Vidiki kazenskega prava pri uporabi mobilnih naprav in dostopanju do korporativnih podatkov

Blaž Markelj, Univerza Maribor, Fakulteta za varnostne vede
Sabina Zgaga, Univerza Maribor, Fakulteta za varnostne vede

Namen prispevka:
Organizacije čedalje pogosteje uporabljajo moderne tehnologije pri vsakodnevnem delu. V zadnjem času so posebej aktualne mobilne naprave, ki uporabnikom zagotavljajo neprestan dostop do informacij, tudi tistih znotraj zaprtega informacijskega okolja organizacije. Posebej je pomembno vprašanje, kateri so tisti podatki, ki ji prenašamo po teh napravah, in jih s tem izpostavljamo morebitnim informacijsko-varnostnim grožnjam. Vsaka organizacija bi morala imeti pravilnike, ki bi določali varne načine uporabe mobilnih naprav in prenosa podatkov. V primeru neprimerne zaščite podatkov in morebitnega razkritja teh nepooblaščenim tretjim osebam lahko namreč pride do kazenskopravnih posledic za delavce in za samo organizacijo.

Metodologija:
Opravljeni je pregled aktualne literature, analiza groženj, ki pretijo uporabnikom pri nevestnem upravljanju mobilnih naprav, in kritična analiza veljavne kazenskopravne zakonodaje v primeru kršitve tajnosti podatkov.

Ugotovitve:
Tema je razmeroma nova, zato pričakujemo, da so organizacije šele v začetni fazi zavedanja groženj informacijski varnosti in implementacije pravilnikov varne uporabe mobilnih naprav ter prenosa podatkov. Z vidika kazenskega prava naj bi prispevek pokazal glavne pravne podlage za kazensko odgovornost delavcev organizacij za razkritje podatkov in njihove bistvene pomanjkljivosti.

Omejitve:
Prispevek obravnava temo, ki je še dokaj neraziskana, zato so skope tudi objave dosedanjih raziskav in aktualnih znanstvenih člankov.

Praktična uporabnost:
Organizacije bodo dobile celovit vpogled v grožnje, ki pretijo informacijski varnosti pri uporabi mobilnih naprav in prenosu podatkov; v pomembnost internih pravilnikov, ki zagotavljajo uporabnikom s strani organizacije verificirano uporabo izročenih sredstev; v pomembnost pravilnega ravnanja s temi podatki; in vidike kazenskega prava glede morebitne odtujitve podatkov ter nespoštovanja internih pravilnikov.

Izvirnost:
Gre za novo temo; predvsem je nova povezava med kazenskim pravom, grožnjami informacijski varnosti in internimi pravilniki, ki so organizacijam v pomoč pri zagotavljanju informacijske varnosti.

Ključne besede: kombinirane grožnje, mobilne naprave, informacijska varnost, kazenska odgovornost

1 UVOD

Mobilne naprave, od teh predvsem pametni telefoni in tablični računalniki, so v zadnjem obdobju v visokem porastu (Chicone, 2009; Riedy, Beros and Wen, 2011). Raziskava, ki jo je izvedlo podjetje IDC (2011), nakazuje, da se bo prodaja mobilnih telefonov do leta 2015 povečala za 200 odstotkov. Samo v primerjavi z letom 2010 se je prodaja mobilnih telefonov povečala za 55 odstotkov. Mobilne telefone smo poznali že v preteklosti, vendar ne v taki obliki. Preporod se je začel s predstavitvijo pametnih telefonov (npr. Apple Iphone, Androide ipd.) in kasneje tabličnih računalnikov (npr. Ipad). S številnimi uporabnimi funkcijami, ki jih pametni telefoni ponujajo, so čez noč postali nenadomestljivi

