NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SK CERT

POLITIKA PRE ZODPOVEDNÉ OZNAMOVANIE ZRANITEĽNOSTI

OBSAH

ÚVOD

Bezpečnosť každého systému je definovaná jeho najslabším článkom. Existencia zraniteľností otvára útočníkom cestu na uskutočňovanie svojich cieľov, či už je to kompromitácia systému, prístup k citlivým dátam, osobným údajom a vo veľa prípadoch aj k celkové ovládnutie napadnutého systému.

V kontexte informačnej bezpečnosti sa pod zraniteľnosťou rozumie slabina alebo chyba v softvérovom alebo hardvérovom systéme. Narušenie bezpečnosti zneužitím zraniteľnosti má za následok porušenie jedného či viacerých z troch základných atribútov bezpečnosti: dôvernosť, integrita či dostupnosť.

Keďže vzniku zraniteľností aj pri najlepšej snahe nie je možné úplne predísť, je veľmi dôležité, aby čas medzi vznikom a opravou zraniteľnosti bol čo najkratší. Takisto je rozhodujúce, aby zraniteľnosť našiel prvý niekto, kto si informáciu o nej nenechá pre seba, nezneužije ju alebo ju nepredá. Naopak, zodpovedne ju oznámi výrobcovi alebo prevádzkovateľovi, aby ten mohol ihneď urobiť nápravu.

Táto politika vysvetľuje základné pojmy v súvislosti so zraniteľnosťami a popisuje metodiku ich zodpovedného nahlasovania a riešenia.

ZRANITEĽNOSŤ

Všeobecne je zraniteľnosťou každá okolnosť, ktorá znižuje odolnosť voči hrozbám.

Pojem zraniteľnosť je štandardizovaným pojmom, ukotveným v niekoľkých normách. Na účely tohto návodu sú použiteľné nasledujúce definície pojmu zraniteľnosť:

ISO/IEC 27000:2022

(Information technology - Security techniques - Information security management systems - Overview and vocabulary)
Slabina aktíva alebo opatrenia, ktorá by potenciálne mohla byť zneužitá jednou alebo viacerými hrozbami.

ISO/IEC 29147:2018

(Information technology – Security techniques – Vulnerability Disclosure)
Funkčné správanie sa produktu alebo služby ktoré porušuje implicitnú alebo explicitnú bezpečnostnú politiku.

NIST 800-37 (Risk Management Framework for Information Systems and Organizations)

Slabé miesto v informačnom systéme, postupoch zabezpečenia systému, interných opatreniach alebo v implementácii, ktorú by mohol zneužiť alebo spustiť zdroj hrozby.

Metodika analýzy rizík kybernetickej bezpečnosti (Národný bezpečnostný úrad)

Slabé miesto fyzického, alebo informačného aktíva, slabé miesto v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať, alebo využiť nositeľ hrozieb (resp. hrozba, škodlivá udalosť, scenár rizika)

Definícia v CVE slovníku pojmov

Chyba v softvéri, firmvéri, hardvéri alebo komponente služby vyplývajúca zo slabiny, ktorú možno zneužiť, čo má negatívny vplyv na dôvernosť, integritu alebo dostupnosť ovplyvneného komponentu alebo komponentov.

Definícia v RFC 2828

Chyba alebo slabina v návrhu, implementácii alebo prevádzke a správe systému, ktorá by mohla byť zneužitá na porušenie bezpečnostnej politiky systému

VÝZNAM ZRANITEĽNOSTI

Existencia zraniteľnosti významne vstupuje do analýzy a riadenia rizík. Hrozba je viazaná na existujúcu zraniteľnosť, pričom samotná podstata zraniteľnosti ovplyvňuje pravdepodobnosť, že hrozba nastane a možné negatívne dopady hrozby. Naopak, ak existuje proces na ošetrovanie a riadenie zraniteľností, takéto opatrenie dokáže efektívne znižovať riziko vzniku a uplatnenia hrozby.

VZNIK ZRANITEĽNOSTÍ

Neexistuje dokonalý produkt. Rýchlosť vývoja, tlak na stále nové funkcie, ako aj množstvo výrobkov, procesov a služieb a ich komplexnosť doslova predpokladajú, že v nich bude jedno alebo viac slabých miest, ktoré môže niekto zneužiť. Existuje hneď viacero dôvodov, prečo zraniteľnosti vznikajú a existujú:

Bezpečnosť je častokrát v rozpore s tlakom na nové funkcie aplikácií a služieb a rýchlosťou vývoja a nasadenia. Benefity bezpečného dizajnu a s nimi spojená úspora sa pritom prejavujú až v neskoršej dobe, počas prevádzky. Túto súvislosť však autori aplikácií často podceňujú.

ako tomu predísť: aplikovať princíp „security by design [1] “, ktorý vo výsledku znižuje mieru vzniku a existencie zraniteľností a z dlhodobého hľadiska šetrí prostriedky; zaviesť v organizácii kultúru, ktorá podporuje odhaľovanie zraniteľností a dáva dôraz na kvalitu kódu, nie na rýchlosť dodania,

Vývoj softvéru kombinuje znalosti programovacieho jazyka, knižníc, databáz, komunikačných protokolov (voči iným aplikáciám, databázam, serverom, používateľovi) a súborových formátov. Získať a udržiavať si špičkové znalosti z najnovších bezpečnostných praktík vo všetkých týchto oblastiach je pre programátora extrémne obtiažne. Myslieť na všetky prípady a nedopustiť sa žiadnej chyby, aj keď ich programátor pozná, je prakticky nemožné.

ako tomu predísť: dodržiavať zásady bezpečného vývoja [2] ; vzdelávať programátorov v témach bezpečného vývoja; zaviesť automatizované bezpečnostné testy zdrojového kódu

Aj keby programátor dodržal vo svojom vlastnom kóde všetky mysliteľné bezpečnostné odporúčania a neurobil žiadne chyby, občas je odhalená úplne nová kategória zraniteľností alebo sa zmení vonkajšie prostredie, následkom čoho treba prerobiť produkt, aby sa novej situácii prispôsobila.

ako tomu predísť: tomuto typu zraniteľností sa nedá predísť, je však možné minimalizovať dopady správnou softvérovou architektúrou a tiež kontinuálnym sledovaním trendov a vydávaním bezpečnostných záplat

[1] Spôsob vývoja, ktorý predpokladá bezpečnosť už pri samotnom návrhu, cez vývoj až po finálne nasadenie produktu.

[2] https://www.sk-cert.sk/sk/chcete-sa-vyhnut-zranitelnostiam-vo-vasej-vami-vyvijanej-aplikacii/

Do produktov sú vnášané aj cudzie chyby z použitých externých knižníc a operačného systému. Tie môžu spôsobiť, že v produkte sa vyskytnú zneužiteľné zraniteľnosti aj napriek tomu, že jej autor dodržal všetky bezpečnostné zásady.

ako tomu predísť: venovať náležitú pozornosť výberu knižníc a ich autorov, vyberať knižnice s dobrou reputáciou a správne nastavenými bezpečnostnými procesmi.

Zraniteľnosti v produktoch môžu vzniknúť aj úmyselne. Existuje viacero spôsobov, ako útočník túto zraniteľnosť do produktu dostane. Môže si napríklad „najať" zamestnanca výrobcu (tzv. insidera), kompromitovať vývojárske prostredie alebo v prípade open-source projektov môže vývojárovi navrhnúť do produktu funkciu, ktorá obsahuje zraniteľnosť (pull request). Ďalším spôsobom je prevziať údržbu projektu, o ktorý sa jeho pôvodní autori prestali starať. Niektoré štáty majú dokonca legislatívu alebo procesy, cez ktorú môžu výrobcovi zavedenie skrytých zraniteľností nariadiť.

