Google

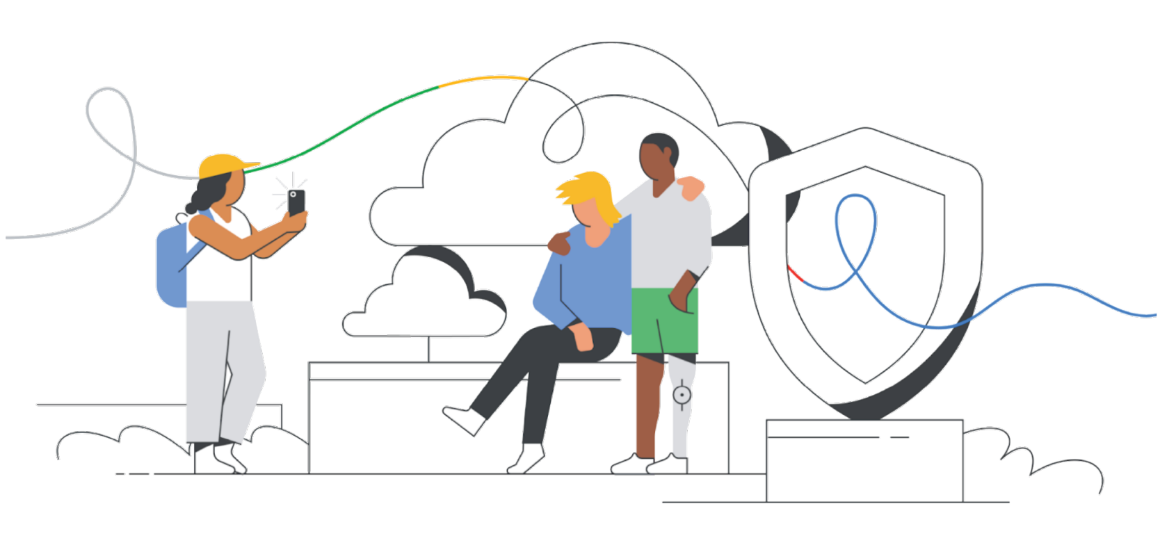
Naše cesta ke kybernetické bezpečnosti v průběhu let

Bezpečnější s Googlem

Zajišťujeme bezpečnost na internetu pro více uživatelů než kdokoli jiný na světě

Vzhledem k dramatickému nárůstu kybernetických útoků sponzorovaných státy a záškodníků na internetu jsme přesvědčeni, že naše produkty a služby jsou jen tak užitečné, jak jsou bezpečné.

Proto se v Googlu nyní víc než dřív zaměřujeme na ochranu lidí, organizací a vlád. Sdílíme své odborné znalosti, pomáháme společnosti čelit neustále se vyvíjejícím kybernetickým rizikům, snažíme se zvyšovat kybernetickou bezpečnost a vytvářet bezpečnější svět pro všechny.



Neustálé inovace v průběhu času

Od spuštění služby Gmail v roce 2004 až po zavedení služby Protected Computing v roce 2022 je společnost Google průkopníkem v oblasti kybernetické bezpečnosti. Neustále inovujeme produkty, platformy a partnerství s cílem eliminovat celé třídy hrozeb a vytvořit tak bezpečnější budoucnost pro lidi, organizace a společnosti:

- ✓ Vyvíjíme bezpečné produkty a platformy
- ✓ Vytváříme aktivní bezpečnostní týmy
- ✓ Podporujeme programy a partnerství
- ✓ Významně financujeme inovace a odbornou přípravu pracovníků

S tím, jak se vyvíjejí potřeby lidí a internet, jsme i nadále v čele nových technologií, které zmírňují neustále se měnící kybernetické hrozby a zajišťují, aby byl každý den bezpečnější díky Googlu.

2004
Ochrana Gmailu proti spamu

Jako jedni z prvních jsme vytvořili ochranu e-mailů založenou na umělé inteligenci.

Gmail zablokuje 99,9 % nebezpečných a podezřelých e-mailů

2007
Bezpečné prohlížení

Aktivně pomáháme chránit zařízení po celém světě tím, že uživatele upozorňujeme, když navštíví nebezpečné webové stránky. V roce 2020 jsme tyto online ochrany rozvinuli do funkce Vylepšené Bezpečné prohlížení.

Služba Bezpečné prohlížení chrání 5 miliard zařízení

2008
Správce hesel Google

Zavedení Správce hesel usnadnilo a zabezpečilo přihlašování bez nutnosti pamatovat si heslo nebo ho ručně vypisovat. Nyní se používá u 50 % všech přihlášení v prohlížeči Chrome na různých platformách.

