Najveća krađa osobnih podataka u povijesti

Danas je petak trinaesti, pa ćemo prigodno zaviriti u naličje svijeta, na "tamnu stranu". Ispričat ćemo istinitu priču o tome kako je niz pogrešnih postupaka, nenamjernih i namjernih, doveo do katastrofe koja potencijalno pogađa 200 milijuna žrtava.

Davne 1989. vlada SAD donijela je odluku da će povjeriti osjetljive osobne podatke svojih građana trima velikim financijskim korporacijama: TransUnionu, Experianu i Equifaxu. Ove tvrtke čuvaju podatke o financijskim transakcijama, adresama stanovanja i kreditnu povijest građana SAD.

Sedmog ožujka ove godine razvojni tim Apache Stratusa, java platforme za razvoj aplikacija koju rado koristi financijska industrija, objavio je zakrpu koja rješava otkriveni sigurnosni propust. Sistemci Equifaksa propustili su instalirati zakrpu.

U svibnju (dva mjeseca kasnije) napadači su otkrili da su serveri Equifaxa ranjivi, provalili su i počeli prebacivati podatke. Kradljivci su na miru preko dva mjeseca imali na raspolaganju osobne podatke 143 miliona Amerikanaca, 44 miliona Britanaca i nepoznatog broja Kanađana, ukupno oko 200 miliona ljudi. Radi se o dosad najvećem gubitku osobnih podataka u povijesti informacijske ere, zapravo u povijesti čovječanstva. Podataka koji se mogu iskoristiti za krađu identiteta: imena, rođendani, sadašnje i prethodne adrese stanovanja, identifikacijski brojevi (br. socijalnog osiguranja i vozačke dozvole) i brojevi kreditnih kartica. Kriminalci sad mogu počistiti nečije račune, napraviti dugove i uništiti ljudima kreditni status. Mogu otvoriti nove račune u bankama s ukradenim identitetom, izvaditi nove osobne dokumente i lažno se predstavljati. Ako počine kazneno djelo, policija bi mogla pokucati na vrata čovjeku čiji je identitet ukraden.

Provala je otkrivena 29. srpnja, nakon čega su instalirane zakrpe, sa zakašnjenjem od gotovo pet mjeseci.

Usprkos regulativi koja propisuje da se gubitak osobnih podataka mora prijaviti "nadležnim tijelima" i ugroženim klijentima, uprava Equifaxa odlučila je odugovlačiti s objavom. Menadžeri su prodali svoje dionice Equifaxa u vrijednosti 2,000.000 $, predviđajući da će im cijena nakon objave pasti, što je eklatantni "insider trading", ili u duhu opisne prirode hrvatskog jezika, "zloupotreba povlaštenih informacija u prometu vrijednosnih papira".

Tek su 9. rujna (38 dana nakon otkrića) javnost upoznali s provalom, objavivši na web stranici kontakte za zamrzavanje računa. Nisu omogućili klijentima da zahtjev ispune preko weba, što bi bio najbrži put, nego su objavili brojeve telefona i adrese poštanskih pretinaca.

Ponudili se godinu dana besplatne zaštite od krađe identiteta, ali su u tekst ubacili "sitnim slovima" da se klijenti time odriču prava da protiv Equifaxa dignu tužbu. Tu su klauzulu kasnije povukli pod pritiskom javnosti.

Objavili su web stranicu na kojoj građani mogu provjeriti da li su njihovi podaci ukradeni. Bistri korisnici otkrili su da stranica daje nasumične odgovore i zaključili da u Equifaxu zapravo nemaju pojma čiji su podaci ukradeni.

Kao dodatnu zaštitu klijentima su dodjeljivali automatski PIN, za koji se pokazalo da je samo "timestamp" koji označava trenutak zamrzavanja računa. Ako otkrijete kad je netko zamrznuo račun, eto vam njegov PIN!

Nekoliko političara zatražilo je pokretanje istrage o indcidentu, a jedna odvjetnička tvrtka podiže tužbu vrijednu 70 milijardi dolara protiv Equifaxa. Vidjet ćemo kako će to završiti. Pretpostavljam da će se tvrtka nagoditi i jeftino izvući. Možda mislite da će Equifax izgubiti ugovor s državom i unosnu zaradu?