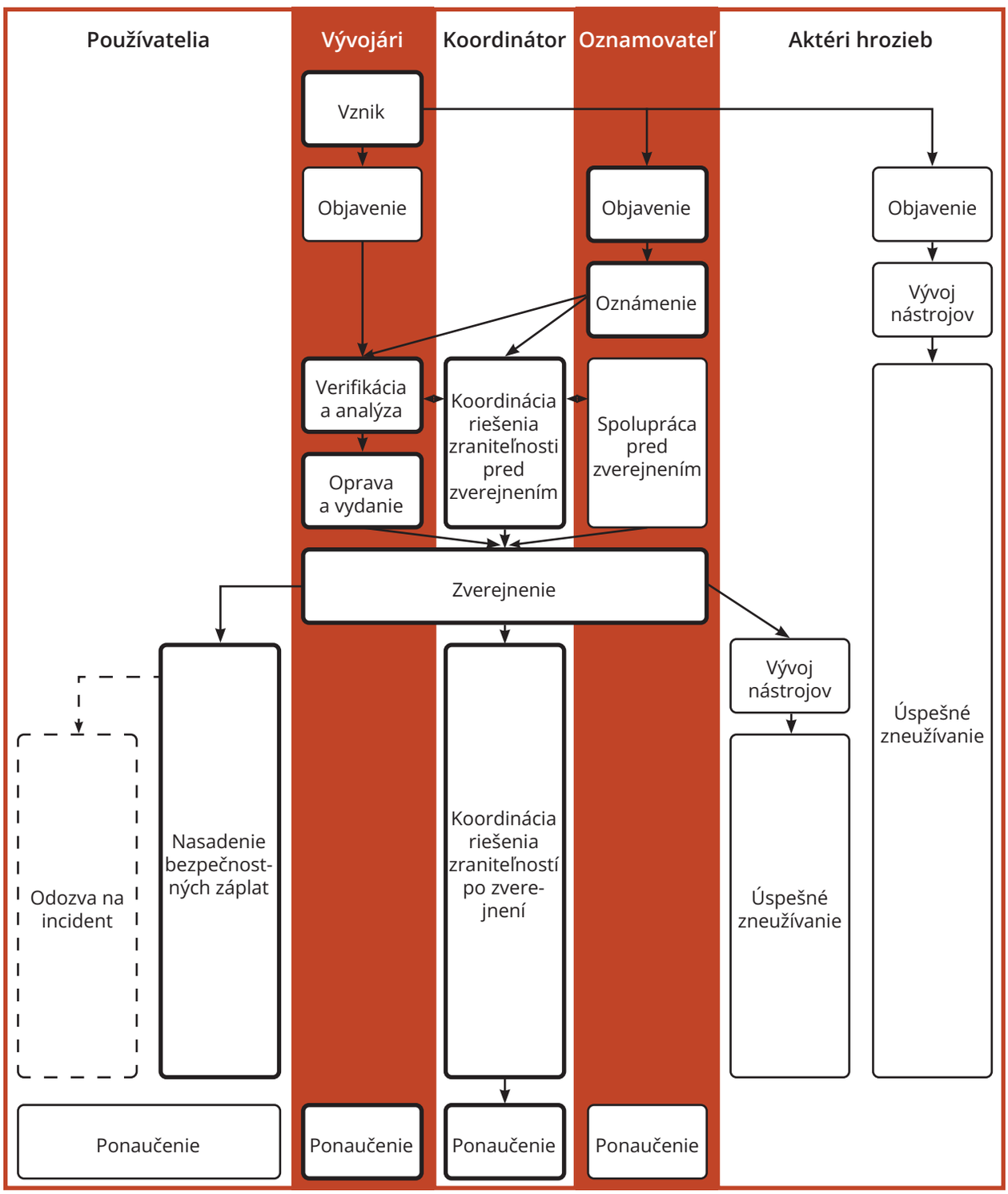
ako tomu predísť - **výrobcovia**

- výrobcovia musia venovať zvýšenú pozornosť bezpečnostnému preverovaniu zamestnancov;
- zaviesť kontrolné procesy (napr. pravidlo štyroch očí);
- zodpovedný výber a kontrola externých knižníc na základe reputácie, autorov, analýzy kódu
- pravidelná kontrola, či sa stav bezpečnosti externých knižníc nezmenil (pokles kvality kódu, zmena vlastníka projektu, publikované zraniteľnosti a podobne)

ako tomu predísť – **zákazníci**

- sledovať bezpečnostné aktuality, týkajúce sa používaného softvéru, jeho zraniteľností a vývoja
- vyhnúť sa softvéru z krajín, ktoré sú známe škodlivými aktivitami v súvislosti so softvérom a hardvérom

ŽIVOTNÝ CYKLUS ZRANITEĽNOSTI



Vznik – zraniteľnosť môže vzniknúť rôznym spôsobom – tak, ako je to popísané v kapitole VZNIK ZRANITEĽNOSTÍ.

Objavenie – od vzniku po objavenie zraniteľnosti môže prejsť veľmi dlhý čas. V najhoršom prípade ju odhalí útočník, vedomosť o zraniteľnosti si nechá pre seba alebo ju predá ďalším záujemcom a útočníci začnú pracovať na vývoji nástrojov. Vedomosť o zraniteľnosti sa k výrobcovi vôbec nemusí dostať, alebo sa o nej dozvie až analýzou niektorého z útokov, pri ktorom bola zraniteľnosť zneužitá.

Zraniteľnosť môže odhaliť aj bezpečnostný výskumník, prevádzkovateľ služby či bežný používateľ. V takom prípade by ju mal oznámiť výrobcovi.

Zraniteľnosť môže odhaliť aj samotný výrobca (vývojár) napr. počas údržby a vylepšovania produktu.

Vývoj nástrojov – ak zraniteľnosť odhalil útočník, typicky miesto nahlásenia začne vyvíjať nástroje, pomocou ktorých je možné zraniteľnosť zneužiť.

Oznámenie – v prípade zodpovedného oznamovania zraniteľností, bezpečnostný výskumník alebo zodpovedný používateľ nahlási organizácii, ktorá koordinuje nahlasovanie zraniteľností (na Slovensku je to Národné centrum kybernetickej bezpečnosti), prípadne výrobcovi alebo prevádzkovateľovi existenciu zraniteľnosti. Hlásenie môže mať rôznu štruktúru a úroveň detailu. Odporúčaný obsah prvotného hlásenia je popísaný v kapitole ZODPOVEDNÉ OZNAMOVANIE ZRANITEĽNOSTÍ. Ak objaví zraniteľnosť samotný výrobca alebo prevádzkovateľ, typicky od objavenia zraniteľnosti prechádza ihneď k verifikácii a analýze.

Koordinácia riešenia zraniteľností – organizácia, ktorá koordinuje riešenie zraniteľnosti, slúži ako mediátor medzi výskumníkom a vývojárom. Dohliada na správnosť celého procesu, udržiava jednotný plán riešenia medzi všetkými zainteresovanými stranami, stará sa o to, aby informácie o zraniteľnosti neboli zverejnené predčasne, ale zároveň aby vývojár venoval zraniteľnosti náležitú pozornosť a alokoval na jej riešenie adekvátne prostriedky. Ak si to výskumník želá, môže koordinátor sprostredkúvať komunikáciu s výrobcom tak, aby identita výskumníka nebola odhalená.

