# Zabezpečenie základov softvérového vývoja

Veríme, že v súvislosti s dramatickým nárastom štátom sponzorovaných kybernetických útokov a škodlivých aktérov môžu byť naše služby užitočné, len ak sú bezpečné. V Googli sa viac než kedykoľvek predtým sústreďujeme na ochranu ľudí, organizácií a vlád tým, že zdieľame svoje odborné poznatky, umožňujeme spoločnosti riešiť neustále sa vyvíjajúce riziká a postupne pracujeme na pokroku v oblasti kybernetickej bezpečnosti s cieľom vybudovať bezpečnejší svet pre všetkých.

Základom moderného internetu sú open source softvéry, teda softvéry s kódom, ktorý je otvorene dostupný pre všetkých. Dá sa používať, upravovať a rozvíjať. Open source vývoj softvérov umožňuje spoluprácu a rýchlejší rozvoj vďaka otvorenému zdieľaniu riešení. Táto otvorenosť, ktorá sprístupňuje online svet pre všetkých, však zároveň spôsobuje výnimočnú zraniteľnosť voči bezpečnostným hrozbám.

## Výzva

### Open source softvéry sú problematické pre všetkých

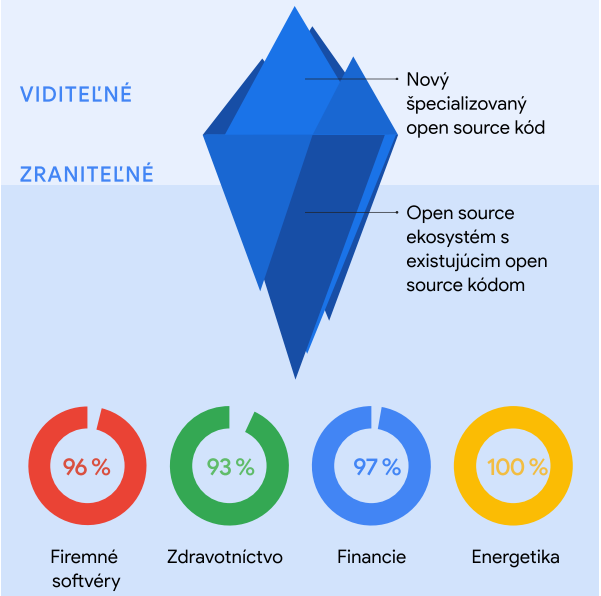
Komunita vývojárov open source softvérov je postavená na transparentnosti a zdieľaní a zároveň prispieva obrovským množstvom kódu do väčšiny aplikácií, ktoré dnes používame.Open source softvéry využívame každodenne v rôznych nástrojoch, od zdravotníckych zariadení až po distribučnú sieť elektriny, preto sa open source projekty stávajú hlavnými cieľmi kybernetických útokov. Za posledné tri roky sme zaznamenali medziročný nárast o 742 %[1] útokov na softvéry dodávateľských reťazcov.

Ekosystém open source softvérov je zložito vrstvený a bezpečnostné chyby sa môžu ukrývať v nepriamych súvislostiach. Práve pre zložité vrstvenie je omnoho náročnejšie manuálne identifikovať potenciálne bezpečnostné hrozby a zabezpečenie tejto časti vývoja softvéru sa stalo celosvetovo naliehavým bezpečnostným problémom.

**Týmto oblastiam je nevyhnutné venovať ďalšiu pozornosť:**

- Vývojári open source softvérov potrebujú poznatky a zdroje na zabezpečenie svojich projektov
- Organizácie musia pochopiť riziká a zraniteľnosti dodávateľského reťazca a na ich základe vypracovať plány na zmiernenie
- Vlády a odvetvie musia spoločne zabezpečiť rozsiahle a efektívne bezpečnostné štandardy[3]

PODIEL OPEN SOURCE SOFTVÉROV V PRÍSLUŠNOM ODVETVÍ[2]




[2] Zdroj: 2022 Synopsys Open Source Security and Risk Analysis Report

## Naše riešenie

### Zabezpečenie open source softvérov pre všetkých

V Googli sa riešeniu tejto výzvy venujeme už roky. Každoročne 10 % zamestnancov spoločnosti Google prispieva do projektov s open source softvérmi. Z našich skúseností vyplýva, že moderná digitálna bezpečnosť môže vzísť práve vďaka využitiu otvorenosti. Otvorené prístupy zaručia rýchle prijímanie najnovších inovácií a umožnia väčšiemu počtu ľudí riešiť bezpečnostné výzvy. Ak však chceme naplno využívať hodnotu open source riešení, musíme vytvárať silnejšie verejno-súkromné partnerstvá a dynamické politické rámce na podporu bezpečnosti pre všetkých. Preto vítame snahy vlády USA o zlepšenie bezpečnosti open source softvérov, ako je napríklad zákon o zabezpečení open source softvérov, ktorý Senát predstavil v roku 2022.

- Vedieme komunitu pomocou bezpečnostných rámcov na vyššej úrovni, ako sú softvérové artefakty na úrovni dodávateľského reťazca (SLSA),[4,5] a vývoj pokročilých nástrojov zabezpečenia.
- Vytvorili sme Graf na pochopenie zloženia artefaktov (GUAC), v ktorom sa v jedinej prehľadávateľnej databáze spájajú informácie o zabezpečení softvérov z rôznych zdrojov. Vďaka GUAC sa demokratizuje dostupnosť informácií o zabezpečení tým, že sa voľne sprístupnia a budú ich môcť využívať všetky organizácie.

