СЛАВИМИР Љ. ВЕСИЋ*
КП „Београдски водовод и канализација”
Београд

UDC: 004.6:351.78
Прегледни рад
Примљен: 04.02.2021
Одобрен: 12.04.2021
Страна: 79–96
DOI: 10.51738/Kpolisa2021.18.1p.1.06

УТИЦАЈ БЕЗБЕДНОСНИХ ИЗАЗОВА У УПОТРЕБИ ИНТЕРНЕТА И МОБИЛНИХ АПЛИКАЦИЈА НА КРЕИРАЊЕ БЕЗБЕДНОСНЕ КУЛТУРЕ

***Сажетак*:** Нарастући број претњи и изазова из сајбер простора, услед све веће употребе Интернета и мобилних апликација као никада раније, захева спровођење безбедносних политика које имају за циљ да очувају информационо-комуникациона средства предузећа. Безбедност се остварује кроз један део мера које су техничко-технолошке природе, а други део је везан за деловање људи у организацији. Познато је да људи чине најслабију карику, а безбедносна култура има за циљ да делује на људе тако да усвоје одређена понашања, изграде навике и успоставе комуникације на начин да могу да одговоре на претње из сајбер простора. Информациона безбедносна култура се успоставља и одржава спровођењем програма који имају за циљ да људе припреме за садашње и будуће изазове из сајбер простора. Једног дана млади људи ће ступити у радни однос, али до док не дође до тог тренутка родитељи у синергији са школским установама треба да их усмере тако да прихвате одређена понашања и норме. Безбедносна култура на тај начин осигурава да се од најранијих дана очува њихова безбедност, па је с’тога на различитим нивоима образовања потребно развити програме који ће то и омогућити.

***Кључне речи*:** информациона безбедносна култура, оквир безбедносне културе, креирање безбедносне културе, сајбер безбедност, безбедност младих

Увод

Излазак светске глобалне мреже повезаних рачунара, Интернета, из круга научне и академске заједнице повезује се са креирањем World Wide Web-a (општеприхваћено Web) и појавом првих претраживача, почетком 90-их година прошлог века. Од тог времена, па до данашњег дана најпознатија глобална мрежа је доживела огромну експанзију. Многи сервиси који се могу користити

* vesic.slavimir@gmail.com

кроз модел услуге Интернета, као што су електронска пошта, претраживање, гледање, креирање и размена различитог садржаја: докумената, слика, видео снимака, и тд., затим повезивање са пријатељима и одржавање контаката у форми социјалних мрежа, чета и тд. су постали неизоставни део наше реалности. Једна од његових најважнијих карактеристика је свеприсутност, која омогућава повезивање било где и било када. Континуално побољшање приступа Интернету, а посебно путем бежичних мрежа, уз тренд опадања цене сензора и актуатора, као и минијатуризацију, а при томе и све веће усвајање парадигме рачунарства у облаку, доводи до огромног пораста у повезивању различитих уређаја на светску мрежу, познатијих под називом интернет „ствари". Почетна идеја комуникације која се остваривала између људи, проширена је тако да људи имају интеракцију са различитим „стварима", а „ствари" такође имају интеракцију међусобно. GSMA удружење које заступа интересе мобилних оператера предвиђа да ће до краја 2025. на мрежи бити око 25 милијарди интернет „ствари" (Research and Markets 2020). Због потребе за увећаним опсегом на глобалном нивоу све више се убрзава усвајање верзије 6 IP комуникационог проткола, који је срж Интернета.

Пре скоро четири деценије појавили су се први мобилни телефони са веома ограниченим функционалностима као што су аларм, калкулатор и календар и тд. Временом је цена мобилних уређаја опадала, па су самим тим били прихватљивији за ширу популацију, што је отворило могућност да се додају нове и прошире постојеће њихове функционалности. Тадашњи произвођачи мобилних уређаја су употребу Интернета преко видели као добар начин привлачења клијената и понудили су им WAP, који је заправо представљао осиромашену верзију HTTP-а, протокола који је кључан за Web. Услед лошег корисничког искуства WAP није широко прихваћен, тако да се масовна употреба светске мреже на мобилним уређајима пролонгирала све до појаве паметних телефона. Паметни телефони, као мултифинкционални уређаји, допринели су смањење тржишта многобројних уређаја као што су GPS, MP3 плејери, диктафони, фотоапарати и тд. Корисници су од њихових почетака у масовној употреби појавом iPhone-а 2007. године, видели многобројне бенефите, па се интеракција са паметним телефонима и екранима на додир веома брзо прихватила. Временом како се тржиште мобилних апликација увећавало корисници су све више користили апликације и то је довело до тога да је данас живот за већину популације готово незамислив без употребе барем неке од мобилних апликација на дневном нивоу. Према неким истраживањима типичан корисник паметног телефона око 63 пута дневно провери свој телефон, просечан корисник у САД има инсталирано око 100 апликација, 87% корисника користи паметни телефон барем 1 сат пре спавања, док 69% користи барем 5 минута пре спавања, око 7 милијарди људи широм света користи мобилне телефоне до краја 2021. године, до краја 2022. број преузетих апликација ће достићи 258 милиона по години (Mroczkowska 2021). Ови наводи показују да је количина интеракције остварена путем паметних телефона огромна и да је за већину корисника то незаменљив уређај. Већина апликација која се развија за мобилни телефон у својој позадини користи Интернет, да би размењивала податке са удаљеним

серверима било да се они налазе у облаку или унутар саме фирме, што показује да Интернет као платформа је готово незаменљив део интеркације просечних корисника. Мрежни саобраћај се додатно интензивира и појавом релативно нових хибридних облика апликација, као што су нпр. Progressive Web Apps, које имају за циљ да понуде најбоље од нативних и мобилних Web апликација (Vesić 2016). Оне имају за циљ да побољшају интеркацију са крајњим корисницима и повећају употребу уређаја.

Сајбер простор је небезбедно место на којем постоје и константно се развијају нови моделитети угрожавања безбедности, јер начин на који функционишу комуникациони протоколи и рачунарске мреже, па тиме и Интернет дају могућност злонамерним актерима да познавањем механизама самих мрежа наруше поверљивост, интегритет и расположивост. Имајући у виду да поменуте претње нису усмерене искључиво на нарушавање безбедности информатичко-комуникационе инфраструктуре и самих информација, већ могу бити опасне и по људски живот, највећу пажњу треба посветити њиховој превенцији и то од нивоа појединца и организација до нивоа саме државе (Bjelajac and Vesić 2020). У том смислу, дефинишу се мере техничке и технолошке природе које је потребно спровести, а које су најчешће део дефинисаних политика организације. Ипак, најслабију карику у том ланцу чине запослени, тј. лица који својим понашањем не поштују свесно или не прописане безбедносне политике и тиме омогућавају злонамерним појединцима и организацијама да искористе рањивости разних информатичких система. Безбедносна култура има за циљ да умањи безбедносне претње запослених у организацији по информационе системе саме организације и она се спроводи дефинисањем низа мера. Поменуте се састоје у подизању свести путем тренинга и разних видова едукације, као и спровођењу специфичне комуникације са тимом запослених који су задужени за информатичку безбедност. Познавањем претњи које могу наступити из сајбер простора могуће је идентификовати потенцијалне претње, дефинисати мере које би запослени требало да поштују, радити на њиховом развоју и тиме обезбедити подизање безбедносне културе на потребан ниво тако да те претње буду сведене на прихватљиву меру.

Деца и млади људи у данашње време све више користе Интернет и разне мобилне апликације и то од најранијих дана. Дакле, један део њиховог живота, а пре него што започну свој радни век, обележен је интеракцијом у дигиталном свету. У том свету постоје многобројне опасности са којима они могу да се суоче, а међу најпознатијима су: Интернет педофилија, дигитално насиље и Интернет зависност. Тада је потребно да родитељи, заједно са програмима осмишљеним у основним и средњим школама делују на њих да усвоје одговарајуће понашање и навике у вези безбедносне културе у дигиталном свету.

Безбедносни изазови у употреби Интернета и мобилних апликација

Перманентан напредак у развоју информационих технологија, заједно са могућностима реализације нових и ефикаснијих пословних модела уз све већу

интеграцију различитих дигиталних сервиса води ка све већој употреби Интернета. Поменути тренд доводи до нарастања претњи из сајбер простора, при чему поред старих начина угрожавања безбедности, појављују се и нови модалитети. Сада ћемо навести неке нападе и претње који су упућене или повезане са запосленима од којих се очекује да реагују на адекватан начин и спрече опасност.

У првом реду је свакако фишинг (*phishing)*, као дигитална форма социјалног инжењеринга која користи лажне e-mail-ове који имају аутентичан изглед у којима се траже информације од корисника или се упућују на лажни Websajt који захтева информације (Stallings 2018, 124). Те информације су најчешће шифра и лозинка за приступ и број кредитне картице, а понекад и сам новац. E-mail делује као да је послат са неког извора важног за крајњег корисника, која има за циљ да га убеди да отвори његов прилог, у којем се налази одређени малициозни програм или да кликне и из претраживача отвори URL адресу лажног Websajta (The European Union Agency for Cybersecurity 2020a). Напреднија варијанта овог напада је спир фишинг (*spear phishing*) у којем је мета којој се прослеђује e-mail веома добро истражена од стране нападача који шаље добро конструисану поруку тако да мета не може да се посумња у њену аутентичност. Најчешће се употребљава у домену пословања и као прилог може да садржи злонамерне програме који су прерушени у форму лажних фактура, пословних докумената или неких других садржаја која су предмет пословања и која су очекивана од стране примаоца (Stallings and Brown 2018, 232).

