

Blog Eugenena Kasperskya: <http://eugene.kaspersky.com/>

## Hibridi so »kul«, hibridi so super. Kaj pa hibridna zaščita?

Že nekaj časa je precej govora o tem, kako lahko tehnologije v oblaku povečajo zaščito proti zlonamernim programjem. Eno od skrajnih prepričanj je, da lahko oblak učinkovito reši vse varnostne probleme naenkrat.

Strinjam se, da imajo varnostne rešitve, ki vključujejo tehnologije v oblaku, številne prednosti tako za končne uporabnike kot tudi ponudnike. Omogočajo hitrejša zaznavanja groženj, hkrati pa uporabnikom zagotavlja tudi potrebne posodobitve. Kljub temu, pa nisem zagovornik evforije, ki promovira ta pristop kot samozadostno tehniko, zmožno samostojnega upravljanja z varnostnimi grožnjami. Zaščita mora biti več plastna in vsak plast mora dopolnjevati ostale. Prispevati mora k celotni zaščiti in ščititi računalnik v kateremkoli okolju, oboje pa mora biti uravnoteženo, tako da ohranja optimalno delovanje računalnika.

Obstajajo trije glavni dejavniki, ki močno omejujejo obseg delovanja zaščite v oblaku, ko ta deluje neodvisno od ostalih oblik zaščite.

**Prvič**, razpoložljivost. Zaščita na osnovi tehnologije oblaka deluje le, ko je računalnik povezan v splet. Ko se povezava prekine, postane ranljiv za raznolike lokalne grožnje. Na primer, pomnilniški ključ (USB) lahko z lahkoto okuži računalnik z zlonamernimi programi, ki se namestijo sami. Zlonamerne vsebine so lahko prisotne tudi na zgoščenkah in DVD-jih, prenesejo pa se lahko tudi ob sinhronizaciji ali izmenjavi podatkov z drugimi računalniki.

**Drugič**, sama narava zaščite v oblaku. Poenostavimo: nikoli ne moremo biti sto odstotno prepričani, da je oblak sam po sebi povsem imun na varnostne napade. Pravzaprav o nasprotnem priča nedavni incident s Sony Playstation Network (več o tem lahko preberete [tukaj](#), [tukaj](#) in [tukaj](#)) – oblak postaja glavna tarča hekerjev. Brez zaščite vsakega računalnika oz. delovne postaje, lahko en sam vdor v oblak takoj zruši celotno zaščito naprave, slednja pa ostane brez varnostnih alternativ. Vdor v oblak lahko hekerjem omogoči pridobitev nadzora nad celotnim oblakom, odvisno od načina interakcije oblaka z napravami. Nenazadnje, pomanjkljiva zaščita računalnikov pomeni pomanjkljivost v samoobrambi oblaka, kar lahko zlonamernim programom omogoči, da preprečujejo dostop do oblaka.

**Tretjič**, zaščito, zaznavanje in odstavitev zlonamerne programske opreme za pridobitev skrbniškega nadzora, polimorfnih ter ostalih visoko sofisticiranih zlonamernih programov, je izjemno težko, če celo nemogoče izpeljati zgolj z zaščito v oblaku. Še vedno je potrebna tudi močna zaščita na končnih napravah, odlikovati pa jo mora globoka integracija z operacijskim sistemom.

*Naj še enkrat ponovim: Všeč mi je ideja oblaka, ne strinjam pa se z idejo zanašanja zgolj in samo na to rešitev.*

Za zagotavljanje maksimalne zaščite uporabniki potrebujejo tako tehnologijo v oblaku kot tudi lokalno prisotne rešitve, ki niso odvisne od povezave s spletom. Dvomim, da bo v bližnji prihodnosti mogoče takšno kombinacijo nadomestiti zgolj z oblakom. Tudi če dosežemo popolno globalno pokritost s spletom in morda celo sto odstotno pokritost z zaščito v oblaku, bodo vedno obstajali lokalni varnostni problemi in seveda sofisticirani zlonamerni programi, katerih se lahko lotimo le z močno zaščito naprav.

Točno to pa počne naša [hibridna zaščita](#). Združuje najboljše aspekte »obeh svetov«. Zato so hibridi »kul« in super: [http://www.youtube.com/wa\\_tch?v=jbY0GAE77k4](http://www.youtube.com/wa_tch?v=jbY0GAE77k4).

---

Z veseljem vas obveščam, da bo hibridna zaščita odlikovala tudi prihajajočo različico [rešitev za podjetja](#), ki jo bomo v Kaspersky Labu naznanili v oktobru.