### Naše záväzky:

- Investovať 100 miliónov USD do zabezpečenia open source, vedúce úlohy v Open Source Security Foundation a priama spolupráca s vývojármi.
- Definovať a zdieľať použiteľné bezpečnostné štandardy, pokyny, bezplatné nástroje a osvedčené postupy, ktoré používame interne, s celou open source komunitou.
- Používať pokročilú detekciu, automatizované triedenie a ďalšie spôsoby, ako zabezpečiť tie najskoršie štádiá vývoja.
- Automatizovať nástroje na zabezpečenie bezplatného a dostupného zabezpečenia na úrovni firiem.

## Aplikácie

### Google OSS Fuzz
Naša reakcia na chybu Heartbleed

Chyba Heartbleed bola vážnou slabinou open source softvérov, ktorá mohla potenciálne ovplyvniť takmer všetkých používateľov internetu. V roku 2014 hackeri ukradli mená, adresy, dátumy narodenia, telefónne čísla a rodné čísla približne 4,5 milióna pacientov z databázy jednej z najväčších nemocníc v USA.

Ako reakciu na tento incident Google spustil bezplatnú službu pre komunitu OSS-Fuzz. Fuzz testovanie identifikuje neznáme bezpečnostné hrozby v priebehu niekoľkých minút, na rozdiel od manuálneho testovania, ktoré môže trvať mesiace. Investovali sme do vybudovania infraštruktúry na automatické testovanie stoviek open source projektov. OSS-Fuzz teraz pravidelne skenuje kódy a neustále ho inovujeme, aby vedel rozpoznávať ďalšie triedy chýb.

Fuzz skenuje vyše 800 dôležitých open source projektov v šiestich jazykoch.

## Naše investície do odvetvia a míľniky

**2020 – AUGUST**
**Vstup do Open Source Security Foundation (OpenSSF)** s cieľom usmerňovať a zlepšovať zabezpečenie open source softvérov.

**2021 – MÁJ A JÚN**
**Zavedenie osvedčených postupov v oblasti open source** v súlade s **Nariadením Bieleho domu č. 14028** a prínos do usmernení týkajúcich sa bezpečnostných štandardov softvérov dodávateľského reťazca.

**2021 – JÚN**
**Vydanie SLSA s OpenSSF**, čím sa externalizoval interný bezpečnostný rámec Google a umožnil všetkým používateľom vytvárať bezpečnejší softvér.

**2021 – AUGUST**
**Prísľub 100 miliónov USD na podporu a zabezpečenie open source softvérov**, vrátane partnerstva s vývojármi, s cieľom nájsť a opraviť slabiny.

**2022 – MÁJ**
**Ohlásenie vytvorenia tímu spoločnosti Google na údržbu open source softvérov** počas **summitu DC**. Príslušný tím vývojárov na plný úväzok sa bude venovať priamo zlepšovaniu zabezpečenia open source projektov.

**2022 – MÁJ**
**Ohlásenie produktu Assured Open Source Software**, ktorý pomáha začleniť do pracovných postupov vývojárov rovnaké dôveryhodné open source balíčky, ktoré používa spoločnosť Google.

**Postupy odporúčané Googlom, ktoré pomôžu verejným aj súkromným organizáciám zostať v bezpečí:**

- Implementovať SLSA na posilnenie bezpečnosti softvérov dodávateľského reťazca.
- Kryptograficky podpísať a overiť pravosť svojho softvéru pomocou nástroja Sigstore.
- Automatizovať zisťovanie, sledovanie a vyhodnocovanie zraniteľností pomocou nástrojov OSS-Fuzz a OSV.dev.
- Automaticky vyhodnocovať bezpečnostné riziká svojich dependencií pomocou nástroja Scorecards.

## Náš prístup

Softvér je len taký bezpečný, ako je jeho najzraniteľnejšia časť. Investujeme svoje odborné poznatky a finančné zdroje do zvýšenia bezpečnosti celého open source ekosystému. Náš tím odborníkov na vývoj a bezpečnosť verí, že takto dokážeme ochrániť viac verejných a súkromných organizácií:

Náš tím kontroluje každú fázu životného cyklu produktu, nepretržite skenuje, analyzuje a testuje zraniteľnosti.

Podporujeme otvorený internet, svoje poznatky zdieľame s komunitou vývojárov, aby bol internet bezpečný pre verejný aj obchodný sektor.

Pri zabezpečení myslíme aj na budúcnosť, vyhľadávame sofistikované hrozby, poskytujeme automatizované nástroje a vždy sme o krok vpred oproti vývoju.

Zabezpečenie open source softvérov je spoločnou zodpovednosťou, preto sme odhodlaní ďalej spolupracovať na riešení tohto naliehavého a kritického problému.
g.co/security/gosst

Zdroje: 1. 2022 State of the Software Supply Chain. 2. 2022 Synopsys Open Source Security and Risk Analysis Report. 3. CISA Goes on Tour to Get Feedback on Cyber Incident Reporting Rules. 4. Zdieľanie poznatkov (napr. uverejnenie SLSA či usmerňovania OpenSSF) znamená, že všetci vývojári, nielen v Googli, môžu ťažiť zo skúseností Google a overených bezpečnostných postupov. 5. SLSA je súbor postupov, ktoré pomôžu organizáciám zlepšiť zabezpečenie procesu vývoja ich softvéru. Pomáha splniť rámec bezpečného vývoja softvéru americkej vlády, teda požiadavky stanovené vládou v reakcii na Nariadenie o kybernetickej bezpečnosti. To znamená, že organizácie získajú pokyny, ako dodržiavať federálne smernice, aby bol softvér bezpečnejší pre všetkých.