Једна од веома честих превара која користи спир фишинг је *Business Email Compromise*, скраћено BEC. Ова форма преваре је идентификована од стране FBI-а као најчешћа форма финанасијске преваре путем Интернета, која има различите облике, а најчешћи су (FBI n.d.):

– продавац са којим компанија послује прослеђује фактуру са ажурираном адресом примаоца
– генерални директор компаније тражи од свог помоћника да купи поклон картице које ће послати као награду запосленима, где директор пита за серијске бројеве тако да може одмах да их проследи e-mail-ом
– купац некретнине добија поруку од своје агенције са упутствима о томе како да уплати свој депозит

Према наводима IC3 центра у периоду од 2016. до 2019. године финансијска средства која су добављена BEC преваром износе око 26 милијарди долара (IC3 2019). Током 2003. године основана је радна група за борбу против фишинга, Anti-Phishing Working Group, скраћено APWG, која броји преко 1700 компанија широм света, где су најистакнутији чланови компаније које се баве производњом антивирусног софтвера и превенцијом сајбер претњи као што су: Kaspersky Lab, BitDefender, Symantec McAfee и тд. Сваке године APWG објављује извештај о трендовима, кретањима и учињеној штети од фишинг напада. Закључак тог извештаја је (APWG 2021):

– број фишинг напада сваке године се удвостручава

– BEC преваре све више коштају жртве, где је у последњем тромесечју 2020. дошло до пораста од просечних 75.000 $ у односу на претодно тромесечје у којем је просек износио 48.000 $
– најчешће жртве фишинга су финансијске институције, webmail-ови и сајтови који раде по моделу Software as a service

На велике размере ове врсте напада, а поготово током пандемије COVID-19 указује и европска агенција за сајбер безбедност, ENISA у извештају од јануара 2019. до априла 2020. према којем (The European Union Agency for Cybersecurity 2020a):

– пораст од 667% фишинг напада током једног месеца за време пандемије COVID-19
– 42,8% свих малициозних прилога у email-овима су Microsoft Office документа
– 30% фишинг порука се достави понедељком
– 32,5% свих e-mail порука у свом наслови садржи реч *payment*

Такође постоји још једна форма овог напада под називом *Whaling Attack* или *CEO fraud* у којој запосленом буде прослеђен email који изгледа као да је од неког важног руководиоца нпр. генералног директора или извршног финансијског директора. Овај вид напада захтева значајну припрему нападача, где он потенцијалне везе и односе најчешће истражује путем социјалних мрежа и након тога креира такав email тако да прималац може да му поверује. У том смислу овај напад захтева додатну димензију социјалног инжењеринга, где се искоришћава то што запослени не жели да одбије захтев неког којег перципира као важну особу у компанији (kaspersky 2019). Из свега наведеног може се закључити да је потребно посебну пажњу посветити превенцији од фишинг напада, а поготово зато што он може да буде увод у неки други вид напада. Такође, треба имати у виду и његову велику променљивост и стога је као корисник потребно бити све опрезнији.

Постоји велики број злонамерних програма, тзв. *maleware*-а који наносе штету ИТ инфраструктури неког предузећа. То могу бити разни вируси, тројанци, црви и други који постоје већ годинама, при чему се форме неке од њих мењају са напретком технологије. Један од посебно интересантних и веома заступљених су софтвери за изнуду, тзв. рансомвер (*ransomware)*. Они су форма малициозног софтвера који омогућава хакеру да забрани приступ информацијама од значаја индивидуи или компанији на одређени начин и да за узврат захтева одређену количину новца, у некој форми да би уклонио ту забрану (Brewer 2016). Неке савременије форме овог напада криптују фајлове жртве напада, који постају недоступни све док не плате откуп, где након откупа нападачи декриптују те фајлове. Према извештају европске агенције за сајбер безбедност за 2020. годину, софтвер за изнуду је постао веома полуларан у нападима на државне институције, предузећа и индивидуе, где је (The European Union Agency for Cybersecurity 2020b):

– процењена вредност откупа износи 10,1 милијарду долара током 2019., а плаћен откуп у САД у 2018. години је износио 3,3 милијарде долара

– у односу на 2018. годину дошло је до пораста од 365% у 2019. години напада који су детектовани у пословном домену
– више од 66% организација здравствене заштите је имало искуства са овим типом напада током 2019.
– 45% организација је платило откуп током 2019. године

Према извештају Verizon организације за 2020. годину, софтвери за изнуду чине 27% од укупног малициозоног софтвера који је произвео инциденте (Verizon 2020). Треба напоменути да технике шифровања и дешифровања су део криптографије, науке о чувању података, са циљем да се подаци учине нечитљивим за било којег нападача који би евентуално пресрео поруку. Исти концепти се уједно и користе код софтвера за изнуду, па се у том контексту они припадају криптовирологији, која се бави изучавањем криптографских алгоритама са циљем да се изради малициозни софтвер. Такође, у пракси се понекад јавља проблем да чак и након плаћеног откупа, не уради се декриптовање фајлова, тј. не врати се систем у пређашње стање већ нападач само преузме новац. Новац се најчешће дистрибуира путем криптовалута, као што је биткоин (*bitcoin*), да би се прикрили трагови до нападача. Оно што се може констатовати, јесте да чак и након плаћања откупа мета не може да буде сигурна да је систем враћен у пређашње стање и да неки други проблеми неће веома брзо наступити. Из поменутих разлога израда резервних копија је веома важна активност, а које многа предузећа нису ни до данашњег дана усвојила као праксу. Уколико се нежељени догађај деси, а при томе не постоји резервна копија то може да произведе велике проблеме по пословање, па чак и до његовог престанка.

У циљу да запослени у фирмама буду продуктивнији, као и да се стимулише њихово задовољство и комфор приликом рада, уз могућност да се смање трошкови за куповину засебне опреме, нека предузећа се одлучују да омогуће корисницима да на посао донесу своје уређаје и путем њих користе апликације и податке самог предузећа. Поменут концепт се назива *Bring your own device*, скраћено BYOD и у пракси се реализује тако што запослени на посао донесу своје преносиве рачунаре, таблете и / или мобилне телефоне. Код овог концепта корисници уређаја већ поседују одређена знања и фамилијарни су са употребом уређаја и апликација на њему, па граница између проведеног времена на послу и слободног времена бледи, а сами запослени проводе више времена у обављању посла. Статистички извештаји за 2020. годину потврђују напред наведене чињенице и указују на значајан пораст овог тренда у свету (Georgiev 2021):

– 67% запослених користи личне уређаје на послу
– примена BYOD концепта креира додатних 350$ сваке године по запосленом
– запослени који доноси свој уређај у просеку ради 2 сата више
– 87% пословања је зависно од способности својих запослених да приступе пословним мобилним апликацијама са свог паметног телефона
– 69% доносиоца одлука у ИТ у САД кажу да је BYOD добра ствар

– величина BYOD тржишта се очекује да порасте на 366.95$ милијарди до 2022. године
– 59% организација је усвојило BYOD

BYOD је постао веома популаран у образовне сврхе и многе основне и средње школе, као и факултети су усвојили његову употребу и прилагодили се томе. Неке основне предности које школе виде су: побољшање комуникације и колаборације, смањење трошкова, апсолутна контрола на уређају, дељење информација је једноставно, помаже студентима да приступе додатним информацијама и промовише учење у покрету (Soni 2017). Једна од битних карактеристика у упореби BYOD концепта у образовним институцијама, јесте да поред смањења трошкова где је потребно за сваког ученика обезбедити уређај, ученици своје време ван школе могу користити за учење преко својих уређаја, за разлику од употребе уређаја који се налазе у лабараторијама и који раде само онолико колико лабараторија ради (Afreen 2014). Као и већина концепата која има своје добре стране, постоје и оне лоше, а код BYOD-а те лоше су везане за безбедносне ризике и ризике по приватност које могу бити: технички ризици, затим одсуство безбедносне политике, недостатак безбедносне контроле, недостатак свести о безбедности и недостатак приватности (Alotaibi and Almagwashi 2018). У техничке ризике се сврставају: малициозни софтвер, фишинг, социјални инжењеринг, хаковање, spoofing и мрежни напад, као и губитак или крађа самог уређаја. Код крађе, губитка или продаје самог уређаја проблем може настати уколико подаци или документа предузећа нису уклоњена, а који се могу искористити за конструисање напада. Остали ризици су везани за дефинисање одговарајућих безбедносних политика, као и подизања свести самих запослених.

Поред BYOD-а, један од проблема који се може јавити приликом употребе мобилних апликација, јесте тзв. цурење података. Крајњи корисници могу да користе апликације које нису проверене и да им дају одређена права да могу да користе разне податке. Ти подаци могу да се копирају на сервере, где разни корисници, па и они малициозни могу да их користе.

Приликом употребе мобилних уређаја могу се јавити такође фишинг напади, при чему је један специјализован баш за тај тип уређаја, јер користи SMS поруке и назива се смишинг (*Smishing*). Као и код класичног фишинг напада кориснику долази порука од некога који се представља да је банка, државна или нека друга институција и тражи њихове личне податке, број рачуна и тд.

Примећено је да постоје и неке поруке које су у вези са пандемијом COVID-19, где се жели деловати на људе тако да изврше активности које су у корист злонамерних корисника. Истраживачи су уочили да постоји одређен број лажних COVID-19 Websajtova који приказују мапе заражених људи корона вирусом, где нападачи усмеравају кориснике да посете те сајтове и оставе податке, а при чему се представљају као владине институције. Такође оно што је примећено јесте и да се таргетирају корисници мобилних уређаја.

Треба рећи и да постоје одређени Websajtovi који варају кориснике продавајући им разне препарате у борби против корона вируса, као и тестове, при

чему су веома активни на социјалним мрежама попут Facebook-а, где корисницима то нуде (Waggoner and Markowitz 2021; Bannister 2021).

Поред наведеног, појављује се и одређени број превара које се нуде путем апликација за четовање, као што су Viber и WhatsApp, где корисницима стижу поруке о невероватним попустима за куповину артикала (O'Brien 2020; Singha 2021). Овај вид социјалног инжењеринга узима разне облике и веома је променљив, тако да крајњи корисници је потребно да развију свест о истим.

Значај безбедносне културе младих на Интернету

У употреби Интернета и мобилних апликација поред нарушавања безбедности ИКТ инфраструктуре и безбедности самих информација, постоји један део претњи по људски живот, а посебно за оне старосне границе које имају најмању могућност да се заштите, а то су деца и млади. Како је доступност уређаја и приступа Интернету временом све већи, тако опада и граница са којим деца започињу своју интеракцију у дигиталном свету. Млади родитељи обављају многе улоге данас, у једном убрзаном свету, где перманентно расте количина и проток информација које се размењују на дневном нивоу, а уједно и број обавеза које имају. Због тога они не могу посветити довољно времена свом детету са једне стране, док са друге се труде да своју родитељску улогу обављају најбоље могуће и тиме не желе да њихово дете пропусти било који модеран садржај који се нуди, како би ишло у корак са својом генерацијом. На тај начин, они веома често поспешују интеракцију деце са дигиталним светом, при томе ни не размишљајући о томе које опасности постоје у том свету. У почетку то су у питању одређени мултимедијални аудио или видео садржаји, затим видео игре, а полако се откривају и нове могућности, као што је интеракција путем социјалних мрежа и путем апликација за размену порука (чета), као и могућност да се одређени наставни програми прате путем мреже и тд. Све ове различите врсте интеракције код деце стварају осећај да је Интернет једно добро и забавно место, а касније како одрастају и постају млади људи да дигитални свет је неодвојив део њихове реалности. Дакле на одређен начин, сам модел система и моделоване интеракције постају замена или проширење, у целости или делимично, за систем и интеракције у њему. Измењени односи између реалног света и његовог модела нису без последица, јер није мали број несрећних случајева, где су чак неки од њих са смртним исходом. То се манифестује на примеру неколико изгубљених младих живота употребом TikTok друштвене мреже (Дерикоњић 2021). Други део проблема које граница између реалног и дигиталног света доноси, јесте да се одређене аномалије и девијантна понашања преносе из реалног у дигитални свет и тамо попримају нове димензије, облике и нови интензитет испољавања, а при томе имају исте последице као да су настале у реалном свету. Неке од њих су: Интернет педофилија, дигитално насиље и зависност од Интернета. Специфичност посматраних феномена и њихово дејство на људско понашање како у реалном, тако и у виртуалном свету Бјелајац и Филиповић објашњавају кроз међудејство два троугла,

где први троугао чине Интернет, дигитални уређаји и дигитални садржаји, а други чине интерконективност, интерактивност и анонимност (Бјелајац and Филиповић 2021). Дакле, специфичности у употреби Интернета између све већих група корисника, који при томе не морају да прикажу свој прави идентитет, уз појачану интеракцију даје један велики простор да се описане појаве и реализују. Може се очекивати да ће оне расти у наредном периоду са трендом раста остваренog Интернет саобраћаја, што све људе треба да забрине, али и да их подстакне да се пронађу механизми у њиховом спречавању. Безбедносна култура, дигитална писменост и подизање свести код родитеља да морају да делују на децу у правцу очувања њихове личне заштите на Интернету су мере које треба да буду део предшколских и школских програма, а и посебних видова едукације самих родитеља.

