Avtorja: Marko Zavadlav / PRO.astec
Mihael Nagelj / Gospodarska zbornica Slovenije

VPLIV PROJEKTA CYBER INTERREG EU NA ZAGOTAVLJANJE VARNOSTI V MALIH IN SREDNJIH PODJETJIH TER RAZVOJ NOVIH STORITEV KIBERNETSKE VARNOSTI

Mala in srednja podjetja so v modernem digitalnem svetu enako izpostavljena kibernetskim tveganjem kot velika, le da za učinkovito zagotavljanje varnosti nimajo na voljo ustrezne opreme in kadrov za izvajanje potrebnih nalog varovanja informacij. Kako pomagati malim in srednjim podjetjem, s področja kibernetske varnosti, pri zagotavljanju ustreznih rešitev, je namen projekta Cyber Interreg Europe.

Današnje poslovno okolje zahteva hitre odzive, učinkovitost in natančnost. Z nenehnim in hitrim razvojem so se informacijske tehnologije vključile v vsakodnevno poslovanje. Praktično ni več poslovnega okolja, pa naj bo še tako majhno, ki ne bi bilo podprto z informacijsko tehnologijo. Nihče ne vodi računovodstva in saldakontov ročno, vsi uporabljamo elektronsko pošto za komunikacijo, uporabljamo pisarniške programe, imamo spletne strani in drugo. To pa je šele začetek. Vedno več malih in srednjih podjetij, delujočih v tradicionalnih branžah z nizko stopnjo uporabe informacijske tehnologije, vse intenzivneje digitalizira svoje ključne procese z vedno novimi tehnologijami in novimi koncepti njihove uporabe.

Vsi smo povezani v internet, preko njega so dosegljive naše ključne informacije, za marsikatero sploh nimamo več analogne kopije. Večkrat ste že slišali, če ne doživeli, kako se lahko pripeti, da se z izgubo ali okvaro navadnega mobilnega telefona izgubijo vsi poslovni kontakti (seveda tudi zasebni). Kako je nekdo imel celotno poslovanje na osebnem računalniku, pa je prejel izsiljevalski virus. Nove tehnologije pa poleg koristi prinašajo tudi nove ranljivosti, ki se, s povečevanjem intenzivnosti komuniciranja vse večjega števila naprav na internetu, še povečujejo. V digitalnem okolju številnih koristi in priložnosti so svoje priložnosti našli tudi zlonamerneži in organiziran kriminal. V medijih beležimo velik porast novic o spletnih napadih, o zlorabah, spletnih prevarah in izsiljevanjih, ki se ne dogajajo samo drugje. To je tudi naša realnost.

Splošni cilj projekta CYBER Interreg EU je povečati konkurenčnost malih in srednjih podjetij na področju kibernetske varnosti, in sicer izboljšanjem javnih politik in odpravo skupnih ovir, kot so razdrobljenost trga ali pomanjkanje strokovnega kadra ter izboljšanja eco sistema v celoti.

Ker preprosto ne moremo živeti odrezani od digitalnega sveta, se moramo ustrezno zaščititi tudi sami. Razvoj digitalizacije daje priložnosti tudi malim in srednjim podjetjem s podorčja kibernetske varnosti, da razvijejo nove storitve in izdelke za čas, ki je pred nami. Splošni

cilj projekta CYBER Interreg EU je povečati konkurenčnost malih in srednjih podjetij na področju kibernetske varnosti, in sicer izboljšanjem javnih politik in odpravo skupnih ovir, kot so razdrobljenost trga ali pomanjkanje strokovnega kadra ter izboljšanja eco sistema v celoti. Rešitve vidimo predvsem v povezovanju nosilcev raziskav in razvoja s podjetji na trgu na eni strani in ponudnikov ter uporabnikov storitev na drugi s ciljem razvoja inovativnih in učinkovitih rešitev tudi s sodelovanjem na globalnem trgu. V nadaljevanju govorimo o dveh primerih takšnih rešitev.