Každý den se kvůli riziku úniků prověří jedna miliarda hesel

2009
reCAPTCHA

Získali jsme řešení pro správu podvodů a botů, abychom zabránili útokům typu credential stuffing a přebírání účtů a předcházeli zneužívání ze strany škodlivého softwaru a falešných uživatelů.

Ochráněno 5 milionů webových stránek

2010
Zero Trust

Poté, co jsme ustáli operaci Aurora, řízenou sérii kybernetických útoků, jsme výrazně změnili přístup a vytvořili od počátku zabezpečenou architekturu, která je nyní známá jako „Zero Trust“. Zajišťuje méně vektorů útoku, méně příležitostí ke ztrátě dat a větší kontrolu nad systémy, na kterých jsou uživatelé závislí. Podporujeme úsilí Bílého domu o zavedení modelu Zero Trust v celé federální vládě. Zároveň jsme ho začlenili do BeyondCorp Enterprise, aby ho mohla využívat každá firma.

2010
Threat Analysis Group (TAG)

Po operaci Aurora jsme vytvořili tým specialistů zodpovědných za odhalování, analýzu a narušování podporovaných státy a závažných kriminálních kybernetických hrozeb. Skupina TAG vypátrala, že za Wanna Cry, největším ransomwarovým útokem v dějinách, je zodpovědná Severní Korea, a nedávno sdílela příklady ekosystémů nájemných hackerů z Indie, Ruska a Spojených arabských emirátů.

2010
Google Bug Hunters

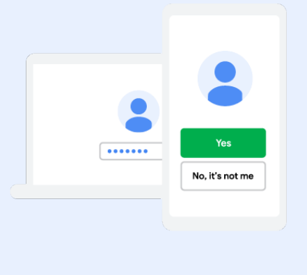
Náš program odměn za odhalování zranitelností láká středoškoláky, právníky, IT profesionály i amatérské programátory, aby za peněžní odměnu hledali chyby v produktech Google. Jejich motivace se různí, ale poslání mají stejné: najít neobjevené zranitelnosti, aby byly online služby bezpečné.

Od roku 2010 jsme na odměnách vyplatili miliony dolarů

2010
The Red Team

Úkolem tohoto týmu je uvažovat jako nepřítel a snažit se hacknout Google, a tím posilovat naši obranu a odhalovat nedostatky. Jeho členové se na celém světě usilovně snaží držet krok s aktuálními hrozbami, zlepšovat bezpečnostní kontroly, provádět detekci/prevenci útoků a eliminovat celé třídy zranitelností zaváděním nových a lepších rámců.

2011
Dvoufázové ověření



Jako jedni z prvních jsme nabídli dvoufázové ověřování (2SV) ve výchozím nastavení a jako první jsme v roce 2021 automaticky aktivovali 2SV pro více než 150 milionů lidí, čímž jsme zajistili bezpečný a snadný způsob přihlašování. Váš účet je chráněný, i když vám ukradnou heslo.

50% pokles ohrožených účtů od zavedení 2SV

2013
Project Shield

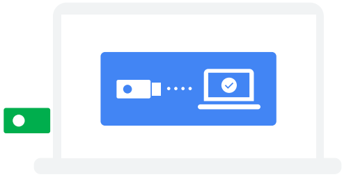
Project Shield pomáhá chránit zpravodajství, lidskoprávní organizace, volební stránky, politické organizace a kampaně před útoky DDoS (Distributed Denial of Service) a jinými kybernetickými útoky ve více než 100 zemích tím, že identifikuje hrozby a umožňuje reakci bezpečnostní komunity a policejních orgánů.

V současnosti chráníme více než 150 webů na Ukrajině

2014
Project Zero

Specializovaná pracovní skupina, která se zabývá vyhledáváním Zero day útoků na internetu – v softwaru, hardwaru, produktech Google i jinde, aby zajistila bezpečný a otevřený internet. Jako první podrobně popsala chyby „Meltdown“ a „Spectre“, čímž umožnila vývojářům rychle řešit zranitelnosti procesorů a provést nápravu v celém dodavatelském řetězci softwaru.

2017
Program pokročilé ochrany (APP)



Mimořádně bezpečná ochrana včetně bezpečnostního klíče pro vysoce viditelné a rizikové uživatele, jako jsou novináři a státní správa.

