KIBERNETSKI NAPADI NA ELEKTRONSKO POŠTO IN KAKO PREPREČITI POSLOVNO ŠKODO – NOVO ZNANJE LAHKO TAKOJ PRENESEMO V PRAKSO

V četrtek, 18. 2. 2021, je v okviru IKT Horizontalne mreže kibernetska varnost potekal webinar »Kibernetski napadi na elektronsko pošto in kako preprečiti poslovno škodo«. Ugledni strokovnjaki s področja kibernetske varnosti so spregovorili o napadih na informacijske sisteme z metodami socialnega inženiringa in podali nasvete o ukrepih ter izogibanju poslovne škode.

Uvodoma je mag. Matjaž Kosem iz podjetja Carbonsec d.o.o. je predstavil problematiko napadov preko elektronske pošte v letu 2020 s številkami, kjer so napadalci dobro izkoristili krizo zaradi Covid-19 in nove okoliščine dela velikega deleža zaposlenih. Število napadov se je v preteklem letu podvojilo. Napovedi kažejo, da bodo do leta 2025 stroški zaradi kibernetskih napadov vsako leto za 15 % višji, kar bi nas moralo skrbeti.

Dvig kulture kibernetske varnosti v podjetjih je ključno za izvajanje ukrepov in zagotavljanje odpornosti na kibernetska tveganja. Veseli smo, da je bilo med udeleženci webinarja velik del vodstvenega kadra, saj brez njihovega angažiranja ni mogoče pričakovati učinkovitega ozaveščanja vseh zaposlenih. Z vidika Sekcije za kibernetsko varnost pri GZS sem predstavil stanje varnostne ozaveščenosti v slovenskem gospodarskem prostoru. Kar 16 % slovenskih podjetij v letu 2018 po podatkih raziskave SURS v 2019 ni izvajalo niti minimalnih varnostnih ukrepov za preprečevanje kibernetskih napadov. Največji delež teh podjetij spada v mala in srednja podjetja. Vzrok je iskati v stopnji ozaveščenosti o kibernetskih tveganjih, ki je prvi korak k spremembi varnostne kulture podjetij in s tem bolj učinkovitega izvajanja ukrepov.

V drugem delu dogodka smo se osredotočili na napade z metodami socialnega inženiringom preko elektronske pošte, saj sta prav »phishing« in »spear phishing« glavni orodji, s katerima hekerji najlažje dobijo vstop informacijski sistem podjetja oz. dostop do podatkov. Doc. dr. Kaja Prislan s Fakultete za varnostne vede UM je predstavila metode zavajanja uporabnikov s psihološkimi triki. Napadalci namreč dobro raziščejo, na katere teme so uporabniki občutljivi in kaj so njihove šibke točke, pa so ustvarjalci napadov dobro izkoristili tudi pandemijo Covid-19, kar je predstavila s praktičnimi primeri.

Vladimir Ban, vodilni ekspert za implementacijo ICT rešitev v podjetju A1 Slovenija d.d., in Grega Prešeren, tehnični direktor v podjetju Carbonsec d.o.o., sta na podlagi primera napada preko elektronske pošte izpostavila dva vidika zaščite pred napadi. Grega Prešeren se je osredotočil na vidik varnostnega ozaveščanja zaposlenih in prepoznavanje elementov v elektronskih sporočilih, ki nakazujejo na ciljan napad. Vladimir Ban pa je izpostavil možnosti opreme, ki lahko pripomore k boljši kibernetski varnosti v organizaciji. Poudaril je, da se sodobna oprema z uporabo tudi umetne inteligence bistveno razlikuje od opreme, ki smo jo poznali pred leti.

Dogodek smo zaključili z okroglo mizo o tem, kako lahko zmanjšamo varnostna tveganja na ravni podjetja in poskrbimo za to, da bo podjetje varno pred zlonamernimi poskusi, ki jim je podjetje izpostavljeno. Dogodek je postregel s sistematičnim prikazom mehanizmov delovanja načrtovalcev napadov in možnosti ukrepanja, z veliko koristnega znanja, ki ga bodo udeleženci lahko uporabili v svojih poslovnih okoljih.

Mag. Mihael Nagelj
IKT Hm Kibernetska varnost
Koordinator