Tveganja v informacijskem svetu lahko v grobem delimo na tista, ki so odvisna od zlonamernežev oziroma kriminalcev, tista, ki so posledica napačnega delovanja opreme, ki jo uporabljamo pri svojem delu in pa na tista, ki so posledica dejanj nas in naših zaposlenih zaradi malomarnosti ali nevednosti. Največ se govori o tveganjih, povezanih s kibernetskimi napadi in zlorabami, zato si jih natančneje oglejmo in jih analizirajmo, saj si ne moremo več zatiskati oči, da se ta tveganja ne morejo uresničiti pri nas. Če poskusimo primerjati analogni in digitalni svet opazimo, da se v analognem svetu lahko gibljemo »pod radarjem«. Malo verjetno je, da nam bo nekdo poskusil ukrasti avto, ki ni vreden več kot 20.000 €, da nam bo kdo vlomil v stanovanje, če bo na daleč jasno, da v njem nimamo primernih dragocenosti. Vlomilci namreč najprej ocenijo, ali se jim splača tvegati. V digitalnem svetu, če seveda ne govorimo o vrhunskih kriminalcih, ki natančno vedo, koga napadajo, ne moremo biti varni. Običajni napadalci namreč vržejo vabo, ki doseže ogromno število ljudi, torej lahko dosežejo dobiček s svojim »poslovnim modelom« že pri majhnih izplenih na posameznika. Digitalizacija namreč omogoča, da ja napadalec lahko kjerkoli, torej lahko doseže ogromno število potencialnih žrtev v izjemno kratkem času. Dodatna težava je tudi v tem, da za izvedbo takega napada ni potrebno veliko znanja ali premetenosti. Danes se na črnem tržišču že za relativno majhen denar lahko nabavi storitve ali programsko opremo za take napade. Če pogledamo primere z izsiljevalskimi virusi, so napadalci od vsake zaklenjene delovne postaje zahtevali recimo 1 bitcoin. Danes to pomeni vrednost okoli 3.000 €. Seveda so lahko zahtevali tudi manj. Za izvedbo celotne kampanje so porabili recimo 10.000 € (nabava strojne in programske opreme, zakrivanje sledi in ostalo), virus so razposlali naokoli, in če se je ujelo 500 posameznikov, je računica izjemna. Celotna kampanja je trajala maksimalno dva meseca. Torej, koliko so zlonamerneži lahko zaslužili v dveh mesecih?

Drugi primer je izguba podatkov zaradi napake v delovanju opreme. Premalokrat se zavedamo, da imamo na računalniški opremi izjemno pomembne podatke, brez katerih težko ali pa sploh ne moremo poslovati. Vedno pa se pojavi problem visokih stroškov opreme.

Tretji primer pa govori o nas samih. Včasih se nam preveč mudi, ne vemo natančno, kaj moramo narediti, nismo dovolj izobraženi ali usposobljeni za izvajanje določenih operacij. Vsi načelno vemo, kaj je potrebno za zagotavljanje ustreznega nivoja varnosti. Gre za varnostne naprave, za vrhunsko opremo ter za usposabljanje in izobraževanje.

Velike organizacije si lažje privoščijo požarne pregrade naslednje generacije, sisteme za zaznavo in preprečevanje vdorov, spremljanje in alarmiranje v primeru zaznanih poskusov zlorabe. Lahko si privoščijo vrhunsko informacijsko opremo, redundantne strežnike, varnostne kopije na več lokacijah ali rezervne lokacije. Za izvajanje varnostnih funkcij lahko izobrazijo lastne strokovnjake, lahko nenehno ozaveščajo in izobražujejo zaposlene.

Kaj pa majhna in srednja podjetja? Običajno imajo mnogo bolj omejene vire. Ne morejo si privoščiti zelo dragih na-