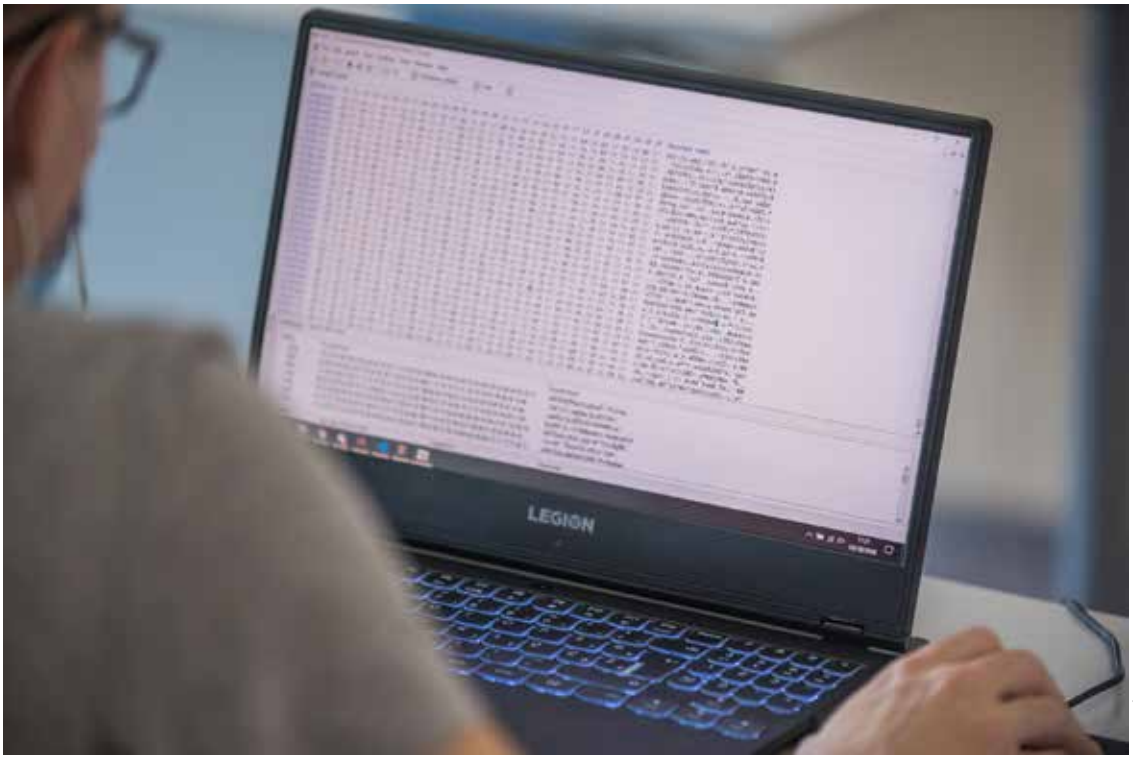

Foto: KrafiART

IKT horizontalna mreža

zit SeKV
Združenje za informatiko in telekomunikacije
Kibernetska varnost

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.

Kibernetska varnost

Slovenija mora bolje povezati svoje zmogljivosti za zagotavljanje informacijske varnosti

V oktobru, ki je mesec kibernetske varnosti, je na Gospodarski zbornici Slovenije (GZS) potekala konferenca o kibernetski varnosti podjetij z naslovom »24/7/365: Kibernetska (ne)varnost nikoli ne počiva. Kaj se dogaja, ko spimo?«.

Maruša Boh, Združenje za informatiko in telekomunikacije (ZIT), GZS

DIHS je za večjo osveščenost objavil Vodnik za prve korake k varnejšemu poslovanju

Celodnevni dogodek je bil priložnost za poglobljeno razpravo o tem, kako zagotavljati učinkovito kibernetsko varnost 24 ur na dan, vsak dan v tednu in vse dni v letu.

Dr. Uroš Svete, direktor Uprave RS za informacijsko varnost, je poudaril, da varnost ni enkraten dogodek, temveč gre za stalni proces. Slovenija mora po njegovem v prihodnje svoje zmogljivosti za zagotavljanje informacijske varnosti bolje povezati, predvsem pa okrepiti. Pri tem bo zelo pomembno sodelovanje vseh deležnikov, torej sodelovanje z gospodarstvom in znanstveno-raziskovalno sfero, predvsem v povezavi z zagotavljanjem novih kadrov.

Kot pravi, si je treba prizadevati za popularizacijo področja informacijske varnosti med mladimi ter za primerne izobraževalne programe v slovenskih izobraževalnih ustanovah, ki bodo ves čas sledili spremembam in napredku na tem področju. Le na ta način in ob sodelovanju vseh deležnikov bo mogoče resnično okrepiti celoten sistem, da bo ta sposoben zagotavljanja informacijske varnosti za vse, je jasen Svete.

Zagotavljanje varnosti ni nekaj, kar traja od 8h do 16h, ampak je proces, ki zahteva nenehno pozornost.