Аутори наводе да је Интернет педофилија специфични вид компјутерског криминалитета јер педофили све више лутају електронским мрежама и траже жртве, поводљиву и лаковерну децу. Интернет је постао ново игралиште доступно педофилима, где су деца перманентно изложена непримереним сексуалним садржајима и узнемирујућим и непријатељским порукама. Савремена криминолошка и виктимолошка истраживања темељно су променила појавну слику сексуалног злостављања деце. Сексуални деликти усмерени према деци често се догађају, недовољно су истражени, тешко их је контролисати, а починитељи су у само ретким случајевима психички неморални. После преживљене виктимизације последице по већину деце су тешке и дуготрајне (Бјелајац and Филиповић 2020). Са аспекта сајбер безбедности и заштите рачунарских мрежа, може се направити одређена паралела између социјалног инжењеринга и Интернет педофилије, у смислу припремних радњи које предатор спроводи према мети. Код педофилије може уочити један много интензивнији напор не само у спровођењу истраживања мете, већ и припреме плана активности у вези са њом као и одржавања везе са истом кроз разне форме манипулација.

Дигитално насиље се односи на такву употребу технологије која проузрокује стид, позива друге на чињење насиља и узнемиравање и наноси психолошку штету (Von Solms and Van Niekerk 2013). Испољава се у виду вршњачког насиља где се узнемираваном детету или младој особи прети слањем порука, објављују се срамотне фотографије и особа извргава руглу. Поред тога могу и да се објављују подаци из приватног живота, па чак и да се на порнографским сајтовима каче садржаји у вези особе. Такве радње могу да доведу младу особу у неслућену опасност, тако што ће усмерити предаторе ка њој.

Бјелајац и Филиповић указују да зависност од Интернета се види кроз то колико се свакодневно функционисање појединаца мења у односу на изложеност одређеним дигиталним садржајима. Интензитет ове врсте зависности се може поредити са зависностима од никотина, алкохола или коцања, а посебно може бити изражена у форми губитка контроле када лице буде лишено дигиталног садржаја (Bjelajac and Filipović 2020). Млади су посебно подложни, а манифестује се: веома честим проверама статуса на друштвеним мрежама, лајковањем људи за које сматрају да су гуруи у некој области која их занима,

дописивању са другим корисницима, играњем онлајн (*online*) игрица и тд. Све ове активности на дугорочно могу имати последица по њихово здравље.

Актуелност проблема

Безбедносни изазови расту у целом свету са порастом саобраћаја на глобалној мрежи из године у годину, а то је додатно наглашено током COVID-19 пандемије где расте тренд сајбер напада и превара којима су изложени појединици, организације па и државе.

Одређени број напада је упућен ка здравственим установама у свету, где долази до крађе картона одређеног броја пацијената. На примеру Elara Caring здравствене установе која пружа кућну негу пацијентима у САД у децембру 2020. дошло је до крађе података за преко 100.000 пацијената, при чему се сумња да је дошло до преузимања њихових имена, датума рођења, адресе, броја телефона, информација о банковним рачуним, броја здрвственог осигурања, броја возачке дозволе (HIPAA Journal 2021). Истрага је у току, а за сада оно што је познато јесте да су са одређеног налога 2 запослена добила фишинг email-ове. Још један случај који је изазвао велику пажњу у заједници, јесте крађа података у серији сајбер напада између 2018. и 2019. године на велику клинику за ментално здравље у Хелсинкију, где су украдени чак и подаци из појединачних терапеутских сесија (Kleinman 2020). Клиника је уцењивана са плаћањем у биткоинима у вредности од око 530.000$, а поред тога су уцењивани и појединци због личних података од 200 до 500EUR, такође у биткоинима. Сличан пример изнуде се појавио и код светски познате компаније Foxconn, где је око 1200 сервера заражено софтвером за изнуду, а сајбер криминална група је тражила откуп у вредности од око 1800 биткоина, што је у том тренутку износило око 33 милиона долара (Riley 2020). Слично искуство је искусила и фирма Barnes & Noble, једна од највећих продавница књига на свету, где је њихов сервис Nook компромитован (Osborne 2020). Монро колеџ у Њујорку је такође био мета напада рабсомвером, где су хакери тражили 2 милиона долара од колеџа за откуп у биткоинима (McKenzie 2019). Једна од превара заступљених на мобилним телефонима и апликацији WhatsApp, јесте да уочи празника Дана жена стижу поруке о многобројним наградама које се могу освојити, а при томе се контакти представљају да су Amazon или Adidas (Smith 2021).

Ситуација у Србији не одудара много од ситуације у остатку света. 7. и 8. априла 2021. године великом броју корисника у Србији је стигао email, где су се сајбер криминалци представили као ЈП Пошта Србије и где се корисници обавештавају да им пакет није испоручен, јер није плаћена царина и да је потребно да плате одређен износ (ЈП Пошта Србије 2021; Nacionalni CERT Republike Srbije 2021). Поменути фишинг напад је медијски испраћен, а и само предузеће се оградило од истог и назначило злоупотребу симбола Поште Србије. У марту 2020. нападнут је информациони систем градске управе Новог Сада у ЈКП „Информатика" (Blic 2020). Сервери поменутог предузећа су заражени софтвером за откуп, а нападачи су за враћање система тражили 50 биткоина,

чији је износ у том тренутку био око 400.000EUR. Напад је покренут прво преко фишинга, где је се након тога инсталирао уцењивачки софтвер PwndLocker и криптовао садржај већег броја рачунара у мрежи и учинио их неупотребљивим.

Сличан напад се догодио у региону, у Хрватској, где је у фебруару 2020. део ИС хрватске нафтне компаније INA неко време био блокиран, тако да нису могли да се издају рачуни, а поред тога настали су проблеми са картицама лојалности и око плаћања рачуна за гас (Bubanja 2020).

Сви наведени случајеви указују да је потребно спровести активности у подизању свести крајњих корисника као и подићи ниво њихове дигиталне писмености и дефинисати јасне сигурносе политике тако да се заштити ИТ инфраструктура. То се спроводи путем безбедносне културе.

Информациона безбедносна култура

Према Бјелајцу и Јовановићу безбедносна култура укључује безбедносне активности које изражавају спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима (Бјелајац and Јовановић 2013). Релизује се препознавањем опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности. Безбедносну културу сачињавају 3 главна елемента: технологија, политика (правила) и корисници, који интерагују на начин да људи политикама утичу на начин употребе технологије, а развојем технологија креирају се нове политике (Milovanović and Radovanović 2015). Оно на шта је потребно обратити пажњу јесте да се безбедносна култура успоставља у дужем периоду и не може „преко ноћи", већ је то једна перманента добро осмишљена радња, подложна промени јер се друштво, људи и њихови односи, наука, технологија, па и безбедносне претње мењају временом.

Све организације имају потребу да дефинишу политике којима се са једне стране штити ИТ инфраструктура, а такође и оне друге које усмеравају кориснике да својим деловањем не угрозе постојеће безбедносне механизме којима се она штити. Информациона безбедносна култура контекстуализује се у понашању људи у организационом контексту како би заштитила информације које организација обрађује кроз поштовање информационих безбедносних политика и процедура и разумевања како се захтеви спроводе на опрезан и пажљив начин уграђени у редовну комуникацију, свесност, тренинг и едукационе иницијативе (da Veiga et al. 2020). Дакле, спровођењем одговарајућих информационих безбедносних политика и процедура, остварује се информациона безбедност, а оне настају адекватним понашањем запослених које се остварује кроз дугорочну комуникацију, тренинг, специфичне видовиме едукације и подизање свести о безбедносно важним информатичким средствима. На тај начин се успоставља информациона безбедносна култура као део укупне безбедносне културе једне организације.

Аутори као што су Цимерман и Рено, због нарастајућег тренда сајбер напада указују да можда полазне основе нису добре и да приступ „човек као део проблема" треба да се напусти или редефинише на начин да постане „човек као део решења" (Zimmermann and Renaud 2019). Њихова аргументација лежи у томе да тренутне активности које се спроводе према људима које их искључују, тренирају, ограничавају и контролишу доводе до тога да се отпор према политикама безбедности увећава. Другачији приступ се састоји у експертизи, флексибилности и учењу из позитивних, али и негативних примера, где се путем комуникације и сарадње смањује отпор прека политикама сајбер безбедности. Описани приступ није још тестиран у пракси, па нема много информација о његовој ефективности и ефикасности, али он је значајан јер указује на то да дизајн програма за креирање информационе безбедносне културе треба да буде такав да избегне да циљана група над којој се спроводи програм не створи јак отпор према безбедносним политикама. Поменута пракса се може тумачити чињеницом да не постоје адекватна експертиза из свих потребних области у односу на активности усмерених ка запосленима, као циљане групе над којом се спроводи програм, већ се поменути програми спроводе изоловано, тј. искључиво са безбедносног и информатичког апсекта.

Да би се поменути проблем превазишао, а истовремено програми који треба да утичу на успостављање и одржавање безбедносне културе били целисходни, одређени аутори дефинишу оквире безбедносне културе. Роер и други су дефинисали оквир безбедносне културе, који је настао као резултат најбољих пракси и он има за циљ да креира програме путем којих се успоставља и одржава информациона безбедносна култура (Roer 2015, 41-51).

Оквир је организован према ПДЦА методи која има за циљ да континуирано побољша резултате и састоји се из 4 дела:

– Метрике
– Организација
– Теме
– Планер

У делу Метрике дефинишу се циљеви шта се жели програмима постићи, тј. шта у вези са безбедносном културом је потребно остварити. Оквир усмерава да се дефинишу 2 типа циљева (The Roer Group 2014a): циљеви орјентисани на резултат и циљеви орјентисани на учење. Примери могу бити:

– циљ орјентисан на резултат - За 6 месеци организација треба да смањи број захтева у вези „заборављених лозинки" за 50%.
– циљ орјентисан на учење - Они који прођу тренинг треба да буду свесни значаја јаких лозинки, да добију искуство у креирању јаких лозинки и да науче како да њима управљају на сигуран начин и да могу да поделе то знање.

