Превенција и заштита малих и средњих предузећа од сајбер напада

Увод

Иако на први поглед може да се учини да то није случај, анализе говоре у прилог томе да су мала и средња предузећа све чешће мете сајбер напада. Без обзира на чињеницу да наслови у медијима најчешће говоре о нападима на велике компаније као што су *Yahoo*, *Sony*, *Facebook* и слично, мала и средња предузећа су веома често на мети хакерских напада. Због тога је неопходно подићи ниво свести руководилаца и запослених у малим и средњим предузећима о могућим нападима и злоупотребама слабо брањених система ових компанија. Приликом планирања буџета оваквих компанија, руководство најчешће има приступ ''превише смо мали да би били нападнути'', што је веома погрешно.

Тренд

Уколико погледамо статистичке извештаје из 2018. године, можемо видети тренд раста хакерских напада на слабо заштићене информационе системе малих и средњих предузећа, односно да су управо те компаније све чешће мете хакерских напада. Када је реч о нападима изнуђивачког типа (ransomware), мала и средња предузећа су жртве у више од 50 одсто случајева. Иста, или слична ситуација је и са другим типовима напада, као што су: упад у информациони систем компаније, крађа личних података, фишинг кампање (енг. *Phishing*), социјални инжењеринг (енг. *Social engineering*), онемогућавање пружања услуга компаније (енг. *DoS/DDoS*), шпијунажа и сл. Најчешћи разлог све већег броја нападана информационе системе малих и средњих предузећаје то што се руководиоци компанија овог профила најчешће одлучују да плате тражену откупнину енкрипционих кључева, како би што пре могли поново да приступе својим закључаним датотекама, а други је да би заштитили репутацију свог предузећа, занемарујући том приликом чињеницу да и поред плаћања изнуде не постоји никаква гаранција да ће компанија добити одговарајуће кључеве, или могућност да након уплате стигне још једна порука, у којој се захтева још новца од стране нападача.

Превентивне мере

Ипак постоје мере које могу бити предузете у циљу превенције и заштите система малих и средњих предузећа, које најпре подразумевају следеће:

- обезбеђивање основног нивоа сајбер хигијене у оквиру компаније, што пре свега подразумева успостављање одговарајућих безбедносних процедура, спровођење редовних обука из домена сајбер безбедности за све запослене у компанији, увођење јединствених идентификационих картица за приступ систему (*ID cards*), управљање налозима и лозинкама и сл.
- креирање профила за приступ систему, како би запослени приступали само оним подацима, односно деловима система који су неопходни за посао који обављају,
- редовно ажурирање свих хардверских, софтверских и апликативних решења, као и креирање резервних копија важних докумената и фајлова (*backup*),
- обавезу коришћења антивирусних софтверских решења за целокупан информациони систем компаније,
- креирање процедура за поступање у случајевима напада на информациони систем компаније и обезбеђивање континуитета пословања.

Применом набројаних мера ниво безбедности система компаније ће бити подигнут на виши ниво, што ће компанију чинити заштићенијом и отпорнијом на нападе хакера. Самим тим ће и могућа изложеност предузећа финансијским губицима бити сведена на минимум, што ће предузећима омогућити да финансијски подрже друге процесе и развију своје пословање, али на безбедан начин.