Mreža, 1.6.2017, str. 44, A3

Evidencijski broj / Article ID: 17390858
Vrsta novine / Frequency: Mjesečna
Zemlja porijekla / Country of origin: Hrvatska
Rubrika / Section:

INTERVJU MJESECA | Keith Gross, predsjednik Odbora za kibernetičku sigurnost Europske

ZAJEDNO p

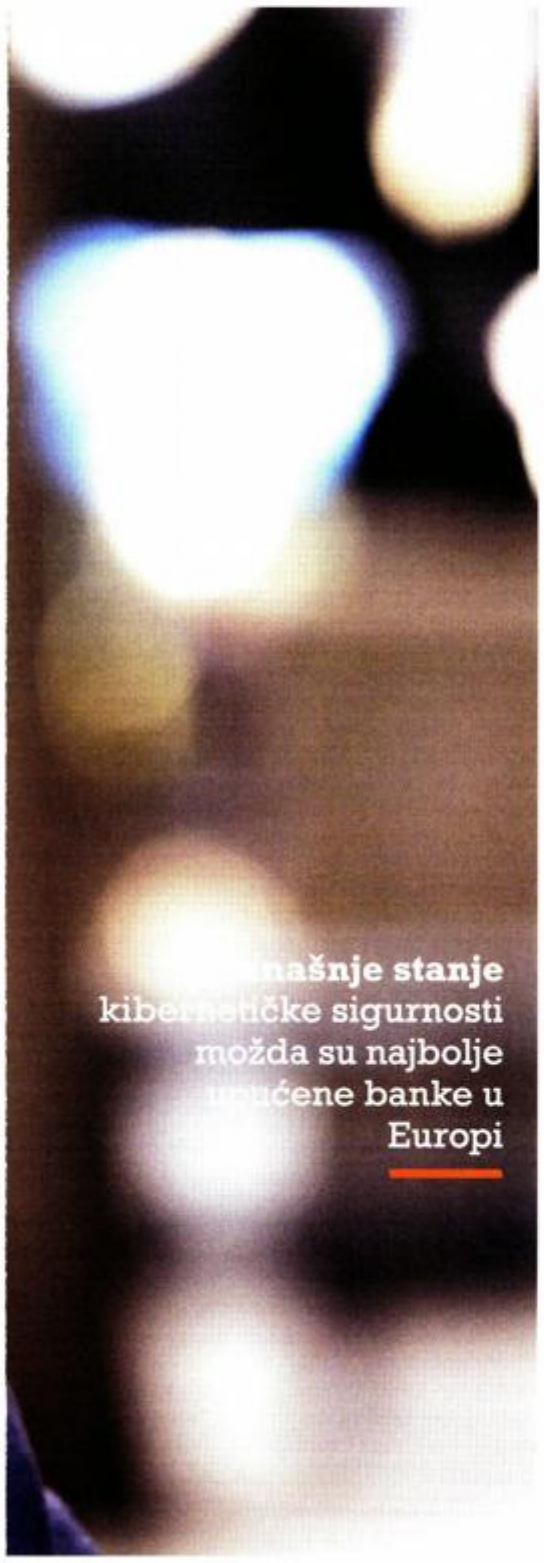
Mreža, 1.6.2017, str. 45, A3

Evidencijski broj / Article ID: 17390858
Vrsta novine / Frequency: Mjesečna
Zemlja porijekla / Country of origin: Hrvatska
Rubrika / Section:

bankovne federacije

rotiv sigurnosnih prijetnji na Internetu

Svi: građani, tvrtke, banke, moraju biti svjesni rizika kojima se izlažu dok su na Internetu. Svatko bi trebao sam moći nadograditi sigurnosni softver koji koristi, svatko bi morao paziti na svoje financijske podatke, i općenito, svi stalno moramo biti svjesni okoline u kojoj živimo i radimo



Piše: Zvonko Pavić

S Keithom Grossom, predsjednikom Odbora za kibernetičku sigurnost Europske bankovne federacije, razgovarali smo početkom travnja u Zagrebu, neposredno prije 11. sjednice odbora, kojem je domaćin bila Hrvatska udruga banaka. Članovi međunarodnog Odbora okupili su se kako bi razmijenili iskustva i raspravili o stanju kibernetičke sigurnosti u Europi te najavili nove sigurnosne inicijative europskih banaka.

