PAM Pokrajinski arhiv Maribor

Moderna arhivistika

Časopis arhivske teorije in prakse
Journal of Archival Theory and Practice

Letnik 2 (2019), št. 1 / Year 2 (2019), No. 1

Maribor, 2019

Moderna arhivistika

Časopis arhivske teorije in prakse

Journal of Archival Theory and Practice

Letnik 2 (2019), št. 1 / Year 2 (2019), No. 1

ISSN 2591-0884 (online)
ISSN 2591-0876 (CD_ROM)

Izdaja / Published by:
Pokrajinski arhiv Maribor / Regional Archives Maribor

Glavni in odgovorni urednik / Chief and Responsible editor:
Ivan Fras, prof., Pokrajinski arhiv Maribor, Glavni trg 7, SI-2000 Maribor,
telefon/ Phone: +386 2228 5017; e-pošta/e-mail: ivan.fras@pokarh-mb.si

Glavna urednica / Editor in chief:
mag. Nina Gostenčnik

Recenziranje / Peer review process:
Prispevki so recenzirani. Za objavo je potrebna pozitivna recenzija. Proces recenziranja je anonimen. / All articles for publication in the conference proceedings are peer-reviewed. A positive review is needed for publication. The review process is anonymous.

Lektoriranje / Proof-reading:
mag. Boštjan Zajšek, mag. Nina Gostenčnik

Prevajanje:
mag. Boštjan Zajšek (slovenščina), mag. Nina Gostenčnik (slovenščina, angleščina), Lučka Mlinarič (bosanščina, hrvaščina, srbščina)

Oblikovanje in prelom / Design and typesetting:
mag. Nina Gostenčnik

http://www.pokarh-mb.si/si/p/3/49/moderna-arhivistika.html

Prejeto / Received: 30. 1. 2019

1.01 Izvirni znanstveni članek *1.01 Scientific Article*

SO OSEBNI IN POSLOVNI PODATKI VARNI NA PAMETNIH TELEFONIH?

Boštjan ŠPEHONJA
Unistar LC d.o.o., Ljubljana, Slovenija
bostjan.spehonja@gmail.com

Danilo BURNAČ
Mariborski vodovod, j.p., d.d.,
Maribor, Slovenija
danilo.burnac@mb-vodovod.si

Sanja ANDROIĆ
Mariborski vodovod, j.p., d.d.,
Maribor, Slovenija
sanja.androic@mb-vodovod.si

dr. Milka PUNGARTNIK
Mariborski vodovod, j.p.,d.d.,
Maribor, Slovenija
milka.pungartnik@mb-vodovod.si

Izvleček:

Vse več podjetij se zaveda nevarnosti uporabe pametnih telefonov v povezavi s poslovnimi, zaupnimi in osebnimi podatki, saj se je pogosto izkazalo, da je ravno pametna naprava vektor odtujitve takšnih podatkov iz podjetja. Uporabniki pametnih telefonov se velikokrat obnašamo, kot da z njimi še vedno samo telefoniramo, v resnici pa je pametni telefon postal nadomestna naprava računalnika. Na njem dostopamo do elektronske pošte, internih podatkov podjetja, upravljamo aplikacije in se na več načinov povezujemo v interno omrežje podjetja. Problem nastane, ko se takšna naprava izgubi in uporabnik nima nastavljenih vseh varnostnih mehanizmov, ki preprečujejo odtujitev podatkov iz naprave. Po drugi strani pa je notranjemu uporabniku najlažje odtujiti podatke iz podjetja ravno preko pametne naprave. Zato v veliko podjetjih že vpeljujejo mehanizme, kako varovati podatke na pametnih napravah, ter imajo vzpostavljena interna pravila za tako imenovane naprave BYOD (Bring Your Own Device). K sprejemu varnostnih ukrepov za zavarovanje osebnih in poslovnih podatkov zavezujejo podjetja področna zakonodaja, zahteve posameznih standardov ter v primeru javnopravnih oseb zahteve za potrditev notranjih pravil.

Deležniki kritične infrastrukture morajo imeti zavedanje o kibernetski varnosti na še višjem nivoju. Priporočljivo je preverjanje in izboljševanje varnosti informacijsko-komunikacijske tehnologije z občasnimi izvedbami notranjih in zunanjih varnostnih pregledov ter najem ali nakup certificirane programske opreme ali storitev. Prikazan bo primer iz prakse podjetja Mariborski vodovod, ki je sprejelo in uvedlo nekaj varnostnih ukrepov za zaščito poslovnih podatkov podjetja in osebnih podatkov, katerih upravljavec je podjetje pred odtujitvijo.

Ključne besede:

osebni podatki, poslovni podatki, pametni telefoni, varnost, BYOD

Abstract:

Is personal and bussiness data safe on smartphones?

More and more companies are aware of the danger of using smartphones for bussiness, confidential and personal data, because precisely the smartphones are the lead to the alienation of such information. A common user of a smartphone many times pretends to only use the gadget for phone calls, but the truth is, this gadget has become a substitute for a computer. We use it to access our email, internal company data, use applications and connect to the internal network of the company. The problem occurs, when the gadget gets lost and the user did not set all the security mechanisms that prevent the alienation of the data from the gadget. On the other hand, for an internal user, the easisest way to get confidential data is by a smart gadget. Because of this, many companies are already implementing security mechanisms for smart gadgets and have internal regulations for the so-called BYOD (Bring Your Own Device) gadgets. By the sectoral law, the requirements of individual standards, and in case of public entities the requirements to confirm the internal rules, the companies are committed to accept security measures for the protection of personal and bussiness data.

The holders of critical infrastructure must have an even higher awareness about cyber security. It is recommended to check and improve the security of the information and communication technologies by an occasional screening of internal and external security check-ups, and highering or buying certified software or services. An example from the company Mariborski vodovod will be shown below. The mentioned company accepted and introduced some security measures that protect the bussiness data and the personal data, managed by the company, against the alienation of data.