Ochráněno více než 300 federálních kampaní

2017
Google Play Protect

Služba Google Play Protect, která je nejrozšířenější službou ochrany před mobilními hrozbami na světě a která se neustále přizpůsobuje a zdokonaluje díky strojovému učení společnosti Google, automaticky zjišťuje přítomnost malwaru v aplikacích a šifruje platby uživatelů v telefonech se systémem Android.

U více než 100 miliard aplikací je denně prověřován výskyt malwaru

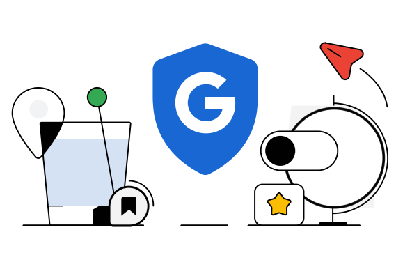
150 milionů plateb uživatelů je denně šifrováno

2018
Bezpečnostní klíč Titan

Bezpečnostní klíč Titan jsme vytvořili pro uživatele, kteří chtějí komplexní řešení od Googlu. Tyto klíče splňují standardy FIDO a lze je použít i jinde, nejen ve službě Google.

2019
Opětovné ověření bez hesla

Rozšířili jsme podporu FIDO v systému Android, aby se uživatelé mohli bezproblémově přihlašovat na webové stránky pouze pomocí kódu PIN nebo biometrických údajů, bez nutnosti zadávat heslo.



2019
Chronicle

Služba Chronicle byla vytvořena jako specializovaná vrstva nad naší základní infrastrukturou, aby poskytovala cloudové zabezpečení podnikům k soukromému uchovávání, analýze a vyhledávání obrovského množství bezpečnostních a síťových dat.

2021
Investice do rozvoje kybernetické bezpečnosti

Jsme odhodláni posilovat kybernetickou bezpečnost, rozšiřovat programy nulové důvěry, chceme pomáhat zabezpečovat dodavatelský řetězec softwaru a zvyšovat bezpečnost otevřených zdrojů. Zavázali jsme se vyškolit 100 000 Američanů v oborech, jako je IT podpora a datová analýza, prostřednictvím programu Google Career Certificate.

Závazek 10 miliard dolarů na iniciativy v oblasti kybernetické bezpečnosti

2021
Google Open Source Security Team (GOSST)

Cílem týmu GOSST je zlepšit zabezpečení softwaru s otevřeným zdrojovým kódem, na který se celý svět spoléhá. Ve spolupráci s nadací Open Source Security Foundation (OpenSSF) jsme vyvinuli a vydali Supply-Chain Levels for Software Artifacts (SLSA), rámec pro zabezpečení dodavatelského řetězce softwaru, čímž jsme umožnili dlouhodobé zabezpečení celého softwarového ekosystému.

100 milionů dolarů vyčleněno na open source bezpečnostní operace třetích stran s cílem opravit zranitelnosti

2021
Confidential Computing

Pro důležité zabezpečení, bezpečnost a ochranu soukromí jsme představili Google Cloud Confidential Computing, průlomovou technologii, která uchovává data zašifrovaná v průběhu zpracování a udržuje je v bezpečí po celou dobu jejich životního cyklu, a to i v klidovém stavu nebo při přenosu. Nyní lze do cloudu bez obav migrovat i ta nejcitlivější data.

2022
Standardizace postkvantové kryptografie

Zaměřujeme se na budoucnost, a proto pokračujeme ve vývoji kryptografických systémů nové generace, které chrání před prolomením kryptosystémů s veřejným klíčem a ohrožením digitální komunikace. Národní institut pro standardizaci a technologie vybral pro standardizaci návrh, na němž se podílela společnost Google (SPHINCS+).

2022
Protected Computing

Oznámili jsme Protected Computing, rostoucí soubor technologií, které mění způsob jak, kdy a kde se data zpracovávají, aby bylo technicky zajištěno soukromí a bezpečnost uživatelů. Toho dosahujeme minimalizací datové stopy, odstraněním identifikace dat a omezením přístupu k citlivým údajům. To znamená, že Android může navrhovat další slovní spojení v textu, přičemž konverzace zůstává zcela soukromá.

