Ljudska strana sigurnosti

Sistemac, kao pravi *techie*, gleda na informacijsku sigurnost kao na tehnički problem: o sigurnosti brinu uređaji, poput vatrozida, e-mail gatewaya, softver koji blokira viruse, maliciozne web stranice itd. Doduše svi znamo da sigurnost ima i svoju ljudsku komponentu, ali linijom svog obrazovanja tehničari nisu toliko vješti u rješavanju problema s ljudima.

Nedavno sam na jednom forumu čitao raspravu koja me navela na razmišljanje. Na *Academia Stack Exchange* jedan je sudionik postavio pitanje: "Je li u redu odbiti laptop koji mi daje sveučilište ako već imam svoj privatni?"

Prevedeno u naše okolnosti, ova dilema izaziva smiješak. Kakvo je to pitanje? Glupo je odbiti računalo koje ti daje fakultet. Uostalom, zašto bi uopće sveučilište davalo svojim studentima računala? Kod nas toga nema, zar ne? Zaboravljamo da se vani studij plaća, pa je trošak računala pokriven. Tim je gluplje odbiti računalo koje si zapravo već platio. Laptop je nastavno sredstvo, studenti na njemu pišu radove, šalju ih profesorima, rješavaju on line testove, dohvaćaju gradivo koje je objavljeno na webu fakulteta...

S druge strane, neki od nas su mrzovoljni jer moraju nositi dva mobitela, privatni i službeni. Laptop je još glomaznija sprava, zašto nositi sa sobom dva? Nekako mi se čini da bi kod nas većina to riješila tako što bi privatni laptop spremila na policu i trošila "službeni".

U nas se još uvijek teško razdvaja privatno i poslovno. S posla se obavljaju privatni telefonski pozivi, na službeni mail dobijamo privatne poruke, softver koji nam je dala organizacija za koju radimo koristi se za poslove "sa strane". Sveučilišni profesori sredstvima projekta kupuju računala i nose ih kući, ponekad ih ne prijavljuju kao osnovna sredstva svog fakulteta. Itd. its.

No vratimo se raspravi na spomenutom forumu. Zanimljiva je, pomalo me podsjeća na Platonove dijaloge (ako ih niste čitali, eto zanimljivog štiva za ljeto).

Dakle glavni lik ovog dijaloga rado bi odbio "službeno" računalo i radio sa svojim privatnim. Jedan sugovornik mu sugerira da to ovisi o tome na koje se sveučilište upisao. U SAD "privilegirane informacije" raznih vrsta ne bi se smjele držati na privatnim računalima, već samo na onima koja su u vlasništvu institucije koja se brine o njihovom održavanju. Korisnik se može naći u nevolji ako loše administrira svoje računalo koje radi toga ne zadovoljava sigurnosne standarde. Isto se odnosi na e-mail, jer su poruke na mail serveru podložne raznim pretraživanjima bez nekog opravdanog razloga. Njegovi kolege ne raspravljaju mailom o osjetljivim temama, jer je u sigurnosnoj politici navedeno da se poruke ne smiju brisati, već se čuvaju "zauvijek".

Glavni lik na to izražava čuđenje. On smatra da sveučilišta trebaju imati "snažan osjećaj slobode razmjenjivanja ideja bez straha od represalija".

U raspravu se uključuje treći sudionik, s donekle kompromisnim stavom: to su objavljena pravila koja se u praksi baš i ne provode. Donesena su radi pravne zaštite institucije u slučaju da dogodi nešto loše. Sveučilište time "covered its @$$" legally" upozorivši korisnike da su sami odgovorni ako su u prekršaju. Ako imate sreće, ništa se loše neće dogoditi, ali sami trebamo procijeniti u kakav bi loš scenarij mogli biti upleteni u slučaju problema.

Ostali postavljaju valjana pitanja: što ako izgubiš, ili razbiješ službeno računalo? Hoćeš li morati

nadoknaditi štetu? A što je sa licencama za software? Ugovorima se mogu dati ***edu*** popusti, ali samo za računala koja su u vlasništvu obrazovne ustanove. U tom slučaju student ne bi imao pravo instalirati programe koji mu trebaju za studij na svoje privatno računalo, odnosno morao bi za njih platiti punu cijenu.