Key words:

personal data, business data, smartphones, security, BYOD

1. VARNOST IN NE-VARNOST PAMETNIH TELEFONOV

Napredek tehnologije je na področju računalništva prinesel velike spremembe. Računalnike in prenosne računalnike so pričele nadomeščati različne mobilne naprave tako na poslovnem in zasebnem področju. Najpogostejša takšna mobilna naprava je pametni telefon. Skozi naš prikaz bomo poskušali najti odgovor na vprašanje, ali so osebni in poslovni podatki na pametnih telefonih varni, ter najti primerne varnostne mehanizme.

Da je informacijska varnost področje, ki je v zadnjih letih precej v ospredju, lahko opazimo na vsakem koraku. Podjetja vseh velikosti aktivno uporabljajo prednosti, ki jih prinaša informacijska tehnologija. Kar nekaj časa pa je minilo, da so se začela zavedati tudi groženj in pasti, ki prežijo na njih. Teh ni malo, na najvišjem nivoju jih lahko razdelimo na tehnične in netehnične. Tehnični napadi so tisti, ki prežijo na našo informacijsko-komunikacijsko okolje, pod netehnične pa štejemo tehnike tako imenovanega socialnega inženiringa, ki cilja na končnega uporabnika. Cilj vsakega podjetja je, da z najrazličnejšimi mehanizmi zaščiti svojo infrastrukturo pred napadi znanih groženj in naredi vse, kar je v njihovi moči, da sistemi niso nezavarovani in izpostavljeni.

Med vsemi grožnjami, ki pretijo tako na uporabnika kot na sisteme, je potrebno posvetiti pozornost tudi pametnim telefonom. Tudi ti se razvijajo s svetlobno hitrostjo in so v nekaj letih bistveno izboljšali uporabniško izkušnjo. Uporabniki z veseljem sprejemamo novosti, ki nam jih razvoj pametnih telefonov prinaša, in pri tem velikokrat pozabimo na varno uporabo. Zavedati se moramo, da so pametni telefoni postali naša potujoča pisarna oziroma velikokrat zamenjava za namizni ali prenosni računalnik. Kar se tiče prenosnih računalnikov, se večina njihovih uporabnikov zaveda, da je koristno, če imajo nameščen protivirusni sistem. Pri mobilnih telefonih se v praksi kaže, da ima protivirusni sistem nameščenih le malo uporabnikov. Pri mobilnih telefonih velikokrat

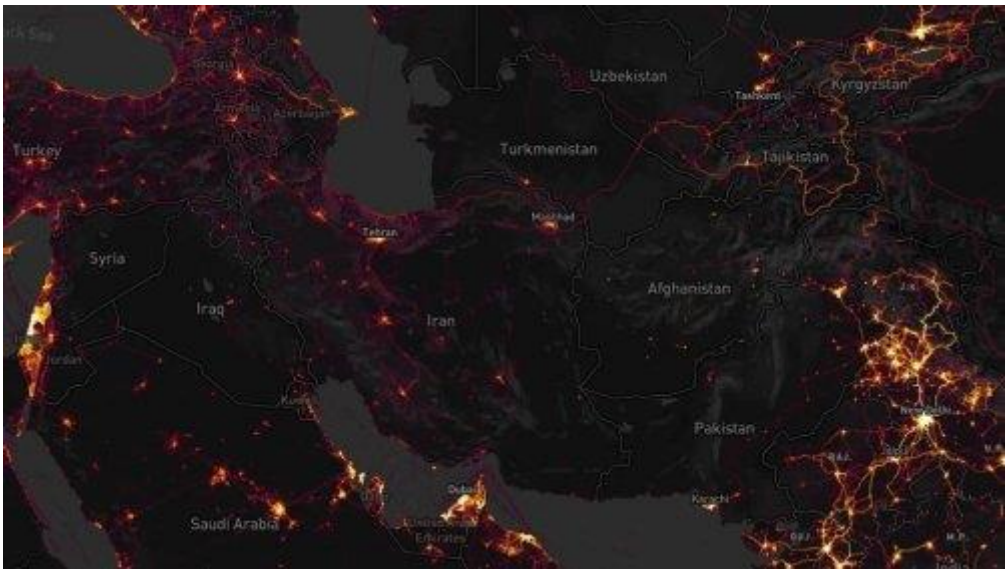
pozabljamo na arhiviranje podatkov, medtem ko nam je na računalniku velikokrat samoumevno, da je potrebno podatke shraniti še na drugo lokacijo. Na mobilnih telefonih imamo povsem enakovredne podatke kot na računalniku. Dostopamo do službene ter osebne elektronske pošte, dostopamo do službenih dokumentov ter zaupnih podatkov podjetja, vzpostavljen imamo dostop do najrazličnejših socialnih omrežij, preko najrazličnejših aplikacij lahko plačujemo na spletu, shranjene imamo kontakte, gesla brezžičnih omrežji, osebne slike, sporočila sms. Ogromno razlogov torej, da je postala mobilna naprava zanimiva za napadalce kot odličen mehanizem za odtujevanje podatkov iz podjetja.

Večina velikih podjetij ter vsa podjetja s kritično infrastrukturo pa imajo zaposlene svoje varnostne strokovnjake, ki se po najboljših močeh trudijo zagotoviti varnost svoje organizacije. Deležniki kritične infrastrukture morajo imeti zavedanje o kibernetski varnosti na še višjem nivoju. Priporočljivo je preverjanje in izboljševanje varnosti informacijsko-komunikacijske tehnologije z občasnimi izvedbami notranjih in zunanjih varnostnih pregledov ter najem ali nakup certificirane programske opreme ali storitev. Kar nekaj podjetij se lahko pohvali, da imajo sisteme relativno dobro postavljene glede na priporočila dobrih praks. Kljub temu pa se jim dogajajo vdori ali opažajo uhajanje ključnih informacij iz podjetja. V tem primeru sta poleg tehničnega vdora možna dva scenarija. Ali gre za neizobražene zaposlene, ki z minimalno napako lahko povzročijo katastrofo v podjetju, ali pa gre za namensko odtujitev podatkov preko internega zaposlenega. Znano je, da je v zadnjih letih najšibkejši člen v varnostni verigi postal neozaveščen človek. Razvoj informacijske tehnologije drvi s svetlobno hitrostjo, ravno tako neomejene ideje spletnih prevarantov ter zlonamernih napadalcev. Če končnega uporabnika, ki dela z informacijsko tehnologijo, ne izobrazimo o grožnjah, s katerimi se sooča, je vprašanje hekerskega napada le vprašanje časa.