Kako biste opisali današnje stanje kibernetičke sigurnosti u Europi – jesmo li dovoljno zaštićeni i kojim smo prijetnjama najviše izloženi?

U današnje stanje kibernetičke sigurnosti možda su najbolje upućene banke u Europi. One kibernetički (računalni i internetski), kriminal prate stalno i pozorno te kontinuirano uvode razna poboljšanja – banke grade nove centre za sigurnosnu zaštitu, formiraju tzv. crvene timove (*red team* – ekipa za brzu reakciju na internetske prijetnje), međusobno se obavještavaju o novim *online* prijetnjama, nadziru mreže i imaju posebne radne skupine za praćenje i analizu sigurnosnih prijetnji. Dakle, banke se zaista trude oko sigurnosne zaštite, no mislim da bi to mogle raditi i bolje i biti još proaktivnije.

TRI NAJOPASNIJE PRIJETNJE

Naime, stalno se pojavljuju nove prijetnje. Navest ću tri možda najopasnije kibernetičke prijetnje s kojima smo danas suočeni. *Ransomware* napadi možda su najstrašnija vrsta napada kojemu danas možete biti izloženi. Ta vrsta napada

Mreža, 1.6.2017, str. 46, A3

Evidencijski broj / Article ID: 17390858
Vrsta novine / Frequency: Mjesečna
Zemlja porijekla / Country of origin: Hrvatska
Rubrika / Section:

Još nisam čuo za zloporabu beskontaktnih kartica. To je sigurna, učinkovita i zgodna metoda plaćanja, i banke ohrabruju svoje klijente na sve širu i češću uporabu tih kartica u izvođenju raznih transakcija

KEITH GROSS – BIOGRAFIJA

Keith Gross voditelj je Radne skupine za kibernetičku sigurnost Europske bankarske federacije. Na toj funkciji već je šest godina. Savjetnik je i Europolova Centra za kibernetički kriminal EC3 (Europol's European Centre for Cybercrime). Keith se specijalizirao za prijevare, e-prijevare, kibernetički kriminal, kibernetičku sigurnost (visokotehnološki kriminal), borbu protiv pranja novca, fizičku sigurnost, probleme vezane uz gotovinske transakcije. Surađuje s organizacijama iz financijskog sektora, ali i sa svim ostalim dionicima, počevši od državnih sigurnosnih agencija i industrije. Odnedavno Keith Gross je izravno uključen u razvoj programa kibernetičke sigurnosti, u koje su uključene banke i akademska zajednica u Irskoj. Studirao je na Institutu za tehnologiju i Institutu za bankarstvo Sveučilišta u Dublinu, u Irskoj. Zvanje magistra kriminologije stekao je na Sveučilištu u Leicesteru, u Ujedinjenom Kraljevstvu. ◂

opasna je za sve – za banke, tvrtke, društvo u cjelini, svakog pojedinog klijenta i građanina. Sljedeća vrsta hakerskog napada prema stupnju opasnosti opći su napadi na računalne mreže. Posebno su opasne nove varijante jedne stare vrste napada na mrežu – DDoS (Distributed Denial of Service) napadi. Ta vrsta ugroze još će dugo biti ozbiljna prijetnja. Banke takvim napadima nastoje doskočiti raznim sustavima za smanjivanje rizika i rano otkrivanje prijetnji u svojim mrežama. Međutim, kriminalci su vješti ljudi – uvijek nađu neki novi način kojim će se ušuljati u nečiju mrežu. Jedna od novijih takvih prijetnji iznimno je napredan DDoS napad, tzv. Mirai Botnet. Riječ je o ugrozi koja mijenja pravila igre u području suvremene IT sigurnosti. Mediji su o tome dosta pisali, i to ne samo oni specijalizirani za financijski sektor, već i tehnički časopisi i publikacije koje prati šira čitalačka publika.

