Google

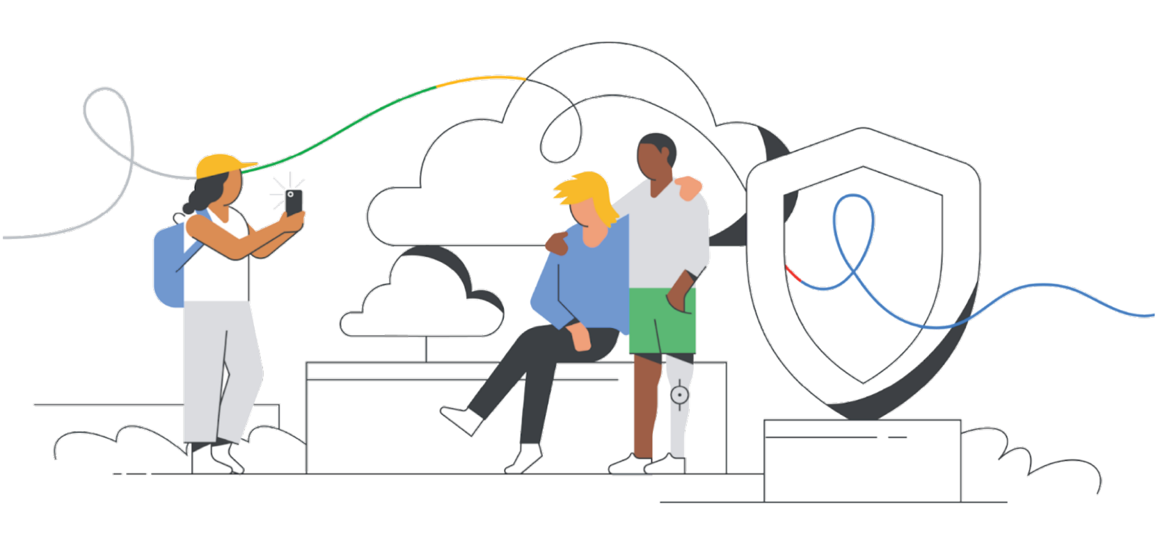
Vývoj našej kybernetickej bezpečnosti v priebehu rokov

Bezpečnejšie s Googlom

Google chráni online viac ľudí než ostatné organizácie

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.



Priebežné inovácie

Od spustenia Gmailu v roku 2004 až po zavedenie Chráneného spracovania údajov v roku 2022 stál Google na čele vývoja technológií kybernetickej bezpečnosti a neustále inovuje svoje služby, platformy a partnerstvá s cieľom eliminovať celé triedy hrozieb a vytvoriť tak bezpečnejšiu budúcnosť pre ľudí, organizácie a spoločnosti tým, že:

- ✓ vytvárame bezpečné služby a platformy,
- ✓ podporujeme programy a partnerstvá,
- ✓ budujeme pružné bezpečnostné tímy,
- ✓ poskytujeme financovanie inovácií a odbornej prípravy pracovnej sily.

Keďže potreby ľudí a internet sa vyvíjajú, aj naďalej sa zameriavame na nové technológie a zmierňovanie neustále sa meniacich kybernetických hrozieb. Vďaka tomu je každý deň s Googlom bezpečnejší.

2004
Ochrana pred spamom v Gmaile

Ako prví sme zaviedli zabudovanú ochranu e-mailov s využitím umelej inteligencie.

Gmail blokuje 99,9 % nebezpečných a podozrivých správ

2007
Bezpečné prehliadanie

Proaktívne pomáhame chrániť zariadenia po celom svete tým, že upozorňujeme používateľov, keď navštívia nebezpečný web. Táto online ochrana sa v roku 2020 vyvinula na Zlepšené bezpečné prehliadanie.

Bezpečné prehliadanie Googlu chráni viac než päť miliárd zariadení.

2008
Správca hesiel Google

Zavedením Správcu hesiel Google sme zjednodušili prihlasovanie a zvýšili jeho zabezpečenie tak, aby ste si nemuseli pamätať alebo zadávať svoje heslá. Momentálne sa používa pri 50 % všetkých prihlásení v prehliadači Chrome.

Denne skontrolujeme miliardu hesiel

2009
reCAPTCHA

Získali sme riešenie na správu podvodov a botov, aby sme zastavili hromadenie účtov a prevzatí účtov a zabránili zneužívaniu zo strany škodlivého softvéru či falošných používateľov.