pripomoček pri vodenju vsakodnevnih poslovnih in zasebnih opravil. Hkrati se je s tem tudi zabrisala meja med zasebno in poslovno rabo pametnih telefonov. Pametni telefoni, s pomočjo številnih dodatnih programskih paketov, uporabnikom omogočajo, da so neprestano v stiku z najnovejšimi informacijami. Sinhronizacija elektronske pošte, dostop do podatkov znotraj informacijskega sistema organizacije in vodenja bančnega poslovanja s pomočjo pametnih telefonov danes, pri vsej sodobni tehnologiji, niso več nič posebnega. Vsa raznovrstna dodatna programska oprema nam je enostavno dostopna na spletu. Vse premalokrat pa se sprašujemo o informacijski varnosti pri uporabe sodobnih tehnologij. Velikokrat pozabljamo, da so podatki, s katerimi dnevno delamo, lahko za nekoga zelo pomembni. Navsezadnje hitrost dostopa do pomembnih in novih informacij danes za organizacijo in posameznika predstavlja konkurenčno prednost.
Načinov kako lahko dostopamo do informacij, tudi tistih, ki se nahajajo znotraj zaprtega informacijskega sistema organizacije, je več. Mobilne naprave danes omogočajo že avtomatsko iskanje odprtih brezžičnih omrežij, na katere se samodejno povežejo, v nasprotnem primeru pa uporabijo tehnologijo, ki jo omogoča mobilni operater.
Grožnje, ki pretijo uporabnikom mobilnih naprav so številne. Delujejo lahko posamično ali simultano, vedno pa z namenom pridobitve neke koristi. Razdelimo jih na neposredne, kot je na primer fizična odtujitev naprave, ali posredne, ki so bolj zahrbtne in velikokrat sploh ne vemo, da so aktivne na naši mobilni napravi (npr. *rootkiti*, *malware* idr.). Rezultati raziskave podjetja Lookout (2011) kažejo, da se je v zadnjih šestih mesecih zelo povečalo število groženj, temelječih na aplikacijah programa *malware*, predvsem v primerjavi s programi *spyware*, kar za 14 odstotkov. Obstaja verjetnost, da se pri nalaganju programske opreme »okuži« od 1 do 4 odstotke mobilnih naprav. Poročilo, ki ga je izdelalo podjetje Juniper (2011) navaja, da se je od poletja 2010 dalje število mobilnih naprav, ki delujejo na platformi Android, in so se okužile s programi *malware*, povečalo za 400 odstotkov. V poročilu zasledimo tudi, da ima 85 odstotkov uporabnikov na svojem mobilnem telefonu neuporabno zaščito. Proizvajalci programske opreme za mobilne naprave si dovolijo vgraditi “zadnja vrata”, program, ki brez vednosti uporabnika upravlja z nastavitvami vse programske opreme na mobilni napravi; samodejno pošilja podatke o tem, kje se imetnik naprave nahaja (pošiljanje GPS lokacije) in lahko prevzame nadzor nad mobilno napravo (Lookout, 2010).
V preteklosti smo se navadili na statične računalnike, kjer ni bilo veliko različnih načinov povezovanja v splet in dostopanja do raznovrstnih podatkov, vendar so številne organizacije že takrat uvajale pravilnike in priporočila o pravilni uporabi izročenih sredstev. Danes, ko vsakodnevno spremljamo novosti na tehnološkem področju, pa bi moralo biti pravilnikov za zagotavljanje informacijske varnosti pri rabi izročenih sredstev in izobraževanj o tem še veliko več. Veliko je že bilo narejenega na tehničnem področju zagotavljanja informacijske varnosti pri uporabi mobilnih naprav in veliko bo še moralo biti narejenega. V celotnem segmentu zagotavljanja informacijske varnosti pri uporabi mobilnih naprav in prenosu podatkov je potrebno najbolj poskrbeti za najšibkejša člena. To sta mobilna naprava in njen uporabnik. Uporabnikovo nepoznavanje varne uporabe mobilne naprave, njene programske opreme, varnega povezovanja v omrežja in prenosa podatkov ter vsaj osnovnih funkcij, ki jih omogočajo mobilne naprave, lahko organizacijo privedejo v veliko informacijsko ogroženost.

