Uvod

Iako na prvi pogled može da se učini da to nije slučaj, analize govore u prilog tome da su mala i srednja preduzeća sve učestalije mete sajber napada. Bez obzira na činjenicu da naslovi u medijima najčešće govore o napadima na velike kompanije kao što su Yahoo, Sony, Facebook i slično, mala i srednja preduzeća su veoma često na meti hakerskih napada. Zbog toga je neophodno podići nivo svesti rukovodilaca i zaposlenih u malim i srednjim preduzećima o mogućim napadima i zloupotrebama slabo branjenih sistema ovih kompanija. Prilikom planiranja budžeta ovakvih kompanija, rukovodstvo najčešće ima pristup "previše smo mali da bismo bili napadnuti", što je veoma pogrešno.

Trend

Ukoliko pogledamo statističke izveštaje iz 2018. godine možemo videti trend rasta hakerskih napada na slabo zaštićene informacione sisteme malih i srednjih preduzeća, odnosno da su upravo te kompanije sve češće mete hakerskih napada. Kad govorimo o napadima iznuđivačkog tipa (eng. *Ransomware*), mala i srednja preduzeća su žrtve u više od 50 odsto slučajeva. Ista, ili slična situacija je i sa drugim tipovima napada, kao što su: upad u informacioni sistem kompanije, kradja ličnih podataka, fišing kampanje (eng. *Phishing*), socijalni inženjering (eng. *Social engineering*), onemogućavanje pružanja usluga kompanije (eng. *DoS/DDoS*), špijunaža i sl. Najčešći razlog sve većeg broja napada na informacione sisteme malih i srednjih preduzeća je to što se rukovodioci kompanija ovog profila najčešće odlučuju da plate traženu otkupninu enkripcionih ključeva, kako bi što pre mogli ponovo da pristupe svojim zaključanim datotekama, a drugi je da bi zaštitili reputaciju svog preduzeća, zanemarujući tom prilikom činjenicu da i pored plaćanja iznude ne postoji nikakva garancija da će kompanija dobiti odgovarajuće ključeve, ili mogućnost da nakon uplate stigne još jedna poruka, u kojoj se zahteva još novca od strane napadača.

Preventivne mere

Ipak, postoje mere koje mogu biti preduzete u cilju prevencije i zaštite sistema malih i srednjih preduzeća, koje najpre podrazumevaju sledeće:

- obezbeđivanje osnovnog nivoa sajber higijene u okviru kompanije, što pre svega podrazumeva uspostavljanje odgovarajućih bezbednosnih procedura, sprovođenje redovnih obuka iz domena sajber bezbednosti za sve zaposlene u kompaniji, uvođenje

jedinstvenih identifikacionih kartica za pristupanje sistemu (*ID cards*), upravljanje korisničkim nalozima i lozinkama i sl,
- kreiranje profila za pristup sistemu, kako bi zaposleni pristupali samo onim podacima, odnosno delovima sistema koji su neophodni za posao koji obavljaju,
- redovno ažuriranje svih hardverskih, sistemskih i aplikativnih rešenja, kao i kreiranje rezervnih kopija važnih dokumenata i fajlova (*backup*),
- obavezu korišćenja antivirusnih softverskih rešenja za celokupan informacioni sistem kompanije,
- kreiranje procedura za postupanje u slučajevima napada na informacioni sistem kompanije i obezbeđivanje kontinuiteta poslovanja.

Primenom nabrojanih mera nivo bezbednosti sistema kompanije će biti podignut na viši nivo, što će kompaniju činiti zaštićenijom i otpornijom na napade hakera. Samim tim će i moguća izloženost preduzeća finansijskim gubicima biti svedena na minimum, što će preduzećima omogućiti da finansijski podrže druge procese i razviju svoje poslovanje, ali na bezbedan način.