Mirai Botnet zloćudni je računalni program koji sve napadnute uređaje na mreži (računala, mobitele, itd.) pretvara u prijenosnike ("botove") opasnog softvera. Iznimno je strašna prijetnja. Treće, gledano iz perspektive banaka, prijevare na platnim i kreditnim karticama i dalje će biti sigurnosni izazov. Podaci o tim karticama stalno se pokušavaju ukrasti i prodati na raznim kriminalnim internetskim forumima. Postižu razne cijene, a prodaju se nevjerojatno otvoreno, i vrlo ih jednostavno nabaviti. Na tom, tamnom, Internetu (Dark Web) možete naći doista svakakvih informacija. Kriminalni forumi poseban su izazov za današnje bankovno poslovanje. Zato o tome svi – javnost, korisnici, klijenti, baš svi – moraju o tome biti informirani. Ljudi se moraju educirati i shvatiti da svoje osobne i financijske podatke moraju – i stalno i bolje zaštititi.

Mreža, 1.6.2017, str. 47, A3

Evidencijski broj / Article ID: 17390858
Vrsta novine / Frequency: Mjesečna
Zemlja porijekla / Country of origin: Hrvatska
Rubrika / Section:

Kad već govorimo o tome, jesu li beskontaktne kartice sigurne? Ili barem, dovoljno sigurne?

Još nisam čuo za zloporabu beskontaktnih kartica. To je sigurna, učinkovita i zgodna metoda plaćanja, i banke ohrabruju svoje klijente na sve širu i češću uporabu tih kartica u izvođenju raznih transakcija. Ipak, mislim da je i u tome važna prava mjera – kako se definira najniži iznos ograničenje troška po kartici. Primjerice, u Irskoj je to ograničenje postavljeno na trideset eura. To je dosta nisko. Zapravo, čuo sam za jedan pokušaj prijevare na tim karticama; riječ je bila o korisniku koji je pokušao resetirati ograničenje i tako, neovlašteno, izvući više novca. Ograničenje troška po kartici iznimno je važna stvar i bit će sve važnija u budućnosti. Ako je to ograničenje postavljeno visoko, to će tamniju stranu našeg društva navesti na zločin, navest će ih na pokušaj provale u sustav. Današnji bankarski sustav dovoljno je robusno zaštićen da se može oduprijeti takvim napadima.

Postoji li učinkovit način obrane od ransomware napada?

Znam da se Europol EC3 udružio s nekoliko proizvođača IT sigurnosnih rješenja i pokrenuo inicijativu koju su nazvali "no more ransom". Riječ je o sjajnoj inicijativi, s vlastitom internetskom stranicom, na kojoj možete pronaći razne sigurnosne alate. Softver za dešifriranje napadnutih računala možete pronaći i na stranicama proizvođača IT sigurnosnih rješenja, na internetskoj stranici Europola i vašeg Ministarstva unutrašnjih poslova, itd. *Ransomware* napadi mogu nanijeti velike štete u poslovanju. Unatoč tome što policija i druge agencije za provođenje zakona savjetuju žrtvama da ni slučajno ne plate otkupninu, nekoliko tvrtki u Ujedinjenom Kraljevstvu, Irskoj, Hrvatskoj i u drugim zemljama u Europi, podleglo je pritisku i platilo taj namet. Te tvrtke procijenile su da bi šteta nanesena njihovoj reputaciji bila prevelika kada bi se saznalo da su bile napadnute. Jednostavno, nisu htjele da javnost to sazna. Zastoji u poslovanju mogu biti vrlo skupi, gubici u intelektualnom vlasništvu iznimno veliki – toliko veliki da se ne mogu nadoknaditi. Zato moramo imati obzira prema tvrtkama koje su podlegle ucjeni – sve što su one željele bilo je nastaviti poslovati kao što su poslovale prije nego što su postale žrtve *ransomware* napada. Nadam se da su naučile lekciju te kako će se ubuduće bolje zaštititi.

ZAŠTITA KOŠTA

Imate li kakve procjene o gubicima koji su nastali kao posljedice kibernetičkih napada u Europi?

U GDPR popisu pravila ima zahtjeva koje će biti vrlo teško ispuniti, kako bankama, tako i drugim ustanovama i tvrtkama

Vrlo je teško tu istaknuti neki precizan broj. Europska bankovna federacija teško dolazi do tih podataka. Mnogo je jednostavnije ustanoviti kolike su štete od nekih tradicionalnih vrsta prijevara, jer o napadima izvedenima preko Interneta, banke i druge organizacije nerado govore. Mogu samo reći da je riječ o vrlo velikom broju te kako će on u neposrednoj budućnosti biti i veći. No, to nije puko ekonomsko pitanje. To je nešto čime se treba baviti cijelo društvo, jer su građani korisnici oni koji na kraju plaćaju taj trošak.

