Da li je poslodavac dužan da obezbedi HTZ opremu za rad od kuće?

Piše: Branko Pavlović, *predsednik Udruženja aktuara Srbije*

Pojedini zaposleni koji rade od kuće na svojoj opremi, za posao koriste servise i aplikacije koje IT stručnjaci njihovih kompanija nisu odobrili, kao na primer servise za video konferencije, dopisivanje ili skladištenje fajlova. Pored nepouzdanosti servisa i rizika od mogućeg gubitka podataka, zaposleni na taj način dovode kompaniju u opasnost od kazni za korišćenje servisa u poslovne svrhe bez plaćanja licenci ili sa neodgovarajućim načinom licenciranja

Iako pitanje iz naslova zvuči kao šala, zahvaljujući presudi ciriškog kantonalnog suda u Švajcarskoj da je poslodavac dužan da plati deo kirije zaposlenima koji rade od kuće, eksperti za radno pravo smatraju da je poslodavac dužan da obezbedi zaposlenima odgovarajuću opremu za rad od kuće, uključujući kancelarijsku stolicu. *Bez obzira na to šta je sve poslodavac* dužan da obezbedi zaposlenima koji rade od kuće, postavlja se pitanje kako da se poslodavac obezbedi da kompanija ne postane žrtva povećanih IT rizika zbog rada od kuće.

Popularnost i masovnost rada od kuće, koju je uslovila pandemija, donosi mnoge novosti. Dok određenoj grupi zaposlenih, koja štedi vreme za putovanje do radnog mesta, rad od kuće odgovara, drugi koji imaju velike obaveze oko dece, jedva čekaju da se vrate u kancelariju. Ipak, svi zaposleni pomalo brinu da li će imati gde da se vrate kada pandemija prođe, ili će samo u jednom trenutku biti obavešteni da njihova radna mesta više ne postoje.

S druge strane, poslodavci delimično gube kontrolu nad produktivnošću zaposlenih, ali zato štede na troškovima zakupa prostora, struje, itd. Novi način rada od kuće velikog broja zaposlenih donosi nove IT rizike i pojačava brigu zbog povećanja intenziteta poznatih rizika. Ranjivost kompanija na poznate hakerske tehnike kao što su ransomware i phishing je značajno porasla.

Ransomver (od engl. ransome što znači ucena) je virus koji se najčešće nalazi u prilogu poruke elektronske pošte. Kada korisnik otvori prilog virus šifrira podatke u korisnikovom računaru, tako da postanu neupotrebljivi, a onda od korisnika zahteva otkup ključa koji će ih vratiti u prvobitno stanje. Pošto se rad od kuće bazira na komunikaciji elektronskom poštom i čestom razmenjivanju dokumenata, to je opasnost da u nekom od priloga bude i virus ransomver mnogo veća nego u uslovima regularnog rada na zaštićenoj kompanijskoj mreži.

Fišing (od engl. phishing što znači pecanje) je lažno predstavljanje, najčešće preko falsifikovane web stranice, kao neko kome se inače veruje, kao što je banka ili poslodavac. Kada se korisnik upeca na tekst iz poruke elektronske pošte i klikne na link koji ga odvede na falsifikovani sajt, na toj stranici na prevaru obično ukradu lične podatke korisnika, kao što su korisničko ime i lozinka npr. za pristup kompanijskoj mreži poslodavca. S obzirom na povećanu količinu poruka tokom rada od kuće, zaposleni su manje oprezni i lakše se upecaju na ovaj način.

Čak i za zaposlene koji nauče da se odupru hakerskim napadima postoje objektivne okolnosti koje utiču na niži nivo bezbednosti njihovog rada nego inače. S obzirom da u većini kompanija nemaju svi zaposleni prenosne računare, prinuđeni su da rade od kuće koristeći sopstvenu računarsku opremu i vezu ka Internetu. Na taj način izlažu kompanijske podatke virusima, jer kućni kompjuteri po pravilu nemaju ažuran anti-virus softver, niti zakrpe operativnog sistema. Često zaposleni koji rade od kuće na svojim računarima nemaju uključen firewall, ili im firewall nije dobro podešen, jer prosečni korisnici nemaju dovoljno informatičkog iskustva za to. Takođe, zastarele verzije operativnih sistema kućnih računara, za koje Majkrosoft više ne obezbeđuje ažuriranja ni zakrpe su znatno ranjivije od standardnih u kompanijskom okruženju. Vrlo mali broj korisnika ima adekvatno rešenje za back-up podataka na kućnom kompjuteru. Podaci koje šalju običnom, nekriptovanom elektronskom porukom, putem interneta mogu biti presretnuti i kompromitovani.

Zaposleni koji imaju prenosne računare često dolaze u iskušenje da rad od kuće pretvore u rad iz kafića, restorana ili sa plaže i pri tom koriste javne Wi-Fi mreže. Bez obzira na stepen zaštite kompjutera, povezivanje na javnu bežičnu mrežu nosi veliki rizik od hakerskog napada i gubitka ličnih ili kompanijskih podataka. Ne treba zanemariti ni mogućnost da neko, slučajno gledajući u ekran zaposlenog koji radi na javnom mestu, sazna važne i osetljive informacije iz poslovanja kompanije, čiji zaposleni rade iz kafića i sličnih mesta.

Pojedini zaposleni koji rade od kuće na svojoj opremi, za posao koriste servise i aplikacije koje IT stručnjaci njihovih kompanija nisu odobrili, kao na primer servise za video konferencije, dopisivanje ili skladištenje fajlova. Pored nepouzdanosti servisa i rizika od mogućeg gubitka podataka, zaposleni na taj način dovode kompaniju u opasnost od kazni za korišćenje servisa u poslovne svrhe bez plaćanja licenci ili sa neodgovarajućim načinom licenciranja.

U novim okolnostima, u cilju zaštite od rizika rada od kuće, poslodavci bi trebalo da što pre obezbede zaposlenima specifične smernice za podizanje svesti o sajber bezbednosti, *kao i obuku namenjenu zaštiti* od pomenutih potencijalnih rizika. ■