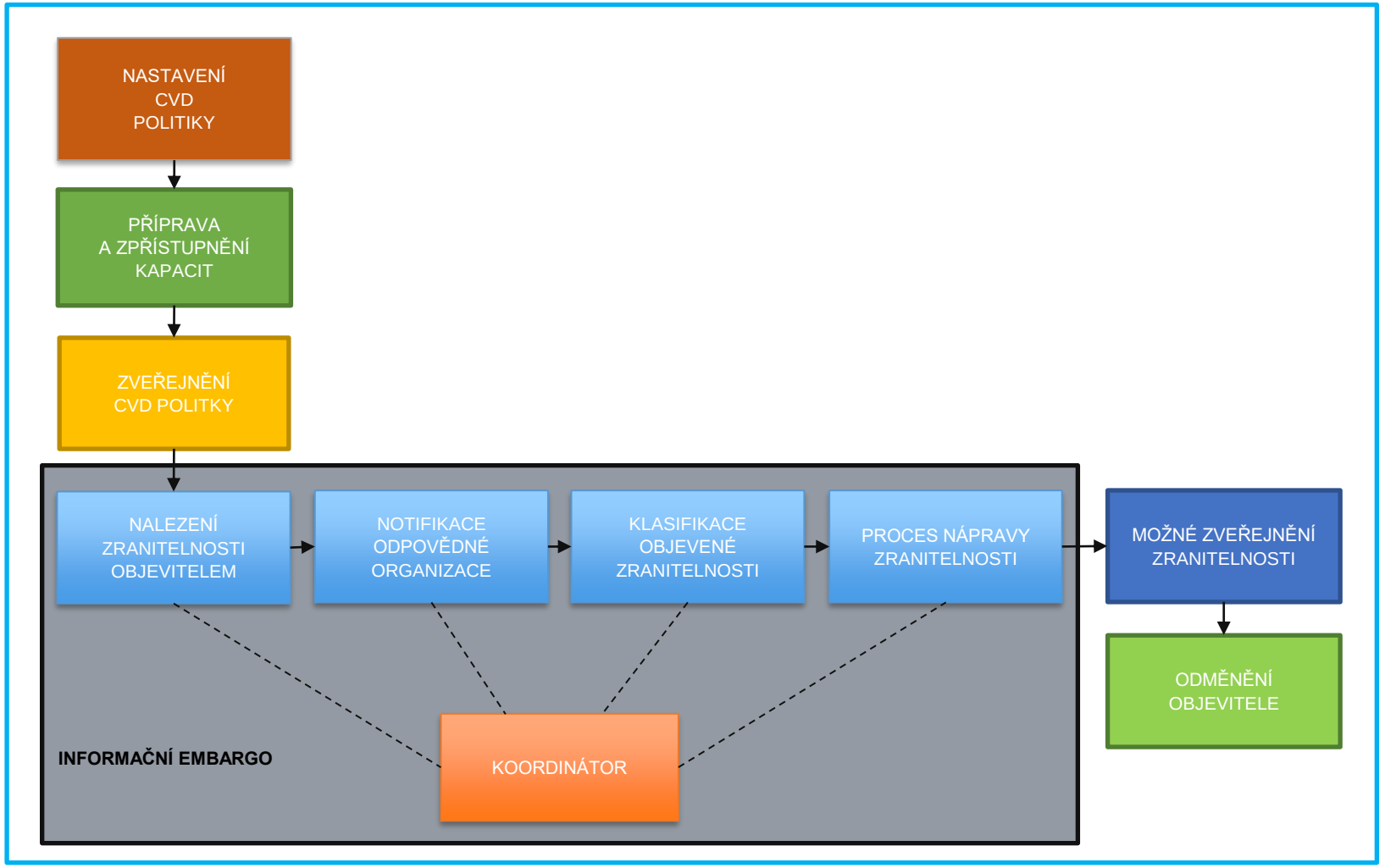
- Užitečné, efektivní, legální a levné zjišťování zranitelností v ICT produktech
  levné testování ICT produktů za podmínek stanovených odpovědnou organizací

- Navýšení bezpečnosti ICT produktů
  možnost dlouhodobého a opakovaného testování zranitelností v ICT produktech

- Důvěra v ICT zabezpečení
  demonstrace snahy o vysokou kybernetickou bezpečnost ICT produktů

- Garance důvěrnosti
  zajištění důvěrnosti s objevitelem zranitelnosti a ochrany informací

Implementace CVD v konkrétní organizaci



Národní politika CVD v České republice

Vizí je vytvoření Národní politiky CVD, jež by měla být právně-technickou metodikou umožňující snadnou implementaci CVD v rámci konkrétních soukromých subjektů i orgánů státu.

CVD jako úkol pro NÚKIB

- **Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025:**

10.	Zpracovat návrh národní politiky koordinovaného zveřejňování zranitelností.	NÚKIB

- **Směrnice NIS 2:**
  a) Přijmout politiku řešení zranitelností, včetně prosazování a usnadňování koordinovaného zveřejňovaní zranitelností [čl. 7 odst. 2 písm. c) NIS 2]

  b) Určit jeden z týmů CSIRT jakožto koordinátora CVD [čl. 12 odst. 1 NIS 2]

  c) Zajistit, aby fyzické nebo právnické osoby mohly koordinátorovi oznámit zranitelnost na požádání anonymně [čl. 12 odst. 1 NIS 2]

Přístupy jiných států:

- Belgie
  - Přijetí legislativy: vytvoření trestně právního bezpečného přístavu

- Nizozemsko
  - Národní politika CVD akceptovaná státem i veřejností, která vytváří bezpečný přístav

- Francie
  - Procesní ochrana objevitele v zákoně (absence povinnosti nahlásit trestnou činnost)

Klíčová otázka:

Do jaké míry může stát umožnit neřízené testování zranitelností na úkor práva na nerušené užívání majetku (ICT produktu) odpovědné osoby?

Implementace NIS 2 a vymezení role koordinátora

- Povinnost určit jednoho z CSIRT jakožto koordinátora CVD – vládní CERT

- Úloha koordinátora dle NIS 2:

a) identifikace a kontaktování dotčených subjektů (odpovědná organizace, objevitel zranitelností, uživatelé ICR produktu, jiní koordinátoři)
b) pomoc fyzickým nebo právnickým osobám oznamujícím zranitelnost
c) dojednávání lhůt pro zveřejnění a řešení zranitelností, které mají dopad na více organizací

- Možnost koordinace jinou osobou?

Děkuji za pozornost!

Oddělení národních strategií a politik