Dobro, koliko europske banke ulažu u kibernetičku sigurnost, barem u postotku godišnjeg prihoda?

Može se reći da su veće banke više fokusirane na zaštitu od kibernetičkih rizika i na samu internetsku sigurnost od manjih banaka, koje u to ulažu manje novca. To je jednostavno zato što manje banke imaju manje novca. Međutim, kad se gleda gospodarstvo u cjelini, bankarski sektor najviše ulaže u informatičku sigurnost. Ne bih baš rekao da je to deset posto ukupnog godišnjeg prihoda, naime, to je broj koji sam

DOBRI IZVORI INFORMACIJA O IT SIGURNOSTI NA INTERNETU

Što savjetujete onima koji žele poboljšati svoje znanje o informatičkoj sigurnosti, koga pratiti i čitati da bismo bili upućeni u najnovije događaje?

Gledajte što rade banke glede tog pitanja. Gotovo svaka banka ima posebnu internetsku stranicu posvećenu kibernetičkoj sigurnosti. Primjerice, u Hrvatskoj imate fantastičnu i nagrađivanu stranicu o internetskoj sigurnosti koju je pokrenula Hrvatska udruga banka – www.sigurnostnainternetu.hr. Na Internetu je dobro pratiti sve što napišu Brian Krebs (krebsonsecurity.com), zatim profesor Tyler Moore (tylermoore.ens.utulsa.edu) i Ross Anderson (www.cl.cam.ac.uk/~rja14). Neki njihovi radovi iznimno su zanimljivi. Posebno preporučujem dr. Mary Aiken (www.maryaiken.com) – kiber-psihologinju. Njene knjige pune su zanimljivih uvida. Internetske stranice proizvođača IT sigurnosnih rješenja dobar su izvor informacija o zaštiti na Internetu. Stranica organizacije Europol EC3 iznimno je dobar izvor informacija o kibernetičkoj sigurnosti. Njihov godišnji izvještaj o prijetnjama iOCTA – nezaobilazno je štivo. ◂

Mreža, 1.6.2017, str. 48, A3

Evidencijski broj / Article ID: 17390858
Vrsta novine / Frequency: Mjesečna
Zemlja porijekla / Country of origin: Hrvatska
Rubrika / Section:

NATO Cyber Article 5

/ Što mislite o kibernetičkom Članku 5 NATO pakta? Jesmo li blizu aktiviranja te klauzule?

Prema nekim procjenama, 90 posto sveg zloćudnog softvera koji se danas pojavljuje na Internetu svoje porijeklo ima u Rusiji. To moramo shvatiti vrlo ozbiljno. Neke zemlje, primjerice, još nisu potpisale Budimpeštanski sporazum (Budapest Convention – prvi je međunarodni sporazum o zločinu koji se izvodi preko Interneta i drugih računalnih mreža, nap. a.). To je problem. Moramo se zapitati jesu li spremne obraniti se od kibernetičkog napada? Jesu li spreme za borbu? Nadajmo se da će ubrzo biti. Svaka zemlja članica EU mora biti spremna za obranu od kibernetičkog napada.

nedavno čuo na jednoj konferenciji, prije će to biti oko dva posto ukupnog prihoda. To nije malo, no u tehnologije sigurnosne zaštite trebat će uložiti mnogo više. Zaštita košta – pogledajte koliko su banke nedavno potrošile na fizičku sigurnost svojih poslovnica, u mjere zaštite pristupa i videonadzor. Kibernetička zaštita će – posebno sada kad sve više banaka prelazi na nove tehnološke platforme i prolazi kroz procese digitalne transformacije – također biti iznimno visok trošak.

JA DANAS – TI SUTRA

Postoje li neke razlike u vrsti i tipu napada i internetskih prijetnji kad gledamo regije u Europi?