Chránime päť miliónov webov

2010
Zero Trust

Po sérii koordinovaných kybernetických útokov pod názvom Operácia Aurora sme zmenili prístup k budovaniu štandardnej architektúry zabezpečenia, ktorá je teraz známa ako Zero Trust. Tento prístup zabezpečuje menší počet zdrojov útokov, eliminuje príležitosti na stratu údajov a poskytuje väčšiu kontrolu nad systémami, ktoré sú pre používateľov dôležité. Podporujeme snahy Bieleho domu o zavedenie modelu Zero Trust vo federálnej vláde a tiež sme ho zahrnuli do balíčka BeyondCorp Enterprise, aby ho mohli využívať všetky firmy.

2010
Skupina Googlu na analýzu hrozieb (TAG)

Po operácii Aurora sme vytvorili tím odborníkov zodpovedných za odhaľovanie, analýzu a narúšanie vládou podporovaných a závažných kriminálnych kybernetických rozieb. Skupina TAG vystopovala najväčší ransomvérový útok v dejinách Wanna Cry do Severnej Kórey a nedávno zdieľala príklady ekosystémov nájomných hackerov z Indie, Ruska a Spojených arabských emirátov.

2010
Google Bug Hunters

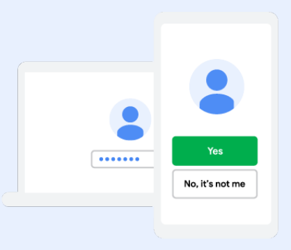
Náš program odmien za odhaľovanie zraniteľnosti Vulnerability Rewards láka stredoškolákov, právnikov, IT profesionálov a nadšencov, aby hľadali chyby v produktoch Google s možnosťou získať finančnú odmenu. Motívy majú rôzne, ale poslanie rovnaké: objaviť nepoznané zraniteľné miesta a pomáhať udržať online služby bezpečné.

Od roku 2010 boli v odmenách vyplatené milióny dolárov

2010
Tím Red

Vytvorený s cieľom pochopiť myslenie nepriateľa a hacknúť Google, aby sme posilnili svoju obranu a odhalili nedostatky. Spolupracujú z rôznych miest po celom svete, aby držali krok s modernými hrozbami, zlepšujú stav bezpečnosti a vykonávajú útoky s cieľom zistiť skutočné hrozby a predchádzať im. Vytváraním nových a lepších rámcov tak eliminujú celé triedy zraniteľností.

2011
Dvojfaktorové overenie



Medzi prvými sme ponúkli predvolené dvojfaktorové overenie a v roku 2021 sme takisto ako prví automaticky aktivovali dvojfaktorové overenie pre viac než 150 miliónov ľudí, čím sme im zabezpečili bezpečný spôsob prihlasovania. Váš účet je tak chránený aj po krádeži hesla.

50 % pokles krádeže účtov vďaka dvojfaktorovému overeniu

2013
Project Shield

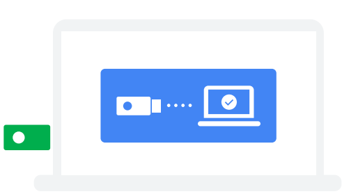
Nástroj Project Shield chráni spravodajské a ľudskoprávne organizácie, volebné weby, politické organizácie a kampane pred útokmi typu DDoS (Distributed Denial of Service) vo viac než 100 krajinách tým, že identifikuje hrozby a umožňuje ich riešenie v bezpečnostnej komunite a presadzovaním práva.

150+ webov momentálne chránime na Ukrajine

2014
Project Zero

Špecializovaná pracovná skupina, ktorá sa venuje vyhľadávaniu nevyriešených chýb na internete – v softvéri, hardvéri, službách Google a ďalších miestach s cieľom zaistiť bezpečný a otvorený internet. Ako prví podrobne popísali hardvérové zraniteľnosti Meltdown a Specter a umožnili tak vývojárom rýchlo riešiť zraniteľné miesta CPU a vyriešiť problémy v softvéri dodávateľského reťazca.

2017
Program rozšírenej ochrany



Mimoriadne zabezpečenie vrátane bezpečnostného kľúča pre používateľov s vysokou viditeľnosťou a rizikom, ako sú novinári a vládni úradníci.

Chránime 300+ federálnych kampaní

2017
Google Play Protect

Google Play Protect je najrozšírenejšia služba ochrany pred mobilnými hrozbami na svete. Neustále sa prispôsobuje a zdokonaľuje pomocou strojového učenia Google, automaticky skenuje aplikácie na prítomnosť škodlivého softvéru a šifruje platby používateľov v telefónoch s Androidom.