Да би се циљеви јасно дефинисали потребно је одредити тренутно стање, а затим одредити које је то жељено стање. Зато је потребно спровести одговарајућа мерења да би се утврдило тренутно стање. Ово је најтежа активност у овом поступку, јер од ње све остале зависе. Орехек и Петрич су дали детаљан

преглед метода за мерење безбедносне културе и утврдили да већина приступа нуди ограничене резултате у погледу валидације скале и да се строгост којом се вреднују скале информационе безбедносне културе веома разликује и да ниједна не задовољава све критеријуме оцењивања (Orehek and Petrič 2020). Ову чињеницу је потребно посебно имати у виду приликом спровођења програма, јер уколико не меримо адекватно, тј. не користимо исправно мерни апарат не можемо имати праву слику о тренутном, а и жељеном стању.

У делу Организација је са једне стране потребно да се одреди који људи ће чинити тим који ће да планира и води програм, а са друге да се одреди која је то група запослених која ће похађати тај програм. Тим људи који води програме требало би најмање да има компетенције из следећих области: безбедност, комуникација, култура и тренинг. Самим тим потребно је да буду укључени запослени из организационе јединице за безбедност, затим за маркетинг и комуникацију, као и неко из организационе јединице за људске ресурсе (Roer 2015, 44). Тај тим је потребно да направи план и одреди листу активности који ће се спроводити над групи запослених, тј. да креира кампању за сваку групу корисника. Сваку групу корисника је важно пажљиво анализирати и одредити како ће се активности у тој групи реализовати, јер свака од њих је специфична за себе и зато не постоји универзалан приступ, већ су све активности подложне модификацији. Такав приступ омогућава да се значајно смањи отпор запослених у усвајању нових политика.

У делу Теме прво је потребно одредити које су то безбедносно важне теме или изазови, који ће бити обухваћени програмом. При томе, треба имати у виду да оне морају да буду у корелацији са циљевима који се желе постићи. Неке од тема могу бити: социјални инжењеринг, фишинг, BYOD, управљање шифрама, рад на социјалним мрежама и тд. Након тога је потребно одредити активности које је потребно спровести, а које су у вези са одабраном темом. Неке од њих могу бити (The Roer Group 2014b): е-учење, курс, демонстрација уживо, видео демонстрација и тд.

У делу Планер се креира детљан план који се састоји од: дефинисаних циљева, циљаних група, различитих активности и када их је потребно спровести, а затим и када измерити напредак. Упрошћена реализација програма информационе безбедносне културе може да се спроведе тако што (Kassner n.d.):

– одреди се тим за креирање програма
– дефинишу се циљеви програма
– утврди се тренутни статус (мерење)
– дефинишу се циљане групе
– одаберу се теме
– планира се и спроведе тренинг
– поново се спроведе мерење
– изврши се ревизија
– понови се поступак

Поменути начин осигурава да се дугорочно иде ка успостављању, а затим и одржавању информационе безбедносне културе. Прво се спроведе про-

грам који обради једну тему, нпр. фишинг, након тога се одабере нова тема, нпр. управљање шифрама, и тако једна по једна тема док се не обраде све теме који један програм треба да испуни. Дакле, ради се о перманентној активности која има за циљ да прво креира, а затим увећа и одржи информациону безбедносну културу, јер појављивањем нових модалитета угрожавања безбедности или мењањем начина реализације постојећих, фонд безбедносних претњи се увећава, па је потребно и адекватне одговоре на исте омогућити. На тај начин се утиче на идеје, навике и понашање запослених тако да омогуће да организација буде ослобођена безбедносних претњи.

Сличан поступак се може применити у дефинисању безбедносних програма које треба да утичу на дефинисање и одржавање информационе безбедносне културе младих. Такође, постоје одређене модификације које би требало да се спроведу, а оне се односе пре свега у инкорпорирање родитеља у програм, где би се уједно и дефинисао део активности које они треба да спроводу са својом децом да би ефекти програма били задовољавајући. Поред тога, требало би организовати програме у склопу школа, где у склопу наставног плана и програма, млади људи би створили потребне навике и усвојили жељена понашања која би им помогла у очувању личне безбедности.

Закључак

Информациона безбедносна култура има за циљ да обезбеди дугорочне навике и понашања запослених у односу на изазове који долазе из сајбер простора. Велики део тих изазова настаје у употреби Интернета и мобилних апликација које запослени користе и тиме стварају могућности да дође до нарушавања безбедности самих информација, информатичко-комуникационе инфраструктуре, а у неким случајевима чак и до креирања опасности по људски живот. Познавајући те претње, ствара се могућност да се кроз оквир безбедносне културе, путем којег се креирају едукативни програми, креира и одржава информациона безбедносна култура. Пажљиво осмишљени програми омогућавају да се пракса у поступању према различитим безбедносним изазовима у континуитету прати, анализира и мери, а затим да се спроводу оне активности које имају за циљ да креирају и одрже идеје, навике и понашања запослених дугорочно у вези са поменутим изазовима. На тај начин се осигурава да се отпор који запослени имају у спровођењу дефинисаних политика безбедности умањи, а самим тим и очувају информатичко-комуникациона средства организације. Пре него што постану запослени, млади људи такође могу да имају многе проблеме које настају у употреби Интернета и мобилних апликација, где последице по њихов живот могу да буду велике. Зато је важно да се родитељи од најранијих дана, када њихово дете ступи у интеракцију на Интернету, побрину и усмере га тако да усвоји норме које му помажу да очува своју безбедност. На том путу безбедносна култура, дигитална писменост и едукација родитеља су кључни у остваривању поменутих циљева. Разумевањем и усвајањем специфичности које носи Интернет које се огледају у његовој интерконективности, интерактивности и анонимности, омогући ће младој особи да се заштити.

Литература

1. Afreen, Rahat. 2014. "Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges." *International Journal of Emerging Trends & Technology in Computer Science* III (1): 233–236.
2. Alotaibi, Bashayer, and Haya Almagwashi. 2018. "A Review of BYOD Security Challenges, Solutions and Policy Best Practices." In *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*, 1–6. IEEE. https://doi.org/10.1109/CAIS.2018.8441967.
3. APWG. 2021. "Phishing Attack Trends Report – 4Q 2020." https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf.
4. Bannister, Adam. 2021. "Fake Covid-19 Vaccines Pose 'Serious Health Hazard', Warns Interpol.", poslednji pristup 05.04.2021. https://portswigger.net/daily-swig/fake-covid-19-vaccines-pose-serious-health-hazard-warns-interpol.
5. Бјелајац, Жељко Ђ., и Милован Б. Јовановић. 2013. „Поједини аспекти безбедносне културе на Интернету", *Култура полиса*, X (21): 99-114
6. Бјелајац, Жељко Ђ., и Александар М. Филиповић. 2020. „Интернет и друштвене мреже као неограничени простор за концентрацију и мултиплицирано присуство педофила", У „Педофилија – узроци и последице", ур. Жељко Бјелајац и Александар М. Филиповић, посебно издање, *Култура полиса*: 29-40.
7. Бјелајац, Жељко Ђ., и Александар М. Филиповић. 2021. „Флексибилност дигиталних медија за манипулативно деловање сексуалних предатора", *Култура полиса*, XVIII (44): 51-67.
8. Bjelajac, Željko Đ., and Aleksandar M. Filipović. 2020. "Internet Addiction Disorder (IAD) as a Paradigm of Lack of Security Culture.", *Kultura polisa*, XVII (43): 239-258.
9. Bjelajac, Željko Đ., and Slavimir Lj. Vesić. 2020. "Security of Information Systems." *Pravo - Teorija i Praksa* XXXVII (2): 63–76. https://doi.org/10.5937/ptp2002063b.
10. Blic. 2020. „Kako su hakeri napali Novi Sad - sve o najvećem napadu ikada: Tražili pola miliona evra i danima ucenjivali Srbiju." poslednji pristup 05.03.2020. https://www.blic.rs/vesti/drustvo/kako-su-hakeri-napali-novi-sad-sve-o-najvecem-napadu-ikada-trazili-pola-miliona-evra/5g8dqe2.
11. Brewer, Ross. 2016. "Ransomware Attacks: Detection, Prevention and Cure." *Network Security* MMXVI (9): 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1.
12. Bubanja, Branislav. 2020. "Ransomware napad na hrvatsku naftnu kompaniju INA." poslednji pristup 17.11.2020. https://pcpress.rs/ransomware-napad-na-hrvatsku-naftnu-kompaniju-ina/.
13. Дерикоњић, Мирослава. 2021. "„Тикток" изазов као позив на самоубиство." poslednji pristup 03.03.2021. http://www.politika.rs/scc/clanak/471881/Tiktok-izazov-kao-poziv-na-samoubistvo.

14. FBI. n.d. “Business Email Compromise.” Accessed March 27, 2021. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise.
15. Georgiev, Deyan. 2021. “41 Stunning BYOD Stats and Facts to Know in 2020.” poslednji pristup 01.04.2021. https://techjury.net/blog/byod/.
16. HIPAA Journal. 2021. “PHI of More Than 100,000 Elara Caring Patients Potentially Compromised in Phishing Attack.” poslednji pristup 31.03.2021. https://www.hipaajournal.com/phi-of-more-than-100000-elara-caring-patients-potentially-compromised-in-phishing-attack/.
17. IC3. 2019. “Business Email Compromise The $26 Billion Scam.” poslednji pristup 18.03.2021. https://www.ic3.gov/Media/Y2019/PSA190910.
18. ЈП Пошта Србије. 2021. „Упозорење - злоупотреба симбола Поште Србије.” poslednji pristup 09.04.2021. https://www.posta.rs/cir/info/vest-detaljnije.aspx?ID=7028.
19. kaspersky. 2019. “What Is a Whaling Attack?” poslednji pristup 01.04.2021. https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack.
20. Kassner, Michael. n.d. “Create a Security Culture Framework to Protect against Threats.” Accessed April 4, 2020. https://www.techrepublic.com/article/create-a-security-culture-framework-to-protect-against-threats/.
21. Kleinman, Zoe. 2020. “Therapy Patients Blackmailed for Cash after Clinic Data Breach.” poslednji pristup 03.04.2020. https://www.bbc.com/news/technology-54692120.
22. McKenzie, Lindsay. 2019. “Hackers Demand $2 Million From Monroe.” poslednji pristup 17.03.2021. https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack.
23. Milovanović, Zoran, and Radovan Radovanović. 2015. “ Informaciono-bezbednosna kultura - imperativ savremenog društva.” *NBP – Journal of Criminalistics and Law* XX (3): 45–65.
24. Mroczkowska, Agnieszka. 2021. “What Is a Mobile App? | App Development Basics for Businesses.” poslednji pristup 10.04.2021. https://www.thedroidsonroids.com/blog/what-is-a-mobile-app-app-development-basics-for-businesses.
25. Nacionalni CERT Republike Srbije. 2021. „Phishing kampanja za korisnike poštanskih usluga.” poslednji pristup 10.04.2021.
26. O’Brien, Jim. 2020. “DHL and Viber SMS Scams to Watch Out.” poslednji pristup 04.01.2021. https://techbuzzireland.com/2020/02/28/dhl-viber-scams-sms-phishing/.
27. Orehek, Špela, and Gregor Petrič. 2020. “A Systematic Review of Scales for Measuring Information Security Culture.” *Information and Computer Security*. https://doi.org/10.1108/ICS-12-2019-0140.
28. Osborne, Charlie. 2020. “Barnes & Noble Confirms Cyberattack, Ransomware Group Leaks Allegedly Stolen Data.” poslednji pristup 31.03.2021. https://www.zdnet.com/article/barnes-noble-confirms-cyberattack-customer-data-breach/.