2 NAČINI ZAŠČITE NA MOBILNIH NAPRAVAH

Na tržišču najdemo različne rešitve. Mobilni telefon nam praviloma omogoča nastavitev gesel za dostop do kode PIN in kasneje za vstop do programov in posameznih funkcij telefona. Vse pomembne podatke lahko kriptiramo s pomočjo temu namenjene programske opreme. Za varnejši prenos podatkov med mobilnim telefonom in drugimi informacijskimi sistemi pa poskrbimo z vzpostavitvijo povezave VPN ali uporabimo protokol https/ssl (Booz Allen Hamilton, 2009). Vendar vse tehnične rešitve ne pomenijo veliko, če jih uporabnik ne pozna ali jih ne zna uporabljati. Zato organizacije morajo poskrbeti za ustrezno izobraževanje zaposlenih.
Pravilniki za uporabo izročenih sredstev, bi morali določati standarde informacijske varnosti pri uporabi mobilnih naprav. Vsebovati bi morali sezname programske opreme za mobilne naprave, ki jo organizacija dovoli uporabljati, poleg tega pa še standarde varnega ravnanja z mobilnimi napravami, povezovanja v druga ali lastna omrežja ter prenašanja in hranjenje podatkov. Zagotovljeno bi moralo biti tudi primerno izobraževanje uporabnikov. Pravilniki, bi morali biti potrjeni s stani vodstva

organizacije. Vsako nespoštovanje pravilnika bi moralo biti sankcionirano. Predvsem v primeru, da bi, zaradi nespoštovanja pravilnika, prišlo do namernega oškodovanja organizacije ali tretje osebe.

3 DEFINICIJA RELEVANTNIH PODATKOV (OSEBNI PODATKI, TAJNOST, POSLOVNA SKRIVNOST, POKLICNA SKRIVNOST)

Pri mobilnih napravah in prenašanjem podatkov med njimi imamo lahko opravka s štirimi vrstami podatkov: z osebnimi podatki, (uradno, vojaško) tajnostjo, poklicno skrivnostjo in poslovno skrivnostjo. Ker nas zanima kazenska odgovornost, je treba specialno definicijo teh podatkov najprej iskati v Kazenskem zakoniku-1 (v nadaljevanju KZ-1), v primeru njene odsotnosti pa v pravnih aktih z matičnih pravnih področij.

Poslovna skrivnost je tako z novelo KZ-1B definirana s KZ-1, in zanjo tako štejejo se štejejo listine in podatki, ki so z zakonom, statutom, pravili ali drugim splošnim aktom ali odredbo pristojnega organa ali druge upravičene osebe razglašeni za industrijsko, bančno ali drugo poslovno skrivnost in so tako pomembni, da so z njihovo izdajo očitno nastale ali bi lahko nastale hujše škodljive posledice, kar v bistvu ustreza definiciji poslovne skrivnosti iz Zakona o gospodarskih družbah[1], katero je bilo pred zadnjo novelo KZ-1B treba upoštevati za relevantno kaznivo dejanje izdaje in neupravičene pridobitve poslovne skrivnosti.[2] Poslovno skrivnost torej določi sama oseba, na katero se poslovna skrivnost nanaša, ali pa gre za tak podatek, za katerega je očitno, da bi z njegovo izdajo nastale škodljive posledice. Primer poslovne skrivnosti bi bila receptura za Coca Colo, ki je ena izmed najbolj varovanih skrivnosti v poslovnem svetu.

Tajen podatek ni definiran s KZ-1, ampak z Zakonom o tajnih podatkih, in sicer kot dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije, znanstvene, raziskovalne, tehnološke, gospodarske in finančne zadeve, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije, ki ga je treba zaradi razlogov določenih v tem zakonu zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno. Bistveno je torej, da je podatek določen za tajnega s strani pooblaščene osebe, ker je tako pomemben, da bi z njegovim razkritjem nepoklicani osebi nastale, ali bi očitno lahko nastale, škodljive posledice za varnost države ali za njene politične ali gospodarske koristi.[3] Primer tajnega podatka bi lahko bila pogodba Republike Slovenije za nabavo določenega orožja za Slovensko vojsko z dobaviteljem tega orožja.

