Što zapravo znači "prihvaćanje rizika"?

Danas je petak 13-ti, dan kada se, po pučkoj predaji događaju nesreće. Ovu kolumnu posvećenu informacijskoj sigurnosti nazvali smo Petak 13. Objavljujemo članke svakog trinaestog u mjesecu. Dok sve radi kako treba, o sigurnosti i ne razmišljamo. Problemi se događaju drugima, tamo negdje daleko. Pitalo me nekoliko kolega zašto sam, zaboga, za piktogram rubrike odabrao djetelinu s četiri lista? Šala mala, odgovaram, ali velika istina! Većina ustanova iz Akademije oslanja se na sreću, računaju na da su premali i da nemaju važne podatke, beznačajne su mete, pa zašto bi onda brinuli o sigurnosti i ulagali u nju? Neće baš njih zadesiti peh, zar ne?

Stručan izraz, da ne kažemo znanstven, za takav pristup je "prihvaćanje rizika". Ne ulažemo u zaštitu, radije prihvaćamo rizik. Kako voli reći prijatelj i kolega Kost, "Da nas mogu naći na karti svijeta, možda bi nas napadali, ovako smo sigurni." :)

Ali za dva dana naši će nogometaši postati svjetski prvaci (ja držim palčeve, a i vi, siguran sam), a onda će nas svi potražiti na karti svijeta. Što ćemo tada sa informacijskom sigurnošću?

Što se to događa na "petak 13.", kakve se havarije,makar u malim razmjerima, događaju u ovom zabačenom raju na zemlji?

Nedavni pokušaj spašavanja poslovnih podataka male privatne tvrtke, čiji mi se vlasnik obratio za pomoć, ponukao me da još jednom promislim cijeli postupak zaštite vrijednih podataka koje svi mi, i informatičari i korisnici, čuvamo na računalima. Tko je odgovoran za zaštitu podataka, te koja je pri tome uloga sistemca - to su dva pitanja na koja prije svega želimo jasan odgovor.

Nažalost nisam uspio spasiti podatke spomenute privatne tvrtke. Najprije je otišla matična ploča, stara barem desetak godina. Na njoj je bio PATA disk kontroler, i dva PATA diska od kojih je samo jedan radio. Tko se još sjeća PATA diskova? Paralelni ATA bio je prijelazna tehnologija od ATA do SATA diskova (serial ATA). Drugi disk bio je posve "mrtav", nije mu se moglo pristupiti ni na fizičkoj razini. Nazivajući kolege koji su u mirovini, uspio sam pronaći, na nečijem tavanu, računalo s PATA kontrolerom. Kad smo u njega prebacili diskove, učitao se DOS i pokrenula knjigovodstvena aplikacija. Prebacili smo u novo kućište iOmega ZIP drive, s disketama od 100 MB (sjećate li se toga?), na kojeg su snimani backupi. Vlasnik je bio sretan da mu aplikacija radi, odnio je odmah računalo jer mu je trebalo za rad. Upozorio sam ga da bi najprije trebalo napraviti kopiju cijelog sadržaja diska. Obećao je da će se javiti. Nije se javio, sve dok mu i tvrdi disk nije otkazao. Tada mi je ponovo donio računalo. Disku se moglo pristupiti na fizičkoj razini, napravio sam bitcopy cijelog diska koristeći ddrescue. No disk je velik 10 GB, a preslika koju sam dobio imala je samo 3 GB! Iz nje se nije moglo izvući niti jednu datoteku koja bi imala veze s poslom. Vlasnik je fakture, primke i otpremnice nastavio pisati "ručno", u tekst procesoru. Nije mu preostalo drugo nego kupiti novu aplikaciju, unijeti početno stanje iz lanjske bilance, pa zatim ponovo utipkati sve ovogodišnje dokumente iz registratora. Bio je toliko očajan da nije ni došao po staro računalo.

Tko je tu "kriv" za gubitak podataka? Sam vlasnik, bez ikakve sumnje. Spremao se u mirovinu, nadao se da će računalo izdržati dok ne rasproda svu robu sa skladišta. Nije razmislio o riziku koji predstavlja prastaro računalo koje može svakog časa otkazati. Štoviše, programer koji mu je prodao aplikaciju preminuo je prije nekoliko godina. Rekao sam mu da je istog časa trebao prijeći na novu aplikaciju, jer što vrijedi aplikacija bez podrške? Ali to bi bio dodatni trošak, a trošak je nešto što treba izbjeći po svaku cijenu. Uzdamo se u sreću, "prihvaćamo rizik".

