

Enkripcija

Tehnologije enkripcije omogućavaju korisnicima interneta da zaštite integritet i povjerljivost svojih podataka i komunikacije. Od ograničavanja posljedica curenja podataka do čuvanja privatnosti poruka, enkripcija je neophodan alat digitalne bezbjednosti. Kao tehnički temelj povjerenja na internetu, enkripcija podstiče slobodu izražavanja, trgovinu, privatnost i povjerenje korisnika i pomaže da se podaci i komunikacija zaštite od zlonamjernih aktera.



Internet Society smatra da enkripcija treba da bude standard za internet saobraćaj i čuvanje podataka.

Šta je enkripcija?

Enkripcija je postupak šifrovanja podataka tako da ih može pročitati samo onaj ko ima način da ih vrati u izvorno stanje. Obično se koristi za zaštitu podataka sačuvanih na računarskim sistemima (**podaci u mirovanju**) i podataka koji se prenose računarskim mrežama, uključujući internet (**podaci u prenosu**). Podaci u prenosu se uglavnom šifruju javnim, a dešifruju privatnim ključem. Kod podataka u mirovanju, tajnu vrijednost obično zna samo vlasnik podataka.

Enkripcija s kraja na kraj

Enkripcija s kraja na kraj (E2E) je svaki oblik enkripcije kod kojeg samo pošiljalac i namijenjeni primalac imaju ključeve za dešifrovanje poruke. Najvažnije je to što nijedna treća strana, čak ni ona koja pruža uslugu komunikacije, ne zna ključeve za šifrovanje.



Enkripciju koristimo svaki dan



Surfovanje internetom

Pretraživači i sajtovi koriste HTTPS, šifrovani protokol, za bezbjednu komunikaciju. Tako kriminalci ne mogu da pročitaju naše podatke dok putuju mrežom.



Online trgovina

Kada kupujemo na internetu, koristimo elektronsko bankarstvo ili plaćamo usluge preko eUprave, vjerujemo da će naši finansijski podaci biti zaštićeni. Enkripcija je važan način da se to postigne.



Bezbjedne poruke

Kada koristimo aplikaciju za poruke, očekujemo da poruke ostanu privatne. Neke aplikacije šifruju poruke dok putuju mrežom. Druge koriste enkripciju s kraja na kraj, pa poruke mogu pročitati samo pošiljalac i primalac – npr. Signal, WhatsApp, Viber i iMessage.

Šta je vanredni pristup?

Kada se govori o vanrednom pristupu (engl. *exceptional access*), obično se misli na neki način da organi za sprovođenje zakona zakonito pristupe sadržaju komunikacije i podacima u nešifrovanom obliku.

Zašto vanredni pristup? Budući da i zlonamjerni akteri mogu koristiti enkripciju da sakriju svoje aktivnosti, policija i neki drugi zabrinuti su da bi enkripcija mogla otežati zaštitu građana i sprovođenje zakona. Neki smatraju da bi policiji trebalo omogućiti vanredni pristup sadržaju šifrovane komunikacije i uređaja.

Problemi sa vanrednim pristupom

1

Bez obzira na metod, vanredni pristup olakšava drugima – na primjer kriminalcima i drugim vladama – da dođu do zaštićenih podataka. Stručnjaci za informacionu bezbjednost se slažu da mehanizmi vanrednog pristupa uvijek povećavaju složenost sistema, što dovodi do ranjivosti. Te ranjivosti mogu postati ulazne tačke koje bilo ko može otkriti.

2

Prijedlozi za vanredni pristup teško da će spriječiti kriminalce da tajno komuniciraju. Onima koji imaju malo iskustva s računarima prilično je lako da pronađu druge alate za šifrovanje podataka u mirovanju ili u prenosu. Komunikacija odlučnih kriminalaca mogla bi ostati nedostupna za nadzor, dok bi komunikacija običnih korisnika ostala izložena nadzoru i presretanju od strane onih koji otkriju kako da zloupotrijebe ranjivosti nastale vanrednim pristupom.

Neki prijedlozi za vanredni pristup



Zadnja vrata (backdoor) u enkripciji obično označavaju izmjenu protokola, aplikacije ili servisa za šifrovanje, s ciljem da se ovlaštenoj trećoj strani omogući pristup šifrovanim podacima. Jedan način je **slabljenje enkripcije**, odnosno njenih mehanizama ili sistema na koje se oslanja. Zadnja vrata bilo koje vrste su ranjivosti koje mogu otkriti i iskoristiti kriminalci i drugi zlonamjerni akteri.



Deponovanje ključeva (key escrow) obično označava ideju da se ključevi za dešifrovanje čuvaju kod pouzdane treće strane, kako bi ih policija kasnije mogla koristiti. Ali svi sačuvani ključevi izloženi su riziku da ih zloupotrijebe kriminalci i drugi zlonamjerni akteri.

Razmatranja o vanrednom pristupu

Ako se enkripcija ili drugi bezbjednosni mehanizmi oslabe kako bi se omogućio forenzički pristup, svakome postaje lakše da dođe do podataka (posebno organizovanom kriminalu, kompanijama uključenim u industrijsku špijunažu i državnim akterima). To ugrožava i legitimne interese građana i kompanija, jer olakšava krađu identiteta i pristup osjetljivim informacijama o imovini, uključujući finansijsku i intelektualnu svojinu.

Internet Society razumije zabrinutost organa za sprovođenje zakona i čvrsto vjeruje da je enkripcija važno tehničko rješenje koje bi svi korisnici interneta trebalo da koriste za zaštitu svoje komunikacije i podataka. Pravni i tehnički pokušaji da se ograniči upotreba enkripcije, čak i kada su dobronamjerni, negativno će uticati na bezbjednost građana koji poštuju zakon i interneta u cjelini.

Prijedlozi za vanredan pristup malo doprinose rješavanju problema tajne komunikacije kriminalaca, a donose značajan rizik za građane koji poštuju zakon. Vanredan pristup bi donio nove probleme, a ne bi ponudio efikasno rješenje.



Brave za prtljag – metafora za zadnja vrata u enkripciji

Brave za prtljag koje odobrava TSA (američka Uprava za bezbjednost saobraćaja) napravljene su tako da putnici mogu zaključati kofer, a da TSA i dalje može da ga otvori i pregleda sadržaj iz bezbjednosnih razloga, koristeći glavni ključ koji drži TSA.

Nažalost, glavni ključevi nijesu ostali tajna: njihov dizajn je otkriven, pa se kopije mogu napraviti 3D štampačem ili kupiti na internetu za svega 10 dolara.

Sada svako može nabaviti glavni ključ i otvoriti brave koje je odobrila TSA.

Ovakve brave imaju i mnogi koferi koji se prodaju u Crnoj Gori – prepoznacete ih po crvenom znaku u obliku romba pored brave. Glavni ključ koji „samo vlasti“ mogu da koriste, u praksi može da koristi svako.



Zašto je ovo važno za Crnu Goru

- Krajem avgusta 2022. sajber napad ozbiljno je poremetio rad informacionih sistema državnih institucija i elektronskih usluga.
- Elektronsko bankarstvo, eUprava i aplikacije za poruke koje svakodnevno koristimo oslanjaju se na enkripciju.
- Sajber incident možete prijaviti Nacionalnom timu za odgovor na računarske incidente – CIRT.ME: gov.me/cirt