Najpogostejša ranljivost v podjetjih je dopuščanje priklopa neavtenticirane oz. neznane naprave, ki so lahko okužene, in to so največkrat ravno mobilne naprave, v lokalno omrežje samega podjetja, zaradi česar se pojavi nenamerna ali namerna škoda v notranjem omrežju podjetja. Druga najbolj pogosta ranljivost pa so elektronske naprave brez nameščenih popravkov in posodobitev, ki lahko predstavljajo tudi visoko tveganje za podjetje (Burnač, Androić in Špehonja, 2018, str. 288). Večina posameznih uporabnikov pametnih telefonov v praksi velikokrat ne namešča posodobitev ali pa jih kar nekaj časa prelaga na kasnejši čas. Aktualni napadi zlonamernih hekerjev so v zadnjem času usmerjeni na neukega končnega uporabnika z metodami socialnega inženiringa, saj so ugotovili, da je hitreje in ceneje od izvedbe visokotehnoloških naprednih hekerskih napadov usmeritev le-teh na izrabo uporabnika. Za celovito kibernetsko varnost mora imeti skrb vsak posamezen zaposleni, saj so podjetja varna, kolikor je varen njegov najšibkejši člen, in samo skrb informatikov ni več dovolj (Burnač, Androić in Špehonja, 2018, str. 288).

Primeri dobrih praks kažejo, da se mobilne elektronske naprave ne priklapljajo v lokalno omrežje organizacije preko brezžičnega omrežja. Kot je bilo že predhodno omenjeno, na mobilnih napravah ne uporabljamo protivirusnega sistema. Uporabniki na mobilne naprave nameščajo najrazličnejše aplikacije, ki velikokrat niso preverjene, in hitro se lahko zgodi, da z namestitvijo aplikacije okužimo mobilno napravo. Takšno napravo priklapljati v katero koli omrežje postane rizik tudi za ostale naprave, saj poznamo zlonamerno kodo, ki se zna sama širiti v omrežju. Če se uporabniki želijo povezati na brezžično omrežje, je priporočljivo, da ima organizacija postavljeno ločeno brezžično omrežje. Preko tega lahko brskajo po internetu, ne morejo pa dostopati do notranje strežniške in druge infrastrukture.

Kako hitro lahko naš prijatelj postane naš sovražnik, je moč videti iz primera, ki se je zgodil v začetku leta 2018. Proizvajalec mobilne aplikacije za sledenje športnim aktivnostim, Strava, se je odločil, da bo ponosno objavil vse svoje zapise v obliki zemljevida, ki je dostopen na spletni strani (Strava, 2018). Gre za fitnes aplikacijo, ki svojim uporabnikom sledi preko sistema GPS in podatke prenaša na svoje strežnike. Objava podatkov se je zdela za podjetje velik uspeh, saj ima v svoji bazi zabeleženih preko 700 milijonov aktivnosti ter preko 1,4 milijarde GPS-lokacij. Ob podrobnem pregledu zemljevida pa je bilo ugotovljeno, da ta izdaja ameriške tajne podatke. Na zemljevidu je bilo mogoče odkriti ameriške vojaške baze po vsem svetu. Ameriški vojaki aplikacijo namreč uporabljajo za beleženje svojih dnevnih športnih aktivnosti, kar se je na zemljevidu videlo kot svetlejše točke, kar prikazuje slika 1.



Slika 1: Razkrivanje ameriških vojaških baz preko mobilne fitnes aplikacije (Strava, 2018)

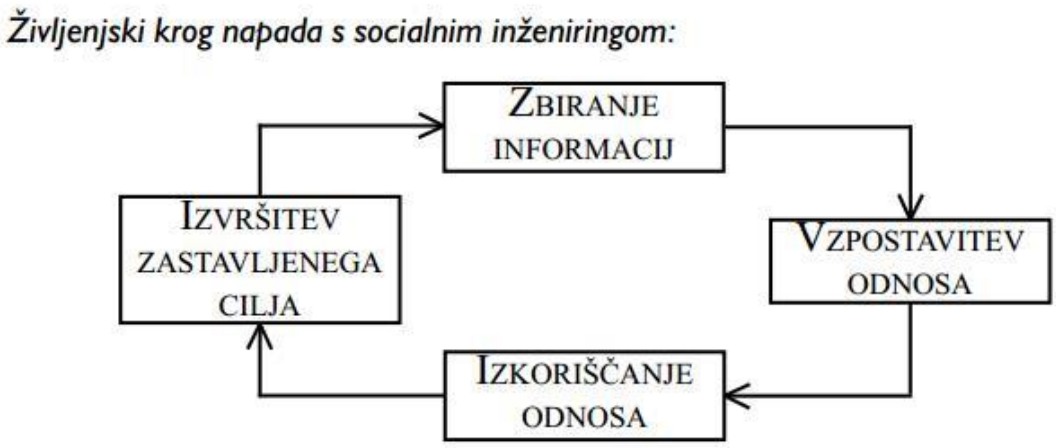
Na ta način so bile razkrite potencialne ameriške vojaške baze v Afganistanu, Siriji in Somaliji, Area 51, ruska vojaška baza v Ukrajini, baza NSA v Havajih in druge. Ker gre za tajne lokacije, so bili s tem razkriti državni tajni podatki, kar je nedvomno povzročilo vsaj povišano stopno ogroženosti na razkritih lokacijah.