100+ miliárd aplikácií skenujeme denne

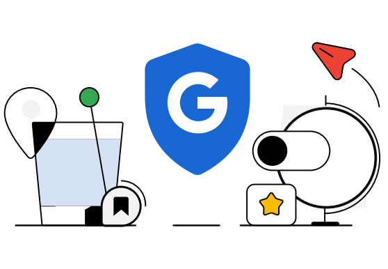
150 miliónov platieb používateľov šifrujeme denne

2018
Bezpečnostný kľúč Titan

Pre používateľov, ktorí chcú komplexné riešenie od Googlu, sme vytvorili bezpečnostný kľúč Titan. Kľúče spĺňajú štandardy FIDO a dajú sa použiť kdekoľvek, nielen v Googli.

2019
Opätovné overenie bez hesla

Rozšírili sme podporu FIDO v Androide, aby sa používatelia mohli jednoducho prihlasovať na weby bez hesla, len pomocou kódu PIN alebo biometrie.



2019
Chronicle

Služba Chronicle bola vytvorená ako špecializovaná vrstva našej základnej bezpečnostnej infraštruktúry a zavedená s cieľom poskytovať cloudové zabezpečenie pre podniky na súkromné uchovávanie, analýzu a vyhľadávanie obrovského množstva bezpečnostných a sieťových údajov.

2021
Investícia do rozvoja kybernetickej bezpečnosti

Zaviazali sme sa posilňovať kybernetickú bezpečnosť, rozširovať programy s modelom Zero Trust, pomáhať pri zabezpečovaní softvéru dodávateľského reťazca a zlepšovať bezpečnosť open source. Zaviazali sme sa prostredníctvom programu Google Career Certificate vyškoliť 100 000 Američanov v oblastiach, ako sú podpora IT a dátová analytika.

10 miliárd USD sme prisľúbili na iniciatívy v oblasti kybernetickej bezpečnosti

2021
Tím Googlu pre zabezpečenie open source

Tím Googlu pre zabezpečenie open source vznikol s cieľom posilniť bezpečnosť open source softvérov, ktoré sú pre svet nevyhnutné. V spolupráci s organizáciou Open Source Security Foundation (OpenSSF) sme vyvinuli a uverejnili softvérové artefakty na úrovni dodávateľského reťazca (SLSA), rámec na zabezpečenie softvéru dodávateľského reťazca a umožnenie dlhodobej bezpečnosti pre celý softvérový ekosystém.

100 miliónov USD sme prisľúbili na podporu operácií tretích strán v oblasti zabezpečenia open source na opravovanie slabých miest

2021
Súkromné spracovanie údajov

Na účely kritického udržania zabezpečenia, ochrany a súkromia sme predstavili Google Cloud Confidential Computing – prelomovú technológiu, ktorá uchováva údaje počas spracovania šifrované, vďaka čomu zostávajú v bezpečí počas celého životného cyklu, vrátane uchovávania alebo počas presunu. Teraz je možné s istotou presúvať do cloudu aj tie najcitlivejšie údaje.

2022
Štandardizácia postkvantovej kryptografie

So zameraním na budúcnosť pokračujeme vo vývoji kryptografických systémov novej generácie, ktoré chránia pred prelomením kryptosystémov s verejnými kľúčmi a ohrozením digitálnej komunikácie. Národný inštitút pre štandardy a technológie vybral na štandardizáciu príspevok so zapojením spoločnosti Google (SPHINCS+).

2022
Chránené spracovanie údajov

Ohlásili sme vytvorenie chráneného spracovania údajov. Ide o rozrastajúci sa súbor nástrojov, ktorý mení to, ako, kedy a kde sa údaje spracúvajú, s cieľom technicky zabezpečiť súkromie a bezpečnosť vašich údajov. Robíme to pomocou minimalizovania dátovej stopy, anonymizáciou údajov a obmedzením prístupu k citlivým údajom. To znamená, že zariadenia s Androidom môžu navrhovať slová pri písaní a zároveň zachovávať súkromie konverzácií.