Več kot polovica napadov na MSP

Čeprav Slovenija na videz ni med najbolj zanimivimi državami za kibernetske napade, to ne pomeni, da smo popolnoma varni in da se na področju kibernetske varnosti ne more zgoditi nič. Kriza COVID-19 situacije ni poslabšala, je pa dejstvo, da se je s pospešeno digitalizacijo povečal tudi prenos podatkov na internetnih omrežjih, kar je povečalo tudi število kibernetskih napadov. Pri tem velja izpostaviti, da

Foto: KraftART

Treba si je prizadevati za popularizacijo področja informacijske varnosti med mladimi.

Kriza je zaradi novega koronavirusa povzročila izjemno hitre spremembe v načinu dela in v uvajanju digitalnih orodij. Bili smo prisiljeni hitro reagirati in se prilagoditi novi situaciji. Bolj kot se družba digitalizira, več je prostora za napade, večja so tveganja in večje so posledice napadov. Zagotavljanje varnosti zato zahteva nenehno pozornost.

S pospešeno digitalizacijo med pandemijo se je povečal tudi prenos podatkov na internetnih omrežjih, kar je povečalo obseg kibernetskih napadov.

je bila več kot polovica vseh kibernetskih napadov usmerjena na mala in srednja podjetja (MSP). Bolj usmerjene napade je bilo zaznati tudi na komitente bank, epidemijo pa se je izkoriščalo tudi za poskuse okoriščanja z različnimi prijemi družbenega inženiringa, smo slišali na konferenci.

Gorazd Božič, vodja Nacionalnega odzivnega centra za kibernetsko varnost SI-CERT, je predstavil lekcije, ki so jih v SI-CERT identificirali v tem letu. Ali se bomo od njih uspeli tudi kaj naučiti in naučeno uveljavili v praksi? Pravi, da se manjša in srednja podjetja še vedno premalo zavedajo vseh nevarnosti in groženj, ki jim pretijo.

»Zadnja leta se veliko posvečamo trudu, da bi vodstva MSP prepričali, da bi se ukvarjali z ozaveščanjem zaposlenih o tem, kakšne so možnosti tveganja in kako jih prepoznati, kajti človeški faktor je tisti, ki je pogosto kriv, da v podjetje pride izsiljevalski virus,« je povedal Božič in dodal, da »žal večina MPS kibernetsko varnost tradicionalno razume kot strošek, dokler se ne zgodi nekaj neprijetnega«.

Foto: KraftART

Pomen informacijsko varnostne kulture in pomanjkanje kadra

Dvig informacijsko varnostne kulture postaja pomemben za kibernetsko varnost družbe. Ljudje bodo morali bolj odgovorno uporabljati pametne tehnologije, saj bodo le tako zmanjšali tveganje v prihodnje. »S svojim vedenjem, ozaveščenostjo in pristopom lahko bistveno zmanjšamo možnosti za zlorabo in s tem dvignemo raven informacijske varnosti – tako v zasebnem, kot tudi poslovnem okolju,« je povedal Božič.

Milan Gabor je certificirani etični heker, ki podjetjem in organizacijam pomaga dvigati raven informacijske varnosti, na dogodku pa je o etičnemu hekerju govoril v luči poklica prihodnosti. Ponudil je vpogled v stanje glede kadrov na področju informacijske varnosti, ki ni preveč rožnato. Nekatere napovedi kažejo, da bo v Evropi do leta 2022 primanjkovalo veliko kadra s tega področja, po nekaterih napovedih do 350.000 strokovnjakov.

Da je kibernetska varnost z razvojem digitalizacije še kako pomembna in da izobraževanje in ozaveščanje ljudi lahko poskrbita za varnejšo družbo in delovanje podjetij, je izpostavila Katja Mohar Bastar, direktorica Digitalnega inovacijskega stičišča Slovenije (DIHS). Povedala je, da so spodbude v obliki vavčerja za kibernetsko varnost, ki MSP omogoča sofinanciranje sistemskega varnostnega pregleda in penetracijskega testiranja, le ena oblika pomoči, kako povečati odpornost na kibernetske grožnje. Ob tej priložnosti je DIHS objavil Vodnik za prve korake k varnejšemu poslovanju kot del aktivnosti osveščanja. gg

Sistema, ki bi zagotavljal 100 % varnost podjetja, ni. Lahko pa povečamo odpornost na kibernetske napade. Odsotnost varnostnih kontrol, pomanjkanje kadra in vedno bolj napredni hekerji so tisti indikatorji tveganja, ki lahko povzročijo hude motne v poslovanju, vključno s finančno škodo in škodo ugleda. Pred napadi se moramo ustrezno zavarovati, zato je dvig ravni informacijske in kibernetske varnosti v celotni družbi izrednega pomena.

Tiskano na papirju Viprint, 80 g, papirnice VIPAP VIDEM KRŠKO, d. d.