Incident se lako mogao izbjeći: zašto nisu odmah instalirane zakrpe? Je li to vječni sukob između sistemaca i aplikativaca: sistemci bi odmah instalirali sve zakrpe, ali aplikativci im to brane, jer je moguće da nakon toga neke aplikacije više neće raditi. Rješenje je jednostavno: lab u kojem se zakrpe instaliraju na testne servere, pa onda u produkciju. Nije previše teško, zar ne?

Zanimljiv je redoslijed prioriteta u glavama Equifaxovih menadžera. Najprije su se pobrinuli za sebe, rasprodavši dionice, zatim za tvrtku, kupujući vrijeme dok smisle kako smanjiti štetu. Na trećem im je mjestu bilo poštivanje zakona, ali taj dio su manje više loše odglumili. Briga o građanima dolazi tek na kraju. Equifax se očigledno ne boji posljedica, jer drsko izjavljuje da menadžeri koji su prodavali dionice nisu u tom trenutku znali za krađu podataka! Pa nek sad netko dokaže suprotno!

Što se savjetuje potencijalnim žrtvama? Preporuka je da odmah zatraže svoje bilance, odnosno financijske kartice. Iz toga se vidi da li je netko već počeo trošiti njihove novce, a ako nije, može se dokazati nulto stanje prije mogućeg odljeva sredstava. Nakon toga treba zatražiti "zamrzavanje" računa. Ispuni se on-line obrazac i uplati 10$. Ali to treba, čini se, napraviti za svaku financijsku ustanovu posebno! Nakon zamrzavanja mogu se otplaćivati postojeći krediti i rate ranijih kupovina, ali ne može se ulaziti u nove slične aranžmane. Poanta je da tako blokirate i kradljivca vašeg identiteta. Nadalje, savjetuje se da imate pri ruci izvode iz matičnih knjiga za sve članove obitelji - to je najbolji dokaz identiteta. I na kraju, savjetuju im da što prije predaju poreznu prijavu!? Zašto? Zato što kriminalci to znaju napraviti umjesto žrtve, pa pokupiti povrat poreza!

Načelan savjet stanovnicima SAD jest da se ubuduće ponašaju kao da su njihovi osobni podaci postali javni! Treba biti na oprezu kad vam se obraćaju nepoznati ljudi koji se predstavljaju kao predstavnici banaka ili drugih institucija. To što znaju vaše osobne podatke nije dokaz za zaista rade za ustanovu koju navodno predstavljaju.

Stručnjaci za sigurnost gledaju u budućnost i razmišljaju kako bi se ovakvi problemi mogli spriječiti. Obična šifra kao što je broj socijalnog osiguranja (kod nas OIB ili JMBG) više nije dovoljna kao dokaz identiteta. Trebalo bi uvesti složenije zaštite, nešto poput javnog i privatnog ključa. Tvrtke poput Equifaxa tada bi čuvale samo javni ključ, s kojim kriminalci ne mogu ništa. No tada bismo sami bili odgovorni za čuvanje privatnih ključeva.

Dodatnu dimenziju ovoj priči dao je legendarni Bruce Shneier. Po njemu, tržište nije u stanju riješiti ovaj problem. Jer građani SAD nisu birali kojoj će tvrtki povjeriti čuvanje osobnih podataka, taj je izbor netko učinio za njih. Po njemu, Equifax je samo "data broker". Equifax i slične tvrtke nisu samo zadužene za provjeru naše kreditne sposobnosti, one žive od prodaje tih podataka. Naši osobni podaci su vrijedni, ako mi to sami ne znamo, onda to znaju banke koje nas žele provjeriti prije nego nam odluče dati kredit, poslodavci koji razmišljaju da li da nas zaposle, iznajmljivači koji žele znati tko će im se useliti...