Iz primera lahko vidimo, kako pomembno je, katere aplikacije nameščamo na pametne naprave ter katera dovoljenja potrdimo aplikaciji. V mislih moramo imeti, da aplikacije za svoje delovanje navadno želijo veliko več dovoljenj in podatkov uporabnikov, kot jih dejansko potrebujejo. Velikokrat gre za vse informacije, kar vključuje fotografije, telefonske številke, dostop do datotek na lokalnem pomnilniku ter spominski kartici, dovoljenje za snemanje zvoka brez dodatnega obvestila, aktiviranje morebitne plačljive storitve in drugo. In vse to brez posebnega obvestila, saj je uporabnik aplikaciji ob namestitvi dovolil vse pravice. Zato je še posebej pomembno, da v nastavitvah preverimo, katere pravice posamezna aplikacija potrebuje, in nepotrebne ustrezno odstranimo.

1.1 Socialni inženiring

Socialni inženiring je ena izmed najbolj podcenjenih, hkrati pa najnevarnejših metod zlorabe človekovega zaupanja. To pomeni, da je človek v primeru napadov socialnih inženirjev, predvsem pri kibernetskih napadih, med najšibkejšimi členi varnostnega sistema. Napadalec, ki uporablja metode socialnega inženiringa, se poslužuje majhnih laži, prevar in zvijač. Napadenega izkorišča z različnimi čustvenimi in psihičnimi stanji. Velikokrat tudi izkorišča nezadovoljstvo v službi oz. »prijateljstvo na delovnem mestu« ali vlogo »prijazne« stranke ali poslovnega partnerja. Socialni inženir uporabi vse metode »idealne«, prijazne in zaupanja vredne osebe, ki jo žrtve napada z veseljem spustijo v svojo bližino (Potokar in Androić, 2015).

Socialni inženiring je tehnika napada, s katero se manipulira človeka z namenom pridobivanja osebnih ali poslovnih informacij ali podatkov. Napad s socialnim inženiringom lahko opišemo z naslednjimi štirimi stopnjami, ki so razvidne na sliki 2: zbiranje informacij, vzpostavitev odnosa, izkoriščanje odnosa in izvršitev zastavljenega cilja. Pri vseh korakih pa je ključen človeški vir, saj se večina napadov na informacijske sisteme s pomočjo socialnega inženiringa zgodi ravno zaradi napak le-tega (Androić in Špehonja, 2015).



Slika 2: Življenski krog napada s socialnim inženiringom (Informacijski pooblaščenec, 2009)

Tehnike zlorab socialnega inženiringa, ki bi se jih napadalci lahko poslužili pri napadu na pametni telefon ali s pomočjo pametnega telefona, so lažno predstavljanje – ribarjenje, »vishing« (glasovno lažno predstavljanje), »smishing« (lažno predstavljanje preko sporočila), škodljiva programska oprema, lažne spletne trgovine, lažni prodajalci blaga po telefonu itd. Pri lažnem predstavljanju napadalci pošiljajo lažna e-sporočila, v katerih pozivajo naslovnika, naj obišče spletno mesto preko spletne povezave, ki je vključena v sporočilo. Takšna sporočila izgledajo pristna in z obiskom »lažne« spletne strani žrtev naslovnik sama posreduje podatke, ki jih napadalec potrebuje za uspešno zlorabo. »Vishing« in »smishing« sta podobna, saj pri obeh napadalci izkoriščajo internetno telefonijo. Žrtev prejme telefonski klic ali sporočilo, ki zahteva določeno akcijo, ob kateri se zahtevajo npr. osebni podatki, podatki o poslovni kartici, geslo itd. Napadalci lahko s pomočjo škodljive programske opreme (trojanski konji, orodja za snemanje dejavnosti žrtve, npr. pritiskov tipk tipkovnice) brez uporabnikove vednosti pridobijo

veliko podatkov, npr. podatke o številkah kartice za spletni nakup ipd. V primeru lažne spletne trgovine je žrtev zavedena z ugodno ponudbo k nakupu, pri katerem napadalec pridobi finančne in osebne podatke. Podobni so lažni prodajalci blaga preko telefona, ki z igranjem na karto zaupanja ponujajo žrtvi lažno blago ali storitve z namenom pridobitve podatkov žrtve (Potokar in Androić, 2015). Ena od najpogostejših tehnik socialnega inženiringa je ravno pridobivanje informacij po telefonu, ki na prvi pogled izgleda zelo nedolžno. Napadalec v tem primeru vzpostavi kontakt s žrtvijo in se poskuša skozi telefonski pogovor dokopati do uporabnih podatkov. Lahko se npr. predstavlja kot oseba za tehnično pomoč, nadrejena oseba itd. Večinoma se s tem načinom pridobi uporabniško ime zaposlenega in e-pošto, ki se jo uporabi za nadaljevanje napada. Napad preko elektronske pošte se lahko, kot smo že omenili, izvede s pomočjo lažnih linkov, s sporočili z zahtevami za vpis podatkov, okuženimi priponkami itd. Zaskrbljujoča za neukega uporabnika je možnost pošiljanja elektronske pošte v imenu nekoga drugega, ki jo lahko zlonamerni napadalec pošlje v primeru, ko SMTP-strežniki niso pravilno varnostno konfigurirani (Androić in Špehonja, 2015). Tako lahko npr. – kot se je že zgodilo kateremu podjetju – pošlje napadalec kot direktor podjetja svojemu računovodji elektronsko sporočilo z navodilom za izplačilo, ta pa to izvede, saj ne podvomi v pristnost elektronskega sporočila in pošiljatelja.