U raspravu se uključuje novi sudionik sa zanimljivim primjerom. Imali su slučaj čovjeka koji je preminuo na poslu. Sveučilište mu je dalo dva diska (particije?), jedan za službene i drugi za privatne stvari. No on je na mrežnom disku čuvao backup svega zajedno, što je stvorilo pravnu zavrzlamu. Napravili su popis datoteka, a zatim su uz prisustvo predstavnika uprave, pravnika Sveučilišta i izvršitelja oporuke imali jedan sat da preuzmu datoteke koje su bile potrebne instituciji. Nakon toga sve je bilo zapečaćeno i spremljeno za narednih 50 godina. Sudionik kaže da ne radi u SAD, takvi su njihovi lokalni zakoni. Ne kaže gdje živi.

Uh! Zna li itko kakvi su naši lokalni zakoni po tom pitanju? Imaju li vaše institucije uopće donesenu sigurnosnu politiku? Je li država nešto regulirala? Kakvi su ugovori Ministarstva s dobavljačima softvera koji koriste studenti/zaposlenici/postdiplomci?

U diskusiju se umiješao (čini se pravnik, ili sigurnjak) koji je lijepo sistematizirao cijelu problematiku. Evo, ukratko, kako je on postavio stvari:

- Svima savjetuje da strogo odvajaju poslovno i privatno, iz pravnih razloga.
- Poslodavac je vlasnik službenog računala i može ga "konfiscirati" u bilo kom trenutku, iz bilo kakvih razloga. Prema tome morate prihvatiti činjenicu da poslodavac ima pristup vašim privatnim podacima na tom računalu. To može biti porezna prijava, privatna korespodencija, prijave za posao kod konkurentske tvrtke, kritički osvrti na upravu itd. its.
- Ako radite nešto "sa strane", kako bi se kod nas reklo, poslodavac može polagati intelektualna prava na sve što se nalazi na službenom računalu.
- Poslodavac u nastavi koristi softver za koji ima specifičnu, najčešće "site licencu", što bi značilo da se taj softver može instalirati na računala u vlasništvu poslodavca i koristiti samo za vrijeme studija - ako ste ga instalirali na privatno računalo u prekršaju ste, pogotovo ako ga koristite nakon gubitka studentskih prava.
- Osim na aplikacije, to se može odnositi i na operativni sustav, VPN klijente za spajanje u sveučlišnu mrežu, uredske programe itd.

U svakom slučaju, korištenje privatnog računala za poslovne svrhe izaziva cijeli niz pravnih rizika. Diskusija završava umirujućim savjetom: najbolje se raspitati na fakultetu koje su implikacije korištenja privatnog računala, pa ako vam oni kažu da to nije pametno, navedu radi čega, onda prihvatiti službeno računalo.

Izgleda li vam sve ovo kao SciFi? Ili se i u vašoj poslovnoj sredini događaju slični problemi? U svakom slučaju, mi *techies* s manje ili više lakoće rješavamo tehničke probleme, dok nam *humanware* zadaje više muke i tu nam treba pomoć uprave koja stvari treba postaviti na mjesto.

Mediji su nas preko vikenda zasipali upozorenjima o novoj *ransomware* napasti koja hara svijetom. Upozorili su nas da pazimo kad u ponedeljak uključimo računalo, da ne bi izgubili datoteke. Uglavnom su prećutali da je crv napravljen koristeći softver koji je procurio iz NSA, te da je Microsoft već izdao zakrpu u ožujku (prema tome ste, kao sami krivi ako ste pokupili *malware*). Pristalice teorije zavjere sad pričaju kako je zakrpa izdana tek kad se saznalo da je NSA izgubila svoj "metasploit".

Zapitajte se što bi se desilo da vam ***WannaCry*** zakriptira službene dokumente na vašem privatnom računalu? Da li bi vaša ustanova platila da ih dobije nazad? Vjerojatno ne bi, nego bi vas smatrali odgovornim za taj incident. Ako se to dogodi na službenom računalu, onda će osoblje koje održava računala morati objašnjavati što su poduzeli da se incident spriječi. Kako god, ispada da je zdravo odvajati službeno i privatno, posao i hobi, koliko god nekima od nas teško padala takva podvojenost ličnosti.

Radoznalci mogu pogledati raspravu na ovom linku [1].

sub, 2017-05-13 13:38 - Aco Dmitrović**Kategorije:** Kolumna [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: informacijska sigurnost [3]

Source URL: https://sysportal.carnet.hr/node/1739

Links
[1] http://academia.stackexchange.com/questions/87241/is-it-okay-to-refuse-a-laptop-from-a-new-university-if-you-already-have-your-own
[2] https://sysportal.carnet.hr/taxonomy/term/71
[3] https://sysportal.carnet.hr/taxonomy/term/101