2022
Mandiant a Google Cloud

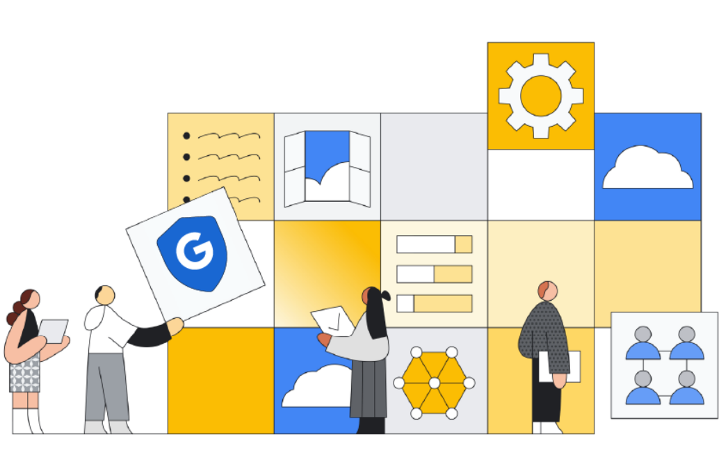
Mandiant v reálnom čase prináša hĺbkové informácie o hrozbách získané najväčšími organizáciami z prvej línie kybernetickej bezpečnosti. V kombinácii so zabudovanými cloudovými bezpečnostnými možnosťami služby Google Cloud pomáhame podnikom a agentúram verejného sektora zostať chránenými počas celého životného cyklu zabezpečenia.

2023
Prístupový kľúč: Budúcnosť bez hesiel

Už viac ako desať rokov sa pripravujeme na budúcnosť bez hesiel. V roku 2013 sme sa pripojili k aliancii FIDO s cieľom podporiť otvorené štandardy pre svet bez hesiel a teraz, keď v roku 2023 rozšírime podporu štandardov prihlasovania FIDO pre zariadenia s Androidom a prehliadač Chrome prostredníctvom technológie prístupových kľúčov, konečne budeme mať platformu pre budúcnosť skutočne bez hesiel.

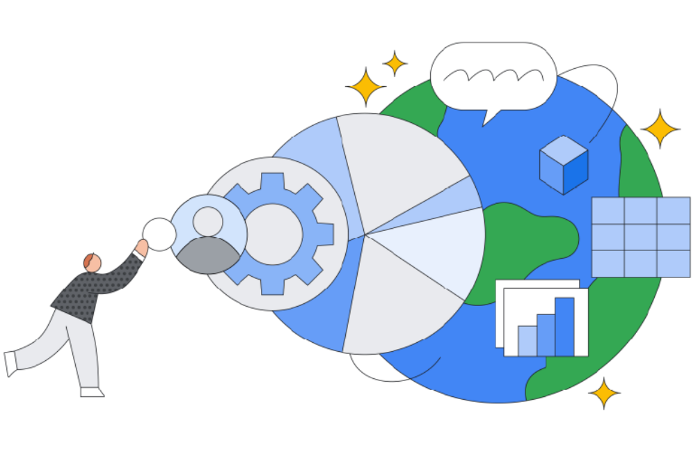
Ak chceme v období neustáleho technologického rastu využiť plný potenciál spoločnosti, je kľúčové udržať dôveru v technológie.

Pri zavádzaní našich poznatkov o bezpečnosti do praxe budeme naďalej spolupracovať s ľuďmi, firmami a vládami, aby sme ich chránili a začali novú éru kybernetickej bezpečnosti.



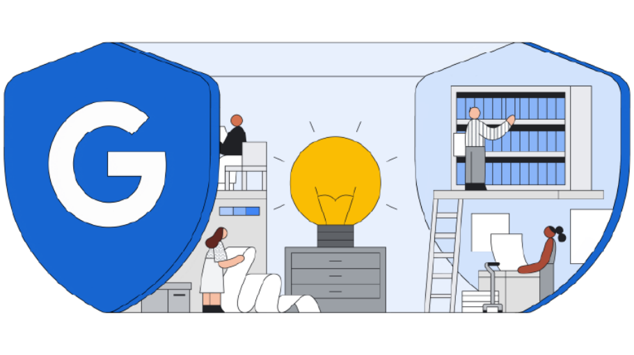
Chránime ľudí, firmy a vlády

Základným kameňom našej produktovej stratégie je bezpečnosť. Preto majú všetky naše produkty zabudovanú ochranu, vďaka ktorej sú štandardne zabezpečené.



Pomáhame spoločnosti pri riešení rastúcich hrozieb v oblasti kybernetickej bezpečnosti

Umožňujeme spoločnostiam využiť celý potenciál open source softvérov a transparentne zdieľame svoje znalosti a odborné poznatky v odvetví s cieľom vytvárať bezpečnejšie ekosystémy.



Pokrok v technológiách budúcnosti

Chceme chrániť spoločnosť pred ďalšou generáciou kybernetických hrozieb. Na základe našich odborných poznatkov v oblasti umelej inteligencie navrhujeme úpravu architektúr, aby sme posunuli hranice bezpečnostných inovácií.

S Googlom ste každým dňom viac v bezpečí

Navštívte g.co/safety/cyber

Google