1.2 BYOD

Vse več podjetij se zaveda nevarnosti uporabe pametnih telefonov v povezavi s poslovnimi, zaupnimi in osebnimi podatki, saj se je pogosto izkazalo, da je ravno pametna naprava vektor odtujitve takšnih podatkov iz podjetja. Uporabniki pametnih telefonov se velikokrat obnašamo, kot da z njimi še vedno samo telefoniramo, v resnici pa je pametni telefon postal nadomestna naprava računalnika. Na njem dostopamo do elektronske pošte, internih podatkov podjetja, upravljamo aplikacije in se na več načinov povezujemo v interno omrežje podjetja. Problem nastane, ko se takšna naprava izgubi in uporabnik nima nastavljenih vseh varnostnih mehanizmov, ki preprečujejo odtujitev podatkov iz naprave. Po drugi strani pa je notranjemu uporabniku najlažje odtujiti podatke iz podjetja ravno preko pametne naprave. Zato v veliko podjetjih že vpeljujejo mehanizme, kako varovati podatke na pametnih napravah, ter imajo vzpostavljena interna pravila za tako imenovani sistem BYOD (Bring Your Own Device – prinesite svojo napravo). K sprejemu varnostnih ukrepov za zavarovanje osebnih in poslovnih podatkov zavezujejo podjetja področna zakonodaja, zahteve posameznih standardov ter v primeru javnopravnih oseb zahteve za potrditev notranjih pravil.

Velik izziv za podjetja je takšna zaščita vsebine na mobilnih napravah, da je uporabniki ne bi posredovali tretjim osebam. Ko zaposleni prekine delovno razmerje z delodajalcem, ta nima pravice do vpogleda v mobilno napravo, kljub temu da je imel uporabnik na napravi službene podatke. To mu preprečujeta 46. člen Zakona o delovnih razmerjih (ZDR-1), ki pravi, da »*delodajalec mora spoštovati in varovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost*«, ter 48. člen – »*varstvo delavčevih osebnih podatkov: Osebni podatki delavcev se lahko zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem*.« Kar se pri mobilnih telefonih oglašuje kot največja prednost, je za varnostne strokovnjake največja grožnja – kako ustrezno obvladovati tveganje odtujitve podatkov (Informacijski pooblaščenec, 2016).

S porastom koncepta BYOD se povečuje tudi trg z rešitvami za upravljanje mobilnih naprav – MDM (Mobile Device Management). Gre za sistem, preko katerega lahko varnostne in druge nastavitve na mobilni napravi upravljamo centralizirano iz oddaljene lokacije. To pa v nekaterih primerih pomeni, da lahko globoko posežemo v zasebnost zaposlenega. Informacijski pooblaščenec v svojih smernicah o uporabi rešitev MDM navaja: »*Zavedati pa se moramo, da ne gre zgolj za varnostna tveganja, temveč tudi za tveganja glede zagotavljanja skladnosti z zakonodajnimi zahtevami varstva osebnih podatkov, tajnih podatkov, delovnega in konkurenčnega prava. Vsaka organizacija, ki se zato odloča za vpeljavo koncepta BYOD, mora pravočasno analizirati tveganja ter zagotoviti postopke in ukrepe, s katerimi bo zmanjšala ali izničila tveganja za zahtevano raven zakonitosti in varnosti svojega poslovanja*.« Z uporabo rešitev MDM lahko globoko posežemo v zasebnost uporabnika, zato tudi uvedba te rešitve ni tako trivialna (Informacijski pooblaščenec, 2016).

2. PRIMER IZ PRAKSE JAVNEGA PODJETJA MARIBORSKI VODOVOD D. D.

Podjetje Mariborski vodovod je v zadnjem obdobju prešlo iz delovno intenzivnega podjetja v poslovno učinkovito podjetje, ki stalno spreminja poslovne procese klasičnega komunalnega podjetja. Ob tem je uvedlo e-poslovanje, GIS in se digitalno transformiralo, kar pa prinaša tudi nevarnosti (Burnač, Androić in Špehonja, 2018). Družba sodi v sektor upravljanja kritične infrastrukture posebnega družbenega pomena. Oskrba s pitno vodo sodi v četrti sektor kritične infrastrukture, kar ji na podlagi določil Zakona o kritični infrastrukturi (ZKI) nalaga naslednje vrste nalog:

»(1) Upravljavci kritične infrastrukture zagotavljajo neprekinjeno delovanje kritične infrastrukture.

(2) Upravljavci kritične infrastrukture določijo kontaktno osebo ali več takih oseb za sodelovanje na področju kritične infrastrukture z drugimi upravljavci kritične infrastrukture, nosilci sektorjev kritične infrastrukture in ministrstvom« (ZKI, 19. člen).

Zanimivo je izhodišče, ki ga zagovarja Kotnik (2012), ki meni, *»da je ranljivost kritične infrastrukture sorazmerna s ranljivostjo kibernetskega prostora. Dejanska stopnja varnosti kritične infrastrukture je odvisna od stopnje tveganja napada na kritično infrastrukturo iz kibernetskega prostora.«* Bernik in Markelj (2016) menita, da *»ko se grožnja enkrat uresniči, poti nazaj ni več, zato je treba za kibernetsko varnost poskrbeti že prej«*.

Za ugotovitev stopnje varnosti kritične infrastrukture je potrebno narediti vsaj oceno tveganja in analizo ogroženosti, ki sta osnova za nadaljnje varnostne ukrepe. Primeri v preteklosti so nam že pokazali ranljivost kritične infrastrukture. Takšen primer je bil električni mrk v ZDA leta 2013, ko je brez elektrike ostalo cca. 55 milijonov ljudi. Zaradi tega je nastala tudi kolateralna škoda, kot je prenehanje delovanja čistilnih naprav za zagotavljanje pitne vode, ustavitev javnega prevoza s vlakom, izpraznjenost baterij mobilnih telefonov, zaprtje oziroma nezmožnost delovanja podjetij itd. Izpad električne energije pred leti v Sloveniji zaradi žleda nam je žal že nakazal, kakšne posledice so na področju vodne oskrbe v obliki kolateralne škode. Potrebno je omeniti, da vse človeštvo porabi kar 8 % vse svetovne proizvodnje energentov za črpanje in distribucijo vode. Dobro izpeljan zlonamerni kibernetski napad pa bi lahko povzročil še večjo škodo, vključno s posledicami, saj obstaja možnost, da bi zlonamerni hekerski napadalec lahko prevzel tudi nadzor nad določenim upravljanjem oskrbe s pitno vodo (Burnač, Androič in Špehonja, 2018). Tveganje na področju informacijskega sistema je v družbi Mariborski vodovod prepoznano v operativnem tveganju. V tem poglavju je bil izpad informacijskega

sistema zaznan kot zmerno tveganje. Takšen napad bi lahko napadalec izvedel tudi s pomočjo pametnega telefona ali izrabo le-tega.