Verifikácia a analýza – po nahlásení zraniteľnosti musí vývojár overiť, či zraniteľnosť naozaj existuje a či sa dá zneužiť spôsobom, akým to popisuje hlásenie, prípadne či má ďalšie dopady ktoré ani nahlasovateľ neidentifikoval. Zároveň prebieha analýza toho, aká je zraniteľnosť závažná, v akých produktoch sa nachádza, koľko používateľov môže zasiahnuť a podobne. Tieto informácie sú dôležité pre prioritizáciu riešenia zraniteľnosti. V tomto pocese môže byť požadovaná súčinnosť nahlasovateľa aj koordinátora.

Oprava a vydanie – aby produkt nemal slabé miesto, je potrebné zraniteľnosť opraviť a sprístupniť túto opravu všetkým používateľom, ktorý používajú zraniteľný produkt. Ak nie je možné opravu vydať alebo oprava bude trvať dlhší čas, výrobca alebo prevádzkovateľ môže vydať usmernenia a odporúčania na mitigáciu zraniteľnosti.

Zverejnenie – zverejnenie informácie o zraniteľnosti, podľa pravidiel zodpovedného oznamovania zraniteľností, by malo prísť až po jej oprave a distribúcii aktualizovaných verzií produktov používateľom. Existujú však výnimky – zraniteľnosť nie je možné opraviť, zraniteľnosť je možné mitigovať iným spôsobom do vydania opravy a podobne. Rozhodnutie o zverejnení zraniteľnosti by však malo byť v ideálnom príprave predmetom trojstrannej dohody výskumníka, vývojára a koordinátora. Ak dohodu nie je možné dosiahnuť, výskumník môže po vyčerpaní všetkých možností v súlade s etickým kódexom informáciu o zraniteľnosti zverejniť aj bez súhlasu vývojára, pri dodržaní všetkých legislatívnych a zmluvných podmienok, ktoré ho môžu viazať. V takomto prípade je potrebné zvoliť takú formu informovania, ktorá v maximálnej miere prispeje k mitigácii zraniteľnosti, ale poskytne čo najmenej informácií užitočných pre zneužitie zraniteľnosti aktérmi hrozieb.

Nasadenie bezpečnostných záplat – je zodpovednosťou používateľov, aby aplikovali bezpečnostné záplaty čo najskôr po ich zverejnení. Niektorí útočníci sa totiž o existencii zraniteľnosti dozvedia až z bezpečnostných aktualizácií produktu. Technickou analýzou aktualizácie môžu identifikovať presné zraniteľné miesto, vyvinúť nástroje a na pôvodnú, neaktualizovanú verziu začať útočiť.

Odozva na incident – hoci nie je priamou súčasťou procesu zodpovedného nahlasovania zraniteľností, používateľ by mal po oprave závažnej zraniteľnosti vykonať kontrolu systému a ak má podozrenie, že zraniteľnosť mohla byť zneužitá, iniciovať process riešenia incidentu. Toto sa obzvlášť týka zraniteľností na verejne prístupných systémoch a zraniteľností, ku ktorým existuje ukážka spôsobu zneužitia (proof-of-concept exploit), alebo je známe že sú verejne zneužívané.

Ponaučenie – výrobca by sa po celom procese mal poučiť z riešenej zraniteľnosti tak, aby už neprichádzalo k vzniku podobných zraniteľností, resp. aby sa minimalizovali možnosti ich vzniku. Takisto by mal na základe procesu riešenia zraniteľnosti prijať adekvátne bezpečnostné opatrenia, vylepšiť svoj proces riadenia zraniteľností alebo vytvoriť/aktualizovať svoju politiku oznamovania zraniteľností, ak je to nutné. Aj ostatní účastníci procesu zodpovedného nahlasovania zraniteľností by mali vykonať ponaučenie, slúžiace na zlepšenie ich procesu.

DATABÁZA A HODNOTENIE ZRANITEĽNOSTÍ

Z dôvodu lepšieho manažmentu a komunikácie o zraniteľnostiach bol vytvorený program CVE (Common Vulnerabilities and Exposures). Tento program zaviedol unifikovaný systém označovania zraniteľností, nazvaný CVE kód (napríklad CVE-2024-3094). Informácie o zraniteľnostiach sú uchovávané v databázach zraniteľností, ktoré sú verejne dostupné. Ich hodnotenie je založené na tzv. CVSS mechanizme.

Common Vulnerabilities and Exposures (CVE)

Ak je zraniteľnosť produktu alebo služby odhalená, v procese oznámenia zodpovednému subjektu (najčastejšie výrobca alebo prevádzkovateľ) je zraniteľnosti pridelený CVE kód – Common Vulnerabilities and Exposures Code. Tento kód môže prideliť niektorý z participujúcich CSIRT tímov, Bug Bounty programov, výrobcov, bezpečnostných výskumníkov alebo organizácia MITRE ako primárna CVE číslovacia autorita. CVE kód slúži na centrálnu evidenciu všetkých známych zraniteľností.

Databázy zraniteľností

Ak je zraniteľnosť produktu alebo služby odhalená, v procese oznámenia zodpovednému subjektu (najčastejšie výrobca alebo prevádzkovateľ) je zraniteľnosti pridelený CVE kód – Common Vulnerabilities and Exposures Code. Tento kód môže prideliť niektorý z participujúcich CSIRT tímov, Bug Bounty programov, výrobcov, bezpečnostných výskumníkov alebo organizácia MITRE ako primárna CVE číslovacia autorita. CVE kód slúži na centrálnu evidenciu všetkých známych zraniteľností.

DATABÁZA CVE (MITRE)

https://cve.org/
Databáza prevádzkovaná organizáciou MITRE, ktorá je aj hlavnou CVE číslovacou autoritou, čo znamená že registruje a vedie databázu CVE čísel. Ide o databázu, z ktorej často čerpajú aj iné databázy zraniteľností, či už neverejné alebo verejné. Nachádzajú sa v nej všetky zraniteľnosti, ktorým bol pridelený alebo rezervovaný kód CVE.

NIST NATIONAL VULNERABILITY DATABASE

https://nvd.nist.gov/
Databáza, ktorá je prevádzkovaná Národným inštitútom pre štandardy a technológie (National Institute of standards and technology – NIST) pod americkým ministerstvom obchodu. Na identifikáciu zraniteľností používa aj CVE kódy, obsahuje však aj zraniteľnosti, ktoré nemajú CVE kód.

Hodnotenie zraniteľností pomocou CVSS

Na hodnotenie zraniteľností sa najčastejšie používa jednotný systém, nazývaný Common Vulnerability Scoring System (CVSS) od organizácie FIRST. Ide o metriku, pomocou ktorej sa identifikuje charakteristika a závažnosť zraniteľností. V čase publikovania tohto dokumentu bola aktuálna verzia CVSS v4.0 a široko používana bola aj predchádzajúca verzia CVSS v3.1.