29. Research and Markets. 2020. "Worldwide Industry for IoT Middleware to 2025 - Manufacturing Expected to Have High Potential Growth." poslednji pristup 31.03.2021. https://www.globenewswire.com/news-release/2020/12/21/2148872/0/en/Worldwide-Industry-for-IoT-Middleware-to-2025-Manufacturing-Expected-to-Have-High-Potential-Growth.html.
30. Riley, Duncan. 2020. "Foxconn Plant in Mexico Struck in DoppelPaymer Ransomware Attack." 31.03.2021. https://siliconangle.com/2020/12/08/foxconn-plant-mexico-struck-dopplepaymer-ransomware-attack/
31. Roer, Kai. 2015. *Build a Security Culture*. Ely, Cambridgeshire: IT Governance Publishing.
32. Singha, Rajiv. 2021. "Beware of the WhatsApp Scam That Promises Free Adidas Shoes!" poslednji pristup 04.01.2021. https://blogs.quickheal.com/beware-adidas-scam-whatsapp1/
33. Smith, Adam. 2021. "WhatsApp Gift Scams From Fake Amazon and Adidas Websites Spread on International Women's Day." poslednji pristup 01.04.2021. https://www.independent.co.uk/life-style/gadgets-and-tech/whatsapp-gift-scam-international-women-day-amazon-adidas-b1814003.html.
34. Solms, Rossouw Von, and Johan Van Niekerk. 2013. "From Information Security to Cyber Security." *Computers and Security* XXXVIII (2013): 97–102. https://doi.org/10.1016/j.cose.2013.04.004.
35. Soni, Aakash. 2017. "6 Advantages Of BYOD In The Classroom." poslednji pristup 01.04.2021. https://elearningindustry.com/byod-in-the-classroom-6-advantages.
36. Stallings, William. 2018. *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. 1st ed. Boston: Addison-Wesley Professional.
37. Stallings, William, and Lawrie Brown. 2018. *Computer Security: Principles and Practice*. 4th ed. New York: Pearson Education Limited.
38. The European Union Agency for Cybersecurity. 2020a. "ENISA Threat Landscape 2020 - Phishing." https://www.enisa.europa.eu/publications/phishing/at_download/fullReport.
39. The European Union Agency for Cybersecurity. 2020b. "ENISA Threat Landscape 2020 - Ransomware." https://www.enisa.europa.eu/publications/ransomware.
40. The Roer Group. 2014a. "Metrics – What to Measure, Why and How." poslednji pristup 03.04.2021. https://securityculturefreamework.net/metrics-what-to-measure-why-and-how/.
41. The Roer Group. 2014b. "Topics Module." poslednji pristup 03.04.2021. https://securityculturefreamework.net/topics-module/.
42. Veiga, Adéle da, Liudmila V. Astakhova, Adéle Botha, and Marlien Herselman. 2020. "Defining Organisational Information Security Culture—Perspectives from Academia and Industry." *Computers and Security* 92: 101713. https://doi.org/10.1016/j.cose.2020.101713.
43. Verizon. 2020. "2020 Data Breach Investigations Report." https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

44. Vesić, Slavimir Lj. 2016. „Progresivne Web aplikacije - Između nativnih i mobilnih Web aplikacija." *InfoM* MMXVI (60): 43–49.
45. Waggoner, John, and Andy Markowitz. 2021. "Beware of Robocalls, Texts and Emails Promising COVID-19 Cures or Stimulus Payments." poslednji pristup 17.03.2021. https://www.aarp.org/money/scams-fraud/info-2020/coronavirus.html.
46. Zimmermann, Verena, and Karen Renaud. 2019. "Moving from a 'human-as-Problem" to a 'human-as-Solution" Cybersecurity Mindset." *International Journal of Human Computer Studies* CXXXI (November): 169–87. https://doi.org/10.1016/j.ijhcs.2019.05.005.

SLAVIMIR LJ. VESIĆ*
PUC "Belgrade Waterworks and Sewerage"
Belgrade

Review work
Received: 04.02.2021
Approved: 12.04.2021
Page: 79–96

THE INFLUENCE OF SECURITY CHALLENGES IN THE USE OF THE INTERNET AND MOBILE APPLICATIONS ON CREATING A SECURITY CULTURE

Summary: The growing number of threats and challenges from cyberspace, due to the increasing use of the Internet and mobile applications as never before, requires the implementation of security policies aimed at preserving the information and communication assets of the company. Security is achieved through one part of measures that are technical-technological in nature, and the other part is related to the actions of people in the organization. People are known to be the weakest link, and security culture aims to act on people by adopting certain behaviours, building habits and establishing communication in a way that they can respond to threats from cyberspace. Information security culture is established and maintained through programs that aim to prepare people for current and future challenges from cyberspace. One day, young people will start working, but until that moment, parents, in synergy with school institutions, should direct them so that they accept certain behaviours and norms. In this way, the security culture ensures that their security is preserved from the earliest days, so it is necessary to develop programs at different levels of education that will enable this.

Keywords*:* information security culture, security culture framework, creating a security culture, cyber security, youth safety

Introduction

The exit of the global network of connected computers, the Internet, from the circle of the scientific and academic community, is associated with the creation of the World Wide Web (generally accepted Web) and the emergence of the first search engines, in the early 90s of last century. Since then, the most famous

* vesic.slavimir@gmail.com

global network has experienced a huge expansion. Many services that can be used through the Internet service model, such as e-mail, searching, viewing, creating and sharing various content: documents, pictures, videos, etc., then connecting with friends and maintaining contacts in the form of social networks, company, etc. have become an indispensable part of our reality. One of its most important features is its ubiquity, which allows it to connect anywhere and anytime. Continuous improvement of Internet access, especially through wireless networks, with the declining price of sensors and actuators, as well as miniaturization, and the increasing adoption of the paradigm of cloud computing, leads to a huge increase in connecting various devices to the World Wide Web - the Internet of Things. The initial idea of communication between people has been expanded so that people interact with different "things" and "things" also interact with each other. The GSMA, an association representing the interests of mobile operators, predicts that by the end of 2025, there will be around 25 billion Internet of things online (Research and Markets 2020). Due to the need for increased scope at the global level, the adoption of version 6 of the IP communication protocol, which is the core of the Internet, is accelerating.

Almost four decades ago, the first mobile phones with very limited functionalities such as alarm, calculator and calendar, etc. appeared. Over time, the price of mobile devices decreased, so they were more acceptable to the general population, which opened the possibility to add new and expand their existing functionalities. Mobile manufacturers at the time saw the use of the Internet as a good way to attract customers and offered them WAP, which was actually an impoverished version of HTTP, a protocol that is crucial for the Web. Due to the poor user experience, WAP is not widely accepted, so the mass use of the World Wide Web on mobile devices has prolonged until the advent of smartphones. Smartphones, as multifunctional devices, have contributed to the reduction of the market of many devices such as GPS, MP3 players, dictaphones, cameras, etc. Since their inception with the advent of the iPhone in 2007, users have seen many benefits, so interaction with smartphones and touch screens has been quickly embraced. As the mobile app market grew, users used the apps more and more, and this has made life almost unthinkable for most people today without using at least some of the mobile apps daily. According to some research, a typical smartphone user checks their phone about 63 times a day, the average US user has about 100 applications installed, 87% of users use a smartphone at least 1 hour before bedtime, while 69% use it at least 5 minutes before bedtime, about 7 billion people around the world use mobile phones by the end of 2021, by the end of 2022 the number of downloaded applications will reach 258 million per year (Mroczkowska 2021). These allegations show that the amount of interaction achieved through smartphones is huge and that for most users it is an indispensable device. Most mobile phone applications use the Internet in their background to exchange data with remote servers, whether they are in the cloud or within the company itself, which shows that the Internet as a platform is an al-

most indispensable part of the interaction of average users. Network traffic is additionally intensified with the appearance of relatively new hybrid forms of applications, such as e.g. Progressive Web Apps, which aim to offer the best of native and mobile Web applications (Vesić 2016). They aim to improve interaction with end-users and increase device usage.

Cyberspace is a dangerous place where new models of security threats exist and are constantly being developed, because the way communication protocols and computer networks work, and thus the Internet, allows malicious actors to violate confidentiality, integrity and availability by knowing the mechanisms of networks. Bearing in mind that the mentioned threats are not aimed exclusively at violating the security of the information and communication infrastructure and the information itself, but can also be dangerous to human life, the greatest attention should be paid to their prevention from the level of individuals and organizations to the state level (Bjelajac and Vesić 2020). In that sense, measures of technical and technological nature that need to be implemented are defined and are most often part of the defined policies of the organization. However, the weakest link in that chain consists of employees, ie. persons who by their behaviour do not consciously or unconsciously respect the prescribed security policies and thus enable malicious individuals and organizations to exploit the vulnerabilities of various information systems. Security culture aims to reduce the security threats of employees in the organization to the information systems of the organization and it is implemented by defining a series of measures. These include raising awareness through training and various forms of education, as well as conducting specific communication with the team of employees in charge of information security. By knowing the threats that can occur from cyberspace, it is possible to identify potential threats, define measures that employees should respect, work on their development and thus ensure the raising of safety culture to the required level so that these threats are reduced to an acceptable level.

Nowadays, children and young people are increasingly using the Internet and various mobile applications from the earliest days. So, one part of their life, and before they start their working life, is marked by interaction in the digital world. There are many dangers they can face in that world, and the most famous are Internet paedophilia, digital violence and Internet addiction. It is then necessary for parents, together with programs designed in primary and secondary schools, to influence them to adopt appropriate behaviours and habits related to safety culture in the digital world.

Security challenges in the use of the Internet and mobile applications

Permanent progress in the development of information technologies, together with the possibilities of realization of new and more efficient business models with the increasing integration of various digital services leads to the

increasing use of the Internet. The mentioned trend leads to an increase in threats from cyberspace, where, in addition to the old ways of endangering security, new modalities also appear. We will now list some attacks and threats that are directed at or related to employees who are expected to respond adequately and prevent danger.