Vodstva podjetij se kot dober gospodar trudijo omejiti tveganja ter uvajajo mehanizme za preprečevanje le-teh. V Mariborskem vodovodu evidentirajo in spremljajo štiri skupine poslovnih tveganj, v katere sodijo tveganje upravljanja in vodenja, tveganje izvajanja javne službe oskrbe s pitno vodo, operativna tveganja in finančna tveganja.

V okviru operativnih tveganj se zaznavajo tudi vse vrste informacijskih tveganj, ki se jih ocenjuje kot zmerna tveganja. V tem primeru gre lahko za izpad informacijskega sistema, sistemov varnostnega informacijskega kopiranja, zbiranja in obdelovanja vseh vrst podatkov. Informacijska tveganja v podjetju presojajo po smernicah ISO 27001. Družba Mariborski vodovod je pred desetletjem ustvarila okrog pet tisoč podatkov na letnem nivoju. V letu 2018 je podjetje zbralo, obdelalo in posredovalo že skoraj 20 milijonov raznih vrst podatkov. Vsled tega zagotavlja zadostne strežniške in diskovne zmogljivosti za vsakodnevno shranjevanje in varovanje vseh podatkov.

V sedmih letih so v podjetju uvedli vse elemente e-poslovanja, s celotno prenovo informacijskih poslovnih procesov. Informacijski poslovni sistem omogoča poslovanje celotne družbe preko poslovnega in tehničnega sistema z vrsto posameznih aplikacij, ki so povezane v funkcijsko celoto. Ob tem podjetje na mesec zamenja okrog tisoč vodomerov, za obdobje petih let. S tem se povečuje mesečna količina odčitanih vodomerov. Velik napor in trud je podjetje vložilo še v vgradnjo 269 kontrolnih vodomerov, ki omogočajo on-line spremljanje pretoka vode v vodovodnem omrežju, ki ga podjetje upravlja. Na podlagi vrste podatkov in na platformi podjetja se lahko dela hidravlične modele, simulacije delovanja sistema z meritvami pretoka in tlaka v vodovodnem sistemu. Vse navedeno je bilo možno ob kadrovski nadgradnji in pomlajevanju zaposlenih v družbi. Vsi novozaposleni so danes že dovolj računalniško pismeni, da lahko hitro usvojijo nove poslovne procese, kar je bilo s starejšimi kadri bistveno težje. V zadnjih treh letih lahko govorimo o hitri digitalni transformaciji vseh poslovnih procesov v Mariborskem vodovodu.

Dostop do teh posameznih poslovnih informacijskih podatkov imajo posamezniki in skupine, največkrat znotraj posameznega sektorja. Nekateri sektorji nimajo dostopa do druge vrste aplikacij in podatkov. Na ta način so v podjetju omejili širokost dostopa, vpogleda in uporabe podatkov, ki bi lahko pomenili varnostno-informacijsko tveganje za družbo. Na drugi strani želi Mariborski vodovod lastnikom občinam in uporabnikom nuditi vrsto podatkov za boljše razumevanje delovanja javne službe oskrbe s pitno vodo. Državni podzakonski predpis zahteva, da se posamezen vodomer popiše najmanj enkrat letno. Podjetje je do konca leta 2018 namestilo že 96 % vodomerov na daljinsko odčitavanje. Sedaj se popisujejo vodomeri enkrat mesečno. S tem je podjetje prijaznejše do uporabnikov, saj imajo uporabniki brezplačno stalno on-line aplikacijo, ki jim omogoča spremljanje porabe vode, popisa stanja porabe in plačila storitve javne službe oskrbe s pitno vodo. Ob tem se količine zbranih podatkov povečujejo na potenco, kar povzroča prenovo poslovnih procesov shranjevanja teh zbirk podatkov podjetja v e-arhiv. Zato pa se pojavlja vrsta novih vprašanja glede varovanja vseh vrst podatkov, do katerih zaposleni dostopajo. Če so še pred petimi leti bile posamezne vrste podatkov v pisni obliki v tabelah programskih orodij Word ali Excel, so današnje vrste zbirk podatkov dostopne na platformi podjetja Mariborski vodovod. Danes popisovalci na terenu zbirajo, odčitavajo in obdelujejo podatke na pametnih telefonih in prenosnih računalnikih. Ob tem morajo biti povezani z bazo podatkov podjetja, da lahko nemoteno preverjajo stanje porabe vode na 46.700 vodomerih. Vse te zbirke podatkov potem zaposleni v obračunu vode, saldakontih in informatiki obdelujejo, kontrolirajo, vse do izdaje in pošiljanja položnic. Če so podatki na podlagi pripravljenih alarmov neprimerni, jih služba kontrole še enkrat preveri na samem terenu. Še dve leti nazaj so imeli popisovalci pri svojem delu

terminale, danes pa vse to delo izvajajo s pametnimi telefoni in tablicami. Ob tem so s strani informatike postavljeni razni alarmi, ki opozarjajo na delo, zbrane in obdelane podatke iz preteklih obdobij. Vse navedeno širi krog upravičencev rabe in obdelave podatkov.