CVSS v4.0

Štvrtá verzia CVSS má štyri hodnotené skupiny: Základ (Base), Hrozba (Threat), Prostredie (Environmental) a Dodatková (Supplemental). Každá skupina obsahuje sadu parametrov, ktoré opisujú vlastnosti zraniteľnosti:

- Parametre základnej skupiny reflektujú závažnosť zraniteľnosti samotnej, ktoré sa nemenia v čase a popisujú najhorší možný dopad zneužitia, bez ohľadu na špecifiká konkrétnych prostredí, v ktorých sú produkty nasadené.
- Skupina hrozba upravuje základné parametre podľa toho, či je zraniteľnosť aktívne zneužívaná, či existuje návod na zneužitie (proof-of-concept) a podobne. Zvolené hodnoty sú platné univerzálne, ale môžu sa meniť v čase podľa toho, ako sa situácia so zraniteľnosťou vyvíja.
- V skupine prostredie je možné upraviť skóre podľa dopadu na konkrétne prostredie, v ktorom je produkt nasadený. Túto kategóriu parametrov dokáže vyplniť len majiteľ / prevádzkovateľ konkrétnej infraštruktúry, pre ktorú bude výsledné skóre platné.
- Dodatková skupina obsahuje atribúty, ktoré pridávajú kontext, ale nie sú súčasťou samotnej zraniteľnosti.

CVSS v3.1

Vo verzii 3.1, ktorá je len mierne aktualizovanou verziou CVSS 3.0, sú tri hodnotené skupiny: Základná (Base), Časová (Temporal) a Environmentálna (Enviromental):

- Základná skupina predstavuje vnútorné charakteristiky zraniteľnosti, ktoré sú stále z časového hľadiska a naprieč používateľskými prostrediami.
- Časová skupina odráža charakteristiky zraniteľnosti, ktoré sa časom menia,
- Enviromentálna skupina predstavuje charakteristiky, ktoré sú jedinečné pre konkrétne používateľské prostredie.

Pre všetky verzie CVSS (teda aj pre verziu 4.0 a 3.1) platí, že zadané hodnoty sú zapisané pomocou textového reťazca, nazývaného CVSS vektor. Príkladom takéhoto vektoru pre konkrétnu zraniteľnosť môže byť:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Tento vektor obsahuje požitú verziu CVSS a všetky zadané hodnoty.

Závažnosť zraniteľnosti na základe vyplených hodnôt v CVSS vektore je možné vyjadriť jednoduchým číselným skóre od 0 (najnižšia závažnosť) po 10 (najkritickejšia závažnosť).
Metriku CVSS je možné použiť nielen na určenie závažnosti zraniteľnosti, ale aj na prioritizáciu jej riešenia, resp. odstránenia. CVSS metrika rozoznáva štyri kategórie zraniteľností:

SKÓRE	ZÁVAŽNOSŤ
0.1 - 3.9	Nízka (Low)
4.0 - 6.9	Stredná (Medium)
7.0 - 8.9	Vysoká (High)
9.0 - 10.0	Kritická (Critical)

Všetky informácie o CVSS je možné nájsť na odkaze https://www.first.org/cvss/ . Nachádza sa tu aj „kalkulačka“ na vizuálnu tvorbu CVSS vektora a výpočet CVSS skóre pre všetky používané verzie CVSS, ako aj detailný návod a názorné príklady na určovanie CVSS.

ZODPOVEDNÉ OZNAMOVANIE ZRANITEĽNOSTÍ

Aby bolo možné zraniteľnosť odstrániť, musí sa o nej autor softvérového či hardvérového produktu alebo prevádzkovateľ služby dozvedieť. Ak by informácie o zraniteľnosti neboli oznámené autorovi či prevádzkovateľovi služieb, boli by tieto služby vystavené riziku útokov od strán, ktoré o tejto zraniteľnosti vedia. Ak by, naopak, bola informácia o zraniteľnosti verejne publikovaná predtým, než výrobca dostal šancu zraniteľnosť opraviť a záplatu distribuovať používateľom, mohlo by to viesť k panike a masovému zneužívaniu zraniteľnosti útočníkmi. Preto je dôležité, aby všetky strany tohto procesu vedeli, aký je správny postup a tento postup dodržiavali.

Oznamovanie zraniteľností môže mať tri podoby:

Plné oznámenie (Full Disclosure)

ten, kto zraniteľnosť nájde, ihneď verejne oznámi všetky informácie o zraniteľnosti. Takýto postup je v rozpore so zodpovedným postupom oznamovania zraniteľností, pretože ktokoľvek môže zraniteľnosť zneužiť až do doby, pokiaľ nebude z produktu odstránená.

Neoznámenie (Non-disclosure)

ten, kto zraniteľnosť nájde, si informáciu o zraniteľnosti nechá pre seba, resp. neoznámi zraniteľnosť výrobcovi alebo prevádzkovateľovi produktu. Najčastejšie tak robia útočníci alebo kriminálne a APT skupiny, pre ktorých sú takéto zero-day zraniteľnosti [3] veľmi hodnotné. Tento postup je najhorším možným postupom a zneužívanie takýchto zraniteľností alebo ich predaj môže mať trestno-právne dôsledky.

Koordinované oznámenie zraniteľnosti (Coordinated Vulnerability Disclosure)

ten, kto zraniteľnosť nájde, postupuje podľa pravidiel koordinovaného oznamovania zraniteľností. Takéto pravidlá môže mať prijaté a zverejnené samotný výrobca alebo prevádzkovateľ alebo môžu byť prijaté na národnej úrovni. Ide o najzodpovednejší postup oznamovania zraniteľností a národné pravidlá a proces je popísaný v tomto dokumente.

Koordinované oznámenie zraniteľností je najlepším spôsobom, ako zraniteľnosť odstrániť s minimom nežiadúcich dopadov. Zároveň poskytuje oznamovateľovi príležitosť získať uznanie odbornej verejnosti a prípadnú odmenu (Bug Bounty). Koordinátor môže oznamovateľovi v prípade potreby poskytnúť anonymitu, alebo ho previesť všetkými krokmi procesu. Výrobcovi umožňuje včasná informovanosť o zraniteľnosti minimalizovať dopady na používateľov a predchádzať majetkovým a reputačným škodám.

Koordinované oznamovanie zraniteľností je neustály proces, nie jednorázová aktivita pri konkrétnej zraniteľnosti. Musí byť uplatniteľný na každú situáciu a každé oznámenie zraniteľnosti, pričom jeho kroky musia viesť k oprave uvedenej zraniteľnosti a zverejneniu informácií o zraniteľnosti tak, aby používatelia produktu mali okamžitú možnosť nasadiť opravu na svojom produkte, resp. aby služba, ktorú používajú, oznámenú zraniteľnosť už neobsahovala.

[3] Zraniteľnosť, ktorá doposiaľ nebola oficiálne odhalená, opravená a publikovaná.

Prečo oznamovať zraniteľnosti?

Koordinované oznamovanie zraniteľností má hneď niekoľko benefitov a to nie len pre postihnutého výrobcu/prevádzkovateľa, ale aj pre samotného oznamovateľa.