Relevanten podatek je lahko tudi poklicna skrivnost.[4] To je vsak podatek, ki ga oseba pridobi pri opravljanju poklica. KZ-1 kot take osebe našteva zagovornika, odvetnika, zdravnika, duhovnika, socialnega delavca in psihologa, seveda pa to niso edine osebe, ki so dolžne varovati poklicno skrivnost. To dolžnost imajo vse osebe, ki opravljajo poklic (Deisinger, 2002: 145), primer poklicne skrivnosti pa so podatki o obdolžencu, do katerih pride odvetnik kot njegov zagovornik.

In ne nazadnje, podatek, s katerimi upravljajo organizacije z mobilnimi napravami, je lahko tudi osebni podatek.[5] Tudi tega KZ-1 ne definira, ampak najdemo definicijo v Zakonu o varstvu osebnih podatkov-1, v skladu s katerim je osebni podatek katerikoli podatek, ki se nanaša na posameznika, ki je določena ali določljiva fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko neposredno ali posredno identificira, predvsem s sklicevanjem na identifikacijsko številko ali na enega ali več dejavnikov, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa ne glede na obliko, v kateri

[1] 39. člen Zakona o gospodarskih družbah.

[2] 236. člen KZ-1.

[3] 2., 10., 11. člen Zakona o tajnih podatkih.

[4] 142. člen KZ-1.

[5] 143. člen KZ-1.

je izražen.[6] Tipični osebni podatki so na primer podatki o pacientu iz zdravstvenih kartonov pri osebnem zdravniku. Seveda lahko določen podatek spada v več kategorij, zlasti se lahko podvajata kategoriji poklicne skrivnosti in ostalih podatkov.

4 KAZENSKOPRAVNE POSLEDICE RAZKRITJA PODATKOV

KZ-1 določa ustrezna kazniva dejanja razkritja podatkov. Tako je na primer opredeljeno kaznivo dejanje izdaje in neupravičene pridobitve poslovne skrivnosti, ki ga izvrši vsakdo, kdor neupravičeno v nasprotju s svojimi dolžnostmi glede varovanja poslovne skrivnosti sporoči ali izroči komu podatke, ki so poslovna skrivnost, ali mu kako drugače omogoči, da pride do njih, ali jih zbira z namenom, da jih izroči nepoklicani osebi.[7] Kako mora biti poslovna skrivnost varovana in kdo jo je dolžan varovati, pa seveda KZ-1 ne določa. To določi gospodarska družba s sklepom, s katerim določi, kateri podatek je poslovna skrivnost.[8] V tem sklepu bi morala družba seveda v primeru elektronskih podatkov določiti tudi vidik informacijske varnosti.

Podobno je opredeljeno kaznivo dejanje izdaje tajnih podatkov,[9] ki ga izvrši uradna oseba[10] ali druga oseba, ki v nasprotju s svojimi dolžnostmi varovanja tajnih podatkov sporoči ali izroči komu tajne podatke ali mu kako drugače omogoči, da pride do njih, ali zbira take podatke, zato da jih izroči nepoklicani osebi. Spet, KZ-1 ne določa načina varovanja tajnih podatkov, ampak to ureja Zakon o tajnih podatkih in številni podzakonski predpisi.[11] V skladu s tem zakonom mora vsaka organizacija sprejeti ustrezne sisteme in postopke varovanja tajnih podatkov, ki ustreza določeni stopnji tajnosti in onemogoča njihovo razkritje nepoklicanim osebam, ti postopki in ukrepi pa morajo biti vnaprej določeni s predpisi.[12] Posebej relevanten predpis je Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, ki ureja tudi vidik informacijske varnosti tajnih podatkov. Kdor (t.j. tisti, ki je dolžan varovati tajnost) krši te dolžnosti, določene z zakonodajo in pravilniki organizacije, izvrši kaznivo dejanje izdaje tajnih podatkov.