S tem je podjetje postalo bolj ranljivo za vdore in nepooblaščene vpoglede v posamezne vrste podatkov. Veliko delo je bilo opravljeno v zvezi z implementacijo geografskega informacijskega sistema, kjer so razvidni celotni podatki o posameznih cevovodih, objektih in napravah, priključkih ter uporabnikih za vseh 118 let izvajanja javne službe oskrbe s pitno vodo v Mariboru. Vse vrste podatkov so v podjetju Mariborski vodovod v celoti prenesli v posamezne aplikacije, zbirke podatkov, kjer so stalno možni posamezni izpisi v obliki preglednic, poročil in sprotnega spremljanja delovanja celotnega vodooskrbnega sistema. Z implementacijo novih poslovnih modelov in procesov je podjetje sedaj pred novimi izzivi cele vrste varnostnih ukrepov in politik, ki morajo biti najprej podprte z notranjimi internimi akti. Podjetje Mariborski vodovod je sprejelo in uvedlo kar nekaj varnostnih ukrepov, ki ščitijo poslovne podatke podjetja in osebne podatke, katerih upravljavec je podjetje pred odtujitvijo. Najpomembnejše varnostne politike, ki so povezane s področjem varnostnih mobilnih naprav, so »Varnostna politika mobilnih naprav«, »Politika varnosti komunikacij«, »Politika nadzora dostopa«, »Politika dela na daljavo«, »Politika uporabe gesel«, »Politika kriptografije«, »Politika varnega e-poslovanja« in »Politika uporabe interneta«. Krovni dokument varnostnih politik je »Poslovnik informacijske varnosti«.

Politika mobilnih naprav strogo prepoveduje priključevanje osebnih mobilnih naprav v informacijski sistem podjetja – vanj se lahko priključujejo zgolj naprave, ki so v lasti podjetja in za katere se vodi seznam v sektorju informatike. Izjema je priključitev na odprto brezžično omrežje znotraj podjetja (odprta dostopna točka MV), kjer je ta na voljo, ali pa v primeru, da Sektor informatike predhodno preveri takšno napravo in izda dovoljenje. Politika gesel predpisuje sestavo gesla iz vsaj 8 znakov različno velikih črk abecede, številk in ločil ter drugih znakov. Geslo si mora uporabnik zapomniti in ne sme biti nikjer zapisano oziroma dostopno komu drugemu kot njemu. Vpeljana je avtomatska zahteva po zamenjavi gesel na vsake tri mesece. Uporabnikom, katerih delo zahteva tudi oddaljen dostop, predvsem na mobilnih napravah (npr. pametni telefoni), se takšen dostop dodeli na podlagi zahteve vodje organizacijske enote, skladno s Politiko oddaljenega dostopa, ki uveljavlja pravila dela na daljavo in mobilnega dela. Oddaljen dostop postavlja dodatna varnostna vprašanja, saj se uporabniki povezujejo v omrežje podjetja preko javno dostopnega omrežja – interneta, ob zahtevi, da bodo imeli na voljo iste storitve in podatke kakor v pisarni. Ker imajo oddaljeni uporabniki enak dostop kot uporabniki znotraj podjetja, vnašajo v informacijski sitem podjetja dodatna varnostna tveganja. Politika kriptografije določa, kdaj in kako uporabiti šifriranje. Vključuje tudi zaščito občutljivih informacij in komunikacij, upravljanje s ključi in postopke za obnovitev šifriranih informacij, kadar je to potrebno. Cilj te politike je ustrezna in učinkovita kriptografija za zaščito zaupnosti, verodostojnosti in/ali celovitosti informacij. Politika kriptografije zajema podporo uporabnikom, ki potrebujejo mobilnost, daljinski dostop, splet, elektronsko pošto, spletne storitve za stranke, varnostne in arhivske kopije ter komunikacije med fizično ločenimi organizacijskimi enotami. Uporabniki, ki se povezujejo v splet in delijo zaupne informacije o družbi ali osebne podatke, morajo to početi preko šifriranih povezav in preko varnih povezav, ki jih predpisuje Politika varnega e-poslovanja (Mariborski vodovod, 2018).

V zadnjem času je bil v podjetju izveden tudi notranji in zunanji varnostni pregled s strani zunanjega strokovnega izvajalca. Podjetje je posodobilo večje število varnostnih politik in kot stalni ukrep izvaja odpravljanje vseh zaznanih varnostnih tveganj.

3. ZAKLJUČEK

Da bi se končni uporabnik karseda približal varni uporabi elektronskih naprav, se svetuje naslednje:

- Namestite protivirusni sistem na pametne naprave.
- Zaklepajte telefon z močnim geslom.
- Protokole imejte vklopljene le v času, ko jih uporabljate, sicer jih izklopite (WiFi, Bluetooth, Mobilni podatki, NFC, Lokacijo, vidnost telefona).
- Nalagajte aplikacije samo iz uradnih spletnih trgovin.
- Pred nastavitvijo aplikacije preverite, kateri so pogoji uporabe ter katera dovoljenja aplikacija potrebuje.
- Redno odstranjujte aplikacije, ki jih ne potrebujete več.
- Kadar je to mogoče, uporabite napredne mehanizme za avtentikacijo.
- Redno ustvarjajte varnostne kopije podatkov.
- Nameščajte posodobitve operacijskega sistema ter aplikacij.
- Izklopite oddajanje svoje geolokacije. Ta naj se uporablja samo takrat, ko jo potrebujete.

Podjetja pa lahko za varnost svojih omrežij in poslovnih mobilnih telefonov poskrbijo z izobraževanjem zaposlenih, uporabo rešitev za upravljanje mobilnih naprav, uvedbo ukrepov BYOD in temu ustreznih predpisov, uporabo različnih drugih varnostnih ukrepov in rešitev, kontrolo varnostne stopnje z občasnimi notranjimi in zunanjimi varnostnimi pregledi, internimi pravnimi akti s predpisanimi pravili, zlasti za področje mobilnih naprav, itd.

Odgovor na zastavljeno vprašanje v naslovu (»Ali so osebni in poslovni podatki varni na pametnih telefonih?«), nam podajajo strokovnjaki spletne strani Varni na spletu, ki trdijo, da si velja pri uporabi pametnih naprav zapomniti naslednje osnovno vodilo: » … *da so pametne toliko, kolikor je pameten njihov uporabnik*« (Varni na internetu, 2017). Iz našega raziskovanja lahko povzamemo, da je stopnja ogroženosti osebnih in poslovnih podatkov na pametnih telefonih visoka, a se jo lahko zniža s predlaganimi varnostnimi ukrepi in mehanizmi. Pametni telefoni pa glede na pospešeno razvijajočo se tehnologijo ne bodo nikoli popolnoma varni, saj klasičen uporabnik ne bo zmogel slediti vsemu razvoju ter vse naprednejšim tehnikam in inovativnostim zlonamernih napadalcev.