Benefity pre oznamovateľa

- oznámením podľa pravidiel môže zabrániť zneužitiu zraniteľnosti nebezpečným útočníkom
- pomôže postihnutému subjektu a zároveň aj používateľom zraniteľného systému alebo služby
- trénuje svoje schopnosti v oblasti kybernetickej bezpečnosti

Benefity pre postihnutého výrobcu/prevádzkovateľa

- dozvie sa o probléme, na ktorý môže ihneď reagovať a tak zabrániť škodlivým účinkom
- dodržiavaním pravidiel zlepšuje svoje produkty a služby, ktoré ponúka svojim zákazníkom
- buduje si dobré meno v bezpečnostnej komunite

Vo všeobecnosti má koordinované oznamovanie zraniteľností hneď niekoľko výhod:

Znižovanie škôd – aj napriek tomu, že zraniteľnosti môžu byť vyriešené, ich vznik, existencia a dopady nemôžu byť úplne eliminované. Neustále vznikajú nové zraniteľnosti a existujú aj také zraniteľnosti, ktoré zatiaľ nikto neobjavil, resp. neoznámil výrobcovi/prevádzkovateľovi (tzv. zraniteľnosť nulového dňa, angl. zero day vulnerability). Práve koordinované oznamovanie zraniteľností prispieva k znižovaniu potenciálnych, ale aj skutočných škôd tým, že o zraniteľnosti sa dozvie subjekt, ktorý s tým môže aj niečo urobiť – či už je to výrobca, prevádzkovateľ alebo koordinačná autorita na oznamovanie zraniteľností.

Minimum neočakávaných situácií – koordinované oznamovanie zraniteľností je jasný proces, v ktorom si je každý, kto do neho vstupuje, vedomý svojich práv a povinností. Čím lepšie je tento proces popísaný a čím zodpovednejšie k nemu jednotlivé subjekty pristupujú, tým menej neočakávaných situácií a negatívnych dopadov vo výsledku vznikne.

Posilňovanie dôvery – bezpečnostná komunita je založená na dôvere. Zdieľanie informácií a výmena skúseností nemôže existovať, ak jednotliví účastníci nemajú k sebe dostatočnú úctu a nie je medzi nimi adekvátna dôvera. Koordinované oznamovanie zraniteľností, keď oznamovateľ informuje relevantné subjekty o existencii zraniteľnosti a tie k takémuto oznámeniu pristúpia seriózne a vykonajú nápravu len posilňuje vzťahy v rámci bezpečnostnej komunity a vytvára prepojenie medzi jednotlivými výrobcami, prevádzkovateľmi, kyberautoritami a bezpečnostnými výskumníkmi.

Podpora výskumníkov – zodpovedným prístupom k oznamovaniu zraniteľností výrobcovia, prevádzkovatelia a kyberautority posilňujú podporu kyberbezpečnostných výskumníkov a etických hackerov, čo zároveň zvyšuje úsilie týchto profesionálov v hľadaní a oznamovaní ďalších zraniteľností.

Roly pri koordinovanom oznamovaní zraniteľností

V procese koordinovaného oznamovania zraniteľností sú definované nasledujúce role:

Oznamovateľ – osoba, ktorá oznámi zraniteľnosť. Môže to byť bezpečnostný výskumník, etický hacker, špecialista na kybernetickú bezpečnosť alebo aj bežný používateľ.

Vývojár – subjekt zodpovedný za vývoj, výrobu a udržiavanie produktu, ktorý obsahuje zraniteľnosť.

Prevádzkovateľ alebo používateľ – prevádzkuje, spravuje či používa produkt, ktorý obsahuje zraniteľnosť.

Koordinátor – subjekt, ktorý koordinuje oznamovanie zraniteľností, komunikáciu medzi oznamovateľom a výrobcom či prevádzkovateľom a vydáva usmernenia a návody na koordinované oznamovanie zraniteľností.
V Slovenskej republike je národným koordinátorom **Národné centrum kybernetickej bezpečnosti**.

Spôsoby objavenia zraniteľnosti

Zraniteľnosti môžu byť objavené rôznymi spôsobmi. Záleží nielen na vlastnostiach samotnej zraniteľnosti, ale aj na schopnostiach toho, kto ju odhalí, resp. sa s ňou stretne. Bez ohľadu na to, ako je zraniteľnosť objavená, musia byť dodržané pravidlá koordinovaného oznamovania zraniteľností. Vo všeobecnosti rozoznávame dva spôsoby objavenia zraniteľnosti:

Náhodné

zraniteľnosť je objavená náhodne pri bežnej používateľskej činnosti. Často takúto zraniteľnosť objaví bežný používateľ. Hrozí riziko, že takto odhalená zraniteľnosť bude ignorovaná alebo nebude považovaná za problém, nakoľko bežný používateľ nemá dostatočné povedomie o zraniteľnostiach a ich dopadoch.

Cielené

zraniteľnosť je objavená aktívnou činnosťou, ktorej zámerom je zraniteľnosť nájsť. Cielené hľadanie môže mať viacero motivácií:

Pomoc zasiahnutému subjektu

zraniteľnosti sú vyhľadávané za účelom pomoci zasiahnutému subjektu lepšie si zabezpečiť svoje produkty. Zvyčajne takúto činnosť vykonávajú etickí hackeri a výskumníci, aj v rámci rôznych bug bounty programov.

Komerčná činnosť

aktivita na základe zmluvy medzi subjektom a etickým hackerom, ktorý v určitom rozsahu vyhľadáva zraniteľnosti v produktoch subjektu. Najčastejšie sa takejto činnosti hovorí penetračné testovanie.

Aktivizmus

ten, kto zraniteľnosti vyhľadáva, sa snaží poukazovať na slabo zabezpečené produkty, najmä tých, ktoré vlastní štát alebo ktoré slúžia verejnému záujmu.

Škodlivé aktivity

zraniteľnosti vyhľadávajú aj útočníci, ktorí ich následne zneužívajú na útoky voči zraniteľným produktom. Výrobca alebo zasiahnutý subjekt pritom nemajú spravidla o existencii zraniteľnosti žiadnu vedomosť.

Motivácie oznamovania zraniteľností

Každý oznamovateľ má vlastnú motiváciu, prečo zraniteľnosť oznamuje. Možno ich rozdeliť na niekoľko typov, no môžu byť aj navzájom previazané:

Bezpečnosť

oznamovateľ má záujem o to, aby produkty boli bezpečné pre ich používateľov.

Vyššie dobro

Niektorí oznamovatelia sa môžu zamerať iba na zraniteľnosti v aplikáciách s celospoločenským dopadom. Často sa stáva, že pri tomto druhu motivácie oznamovateľ nedodrží všetky pravidlá koordinovaného oznamovania zraniteľností a informácie o zraniteľnosti zverejňuje takmer okamžite, bez upozornenia zasiahnutého subjektu alebo koordinátora.

Prestíž

oznamovateľ vidí za hľadaním zraniteľností možnosť uznania jeho práce a rozpoznanie v bezpečnostnej komunite.

Zisk

oznamovateľ si chce prostredníctvom hľadania zraniteľností zarobiť, napríklad cez bug bounty programy.

PRAVIDLÁ KOORDINOVANÉHO OZNAMOVANIA ZRANITEĽNOSTÍ

Každá rola v rámci koordinovaného oznamovania zraniteľností by mala dodržiavať pravidlá, ktoré zabezpečia jednotný, koordinovaný a efektívny proces oznámenia a riešenia zraniteľnosti.