KZ-1 opredeljuje tudi kaznivo dejanje neupravičene izdaje poklicne skrivnosti, ki ga izvrši vsakdo, neupravičeno izda osebno skrivnost, za katero je izvedel kot zagovornik, odvetnik, zdravnik, duhovnik, socialni delavec, psiholog ali kot kakšna druga oseba pri opravljanju svojega poklica.[13] Način varovanja spet ni določen v KZ-1, ampak v področnih predpisih, ki urejajo opravljanje določenega poklica.

Zlorabo osebnih podatkov med drugim izvrši vsakdo, kdor brez podlage v zakonu ali v osebni privolitvi posameznika, na katerega se osebni podatki nanašajo, osebne podatke, ki se obdelujejo na podlagi zakona ali osebne privolitve posameznika, posreduje v javno objavo ali jih javno objavi.[14] Zakon o varstvu osebnih podatkov-1 tako pravi, da so upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje osebnih podatkov ter v svojih aktih predpisati postopke in ukrepe za zavarovanje osebnih podatkov ter določijo osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.[15] Ti akti morajo seveda zajemati tudi vidik informacijske varnosti teh podatkov.

Kadar gre za neupravičeno razkritje najbolj občutljivih podatkov (tajni, poslovna skrivnost), potem je kaznivo dejanje kaznivo tudi, kadar je izvršeno iz malomarnosti (na primer nepazljivo ravnanje s podatki oziroma nosilci podatkov).[16] Razkritje osebnih podatkov in poklicne skrivnosti pa je kaznivo

---

[6] 6. člen Zakona o varstvu osebnih podatkov-1.

[7] 1. odst. 236. člena KZ-1.

[8] 1. odst. 40. člena Zakona o gospodarskih družbah.

[9] 260. člen KZ-1.

[10] Glej 99. člen KZ-1.

[11] Na primer Uredba o varovanju tajnih podatkov, Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, itd.

[12] 38., 40. člen Zakona o tajnih podatkih.

[13] 2. odst. 142. člena KZ-1.

[14] 1. odst. 143. člena KZ-1.

[15] 25. člen Zakona o varstvu osebnih podatkov-1.

[16] Glej 236. in 260. člen KZ-1.

samo takrat, kadar je izvršeno naklepno (na primer, ko nekdo želi prodati poslovno skrivnost ali posredovati določen zdravstveni podatek o pacientu medijem). Verjetno pa je vsaj v primeru osebnih podatkov razkritje zaradi nespoštovanja pravil informacijske varnosti (neuporaba ustreznih zaščit, malomarno rokovanje z napravami, omogočanje dostopa, itd.) najbolj pogosto izvršeno iz malomarnosti, ne pa naklepno. Tega pa kaznivo dejanje iz KZ-1 ne pokriva, razen če je osebni podatek opredeljen še kot poslovna skrivnost ali tajen podatek.[17]
Druga pomembna značilnost vseh naštetih kaznivih dejanj je, da seveda sam KZ-1 ne določa, katero ravnanje predstavlja neupravičeno razkritje podatkov, ampak je to določeno s področno zakonodajo. Gre za blanketne norme, zato je treba poznati tudi področne, zgoraj naštete predpise.
Ker pa lahko pride tudi do prekrivanja različnih kategorij podatkov, se zastavi vprašanje, kakšno je razmerje med omenjenimi kaznivimi dejanji. Kaznivo dejanje neupravičene izdaje poklicne skrivnosti je tako splošno kaznivo dejanje, tako da v primeru, če gre za razkritje podatka, ki je hkrati poklicna skrivnost in poslovna skrivnost ali tajni podatek, storilec odgovarja za specialno kaznivo dejanje izdaje poslovne skrivnosti ali tajnega podatka (Deisinger, 2002:146)[18] in ne tudi za izdajo poklicne skrivnosti. Tudi osebni podatek je specialen v razmerju do tajnega podatka.