U našoj radnoj skupini za kibernetičku sigurnost često se pozivamo na poslovični izraz "ja danas, ti sutra". To znači da ono što je danas pogodilo neku banku u jednoj regiji ili zemlji Europske unije, sutra može pogoditi neku drugu banku u nekoj drugoj regiji ili zemlji. Kriminalci diljem svijeta koriste se više-manje istim alatima pa su im i metode napada vrlo slične. Toga stalno moramo biti svjesni. Moramo međusobno razmjenjivati sve podatke o napadima. Kako između država, tako i između pojedinih organizacija. Možemo se obraniti od svakog kibernetičkog napada ako se protiv toga borimo zajedno, i to ne samo bankarski sektor, već svi. Moramo razgovarati o tome. Svi, počevši od proizvođača IT sigurnosnih rješenja, telekomunikacijskih tvrtki, državnih agencija. Svi imamo propise i držimo se standarda, no iznimno je važno da o potencijalnim prijetnjama stalno razgovaramo.

Kad gledamo regulative, postoji li u propisima nešto što sprječava bolju informatičku sigurnosti?

Postoji. Riječ je o tome kako shvaćamo osobne podatke i privatnost korisnika, općenito. Propisi, sami za sebe, dobra su stvar, međutim, kad je riječ o provođenju istrage, o tome koje sve informacije trebamo dati na uvid policiji i drugim agencijama za provođenje zakona, moramo biti vrlo pažljivi. Neke od informacija koje banke imaju o svojim klijentima vrlo su osobne informacije. Banke bi morale dva puta promisliti prije nego što odluče dati takve podatke o svojim klijentima. Zaštita osobnih podataka klijenata iznimno je osjetljivo područje.

U tom smislu, što mislite o uredbi EU o zaštiti osobnih podataka (GDPR)? Kako će taj propis utjecati na banke?

Iznimno je dobro da imamo uniformirani popis pravila kad je zaštita podataka u pitanju. Međutim, u GDPR popisu pravila ima zahtjeva koje će biti vrlo teško ispuniti, kako bankama, tako i drugim ustanovama i tvrtkama. Primjerice, zahtjev da se regulator o napadu obavijesti u roku dva dana, vrlo je problematičan. Kako u tako kratkom roku možete ustanoviti o čemu je točno bila riječ? U dva dana ne možete steći potpunu sliku o incidentu. Slični zahtjevi postoje i u nekim drugim propisima kojih se banke moraju pridržavati pa držim da je to tema o kojoj još treba raspravljati.

BLOCKCHAIN, FINTECH, EDUKACIJA

Koliko građani EU znaju o zaštiti od kibernetičkih opasnosti? Jesu li dovoljno educirani?

Mislim da građani nisu dovoljno educirani. Posebno mlađe generacije. Mladi vrlo spretno rukuju novim tehnologijama, no nisu baš dobro upućeni u sve sigurnosne rizike kojima su izloženi, niti u metode kojima se mogu zaštititi. Primjerice, bez razmišljanja dijele informacije o sebi na društvenim mrežama, koriste iste lozinke za ulaz na više platformi. Kao da ih uopće ne zabrinjava to što bi netko mogao podatke koje su objavili zloupotrijebiti ili protiv njih samih, ili za izvedbu neke prijevare. Dakle, imamo mnogo posla u edukaciji građana. Svi u to moramo više ulagati. Banke također. One moraju više ulagati u edukaciju svojih klijenata, provoditi što više inicijativa kojima će svoje korisnike stalno osvještavati o potencijalnim prijetnjama. Svi, građani, tvrtke, banke, moraju biti svjesni rizika kojima se izlažu dok su na Internetu. Svatko bi trebao moći sam nadograditi softver koji koristi, svatko bi morao paziti na svoje financijske podatke, i općenito, svi stalno moramo biti svjesni okoline u kojoj živimo i radimo. Ljudi se moraju zapitati – je li stvar baš toliko hitna da svom internetskom bankovnom računu želim pristupiti preko javne Wi-Fi mreže? Pa, nikad to nije toliko hitno. Brojni su vektori iz kojih može doći kibernetički napad: preko osobnog ili tablet računala koje koristite doma ili na poslu, preko vašeg pametnog mobitela, pa čak i preko novih, pametnih televizora. Mali poduzetnici segment su kojem banke moraju posvetiti posebnu pozornost. U Ujedinjenom Kraljevstvu i Irskoj mnoge banke imaju posebne internetske programe za takve klijente. Stalna edukacija korisnika nužna je u današnjem sve digitaliziranijem svijetu. Uz to, edukacija mora biti rezultat zajedničkih napora banaka, IT sigurnosnih tvrtki i državnih agencija. Kad je informatička, kibernetička sigurnost u pitanju, nikad ne možete biti previše educirani.

