Superračunalniki za boj s koronavirusom

Bitke z boleznijo COVID-19 ne bijejo le pacienti in zdravstveno osebje, temveč tudi znanstveniki. Številna tehnološka podjetja in druge organizacije so se zato odločili, da jim odstopijo več zmogljivosti svojih superračunalnikov za namene analize virusa in iskanja zdravila zanj.

Novoustanovljeni konzorcij visoko zmogljivega računalništva za boj s COVID-19, ki vključuje IT-velikane Amazon, Google, Hewlett Packard Enterprise, IBM in Microsoft ter številne druge organizacije, je znanstvenikom omogočil dostop do izjemnih računalniških zmogljivosti. Znanstvenikom je na voljo kar 16 superračunalniških sistemov s skupaj 775.000 procesorskimi jedri in 34.000 grafičnimi procesorji, ki lahko izvedejo približno 330 trilijonov operacij s plavajočo vejico na sekundo (330 petaflops). Amazon Web Services (AWS) je še dodatno sprožil pobudo v vrednosti 20 milijonov dolarjev za boj proti COVID-19, ter raziskovalnim ustanovam in podjetjem podaril tehnično podporo in promocijske kredite za uporabo programov AWS za namen raziskav na področju diagnoze, zdravljenja in priprave cepiva.

Socialni inženiring je v času karantene še pogostejši

Kot smo že poudarili, je potrebno tudi v času, ko delamo od doma, veliko pozornosti posvetiti kibernetski varnosti. Tokrat bomo dali poudarek socialnemu inženiringu, ki smo mu sedaj še bolj izpostavljeni, saj praktično cel delavnik preživimo za računalnikom, na internetu.

Kako testiranje poteka?

Z izvedbo simulacije socialnega inženiringa preverimo stopnjo ozaveščenosti in usposobljenosti vaših zaposlenih, katerim lahko glede na predhodni dogovor pošljemo:

- *elektronsko sporočilo z navidezno zlonamerno povezavo (Phishing)*
- *elektronsko sporočilo z navidezno zlonamerno priponko (macroji)*

Na pred pripravljenem okolju beležimo koliko uporabnikov je kliknilo na povezavo, koliko uporabnikov je vpisalo svoje podatke na phishing strani in koliko uporabnikov je odprlo navidezno zlonamerno priponko.

Simulacija socialnega inženiringa je kritična komponenta pri ocenjevanju stopnje informacijske varnosti, saj pripomore k identifikaciji tveganj in ranljivosti v organizaciji, ki se jih ne da odpraviti s tehničnimi rešitvami, kot so požarni zidovi ali sistemi za preprečevanje vdorov. Organizacije, ki izvajajo simulacije socialnega inženiringa, drastično zmanjšajo možnosti za uspešnost napadov in posledičnega odtekanja občutljivih podatkov.

Zbral in za objavo pripravil: ***Boris Kožlin, PRU in ROID***