2022
Mandiant and Google Cloud

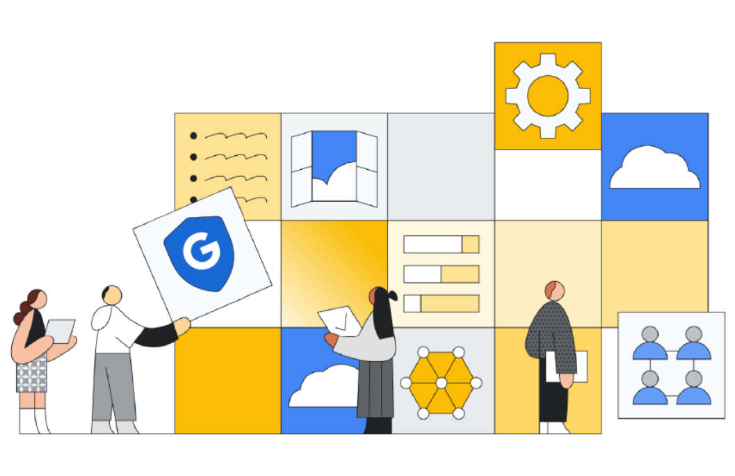
Společnost Mandiant přináší v reálném čase podrobné informace o hrozbách, které získala v první linii kybernetické bezpečnosti u největších organizací na světě. V kombinaci s nabídkou cloudového zabezpečení Google Cloud pomáháme firmám a agenturám veřejného sektoru zajistit ochranu v celém životním cyklu zabezpečení.

2023
Přístupový klíč: budoucnost bez hesel

Již více než deset let připravujeme půdu pro budoucnost bez hesel. V roce 2013 jsme se připojili k alianci FIDO, abychom prosazovali otevřené standardy pro svět bez hesel, a nyní, když v roce 2023 rozšíříme podporu přihlašovacích standardů FIDO na systémy Android a Chrome prostřednictvím technologie přístupových klíčů, budeme mít konečně k dispozici platformu pro budoucnost skutečně bez hesel.

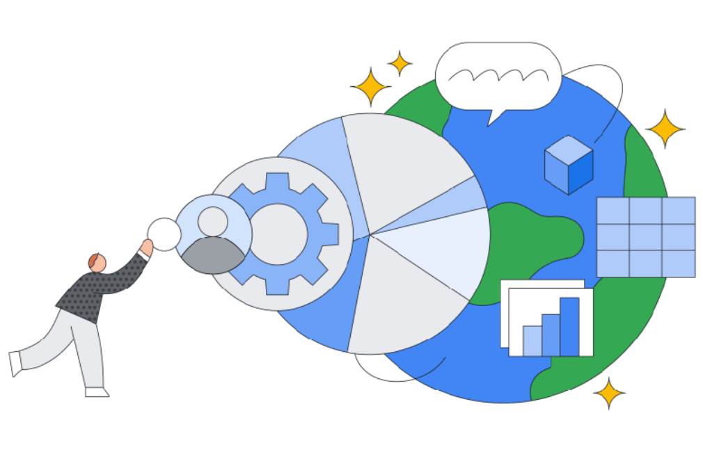
V době stále se rozšiřujícího technologického dosahu je důvěra v technologie klíčem k uvolnění skutečného potenciálu společnosti.

Při uplatňování svých znalostí z oblasti bezpečnosti v praxi budeme i nadále spolupracovat s lidmi, podniky a vládami, abychom chránili jejich bezpečnost a nastartovali novou éru kybernetické bezpečnosti.



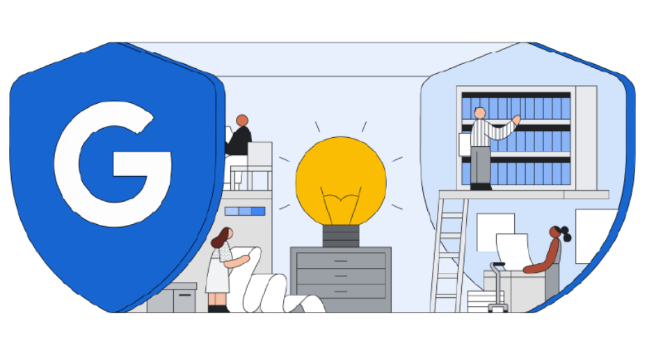
Chráníme lidi, firmy a vlády

Bezpečnost je základním kamenem naší produktové strategie. Proto mají všechny naše produkty vestavěnou ochranu, která je od začátku zabezpečuje.



Umožňujeme společnosti řešit vyvíjející se rizika kybernetické bezpečnosti

Umožňujeme společnostem využít potenciál otevřeného softwaru a transparentně sdílíme své znalosti a zkušenosti s průmyslem pro větší bezpečnost ekosystémů.



Prosazujeme technologie budoucnosti

Chceme chránit společnosti před novou generací kybernetických hrozeb. Na základě svých odborných znalostí v oblasti umělé inteligence navrhujeme další vlnu architektur, které posunou hranice bezpečnostních inovací.

S Googlem jste každý den bezpečnější

Navštivte g.co/safety/cyber

Google