Sila koja trenutno pogoni Internet je "špijunski" kapitalizam (suveilance capitalism), kaže Schneier. Svi nas prate, čim otvorimo neku web stranicu to se bilježi. Facebook je, kaže Schneier, najveća organizacija za nadziranje, praćenje ljudi koju je čovječanstvo stvorilo. Schneier nema račun na Facebooku, ni gmail adresu, ali oni i bez toga imaju mnoštvo informacija o njemu jer većina ljudi s kojima komunicira ima tamo račune. Schneier kaže da "nismo klijenti, već proizvod" takvih tvrtki. Njih zapravo i nije previše briga hoće li izgubiti naše osobne podatke, jer smo time pogođeni samo mi. Oni će pričekati da se medijska prašina slegne i nastaviti po starom. Sjeća li se još netko koliko je osobnih podataka izgubio Yahoo? Bilo pa prošlo! I zato bi Vlada trebala uskočiti, jer je ona jedina u stanju podići letvicu, natjerati tvrtke da brinu o sigurnosti i strože ih kažnjavati ako to propuste.

Ako smo mi kao građani okruženi tvrtkama (koje žele zaraditi na nama) i kriminalcima (koji bi nas rado opljačkali), onda ispada da bi nas država trebala zaštiti i od jednih i od drugih. No, ako malo razmislimo, i država bi htjela znati sve o nama, upravo zato da bi nas štitila!?.

Na primjeru naše domaće vlasti očigledno je da država zadužena do grla ovisi o bankama i njihovim skrivenim vlasnicima, pa je Vladi lakše ostaviti građane na cjedilu nego se zamjerati stvarnim gospodarima svijeta. Na TV smo gledali primjer našeg sugrađana koji vraća kredit koji nije podigao i uzalud banci dokazuje da nije on sklopio ugovor. Banka ima presliku njegove osobne (krivotvorinu, ili je procurila kopija iz neke firme koja nas legitimira, na pr. telekoma?!). Vjerojatno bi se našla i video snimka na kojoj bi se provjerio izgled potpisnika (poslovnice su pune video kamera). No da li je itko zatražio takvu provjeru? Banci je zapravo posve svejedno tko će vratiti kredit. Sjećate se primjera kad su ljudi kupili stan u novogradnji, građevinska tvrtka je propala i ostala dužna banci. Sada banka naplaćuje kredit od stanara, koji moraju dva puta kupiti isti stan. Tako je presudio sud. Sve po zakonu. Tko im kriv što su potpisali loš ugovor? Nitko se u ovoj državi ne pita kako je takav ugovor uopće zakonit? Toliko o brizi države za građane.

Možda je rješenje u građanskom aktivizmu? U TV prilogu se spominje ime banke, ali da li je itko radi toga zatvorio račune u toj banci? Da li je itko pokušao organizirati bojkot? Banka bi se zamislila kad bi klijenti masovno počeli zatvarati račune. Ništa od građanske solidarnosti i aktivizma. Živi se u kolotečini, tuđi problemi su tuđi problemi, svatko se brine za sebe i nada se da će ga zla sreća zaobići.

Znači li to da je svatko prepušten sam sebi? Bojim se da je tako. Rješenje je edukacija i preventiva, a ako to zakaže, treba koristiti sva pravna sredstva, zakone koji nas načelno štite i naći dobrog odvjetnika.

Petak je trinaesti, pa ćemo si dozvoliti veću dozu skepticizma nego inače. Bitka se čini unaprijed izgubljena, jer većina ljudi još misli da živimo u prošlosti, u industrijskoj eri i nespremni su za izazove postindustrijskog, informacijskog doba, u kojem je informacija najvrijednija imovina. Možda nam primjer Equifaxa i njegovih klijenata/proizvoda, omogući da nešto naučimo iz tuđeg iskustva.

pet, 2017-10-13 19:13 - Aco Dmitrović**Vijesti:** Sigurnost [1]
Kategorije: Kolumna [2]
Vote: 0

No votes yet

story_tag: kolumna [3]
informacijska sigurnost [4]
osobni podaci [5]

Source URL: https://sysportal.carnet.hr./node/1768?page=0

Links
[1] https://sysportal.carnet.hr./taxonomy/term/13
[2] https://sysportal.carnet.hr./taxonomy/term/71
[3] https://sysportal.carnet.hr./taxonomy/term/152
[4] https://sysportal.carnet.hr./taxonomy/term/101
[5] https://sysportal.carnet.hr./taxonomy/term/153