Kolika je u svemu tome moja krivica? Odgovoran sam jer sam mu dozvolio da odnese računalo nakon prvog popravka, a da nisam odmah napravio presliku tvrdog diska, dok je još radio. No pitanje je da li bi aplikacija radila da smo presliku naprosto prebacili na drugi disk, jer su u dobra stara vremena DOS-a programeri u aplikacije ugrađivali zaštitu od kopiranja. Naime aplikacija je radila samo na disku na kojeg ju je instalirao vlasnik programa. Prebacivanje na drugo računalo trebao je obaviti sam vlasnik programa, za što je, naravno, tražio novčanu naknadu. A to je, naravno, nepotreban trošak. Tek kad nas pogodi nesreća, Petak 13-ti, dosjetimo se kamo vodi prevelika štednja. Onda se sjetimo i one Engleske poslovice: "Nisam dovoljno bogat da kupujem jeftino."

Mnogo sam puta, radeći u akademskoj zajednici, vodio slične razgovore kao s vlasnikom spomenute tvrtke. Objašnjavo sam upravi da je potrebno raditi dnevni, tjedni, mjesečni, godišnji backup svih podataka važnih za poslovanje. Načelno bi se složili, zatražili pismeno obrazloženje i nekoliko ponuda, a onda bi sve zapelo na novcima. Novca nema dovoljno ni za hladni pogon, a pogotovo za nešto što bi se jednog dana možda moglo dogoditi. Možda ćemo imati sreću, možda neće nesreća pogoditi baš nas... itd. its. Prihvatit ćemo rizik. A kad se nesreća dogodi, trošak je mnogo veći nego da se reagiralo na vrijeme. Ali tako je kako je, još nikdar ni bilo da nekak ni bilo... Pak nikdar ne bu da nekak ne bu... Snaći ćemo se, na ovaj ili onaj način.

Na jednom od prethodnih poslova, ustanova je dobila novi server od Ministarstva. Podigao sam na njemu virtualnu mašinu, Linux, na njega instalirao aplikaciju Backup-PC, podesio servere i korisnička računala tako da dopuštaju pristup *backup daemonu* s te virtualke i naprave dnevni backup podataka. Na klijentska računala nije trebalo instalirati klijentsku aplikaciju, samo podesiti dozvole za pristup. Korisnicima sam objasnio da u svojoj Documents mapi imaju mapu koja se zove Poslovno, neka u nju spremaju sve što im je važno da se sačuva. Iznenadio sam se tada jer većinu korisnika to uopće nije zanimalo! Oni spremaju sve što im je važno na USB stickove, na svoje vlastite vanjske diskove. Svjesni, savjesni korisnici, zar ne? Ali zašto su mi povremeno neki od njih donosili svoje USB stikove i vanjske diskove koji više ne rade, molili me da im pokušam spasiti podatke? Ako se uređaju moglo pristupiti na fizičkoj razini, uspijevao sam spasiti bar nešto. U protivinom... Upravo radi toga želio sam problem, kao pravi sitemac, riješiti "sistemski". S polovičnim rezultatom.

Zaključio sam da korisnici ne žele "službeni backup" je ne žele da itko u ustanovi, ni informatičari ni uprava, vidi što oni rade dok su na poslu. Vjerojatno zato jer rade neke poslove u fušu? Nije me to zanimalo. Bio sam im spreman ponuditi backup svih važnih podataka, ne razmišljajući o tome o da li se radi o "službenim" ili "neslužbenim" podacima.

Satisfakciju sam, moralnu, dobio dvije, tri godine nakon što sam promijenio posao. Pokvarilo se računalo na kojem su bili pohranjeni svi znanstveni radovi nastali od početka postojanja ustanove! Moj je nasljednik uspio sa backup servera spasiti i vratiti na novo računalo sve vrijedne podatke! Nazvao me da me obavijesti o tome, na posredan način mi je zahvalio. Bilo bi lijepo da me nazvao ravnatelj, ali što se tu može.

Dakle tko je u akademskoj ustanovi zadužen za brigu o vrijednim podacima? Ako se spremate na to pitanje odgovoriti "sistemac", niste u pravu. Amerikanci bi rekli da je za podatke odgovoran njihov "vlasnik" (owner). Za knjigovodstvene podatke odgovoran je šef računovodstva ili financijski direktor. Za osobne podatke odgovara osoba koja je za tu funkciju prijavljena Agenciji za zaštitu osobnih podataka. Za znanstvene radove u digitalnom obliku također treba naći "vlasnika". Ne volim taj izraz, "vlasnik", jer na primjer knjižničarka nije vlasnik znanstvenih radova, ona samo brine za njihovo čuvanje. Kad se kaže vlasnik, radi se zapravo o psihološkom triku, jer ljudi bolje brinu o stvarima koje su njihovo vlasništvo, nego o tuđima. Ni financijski direktor nije vlasnik knjigovodstvenih podataka, on je samo zadužen da brine o njima. Dakle kad vam netko dodijeli takvo "vlasništvo", samo je na vas prebacio brigu i odgovornost.

