**Stanislava Zadravec Caprirolo: Uvodni nagovor na javni okrogli mizi**

**Digitalna transformacija in varnostni izzivi, 12.oktober 2023**

Oktober je mesec kibernetske varnosti, ki je skupna kampanja evropskih in nacionalnih institucij na področju na področju ozaveščanja, usmerjenega v spodbujanje in krepitev kibernetske varnosti.

V okviru evropskega meseca kibernetske varnosti se vsako leto zvrstijo številni dogodki, s katerimi še bolj intenzivno, kot tekom leta različne EU institucije in partnerji v vseh državah opozarjajo na varno rabo interneta.

Banke in hranilnice in Združenje bank Slovenije že leta v okviru svojih dejavnosti finančnega opismenjevanja tudi v sodelovanju z drugimi institucijami (SICERt-om, policijo, šolami in drugimi) vedno več časa posvečajo osveščanju o izpostavljenosti kibernetski varnosti in načinih kako se bolje obvarovati pred pastmi, ki smo jim izpostavljeni vsi: podjetja in posamezniki.

V zadnjem desetletju smo priča hitremu tehnološkemu razvoju, predvsem na področju izvajanja plačil in tudi drugih bančnih storitev. Trende digitalizacije je izrazito pospešila Covid kriza, medtem ko je trende povečevanja izpostavljenosti kibernetskim tveganjem pa močno pospešila vojna v Ukrajini.

Digitalizacija in vedno večja digitalna povezanost finančnih storitev seveda nudita veliko dobrobiti strankam:

* razpoložljivost izvajanja transakcij praktično 24 ur 7dni na teden
* možnost izvajanja transakcij od doma
* hitro, tako rekoč takojšnjo izvedbo plačilnih transakcije
* nižje stroške transakcij

Nedavni trendi, stranski učinki globalne pandemije in vojne pa posledično v statističnih podatkih o kibernetski varnosti razkrivajo veliko povečanje vdorov in kraje podatkov, ki so vse pogostejši:

* na delovnem mestu
* mobilnih napravah
* na spletu

Vprašanja kibernetske varnosti postajajo borba vsakodnevnega poslovanja.

Kibernetski prostor je globalno javno dobro, zato mora biti odgovornost zanj skupna odgovornost vlad, javnih institucij, akademske sfere in tudi zasebnega sektorja in se moramo za varnost truditi vsi, tudi uporabniki digitalnih storitev.

Učinkovita strategija zagotavljanja kibernetske varnosti sloni na treh stebrih:

* + regulativa
  + sodelovanje in
  + zavedanje o tveganjih

Tveganja zlorabe podatkov strank je eno med najbolj dinamičnimi tveganji hkrati pa poti za kibernetične „napade“ postajajo izrazito kompleksne.

Dodatno k temu je v resnici stopnja digitalnih veščin/kompetenc državljanov EU relativno nizka :

* + 44% = 169 milijonov evropskih državljanov ne obvlada osnovnih digitalnih veščin ; od tega 77 milijonov nima popolnoma nikakršnega digitalnega znanja
  + 37% = 93 milijonov delovno aktivnih evropskih državljanov ne obvlada osnovnih digitalnih veščin
  + 80% evropskih podjetij je izkusilo kibernetski incident
  + Vsak dan se zgodi cca 4000 raznovrstnih digitalnih napadov
  + 95% vseh kibernetskih incidentov je tak ali drugačen način povezanih s človeško napako[[1]](#footnote-1)

Banke lahko in tudi naredijo zelo veliko za zagotavljanje varnosti in o razvoju tehnologije. O uporabi tehnologije, vključno z umetno inteligenco, tako za namene izboljšanja uporabniške izkušnje, kakor tudi za zagotavljanje čim večje možne stopnje varnosti podatkov in finančnih sredstev bank, bo tekla razprava na današnji okrogli mizi in to v krogu res najodličnejših strokovnjakov tega področja.

Hvala današnjim nastopajočim gostom za čas in pripravljenost sodelovanja.

Kljub temu, da različne institucije in banke ter druge družbe veliko človeških naporov in finančnih sredstev vlagajo v investicije za zagotavljanje čim višje možne stopnje varnosti, pa je vendar tudi iz podatka o tem , da je 95% vseh kibernetskih incidentov na tak ali drug način povezanih s človeškim ravnanjem razvidno, da največ za svojo varnost lahko naredimo sami. Zato je osveščanje še posebej pomembno.

Zato so članice letos, še dodatno k siceršnjim aktivnostim na področju osveščanja, kot že omenjeno, namenile še dodatna zelo obsežna sredstva za kampanjo ozaveščanja kibernetske varnosti , ki jo izvaja združenje skupaj z zunanjo agencijo –kampanja poteka letos in se bo nadaljevala naslednje leto. Upamo, da se ji bodo finančno in vsebinsko pridružili še drugi, predvsem vlada, centralna banka, telekomunikacijski sektor in drugi, da z vključitvijo ostalih deležnikov take kampanje postanejo vseslovenska nacionalna aktivnost.

V želji in pričakovanju, da bo današnja strokovna razprava doprinesla dodaten delček tudi k povečanju zavesti kako čim bolje poskrbeti za skupno in posamično varnost pred izpostavljenostjo kibernetskim tveganjem oziroma zlorabam, predajam besedo moderatorju današnje razprave, gospodu **Goranu Goluboviću**, predsedniku Odbora za informatiko pri Združenju bank Slovenije in pomočniku uprave, Deželna banka Slovenije.

1. Vir: EBF [↑](#footnote-ref-1)