In the first place, there is certainly phishing, as a digital form of social engineering that uses fake e-mails that have an authentic look in which information is requested from users or are directed to a fake website that requires information. (Stallings 2018, 124). This information is most often the user name and password for access and credit card number, and sometimes the money itself. The email appears to have been sent from a source important to the end-user, which aims to persuade him to open his attachment, which contains a certain malicious program or to click and open the URL of a fake website from a browser (The European Union Agency for Cybersecurity 2020a). A more advanced variant of this attack is spear-phishing in which the target to which the email is forwarded is very well researched by the attacker who sends a well-constructed message so that the target cannot doubt its authenticity. It is most commonly used in the domain of business and as an attachment may contain malicious programs disguised in the form of fake invoices, business documents or some other content that are the subject of business and that are expected by the recipient (Stallings and Brown 2018, 232).

One of the very common scams that use spear-phishing is Business Email Compromise, abbreviated BEC. This form of fraud has been identified by the FBI as the most common form of financial fraud via the Internet, which has various forms, and the most common are (FBI n.d.):

– the vendor with whom the company does business forwards the invoice with the updated address of the recipient
– the CEO of the company asks his assistant to buy gift cards to send as a reward to employees, where he asks for serial numbers so he can forward them immediately by email
– the buyer of the property received a message from his agency with instructions on how to pay his deposit

According to the IC3 centre, in the period from 2016 to 2019, the financial resources supplied by BEC fraud amounted to about 26 billion dollars (IC3 2019). In 2003, the Anti-Phishing Working Group, abbreviated APWG, was established, which includes over 1700 companies worldwide, where the most prominent members of the company are engaged in the production of antivirus software and prevention of cyber threats such as Kaspersky Lab, BitDefender, Symantec McAfee, etc. Each year, APWG publishes a report on trends and damage caused by phishing attacks. The conclusion of that report is (APWG 2021):

– the number of phishing attacks doubles each year

– BEC scams are increasingly costing victims, where in the last quarter of 2020 there was an increase of an average of $ 75,000 compared to the previous quarter in which the average was $ 48,000
– the most common victims of phishing are financial institutions, webmail and sites that work on the Software as a service model

The large scale of this type of attack, especially during the COVID-19 pandemic, is also indicated by the European Cyber Security Agency, ENISA, in a report from January 2019 to April 2020, according to which (The European Union Agency for Cybersecurity 2020a):

– an increase of 667% in phishing attacks during one month during the COVID-19 pandemic
– 42.8% of all malicious attachments in emails are Microsoft Office documents
– 30% of phishing messages are delivered on Mondays
– 32.5% of all emails contain the word payment in their subject line

There is also another form of this attack called Whaling Attack or CEO fraud in which an employee is forwarded an email that looks like it was from some important manager e.g. CEO or Chief Financial Officer. This type of attack requires significant preparation of the attacker, where he most often explores potential connections and relationships through social networks and then creates such an email so that the recipient can trust him. In this sense, this attack requires an added dimension of social engineering where because the employee does not want to reject the request of someone he perceives as an important person in the company (kaspersky 2019). From all the above, it can be concluded that special attention needs to be paid to the prevention of phishing attacks, especially because it can be an introduction to another type of attack. Also, one should keep in mind its great variability and therefore as a user, it is necessary to be more and more careful.

There are a large number of malicious programs, the so-called malware that damages a company's IT infrastructure. There can be various viruses, trojans, worms and others that have existed for years, and the forms of some of them change with the advancement of technology. One of the most interesting and very common are extortion software, the so-called ransomware. They are a form of malicious software that allows a hacker to deny access to information of importance to an individual or company in a certain way and to in turn require a certain amount of money, in some form, to remove that prohibition (Brewer 2016). Some more modern forms of this attack encrypt the files of the victims of the attack, which become inaccessible until they pay the ransom, where after the ransom the attackers decrypt those files. According to the European Cyber Security Agency's report for 2020, extortion software has become very popular in

attacks on state institutions, companies and individuals, where (The European Union Agency for Cybersecurity 2020b):

– the estimated redemption value is $ 10.1 billion during 2019, and the paid redemption in the U.S. in 2018 was $ 3.3 billion
– compared to 2018 there was an increase of 365% in 2019 attacks detected in the business domain
– more than 66% of health care organizations had experience with this type of attack during 2019
– 45% of organizations paid the ransom during 2019

According to the Verizon report for 2020, extortion software accounts for 27% of the total malicious software that produced the incidents **(Verizon 2020)**. It should be noted that encryption and decryption techniques are part of cryptography, the science of protecting data, to make the data unreadable to any attacker who might intercept the message. The same concepts are also used in extortion software, so in the current context they belong to cryptovirology, which deals with the study of cryptographic algorithms to create malicious software. Also, in practice, sometimes there is a problem that even after the paid redemption, the decryption of files is not done, ie. the system does not return to its previous state, but the attacker just takes the money. Money is most often distributed through cryptocurrencies, such as bitcoin, to cover up traces of attackers. What can be stated is that even after paying the ransom, the target cannot be sure that the system has been restored to its previous state and that some other problems will not occur very quickly. For these reasons, backup is a very important activity, which many companies have not adopted to date as a practice. If an unwanted event occurs, and there is no backup, it can produce major problems for the business, and even until its termination.

To make employees in companies more productive, as well as to stimulate their satisfaction and comfort at work, with the possibility of reducing the cost of purchasing separate equipment, some companies choose to allow users to bring their devices to work and use applications through them and company data itself. The mentioned concept is called Bring your own device, abbreviated BYOD and in practice, it is realized by employees bringing their laptops, tablets and/or mobile phones to work. With this concept, the users of the device already have certain knowledge and are familiar with the use of the device and applications on it, so the line between time spent at work and free time is fading, and employees themselves spend more time doing work. Statistical reports for 2020 confirm the above facts and indicate a significant increase in this trend in the world (Georgiev 2021):

– 67% of employees use personal devices at work
– the application of the BYOD concept creates an additional $ 350 each year per employee

– an employee who brings his device works on average 2 hours more
– 87% of a business depends on the ability of its employees to access business mobile applications from their smartphone
– 69% of IT decision-makers in the US say BYOD is a good thing
– the size of the BYOD market is expected to grow to $ 366.95 billion by 2022
– 59% of organizations adopted BYOD

BYOD has become very popular for educational purposes and many primary and secondary schools as well as colleges have adopted its use and adapted to it. Some of the basic benefits that schools see from them are: improved communication and collaboration, reduced costs, absolute control over the device, sharing information is easy, helping students access additional information and promoting learning on the go (Soni 2017). One of the important features in the use of the BYOD concept in educational institutions is that in addition to reducing costs where it is necessary to provide a device for each student, students can use their time outside school to learn through their devices, as opposed to using devices in laboratories and who work only as much as the lab does (Afreen 2014). Like most concepts that have their good sides, there are bad ones, and with BYOD these are badly related to security risks and privacy risks which can be: technical risks, then the absence of security policy, lack of security control, lack of awareness of security and lack of privacy (Alotaibi and Almagwashi 2018). Technical risks include: malicious software, phishing, social engineering, hacking, spoofing and network attack, as well as loss or theft of the device itself. Theft, loss or sale of the device itself can cause a problem if the company's data or documents have not been removed, which can be used to construct an attack. Other risks are related to defining appropriate security policies, as well as raising the awareness of the employees themselves.

In addition to BYOD, one of the problems that can occur when using mobile applications is the so-called data leakage. End-users can use applications that have not been tested and give them certain rights to be able to use various data. This data can be copied to servers, where various users, even the malicious ones, can use it.

When using mobile devices, phishing attacks can also occur, and one is specialized for that type of device because it uses SMS messages and is called Smishing. As with the classic phishing attack, the user receives a message from someone who pretends to be a bank, state or some other institution and asks for their personal data, account number, etc.

It has been noticed that there are some messages related to the COVID-19 pandemic, where people want to act to carry out activities that benefit malicious users. Researchers have noticed that several fake COVID-19 Websites display maps of people infected with the Coronavirus, where attackers direct users to

visit those sites and leave data, posing as government institutions. Also, what has been noticed is that mobile users are being targeted.

It should also be said that certain Websites deceive users by selling them various drugs in the fight against the coronavirus, as well as tests, and they are very active on social networks such as Facebook, where they offer it to users (Waggoner and Markowitz 2021; Bannister 2021).

In addition to the above, there are several scams offered through chat applications, such as Viber and WhatsApp, where users receive messages about incredible discounts for the purchase of items (O'Brien 2020; Singha 2021). This type of social engineering takes various forms and is highly variable, so end users need to develop an awareness of it.

The importance of youth safety culture on the Internet

In the use of the Internet and mobile applications, in addition to violating the security of ICT infrastructure and the security of information itself, there is part of threats to human life, especially for those age limits that have the least opportunity to protect themselves, namely children and youth. As the availability of devices and Internet access increases over time, so does the limit at which children begin their interaction in the digital world. Young parents perform many roles today, in an accelerated world, where the amount and flow of information exchanged daily is constantly growing, as well as the number of responsibilities they have. As a result, they cannot devote enough time to their child on the one hand, while on the other they try to perform their parental role to the best of their ability and thus do not want their child to miss any modern content on offer, to keep up with their generation. In this way, they very often facilitate children's interaction with the digital world, without even thinking about the dangers that exist in that world. Initially, these are certain multimedia audio or video content, then video games, and slowly new possibilities are discovered, such as interaction through social networks and through messaging applications (chat), as well as the possibility to attend certain curricula via network, etc. All these different types of interaction in children create the feeling that the Internet is a good and fun place, and later as they grow up and become young people that the digital world is an integral part of their reality. So in a way, the system model itself and the modelled interactions become a replacement or extension, in whole or in part, for the system and the interactions within it. The changed relations between the real world and its model are not without consequences, because there are not a small number of accidents, where even some of them are fatal. This is manifested in the example of several lost lives of young people using the TikTok social network (Дерикоњић 2021). Another part of the problem that the border between the real and digital world brings is that certain anomalies and deviant behaviours are transferred from the real to the digital world and there

take on new dimensions, shapes and a new intensity of manifestation, and have the same consequences as in the real world. Some of them are: Internet paedophilia, digital violence and Internet addiction. Bjelajac and Filipović explain the specificity of the observed phenomena and their effect on human behaviour in both the real and virtual world through the interaction of two triangles, where the first triangle consists of the Internet, digital devices and digital content, and the second consists of interconnectivity, interactivity and anonymity (Бјелајац and Филиповић 2021). Thus, the specifics of the use of the Internet between larger groups of users, who do not have to show their true identity, with enhanced interaction gives a large space for the described phenomena to be realized. It can be expected that it will grow in the coming period with the growing trend of the realized Internet traffic, which should worry all people, but also encourage them to find mechanisms in their prevention. Safety culture, digital literacy and raising awareness among parents that they must act on children to preserve their personal protection on the Internet are measures that should be part of preschool and school programs, as well as special forms of education of parents themselves.