5 ZAKLJUČEK

Pri vedno večji poplavi mobilnih naprav, je uporaba le-teh tudi v poslovne namene pogostejša. Informacije, ki se prenašajo s pomočjo mobilnih naprav so različne narave, velikokrat pa ključnega pomena za organizacijo samo. Zato je bistvenega pomena, da se pri vsaki izgradnji ali posodobitvi procesov, ter implementaciji novih tehnologij, upošteva tudi segment informacijske varnosti. Tehnologija se razvija v smer zagotavljanja večje informacijske varnosti pri uporabi mobilnih naprav in obrambo pred morebitnimi grožnjami in posledično izgubo podatkov, vendar še vedno ostaja uporabnikovo znanje ključni element. To lahko organizacije uredijo s pomočjo izobraževanj in vzpostavitvijo internih pravilnikov o uporabi izročenih sredstev. Interni pravilniki, naj bi definirali standarde uporabe mobilnih naprav, povezovanja v sistem organizacije, prenosa podatkov in uporabe s strani organizacije potrjene programske opreme na mobilnih napravah. Vsako nespoštovanje teh pravilnikov pa bi bilo lahko sankcionirano in bi v primeru izgube zgoraj naštetih vrst podatkov povzročilo tudi kazensko odgovornost. Tako ravnanje namreč lahko predstavlja izpolnitev zakonskih znakov določenih kaznivih dejanj iz KZ-1. Katero kaznivo dejanje je izvršeno, je odvisno od vrste podatka (osebni, tajni, poslovna skrivnost, poklicna skrivnost) in lastnosti storilca. Druga pomembna lastnost teh kaznivih dejanj je, da običajno KZ-1 sam ne določa, kateri podatki so zaščiteni, ampak je to določeno s področno zakonodajo. Gre namreč za blanketne norme. Tretja posebnost je glede krivde storilca. Kadar gre za neupravičeno razkritje ali izgubo najbolj občutljivih podatkov (tajni, poslovna skrivnost), potem je kaznivo dejanje kaznivo tudi, kadar je izvršeno iz malomarnosti, v primeru osebnih podatkov in poklicne skrivnosti pa je kaznivo dejanje kaznivo le, če je izvršeno z naklepom, ne izključuje pa to seveda odgovornosti za ustrezen prekršek.

VIRI

Booz Allen Hamilton (2009). *Mobile Device Security*. Acquired 20. 10. 2011 at http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/7-051909-new-technologies-mobile-devices.pdf

Deisinger, M. (2002). *Kazenski zakonik s komentarjem, posebni del.* Ljubljana: GV založba.

IDC. (2011). *IDC - Press Release.* Pridobljeno 10 .9. 2011 na http://www.idc.com/getdoc.jsp?containerId=prUS22871611.

Juniper Networks. (2011). *Malicious Mobile Threats Report 2010/2011*. Acquired on 10. 9. 2011 at http://www.juniper.net/us/en/dm/interop/go.

Kazenski zakonik-1, Ur. l. RS, 55/2008, 66/2009, 91/2011.

[17] Seveda pa ostaja možnosti odgovornosti za prekršek po ustreznem zakonu ali uredbi.

[18] Komentar, str. 146.

Lookout. (2010). *Zlonamerna koda nad zasebnost uporabnikov mobilnikov Android*. Racunalniske-novice.com. Pridobljeno 7. 9. 2011 na http://www.racunalniske-novice.com/novice/mobilna-telefonija/google/zlonamerna-koda-nad-zasebnost-uporabnikov-mobilnikov-android.html.

Lookout. (2011). *Lookout Mobile Threat Report*. Pridobljeno 10. 9. 2011 na https://www.mylookout.com/mobile-threat-report.

Riedy, M. K., Beros, S. and Wen H. J. (2011). *Management Business Smart Phone Data*. Journal of Internet Law, 3-14.

Zakon o gospodarskih družbah, Ur. l. RS, št. 65/2009, 33/2011, 91/2011.

Zakon o tajnih podatkih, Ur. l. RS, št. 50/2006, 9/2010, 60/2011.

Zakon o varstvu osebnih podatkov, Ur. l. RS, št. 94/2007