Pravidlá pre oznamovateľa

Každý oznamovateľ dodržiava nasledujúce pravidlá:

- Pri každom objavení zraniteľnosti, ako aj pri ich aktívnom vyhľadávaní, postupuje primerane tak, aby neboli prekročené hranice preukázania zraniteľnosti,
- Vždy koná v dobrej viere bez úmyslu poškodiť subjekt, kde zraniteľnosť objavil,
- Po objavení zraniteľnosti bezodkladne informuje
  - Národné centrum kybernetickej bezpečnosti
  - výrobcu alebo prevádzkovateľa zasiahnutého produktu o existujúcej zraniteľnosti, aby bolo minimalizované riziko zneužitia zraniteľnosti útočníkmi,
- Ak má oznamovateľ pochybnosti o tom, že výrobca alebo prevádzkovateľ pristupujú k riešeniu zraniteľností podľa pravidiel koordinovaného oznamovania zraniteľností, nemusí zraniteľnosť sám oznámiť aj výrobcovi. V takom prípade kontakt sprostredkuje Národné centrum kybernetickej bezpečnosti, ktoré zaistí anonymizáciu oznamovateľa zraniteľnosti.
- Oznamovateľ môže v tomto procese využívať služby Národného centra kybernetickej bezpečnosti, napríklad komunikáciu s výrobcom, podporu pri klasifikácii a nezávislom overení zraniteľnosti a podobne. Všetky zodpovednosti a služby NCKB sú popísané v samostatnej kapitole Národná autorita.
- Pri oznámení zraniteľnosti nahlasovateľ uvedie čo možno najväčšiu mieru detailu o nájdenej zraniteľnosti s nevyhnutnou mierou dôkazov. Minimálne by však oznámenie malo obsahovať:
  - na akom produkte sa zraniteľnosť nachádza,
  - akým spôsobom sa oznamovateľ o zraniteľnosti dozvedel,
  - kedy sa o zraniteľnosti dozvedel,
  - na akej verzii produktu sa zraniteľnosť nachádza, prípadne aká konfigurácia produktu je zraniteľná,
  - hodnotenie zraniteľnosti (pomocou CVSS),
  - čo najdetailnejší popis zraniteľnosti,
  - spôsob, akým sa dá zraniteľnosť zneužiť (proof-of-concept),
  - informácie o identifikácii oznamovateľa, ktoré súvisia s preverením existencie zraniteľnosti (napríklad IP adresa a časy, kedy a odkiaľ zraniteľnosť preveroval),
  - čo môže zraniteľnosť spôsobiť,
  - či už zraniteľnosť nahlásil výrobcovi produktu,
  - či už požiadal o pridelenie CVE čísla (Národné centrum kybernetickej bezpečnosti SK-CERT je CVE číslovacia autorita a môže požiadať o priradenie CVE),
  - kontaktné informácie vrátane možností bezpečnej komunikácie (PGP fingerprint a pod.),
  - iné dôležité informácie, súvisiace s objavenou zraniteľnosťou.
- Oznamovateľ môže určiť postihnutému subjektu lehotu na odstránenie zraniteľnosti, počas ktorej zraniteľnosť neoznámi verejne. Ak subjekt nereaguje na oznámenie a lehota uplynie, oznamovateľ môže zraniteľnosť oznámiť verejne. Táto lehota nemôže byť bezdôvodne krátka. Typická lehota môže byť napríklad 30 až 90 dní podľa povahy zraniteľnosti. Ak oznamovateľ nedokáže určiť lehotu pre postihnutý subjekt, môže sa poradiť s Národným centrom kybernetickej bezpečnosti SK-CERT.
- Dobrým zvykom je k oznámeniu zraniteľnosti pridať aj spôsoby riešenia (opravy) alebo mitigácie zraniteľnosti.
- Oznamovateľ aktívne a profesionálne komunikuje so zasiahnutým subjektom, ako aj s Národným centrom kybernetickej bezpečnosti SK-CERT počas celého procesu.
- Ak má zasiahnutý subjekt vydanú politiku koordinovaného oznamovania zraniteľností, oznamovateľ sa musí riadiť aj takouto politikou.

Oznamovateľ sa vyhýba nasledujúcim aktivitám:

- Inštalácii škodlivého kódu v zraniteľnom produkte,
- Kopírovaniu, zmene alebo mazaniu dát, neoprávnenému nakladaniu s nimi a postupovaniu tretím stranám. Ak je potrebné manipulovať s dátami pre preukázanie funkčnosti zraniteľnosti, oznamovateľ by sa mal pokúsiť pristupovať k údajom, na ktoré má právo (napríklad vlastné osobné údaje alebo údaje zo svojho vlastného konta). Všetky získané dáta musí zabezpečiť proti zneužitiu a po ukončení procesu koordinovaného oznamovania zraniteľností ich musí hodnoverne odstrániť. V každom prípade je nutné, aby oznamovateľ zvážil, či sa existencia a funkcionalita zraniteľnosti nedá preukázať iným spôsobom alebo či jej preukázanie neprenechá zasiahnutému subjektu.
- Robiť v produkte zmeny, ak tieto zmeny nevyhnutne nesúvisia s preukázaním zraniteľnosti a to len ak je to nevyhnutné na dokázanie existencie či funkčnosti zraniteľnosti. Oznamovateľ musí zároveň bezodkladne po zadokumentovaní vrátiť všetko do pôvodného stavu.
- Opakovane sa prihlasovať do produktu alebo zdieľať možnosť prihlásenia s tretími stranami.
- Využívať iné spôsoby na hlbší prienik do produktu, pristupovať k iným častiam produktu mimo rozsah samotnej zraniteľnosti, pokúšať sa pristupovať do iných produktov mimo zraniteľného produktu.
- Po objavení zraniteľnosti predať alebo odovzdať informácie o nej tretej strane alebo tieto informácie zverejniť.
- Za oznámenie zraniteľnosti zasiahnutému subjektu vyžadovať finančnú odmenu, pokiaľ pravidlá zasiahnutého subjektu explicitne neuvádzajú takúto možnosť.

Niektoré z týchto aktivít by mohli byť neskôr vyhodnotené ako trestný čin alebo priestupok. Ochrana oznamovateľa zo strany Národného centra kybernetickej bezpečnosti SK-CERT nie je spôsobom, ako sa zbaviť zodpovednosti za spáchanie trestného činu alebo priestupku. Podstatu zodpovedného oznamovania a pomyselných hraníc je možné ľahko pochopiť na nasledovnom príklade z reálneho života: ak si na ulici všimnete auto s otvoreným batožinovým priestorom, typicky zaklopete na dvere najbližšieho domu a zraniteľnosť nahlásite. Neštudujete hlbšie obsah auta, nevstupujete doň a neberiete do rúk predmety v ňom obsiahnuté. Ak by vám majiteľ vozidla neveril, má možno zmysel ponúknuť mu malý dôkaz, nie však vyložiť obsah celého vozidla na ulicu.

Etický kódex etického hackera a výskumníka

Pri aktivitách, spojených s vyhľadávaním a dokumentovaním zraniteľností, ale aj iných aktivitách spojených s kybernetickou bezpečnosťou, musia mať etickí hackeri a výskumníci vždy na zreteli bezpečnosť a blaho spoločnosti, vyššie dobro a zodpovednosť voči profesii. Z toho dôvodu dodržiavajú nasledujúce zásady:

1. Pri výkone svojich kompetencií dbajú v prvom rade na ochranu spoločnosti a vyššieho dobra tak, aby neprišlo k poškodeniu práv a oprávnených záujmov jednotlivcov, organizácií a spoločnosti. Predchádzajú ohrozeniu bezpečnosti, reputácie alebo vzniku ekonomických škôd.
2. Svoju činnosť vykonávajú s ohľadom na ochranu informácií a aktív pred ich zneužitím, zmenou, krádežou alebo zničením.
3. Svoje odborné zručnosti, vedomosti a skúsenosti používajú legálne a čestne tak, aby bol účel ich činnosti splnený bez škodlivých účinkov. Svoje odborné zručnosti, vedomosti a skúsenosti nezneužívajú na vlastné obohatenie nelegálnym, nečestným alebo neetickým spôsobom.
4. Správajú sa zodpovedne. Poznatky, ktoré získajú svojou činnosťou, týkajúce sa zákazníka, inej organizácie alebo kolegu, neodovzdávajú tretím stranám, verejne neprezentujú alebo nezneužívajú vo svoj prospech.
5. Ak objavia alebo sa dozvedia o informácii, ktorá môže znamenať, že bol spáchaný trestný čin, priestupok alebo iné protiprávne konanie, ihneď to oznámia príslušným verejným autoritám.
6. Pri svojej činnosti nepoužívajú softvér, ktorý bol získaný ilegálnou alebo neetickou cestou.
7. Pri svojej činnosti konajú v najlepšom záujme druhej strany, nepovyšujú svoje záujmy nad činnosť, ktorú vykonávajú.
8. Svoju činnosť vykonávajú riadne a svedomito.
9. S kolegami, zákazníkmi, zástupcami organizácií, verejnými autoritami a konkurenciou komunikujú s profesionálnou úctou a rešpektom.
10. Zdržiavajú sa dehonestovania, povyšovania sa, posmeškom a nenáležitému komentovaniu práce iných etických hackerov a výskumníkov, ako aj iných osôb, ktoré pracujú v oblasti kybernetickej bezpečnosti.
11. Napomáhajú rozvoju profesie.

Pravidlá pre zasiahnutý subjekt

(výrobca, vlastník, prevádzkovateľ zraniteľného systému)

Každý subjekt, ktorý zodpovedne pristupuje k oznamovaniu zraniteľností, dodržiava nasledujúce pravidlá:

- Má implementovanú politiku na oznamovanie zraniteľností pre oznamovateľov. Návod, ako túto politiku vytvoriť a implementovať, je uvedený v samostatnej kapitole „Politika na oznamovanie zraniteľností - organizácia“.
- Má politiku na oznamovanie zraniteľností zverejnenú na svojej webovej stránke tak, aby bola jednoducho prístupná. Politika by mala byť dostupná ako v jazykoch používateľov, tak aj v angličtine.
- Má implementovaný aj internetový štandard RFC 9116, ktorý opisuje ako potrebné informácie publikovať v jednoduchom, strojovo spracovateľnom formáte v súbore security.txt.
- Má implementovaný vnútorný proces / štandard na manažment zraniteľností, ktorý zahŕňa aj proces riešenia nahlásených zraniteľností.
- Na každé oznámenie reaguje bezodkladne a adekvátne k povahe oznámenej zraniteľnosti.
- Rieši zraniteľnosti s vysokou prioritou a ak je to technicky a procesne možné, jej oprava je zaradená do najbližšej aktualizácie, prípadne zasiahnutý subjekt vydá mimoriadnu aktualizáciu na opravu zraniteľnosti mimo bežného aktualizačného okna (to platí najmä pre kritické zraniteľnosti).
- Riešenie musí zahŕňať aj identifikáciu potenciálne zasiahnutých obetí a spôsob ich vyrozumenia.
- Prioritne informuje svojich zákazníkov a používateľov na existenciu zraniteľnosti a možnosti, aké majú pri jej mitigácii.
- V spolupráci s koordinátorom a oznamovateľom určí dátum verejného oznámenia zraniteľnosti. Proaktívne oznamovanie zraniteľností v produktoch a službách chráni používateľov týchto produktov a ak je správne podchytené, zvyšuje kredibilitu výrobcu.
- Spoločnosť môže oznamovateľa za oznámenie zraniteľnosti odmeniť. Takisto môže „vypísať odmenu“ za nachádzanie zraniteľností vo svojich produktoch (tzv. bug bounty program). Tento postup odporúčame, nakoľko vedie k zvýšeniu bezpečnosti produktov a služieb spoločnosti. Bug bounty programy slúžia ako motivácia oznamovania zraniteľností v produktoch a procesoch spoločnosti. Návod, ako vytvoriť bug bounty program nájdete nižšie.
- Oznámenie zraniteľnosti treba vnímať ako príležitosť na zlepšovanie produktov a šancu dozvedieť sa o zraniteľnosti skôr, než jej zneužitie spôsobí škody používateľovi, prevádzkovateľovi alebo výrobcovi produktu alebo služby. Preto odporúčame pristupovať k oznamovateľovi s vďakou ako k osobe, ktorá vám chce pomôcť - ako k priateľskému spolupracovníkovi. To, samozrejme, nevylučuje právne kroky v prípade, ak je postup oznamovateľa zjavne neetický či v rozpore so zákonom.

Politika na oznamovanie zraniteľností – organizácia

Vznik alebo existencia zraniteľností dnes už nie je obmedzená iba na organizácie, ktoré vyrábajú softvér, hardvér alebo poskytujú služby. Týka sa aj organizácií, ktoré takýto softvér alebo hardvér prevádzkujú či majú predplatenú službu. Preto každá organizácia, bez ohľadu na svoju činnosť alebo veľkosť, by mala mať zverejnenú politiku na oznamovanie zraniteľností. Tá by mala obsahovať minimálne:

Vyhlásenie o ochote prijímať hlásenia o zraniteľnostiach - transparentné potvrdenie záujmu organizácie dozvedieť sa o zraniteľnostiach v jej systémoch a službách od zodpovedných nahlasovateľov. V tejto časti by sa mala organizácia takisto zaviazať k tomu, že ak bude oznamovateľ postupovať v súlade s nastavenými pravidlami, nehrozí mu žiadna sankcia alebo postih, prípadne legálne následky zo strany organizácie.

Rozsah politiky na oznamovanie zraniteľností - čo najlepšie vymedzený rozsah systémov a služieb, na ktorý je politika aplikovateľná. Samotný rozsah si určuje organizácia, odporúčame však zvoliť čo najširší rozsah systémov a služieb, na ktoré sa politika vzťahuje (odporúčame mať politikou pokryté najmenej všetky systémy a služby, ktoré sú dostupné z internetu, v prípade výrobcu všetky produkty, ktoré je možné verejne používať).

Odkaz na národnú CVD politiku - najmä na pravidlá pre oznamovateľa. Organizácia by mala verejne akceptovať existenciu národnej CVD politiky a riadiť sa ňou.

Špecifické pravidlá oznamovania zraniteľností - ak sa líšia od pravidiel zadefinovaných v národnej CVD politike. Tieto by ale nemali byť diametrálne odlišné od národných pravidiel, aby nedochádzalo k dvojkoľajnosti a nejasnosti pri výklade jednotlivých pravidiel. Špecifickým pravidlom môže byť napríklad určenie časového obdobia, počas ktorého by nemal oznamovateľ zverejniť informácie o zraniteľnosti alebo pravidlá pri určovaní proporcionality a nevyhnutnosti aktivít spojených s detekciou zraniteľnosti.

Spôsob hlásenia - akým spôsobom môže oznamovateľ nájdenú zraniteľnosť nahlásiť (e-mail, reportovací formulár na webe a pod.)

Obsah hlásenia - aké informácie o nájdenej zraniteľnosti organizácia vyžaduje.

Možnosti komunikácie - akým spôsobom môže oznamovateľ komunikovať s organizáciou, vrátane možností zabezpečenej komunikácie.

Dôvernosť a spracovanie osobných údajov - organizácia by si mala určiť ako by mal oznamovateľ nakladať so získanými informáciami, špeciálne s osobnými údajmi, ak sa takéto spracovanie líši od pravidiel v národnej CVD politike.