The authors state that Internet paedophilia is a specific type of computer crime because paedophiles are increasingly wandering electronic networks and looking for victims, pliable and gullible children. The Internet has become a new playground accessible to paedophiles, where children are permanently exposed to inappropriate sexual content and disturbing and hostile messages. Modern criminological and victimological research has fundamentally changed the appearance of sexual abuse of children. Child-centred sexual offences often occur, are under-researched, difficult to control, and are rarely mentally immoral. After surviving victimization, the consequences for most children are severe and long-lasting (Бјелајац and Филиповић 2020). From the aspect of cybersecurity and protection of computer networks, a certain parallel can be made between social engineering and Internet paedophilia, in terms of the preparatory actions that the predator carries out towards the target. In paedophilia, one can notice a much more intensive effort not only in researching the target but also in preparing a plan of activities related to it and maintaining a connection with it through various forms of manipulation.

Digital violence refers to such use of technology that causes shame, calls on others to commit violence and harassment, and causes psychological harm (Von Solms and Van Niekerk 2013). It manifests itself in the form of peer violence where a harassed child or young person is threatened by sending messages, shameful photos are published and the person is subjected to ridicule. Besides, data from private life can be published, and even content related to a person can be uploaded on pornographic sites. Such actions can put a young person in unimaginable danger by directing predators towards them.

Bjelajac and Filipović point out that Internet addiction can be seen through how much the daily functioning of individuals changes to exposure to certain digital content. The intensity of this type of addiction can be compared to nico-

tine, alcohol or gambling addictions, and can be especially expressed in the form of loss of control when deprived of digital content (Bjelajac and Filipović 2020). Young people are especially susceptible, and it manifests itself: very frequent checks of status on social networks, liking people they think are gurus in an area that interests them, corresponding with other users, playing online games, etc. All of these activities can have long-term consequences for their health.

The actuality of the problem

Security challenges are growing worldwide with the increase in traffic on the global network from year to year, and this was further emphasized during the COVID-19 pandemic where the trend of cyber attacks and fraud to which individuals, organizations and even states are exposed is growing.

Several attacks have been directed at healthcare facilities around the world, where many patients' records have been stolen. On the example of Elara Caring, a health care institution that provides home care to patients in the United States in December 2020, data was stolen for over 100,000 patients, and it is suspected that their names, date of birth, address, telephone number, bank information count, health insurance number, driver's license number (HIPAA Journal 2021). The investigation is ongoing, and for now, what is known is that 2 employees received phishing emails from a certain account. Another case that has caused a great deal of attention in the community is the theft of data in a series of cyberattacks between 2018 and 2019 on a large mental health clinic in Helsinki, where even data from individual therapeutic sessions were stolen (Kleinman 2020). The clinic was blackmailed with payments in bitcoins worth about $ 530,000, and besides, individuals were blackmailed for personal data from 200 to 500 EUR, also in bitcoins. A similar example of extortion appeared at the world-famous company Foxconn, where about 1,200 servers were infected with ransomware, and a cybercriminal group demanded a ransom worth about 1,800 bitcoins, which at the time amounted to about $ 33 million (Riley 2020). A similar experience was experienced by Barnes & Noble, one of the largest bookstores in the world, where their Nook service was compromised (Osborne 2020). Monroe College in New York was also the target of a ransomware attack, where hackers demanded $ 2 million from the college for a buyout in bitcoins (McKenzie 2019). One of the scams on mobile phones and the WhatsApp application is that on the eve of Women's Day, messages arrive about the many prizes that can be won, and the contacts are presented as Amazon or Adidas (Smith 2021).

The situation in Serbia does not differ much from the situation in the rest of the world. On April 7 and 8, 2021, a large number of users in Serbia received

an email, where cybercriminals introduced themselves as PE Post of Serbia and where users were told that the package was not delivered to them, because no customs duties were paid and that they had to pay a certain amount (ЈП Пошта Србије 2021; Nacionalni CERT Republike Srbije 2021). The mentioned phishing attack was covered by the media, and the company itself distanced itself from it and indicated the misuse of the symbols of the Post of Serbia. In March 2020, the information system of the city administration of Novi Sad in PUC Informatika was attacked (Blic 2020). The servers of the mentioned company were infected with ransomware and the attackers asked for 50 bitcoins, the amount of which was around 400,000 EUR at that time, to restore the system to its previous state. The attack was first launched through phishing, where the ransomware PwndLocker was then installed and encrypted the contents of many computers on the network and made them unusable.

A similar attack took place in the region, in Croatia, where in February 2020 part of the IS of the Croatian oil company INA was blocked for some time, so that bills could not be issued, there were problems with loyalty cards and payment of gas bills (Bubanja 2020).

All these cases indicate that it is necessary to carry out activities to raise awareness of end-users as well as to raise the level of their digital literacy and define clear policy security to protect the IT infrastructure. This is done through a security culture.

Information security culture

According to Bjelajac and Jovanovic, security culture includes security activities that express readiness to act and behave following the acquired knowledge and skills, as well as by accepted values (Бјелајац and Јовановић 2013). It is realized by recognizing dangers, reacting to them by avoiding dangers, eliminating dangers or referring to those subjects who will react professionally and preserve endangered values. Security culture consists of 3 main elements: technology, policy (rules) and users, who interact in a way that people influence the way technology is used, and the development of technologies creates new policies (Milovanović and Radovanović 2015). What needs to be paid attention to is that the security culture is established over a long period of time and cannot be "overnight", but it is a permanently well-designed action, subject to change because society, people and their relationships, science, technology and even security threats change over time.

All organizations need to define policies that on the one hand protect the IT infrastructure, and also those others that direct users not to jeopardize the existing security mechanisms by which it protects. Information security culture is contextualized in the behaviour of people in the organizational context to pro-

tect the information that the organization processes through compliance with information security policies and procedures and understanding how requirements are implemented carefully and embedded in regular communication, awareness, training and educational initiatives (da Veiga et al. 2020). Therefore, by implementing appropriate information security policies and procedures, information security is achieved, and they are created by adequate behaviour of employees, which is achieved through long-term communication, training, specific types of education and raising awareness of security-relevant information tools. In this way, an information security culture is established as part of the overall security culture of an organization.

Authors such as Zimmermann and Renaud, due to the growing trend of cyberattacks, suggest that the starting points may not be good and that the "man as part of the problem" approach should be abandoned or redefined to become "man as part of the solution" (Zimmermann and Renaud 2019). Their argument lies in the fact that the current activities carried out towards people who exclude them, train them, limit them and control them lead to an increase in resistance to security policies. A different approach consists of expertise, flexibility and learning from positive and negative examples, where resistance to cybersecurity policies is reduced through communication and cooperation. The described approach has not been tested in practice, so there is not much information about its effectiveness and efficiency, but it is important because it indicates that the design of programs for creating information security culture should be such as to avoid strong resistance to security policies of the target group over which the program is implemented. The mentioned practice can be explained by the fact that there is no adequate expertise in all necessary areas concerning activities aimed at employees as a target group over which the program is implemented, but the mentioned programs are implemented in isolation, ie. exclusively from the security and information aspect.

To overcome the mentioned problem, and at the same time the programs that should influence the establishment and maintenance of security culture were expedient, certain authors define the framework of security culture. Roer and others have defined a security culture framework, which has emerged as a result of best practices and aims to create programs through which an information security culture is established and maintained (Roer 2015, 41-51).

The framework is organized according to the PDCA method, which aims to continuously improve the results, and consists of 4 parts:

– Metrics
– Organization
– Topics
– Planner

The Metrics part defines the goals of what the programs want to achieve, ie. what needs to be achieved with the security culture. The framework aims to

define 2 types of goals (The Roer Group 2014a): result-oriented goals and learning-oriented goals. Examples can be:

– result-oriented goal - In 6 months, the organization should reduce the number of requests regarding "forgotten passwords" by 50%.
– learning-oriented goal - Those who are trained should be aware of the importance of strong passwords, gain experience in creating strong passwords and learn how to manage them securely and be able to share that knowledge.

To clearly define the goals, it is necessary to determine the current state, and then determine which is the desired state. Therefore, it is necessary to carry out appropriate measurements to determine the current situation. This is the most difficult activity in this procedure because everything else depends on it. Orehek and Petrič gave a detailed overview of security culture measurement methods and found that most approaches offer limited results in terms of scale validation and that the rigour with which information security culture scales are evaluated varies widely and that none meet all evaluation criteria (Orehek and Petrič 2020). This fact needs to be especially kept in mind when implementing the program, because if we do not measure adequately, ie. we do not use the measuring device correctly, we cannot have a true picture of the current and desired state.

In the Organization part, on the one hand, it is necessary to determine which people will make up the team that will plan and lead the program, and on the other hand, to determine which group of employees will attend the program. The team of people leading the programs should have at least competencies in the following areas: safety, communication, culture and training. Therefore, it is necessary to include employees from the organizational unit for security, then for marketing and communication, as well as someone from the organizational unit for human resources (Roer 2015, 44). That team needs to make a plan and determine the list of activities that will be carried out on a group of employees, ie. to create a campaign for each user group. It is important to carefully analyze each group of users and determine how the activities in that group will be realized because each of them is specific to itself and therefore there is no universal approach, but all activities are subject to modification. Such an approach makes it possible to significantly reduce employee resistance in adopting new policies.

In the Topics section, it is first necessary to determine which security-important topics or challenges will be covered by the program. In doing so, it should be borne in mind that they must be correlated with the goals to be achieved. Some of the topics can be social engineering, phishing, BYOD, code management, work on social networks, etc. After that, it is necessary to determine the activities that need to be carried out, which are related to the selected topic. Some of them may be (The Roer Group 2014b) e-learning, course, live demonstration, video demonstration, etc.

In the Planner section, a detailed plan is created, which consists of defined goals, target groups, various activities and when they need to be implemented,

and then when to measure progress. Simplified implementation of information security culture programs can be realized in this way (Kassner n.d.):

– create a team which will create the program
– define program goals
– determine the current status (measurement)
– define target groups
– choose topics
– plan and conduct training
– perform measurement again
– conduct revision
– repeat procedure

In this way, it is ensured that in the long run, we move towards the establishment and then the maintenance of information security culture. First, a program is implemented that deals with one topic, e.g. phishing, then a new topic is selected, e.g. password management, and so on one topic at a time until all the topics that a program needs to fulfil are covered. Therefore, it is a permanent activity that aims to first create, and then increase and maintain information security culture, because, with the emergence of new modalities of security threats or changing the way of realization of existing ones, the fund of security threats increases, so adequate responses to them need to be available. In this way, it influences the ideas, habits and behaviour of employees to enable the organization to be free from security threats.

A similar procedure can be applied in defining security programs that should influence the definition and maintenance of the information security culture of young people. Also, certain modifications should be implemented, and they relate primarily to the incorporation of parents into the program, where it would also define part of the activities that they should carry out with their children for the effects of the program to be satisfactory. Also, programs should be organized within schools, whereas part of the curriculum, young people would create the necessary habits and adopt desired behaviours that would help them maintain personal safety.