No dobro, vratimo se pitanju: tko je zadužen za brigu o podacima? U pravilu, zaposlenik u čiji to opis posla spada. On je taj koji bi sistemca trebao pitati da li se backup podataka obavlja redovito, te kada je zadnji puta pokušao napraviti "restore" iz "backupa". Sistemac će se pobrinuti da stvari funkcioniraju na tehničkoj razini. Ako nešto zapne na tehničkoj razini, bit će odgovoran sistemac. Ali "Vlasnik" podataka treba se pobrinuti za zaštitu, čiji je dio i "vježba" u kojoj će se simulirati havarija na serveru, gubitak podataka, pokretanje rezervnog servera i vraćanje podataka. Sistemac je tu

samo tehnička podrška. Ali kako stvari stoje u Akedemiji, sistemac je tu usamljeni vitez koji bi htio na sebe preuzeti i tuđu brigu. Svaki savjestan i brižan sistemac brine o tome da svi serveri/servisi, pa i mreža rade kako treba. On predviđa i mogućnost havarije, pa je nastoji preduhitriti. Ali uprava ne misli na isti način. Dapaće, cijelo moje iskustvo CARNetova sistemca govori mi da je Uprava često zapreka i najveća smetnja pravo brizi za informacijsku sigurnost. Uprava je ta koja se oslanja na djetelinu s četiri lista i prihvaća rizike.

Prvi problem u vrednovanju podataka je njihova klasificija. Podatke koje koristi akademska zajednica može klasificirati kao tajnu samo nadležno Ministarstvo. Dekan/ravnatelj može nekim podacima dodijeliti status poslovne tajne. Iako se za tim nekako nerado posiže u Akademiji, koja se diči otvorenošću. Javlja se problem da li su podaci koje proizvode neko istraživanje javni, samo zato jer Ministarstvo znanosti financira hladni pogon ustanove? A što ako je ustanova u potpunosti ili djelomično sama financirala neko istraživanje? Tko onda ima pravo proglasiti te podatke javnima? Pogotovo danas, kad se teži tome da se Akademija poveže s privredom, da se sve većim dijelom financira iz vlastitih prihoda?

Sjećam se predavanja direktora britanskog Geološkog društva (Geological Survey), kojem sam imao čast prisustvovati. Njima država financira 70% (ako se dobro sjećam) hladnog pogona. Ostatak moraju zaraditi sami na tržištu. No Velika Britanija je zrelo društvo koje je u stanju procijeniti važnost znanja i znanosti. Zakonom je propisano da svi koji obavljaju geološka ispitivanja moraju uzorke i rezultate predati u tu državnu ustanovu, kojoj su na "zelenoj livadi" (greenfield investicija) izgradili cijeli mali grad sa skladištima u kojima se čuvaju uzorci. Kako tehnika napreduje, stari se uzorci mogu ispitati novim metodama i dobiti još bolje rezultate. Geološka služba Ujedinjenog Kraljevstva pruža 24-satno dežurstvo i svima je na raspolaganju u slučaju potrebe. Na primjer, kad je harala epidemija slinavke, vojska je eutanazirala cijela stada, ali nisu smjeli zakopavati leševe gdje im padne na pamet. Geološka služba im je davala lokacije gdje je tlo nepropusno, a zemljište državno. Na taj su način spriječili zagađivanje podzemnih voda. Kod nas nema takvih zakona, pa su podaci koji je imala INA otišli Mađarima, a Hrvatske geološki institut ih nije dobio. Ovome ne treba komentara.

Zato prije nego počnemo grditi spomenutog privatnika kako je dozvolio da mu radi prevelike štednje propadnu podaci bez kojih ne može poslovati, trebamo se zapitati nije li to zapravo simptomatično za cijelo naše društvo? Cijenimo li mi svoje podatke onoliko koliko oni to zaslužuju? To nisu problemi kojima bi glavu trebao razbijati sistemac. Ali htio, ne htio, često je baš sistemac u poziciji da ljudima oko sebe objašnjava koliko su vrijedni podaci i što bi trebalo napraviti da se oni zaštite. No sistemac, sam protiv svih, ne može mnogo. To ne znači da treba odustati, zar ne?

pet, 2018-07-13 21:06 - Aco Dmitrović**Kategorije:** Kolumna [1]
Vote: 0

No votes yet

story_tag: rizik [2]
klasificiranje podataka [3]
backup [4]

Source URL: https://sysportal.carnet.hr/node/1815?page=0

Links
[1] https://sysportal.carnet.hr/taxonomy/term/71
[2] https://sysportal.carnet.hr/taxonomy/term/258
[3] https://sysportal.carnet.hr/taxonomy/term/257
[4] https://sysportal.carnet.hr/taxonomy/term/147