Odbor za Kibernetičku sigurnost Europske bankovne federacije

/ Zagrebačka sjednica Odbora za kibernetičku sigurnost Europske bankovne federacije bila je posvećena Godišnjem sigurnosnom izvještaju Europske bankovne federacije, razgovorima o suradnji Federacije i Europske agencije za informacijsku i mrežnu sigurnost (ENISA) te o planu rada EBF Cyber Security radne skupine za 2017. godinu. Sjednici su prisustvovali i gosti predavači iz Europola EC3 i FS ISAC-a, prezentirana je nizozemska inicijativa TIBER (Threat Intelligence Based Ethical Red Teaming) te projekt LEET (Security rating and labelling) i EU OF2CEN. Međunarodni *cyber* stručnjaci od predstavnika našeg Ministarstva unutarnjih poslova imali su priliku čuti i hrvatska iskustva u pogledu zaštite od kibernetičkog kriminala, a predstavljeni su i dosadašnji rezultati domaćeg Odbora za sigurnost Hrvatske udruge banaka. Na sjednici, održanoj u hotelu Dubrovnik u Zagrebu, u prvom tjednu travnja, sudjelovali su brojni članovi Odbora – od predstavnika Irske (predsjednika Odbora, Keitha Grossa) do članova iz Španjolske, Belgije, Bugarske, Češke, Danske, Francuske, Njemačke, Italije, Latvije, Lihtenštajna, Luksemburga, Nizozemske i Portugala.

Mreža, 1.6.2017, str. 49, A3

Evidencijski broj / Article ID: 17390858
Vrsta novine / Frequency: Mjesečna
Zemlja porijekla / Country of origin: Hrvatska
Rubrika / Section:

U Hrvatskoj imate fantastičnu i nagrađivanu stranicu o internetskoj sigurnosti koju je pokrenula Hrvatska udruga banka – www.sigurnostnainternetu.hr

Što mislite o blockchain tehnologiji kao sigurnosnoj tehnologiji? Je li to pravo rješenje?

Rizici su svugdje oko nas i mislim da još nije smišljeno nešto što bismo mogli nazvati sto posto sigurnim. *Blockchain* tehnologija razvoj je u dobrom smjeru – mnoge banke u Europi rade na tome, zajedno s informatičkim tvrtkama partnerima i pokreću laboratorije u kojima iskušavaju sve njene mogućnosti. *Blockchain* će bankama donijeti novu razinu učinkovitosti, prvo interno, u nekim aspektima poslovanja između samih banaka, a onda kasnije, u razvoju novih, i na *blockchainu* utemeljenih usluga za klijente.

Banke i fintech – što su sigurnosni izazovi tog trenda?

Mislim da banke trebaju što više surađivati s financijsko-tehnološkim *startupima*. Mnoge to već čine. To je pravi put. Suradnja banaka i *fintech* tvrtki strategija je koja nas vodi prema naprijed, i koja će naposljetku rezultirati brojnim dobrobitima za korisnike. Naposljetku, sve što radimo – radimo zbog korisnika.

Prema vašem mišljenju, što će biti najveće prijetnje financijskim ustanovama u sljedeće tri godine?

Tu nije potrebno biti prorok. Kriminalci uvijek slijede novac. Oni su dobro umrežena ekipa. Zato, kako bismo im se mogli suprotstaviti, i mi – banke, telekomunikacijske tvrtke i pružatelji pristupa Internetu, državne agencije – moramo postati dobro umrežena ekipa. Moramo se još bolje povezati. Kako banke međusobno, tako i razne industrije međusobno, i države, preko svojih granica. Povezivanje i suradnja najvažnija su stvar kad treba razmijeniti "obavještajne podatke" o incidentima i počiniteljima. Samo zajedno možemo se oduprijeti tim napasnicima – zajedno, svi dionici: banke, IT sektori, državne agencije, regulatori, Europol, EC3, države članice Europske unije. Ako se budemo držali zajedno, moći ćemo se suprotstaviti svakoj budućoj prijetnji.

Prema nekim procjenama, 90 posto sveg zloćudnog softvera koji se danas pojavljuje na Internetu ima svoje porijeklo u Rusiji. To moramo shvatiti vrlo ozbiljno