Conclusion

Information security culture aims to provide long-term habits and behaviours of employees concerning the challenges that come from cyberspace. Many of these challenges arise from the use of the Internet and mobile applications used by employees, thus creating opportunities to disrupt the security of the information itself, information and communication infrastructure, and in some cases even the creation of dangers to human life. Knowing these threats, it is possible to create and maintain an information security culture through the

framework of security culture, through which educational programs are created. Carefully designed programs enable the practice of dealing with various security challenges to be continuously monitored, analyzed and measured, and then to implement those activities that aim to create and maintain the ideas, habits and behaviours of employees in the long run about these challenges. This ensures that the resistance that employees have in the implementation of defined security policies reduce, and thus preserve the ICT assets of the organization. Before becoming employed, young people can also have many problems with the use of the Internet and mobile applications, where the consequences for their lives can be great. That is why parents need to take care of and guide them from the earliest days when their child interacts on the Internet so that they adopt norms that help them maintain their safety. Along the way, safety culture, digital literacy and parental education are key to achieving these goals. By understanding and adopting the specifics of the Internet, which are reflected in its interconnectivity, interactivity and anonymity, will enable a young person to protect himself.

References

1. Afreen, Rahat. 2014. "Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges." *International Journal of Emerging Trends & Technology in Computer Science* III (1): 233–236.
2. Alotaibi, Bashayer, and Haya Almagwashi. 2018. "A Review of BYOD Security Challenges, Solutions and Policy Best Practices." In *1st International Conference on Computer Applications and Information Security, ICCAIS 2018*, 1–6. IEEE. https://doi.org/10.1109/CAIS.2018.8441967.
3. APWG. 2021. "Phishing Attack Trends Report – 4Q 2020." https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf.
4. Bannister, Adam. 2021. "Fake Covid-19 Vaccines Pose 'Serious Health Hazard', Warns Interpol.", poslednji pristup 05.04.2021. https://portswigger.net/daily-swig/fake-covid-19-vaccines-pose-serious-health-hazard-warns-interpol.
5. Бјелајац, Жељко Ђ., и Милован Б. Јовановић. 2013. „Поједини аспекти безбедносне културе на Интернету", *Култура полиса*, X (21): 99-114
6. Бјелајац, Жељко Ђ., и Александар М. Филиповић. 2020. „Интернет и друш-твене мреже као неограничени простор за концентрацију и мултиплицирано присуство педофила", У „Педофилија – узроци и последице", ур. Жељко Бјелајац и Александар М. Филиповић, посебно издање, *Култура полиса*: 29-40.
7. Бјелајац, Жељко Ђ., и Александар М. Филиповић. 2021. „Флексибилност дигиталних медија за манипулативно деловање сексуалних предатора", *Култура полиса*, XVIII (44): 51-67.

8. Bjelajac, Željko Đ., and Aleksandar M. Filipović. 2020. "Internet Addiction Disorder (IAD) as a Paradigm of Lack of Security Culture.", *Kultura polisa*, XVII (43): 239-258.
9. Bjelajac, Željko Đ., and Slavimir Lj. Vesić. 2020. "Security of Information Systems." *Pravo - Teorija i Praksa* XXXVII (2): 63–76. https://doi.org/10.5937/ptp2002063b.
10. Blic. 2020. „Kako su hakeri napali Novi Sad - sve o najvećem napadu ikada: Tražili pola miliona evra i danima ucenjivali Srbiju." poslednji pristup 05.03.2020. https://www.blic.rs/vesti/drustvo/kako-su-hakeri-napali-novi-sad-sve-o-najvecem-napadu-ikada-trazili-pola-miliona-evra/5g8dqe2.
11. Brewer, Ross. 2016. "Ransomware Attacks: Detection, Prevention and Cure." *Network Security* MMXVI (9): 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1.
12. Bubanja, Branislav. 2020. "Ransomware napad na hrvatsku naftnu kompaniju INA." poslednji pristup 17.11.2020. https://pcpress.rs/ransomware-napad-na-hrvatsku-naftnu-kompaniju-ina/.
13. Дерикоњић, Мирослава. 2021. "„Тикток" изазов као позив на самоубиство." poslednji pristup 03.03.2021. http://www.politika.rs/scc/clanak/471881/Tiktok-izazov-kao-poziv-na-samoubistvo.
14. FBI. n.d. "Business Email Compromise." Accessed March 27, 2021. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise.
15. Georgiev, Deyan. 2021. "41 Stunning BYOD Stats and Facts to Know in 2020." poslednji pristup 01.04.2021. https://techjury.net/blog/byod/.
16. HIPAA Journal. 2021. "PHI of More Than 100,000 Elara Caring Patients Potentially Compromised in Phishing Attack." poslednji pristup 31.03.2021. https://www.hipaajournal.com/phi-of-more-than-100000-elara-caring-patients-potentially-compromised-in-phishing-attack/.
17. IC3. 2019. "Business Email Compromise The $26 Billion Scam." poslednji pristup 18.03.2021. https://www.ic3.gov/Media/Y2019/PSA190910.
18. ЈП Пошта Србије. 2021. „Упозорење - злоупотреба симбола Поште Србије." poslednji pristup 09.04.2021. https://www.posta.rs/cir/info/vest-detaljnije.aspx?ID=7028.
19. kaspersky. 2019. "What Is a Whaling Attack?" poslednji pristup 01.04.2021. https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack.
20. Kassner, Michael. n.d. "Create a Security Culture Framework to Protect against Threats." Accessed April 4, 2020. https://www.techrepublic.com/article/create-a-security-culture-framework-to-protect-against-threats/.

21. Kleinman, Zoe. 2020. "Therapy Patients Blackmailed for Cash after Clinic Data Breach." poslednji pristup 03.04.2020. https://www.bbc.com/news/technology-54692120.
22. McKenzie, Lindsay. 2019. "Hackers Demand $2 Million From Monroe." poslednji pristup 17.03.2021. https://www.insidehighered.com/news/2019/07/15/hackers-demand-2-million-monroe-college-ransomware-attack.
23. Milovanović, Zoran, and Radovan Radovanović. 2015. " Informaciono-bezbednosna kultura - imperativ savremenog društva." *NBP – Journal of Criminalistics and Law* XX (3): 45–65.
24. Mroczkowska, Agnieszka. 2021. "What Is a Mobile App? | App Development Basics for Businesses." poslednji pristup 10.04.2021. https://www.thedroidsonroids.com/blog/what-is-a-mobile-app-app-development-basics-for-businesses.
25. Nacionalni CERT Republike Srbije. 2021. „Phishing kampanja za korisnike poštanskih usluga." poslednji pristup 10.04.2021.
26. O'Brien, Jim. 2020. "DHL and Viber SMS Scams to Watch Out." poslednji pristup 04.01.2021. https://techbuzzireland.com/2020/02/28/dhl-viber-scams-sms-phishing/.
27. Orehek, Špela, and Gregor Petrič. 2020. "A Systematic Review of Scales for Measuring Information Security Culture." *Information and Computer Security*. https://doi.org/10.1108/ICS-12-2019-0140.
28. Osborne, Charlie. 2020. "Barnes & Noble Confirms Cyberattack, Ransomware Group Leaks Allegedly Stolen Data." poslednji pristup 31.03.2021. https://www.zdnet.com/article/barnes-noble-confirms-cyberattack-customer-data-breach/.
29. Research and Markets. 2020. "Worldwide Industry for IoT Middleware to 2025 - Manufacturing Expected to Have High Potential Growth." poslednji pristup 31.03.2021. https://www.globenewswire.com/news-release/2020/12/21/2148872/0/en/Worldwide-Industry-for-IoT-Middleware-to-2025-Manufacturing-Expected-to-Have-High-Potential-Growth.html.
30. Riley, Duncan. 2020. "Foxconn Plant in Mexico Struck in DoppelPaymer Ransomware Attack." 31.03.2021. https://siliconangle.com/2020/12/08/foxconn-plant-mexico-struck-dopplepaymer-ransomware-attack/
31. Roer, Kai. 2015. *Build a Security Culture*. Ely, Cambridgeshire: IT Governance Publishing.
32. Singha, Rajiv. 2021. "Beware of the WhatsApp Scam That Promises Free Adidas Shoes!" poslednji pristup 04.01.2021. https://blogs.quickheal.com/beware-adidas-scam-whatsapp1/
33. Smith, Adam. 2021. "WhatsApp Gift Scams From Fake Amazon and Adidas Websites Spread on International Women's Day." poslednji pristup 01.04.2021. https://www.independent.co.uk/life-style/gadgets-and-

tech/whatsapp-gift-scam-international-women-day-amazon-adidas-b1814003.html.
34. Solms, Rossouw Von, and Johan Van Niekerk. 2013. "From Information Security to Cyber Security." *Computers and Security* XXXVIII (2013): 97–102. https://doi.org/10.1016/j.cose.2013.04.004.
35. Soni, Aakash. 2017. "6 Advantages Of BYOD In The Classroom." poslednji pristup 01.04.2021. https://elearningindustry.com/byod-in-the-classroom-6-advantages.
36. Stallings, William. 2018. *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. 1st ed. Boston: Addison-Wesley Professional.
37. Stallings, William, and Lawrie Brown. 2018. *Computer Security: Principles and Practice*. 4th ed. New York: Pearson Education Limited.
38. The European Union Agency for Cybersecurity. 2020a. "ENISA Threat Landscape 2020 - Phishing." https://www.enisa.europa.eu/publications/phishing/at_download/fullReport.
39. The European Union Agency for Cybersecurity. 2020b. "ENISA Threat Landscape 2020 - Ransomware." https://www.enisa.europa.eu/publications/ransomware.
40. The Roer Group. 2014a. "Metrics – What to Measure, Why and How." poslednji pristup 03.04.2021. https://securityculturefreamework.net/metrics-what-to-measure-why-and-how/.
41. The Roer Group. 2014b. "Topics Module." poslednji pristup 03.04.2021. https://securityculturefreamework.net/topics-module/.
42. Veiga, Adéle da, Liudmila V. Astakhova, Adéle Botha, and Marlien Herselman. 2020. "Defining Organisational Information Security Culture—Perspectives from Academia and Industry." *Computers and Security* 92: 101713. https://doi.org/10.1016/j.cose.2020.101713.
43. Verizon. 2020. "2020 Data Breach Investigations Report." https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.
44. Vesić, Slavimir Lj. 2016. „Progresivne Web aplikacije - Između nativnih i mobilnih Web aplikacija." *InfoM* MMXVI (60): 43–49.
45. Waggoner, John, and Andy Markowitz. 2021. "Beware of Robocalls, Texts and Emails Promising COVID-19 Cures or Stimulus Payments." poslednji pristup 17.03.2021. https://www.aarp.org/money/scams-fraud/info-2020/coronavirus.html.
46. Zimmermann, Verena, and Karen Renaud. 2019. "Moving from a 'human-as-Problem" to a 'human-as-Solution" Cybersecurity Mindset." *International Journal of Human Computer Studies* CXXXI (November): 169–87. https://doi.org/10.1016/j.ijhcs.2019.05.005.