Možnosti a spôsob odmeny pre oznamovateľa - ak má organizácia vytvorený program na odmeňovania.

Proces riešenia oznámenej zraniteľnosti - organizácia by mala mať transparentne zverejnený proces, čo sa s informáciami o zraniteľnosti deje po jej ohlásení.

Každá organizácia by následne mala mať implementovaný proces riadenia zraniteľností, ktorý musí obsahovať aj postupy a procedúry, ako riešiť oznámené zraniteľnosti. Tento proces by mal zahŕňať minimálne:

- Spôsob, akým sa oznámené zraniteľnosti evidujú a prideľujú na riešenie
- Spôsob verifikácie oznámenej zraniteľnosti (či sa jedná o zraniteľnosť, či organizácia už rovnaké hlásenie neeviduje a pod.)
- Spôsob hodnotenia oznámenej zraniteľnosti (preferovane pomocou CVSS)
- Pravidlá prioritizácie riešenia oznámených zraniteľností
- Postup riešenia uvedenej zraniteľnosti
- Postup testovania novej verzie zraniteľného produktu
- Postup zverejnenia novej verzie produktu
- Spôsob informovania zákazníkov a používateľov o povahe zraniteľnosti a ako sa ich táto zraniteľnosť mohla dotknúť
- Spôsob informovania zákazníkov a verejnosti o oprave zraniteľnosti
- Spôsob komunikácie s autoritou kybernetickej bezpečnosti o oznámenej zraniteľnosti

Tvorba politík na oznamovanie zraniteľností, ako aj tvorba procesov riadenia zraniteľností je upravená štandardami (napr. ISO/IEC 29147:2018), preto odporúčame každej organizácii implementovať takéto štandardy pre efektívne riadenie zraniteľností a ich oznamovanie.

Tvorba bug bounty programu

Bug bounty program je aktivita organizácie na odmeňovanie za zodpovedné oznámenie zraniteľností. Odmeňovanie motivuje tých, ktorí zraniteľnosť objavili, aby ju nahlásili organizácii. To umožňuje organizácii, aby sa o zraniteľnostiach dozvedela a mala ich šancu včas opraviť a znižuje počet zero-day zraniteľností, ktoré by mohli zneužiť útočníci. Bug bounty program takisto zvyšuje reputáciu organizácie a dobré meno v bezpečnostnej komunite. Ak má organizácia záujem vytvoriť a udržiavať bug bounty program, odporúčame nasledovné:

- Vyčleňte dostatočné financovanie a personálne kapacity na prevádzku bug bounty programu.
- Zainteresujte do bug bounty programu viaceré organizačné zložky, napríklad marketing, IT, právne a iné, ktoré môžu pomôcť vybudovať a udržiavať efektívny bug bounty program.
- Určite si rozsah bug bounty programu, teda pri akých produktoch platí odmeňovanie pri nájdení zraniteľnosti:
  - limitovaný rozsah – môžete limitovať odmeňovanie len na určité produkty alebo len v určitom časovom rámci
  - široký rozsah – zahŕňa viac produktov, nie však všetky produkty organizácie
  - otvorený rozsah – odmeňovanie je aplikované na všetky produkty organizácie
- Určite si „cenu“ zraniteľností podľa ich závažnosti. Vo všeobecnosti platí, že čím viac kritická zraniteľnosť, tým je odmena vyššia/hodnotnejšia.
- Odmena musí mať pre potenciálnych nahlasovateľov reálnu hodnotu. Rozhodnite sa, aké formy odmeňovania budete oznamovateľom udeľovať:
  - finančné – priama finančná odmena
  - nefinančné – vecné odmeny (tričká, medaile, coiny, certifikáty, techniku, zariadenia a pod.)
  - neštandardné – NFT tokeny, kryptomeny, akcie organizácie a pod.
- Úspešným oznamovateľom dajte kredit aj tým, že pri zverejnení informácií o zraniteľnosti uvediete meno, kto zraniteľnosť našiel (ak s tým dotyčný oznamovateľ bude súhlasiť).
- Dobrou praxou je vytvorenie dedikovaného testovacieho prostredia práve na účely hľadania a testovania zraniteľností, ktoré je prístupné výskumníkom a etickým hackerom. Tým sa organizácia môže vyhnúť prípadným škodám, ktoré by z nájdenia zraniteľnosti mohli vzniknúť.
- V rámci bug bounty programu môže organizácia organizovať tzv. hackatony, komunitné, časovo obmedzené stretnutia výskumníkov a etických hackerov, kde sa v testovacom prostredí snažia nájsť zraniteľnosti.
- Pred oficiálnym spustením bug bounty programu otestujte súvisiace procesy aj samotné hľadanie zraniteľností s malou skupinou etických hackerov, výskumníkov alebo vlastného personálu. Vyhnete sa tým prekvapeniam a možným problémom, ktoré by ste bez testovania neodhalili včas.
- Zahrňte informáciu o bug bounty programe do vašej politiky na oznamovanie zraniteľností a aj do celého procesu riadenia zraniteľností. Odporúčame, aby organizácia najprv vytvorila a zverejnila politiku na oznamovanie zraniteľností a následne spustila bug bounty program.
- Propagujte svoj bug bounty program nie len v bezpečnostnej komunite, ale aj v rámci širokej verejnosti – nikdy neviete, kto má spôsobilosti a motiváciu hľadať a oznamovať zraniteľnosti.
- Priebežne komunikujte výsledky bug bounty programu nie len vo vnútri organizácie, ale aj verejne.
- Merajte účinnosť bug bounty programu, aby ste mali istotu, že takýto program je pre vašu organizáciu efektívny a prínosný.

Úloha národnej autority

Národnou autoritou pre tvorbu politiky zodpovedného oznamovania zraniteľností a koordináciu oznamovania zraniteľností je Národný bezpečnostný úrad, konkrétne Národné centrum kybernetickej bezpečnosti. Jeho úlohou je:

- vydávať a udržiavať štandardy a odporúčania pre zodpovedné oznamovanie zraniteľností,
- vytvoriť a udržiavať technickú platformu na nahlasovanie zraniteľností na národnej úrovni,
- prijímať oznámenia o zraniteľnostiach a koordinovať postup s postihnutým subjektom a oznamovateľom,
- poskytovať metodickú pomoc pri riešení zraniteľnosti postihnutému subjektu,
- zabezpečiť pre zraniteľnosť pridelenie CVE čísla,
- v prípade potreby a v súlade s platnými právnymi predpismi zabezpečiť anonymitu oznamovateľa z dôvodu ochrany pred neoprávneným postihom alebo pred zastrašovaním zo strany výrobcu či prevádzkovateľa zraniteľného produktu alebo služby,
- podporovať oznamovanie zraniteľností budovaním bezpečnostného povedomia a motiváciou spoločností, bezpečnostných výskumníkov a iných subjektov,
- pri nahlásení zraniteľnosti, ktorá sa priamo týka národnej autority, postupovať v súlade s odporúčaniami pre postihnutý subjekt,
- V prípade, ak postihnutý subjekt nereaguje, nekomunikuje alebo odmieta spolupracovať, využiť všetky zákonné možnosti na dosiahnutie cieľa zodpovedného oznamovania zraniteľností.

NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

SK NBÚ CERT

Budatínska 30
851 06 Bratislava

e-mail:
sk-cert@nbu.gov.sk

hlásenie incidentov a zraniteľností:
incident@nbu.gov.sk

Telefón:
+421 2 68 69 2915