SUMMARY

IS PERSONAL AND BUSSINESS DATA SAFE ON SMARTPHONES?

Boštjan ŠPEHONJA
Unistar LC d.o.o., Slovenia
bostjan.spehonja@gmail.com

Danilo BURNAČ
Water Utility Company Maribor, Slovenia
danilo.burnac@mb-vodovod.si

Sanja ANDROIĆ
Water Utility Company Maribor, Slovenia
sanja.androic@mb-vodovod.si

Milka PUNGARTNIK, Ph. D.
Water Utility Company Maribor, Slovenia
milka.pungartnik@mb-vodovod.si

The progress in technology has brought great changes in computer science. Different mobile gadgets that serve for personal as well as bussiness use are replacing computers and laptops. The most frequent gadget is a smartphone. It has taken us some time to start recognizing the threats and traps that lie in wait for our smartphones. We can divide these traps and threats in two groups, technical and non-technical.

Amongst all the threats for a single user as well as for systems, we must expose smartphones. Users gladly accept the novelties that the development of smartphones brings, but we very often forget about a safe use. We have to be aware of the fact that smartphones became our office on the go and often a replacement for our computer or laptop. The data on our smartphones is equal to the one we have on our computers. With the smartphone we access our personal and bussiness email, bussiness files and confidential data, different social media, we can also pay online via various applications, we save contacts, wireless network passwords, personal photographies, text messages. There are plenty reasons why this mobile gadget became so interesting for attackers and also a mechanism to steal valuable bussiness data.

However, most of the big companies and all those with a critical infrastructure employ security experts, who try their best to keep their company safe. Especially the companies with a critical infrastructure need to focus on the security on an even higher level. It is recommended to check and improve the security of the information and communication technologies by an occasional screening of internal and external security check-ups, and highering or buying certified software or services. Despite all that intrusions and valuable information leakage still happens. In this case two scenarios besides the technical intrusion are possible. It can either be that the employees are not educated enough and their minimal mistake provokes a catastrophe for the company. The other scenario is a deliberate alienation of data using an internal employee. It is well known that in the last few years the weakest part in the safety chain has become the uninformed man. Information technology development is reaching lightning speed and the unlimited ideas of online fraudsters and malicious hackers are not staying behind at all. If we do not educate the final user, who works with information technology, about threats he can face, the attack of a hacker is just a matter of time.

In order for the final user to get as close as possible to the safe use of electronic gadgets, the following is recommended. The installation of an antivirus system on smart gadgets, locking the smartphone using a strong password, switching on the protocols only at the time of use, downloading applications only from official online stores, checking the conditions and necessary permissions before installing the application, a regular removal of unnecessary applications, a regular back up of the data and the installation of updates, and turning off the geolocation when it is not needed.

Viri in literatura:

Androić, S. in Špehonja, B. (2015). Posledice premalo skrbnega ravnanja z elektronskim in papirnim gradivom. V N. Gostenčnik (Ur.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 14. zbornik mednarodne konference v Radencih 15.-17. april 2015* (str. 35–51). Maribor: Pokrajinski arhiv.

Bernik, I. in Markelj, B. (2016). Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja s mobilno napravo. *Varstvoslovje*. 1, str. 5–15. Ljubljana: Fakulteta za varnostne vede.

Burnač, D., Androić, S. in Špehonja, B. (2018). Obveznosti podjetja Mariborski vodovod kot deležnika kritične infrastrukture na področju nevarnosti e-poslovanja in potreba po varnostnih pregledih IKT-sistemov. *Moderna arhivistika. 1*, str. 279–292. Maribor: Pokrajinski arhiv Maribor

Informacijski pooblaščenec. (2009). *Socialni inženiring in kako se pred njim ubraniti?* Pridobljeno 12. 12. 2018 s spletne strani: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/socialni-inzeniring-in-kako-se-pred-njim-ubraniti.pdf.

Informacijski pooblaščenec. (2016). ***Smernice*** *Informacijskega pooblaščenca. Uporaba zasebnih naprav v službene namene (BYOD)*. Pridobljeno 10. 12. 2018 s spletne strani: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/ Smernice_o_BYODweb.pdf

Mariborski vodovod. (2018*).* *Politika uporabe gesel. Maribor:* Mariborski vodovod.

Mariborski vodovod. (2018*).* *Politika kriptografije. Maribor:* Mariborski vodovod.

Mariborski vodovod. (2018*).* *Politika mobilnih naprav. Maribor:* Mariborski vodovod.

Mariborski vodovod. (2018*).* *Politika oddaljenega dostopa.* Maribor: Mariborski vodovod.

Mariborski vodovod. (2018*).* *Politika varnega e-poslovanja.* Maribor: Mariborski vodovod.

Potokar, M. in Androić, S. (2015). Socialni inženiring – človek kot del varnostnega sistema. V N. Gostenčnik (Ur.), *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja: 14. zbornik mednarodne konference v Radencih 15.–17. april 2015* (str. 53–65). Maribor: Pokrajinski arhiv.

Strava (2018). *Razkrivanje ameriških vojaških baz preko mobilne fitness aplikacije.* Pridobljeno 14. 12. 2018 s spletne strani: https://www.strava.com/heatmap #3.04/-67.12952/43.10004/hot/all.

Varni na internetu (2017). *ABC varnosti in zasebnosti na mobilnih napravah.* Pridobljeno 14. 12. 2018 s spletne strani: https://www.varninainternetu.si/wp-content/uploads/2017/07/Varnost-in-zasebnost-na-pametnih-telefonih_1.pdf .

Zakon o kritični infrastrukturi. (2017). Uradni list RS, št. 75.