Jure Planinšek,
mag. ekonomskih znanosti, univ. dipl. pravnik, vodja pravne pisarne, NIL d.o.o.

Tadej Skok,
dipl. pravnik (UN), študent magistrske stopnje na PF Univerze v Ljubljani

Leta 2018 je internet uporabljalo že skoraj štiri milijarde ljudi. Število uporabnikov in povezanih naprav se izjemno hitro povečuje. Po ocenah strokovnjakov bo leta 2022 na internet povezanih že šest milijard ljudi in več kot 200 milijard pametnih naprav.[1] Ta eksplozija povezljivosti poleg mnogih koristi ponuja tudi neštete priložnosti za kibernetske napade, ki organizacijam[2] povzročajo veliko škodo. Po nekaterih ocenah kibernetski napadi svetovno ekonomijo letno stanejo okoli 600 milijard dolarjev.[3] Poleg poslovne škode imajo kibernetski vdori in varnostni incidenti (vdori) tudi zelo resne pravne posledice: visoke globe, odškodninsko odgovornost ali stečaj.[4] V prvem prispevku predstavljava ključna pravna vprašanja zagotavljanja kibernetske varnosti in podajava pregled ključne zakonodaje s stališča skladnosti poslovanja. V drugem prispevku bova na primeru obravnavala ukrepe za zagotavljanje kibernetske varnosti in s tem povezana pravna vprašanja.

Pravni vidiki kibernetske varnosti (1. del)

Pravo in kibernetska varnost

Poslovne skrivnosti, osebni in drugi (pravno) občutljivi podatki ter informacije v čedalje večjem obsegu »živijo na internetu« ali informacijskih sistemih, ki so povezani z internetom. S tem se tveganja povečujejo, zato lahko v medijih redno beremo o raznovrstnih kibernetskih napadih.[5] V zadnjem letu so bila tarče kibernetskih napadov številna znana podjetja, kot so Marriott International, Facebook, LinkedIn, T-Mobile, British Airways in Uber.[6] Zaradi kompleksnosti in povezanosti informacijskih sistemov je lahko napadalec (*heker*) več tisoč kilometrov stran ali v sosednji sobi (ali oboje) in lahko mesece neopazno preži in čaka na pravi trenutek. Takrat bodisi poseže v občutljive podatke bodisi onesposobi delovanje kritičnih naprav. Če je organizacija nepripravljena, se znajde v igri mačke z mišjo, nastane pa ji lahko več milijard evrov škode.[7] Zato načrtovanje in izvajanje ukrepov kibernetske varnosti postaja eden od ključnih izzivov organizacij.

Kibernetska varnost je zaščita informacijskih sistemov pred krajo ali poškodbami njihove strojne opreme, programske opreme ali podatkov v elektronski obliki, kakor tudi zaradi motenj ali napačno usmerjenih storitev, ki jih zagotavljajo.[8] Popolne zaščite pred kibernetskimi napadi ni. Tveganja pa lahko organizacije obvladujejo s tehničnimi in organizacijskimi ukrepi, predvsem pa s tehničnimi rešitvami, obvladovanjem pravnih odnosov s pogodbenimi partnerji, sklepanjem zavarovanj, pripravo ustreznih internih pravil in usposabljanjem uporabnikov. Te ukrepe zahteva tudi čedalje bolj kompleksna zakonodaja, ki za opustitev skrbnosti predpisuje zelo visoke globe.

Zakaj mora pri zagotavljanju kibernetske varnosti sodelovati pravnik? Razvoj načrtov za zaščito elektronskih podatkov in omrežij ob spoštovanju relevantne zakonodaje in pravilnem vrednotenju tveganj je velik pravni in tehnološki izziv za vsako organizacijo. Pravniki morajo sodelovati predvsem pri pripravi odgovorov na naslednja vprašanja:

- Kakšna je odgovornost organizacije in njenega poslovodstva pri nezadostni kibernetski varnosti (nezadostna skrbnost)?
- Kako zmanjšati in porazdeliti tveganja vdora, da organizacija ni edina, ki nosi tveganja, predvsem kako skleniti ustrezna zavarovanja glede na identificirana tveganja in odgovornosti?
- Kakšne politike, postopke in pravne ukrepe je treba vzpostaviti pred in po vdoru?
- Kako sprejeta pravila in postopke vnesti v pogodbena razmerja z izvajalci ukrepov in jih učinkovito zavezati k spoštovanju in izvajanju?
- Kaj mora v skladu z relevantnimi predpisi organizacija storiti v primeru vdora?
- Kakšne so pravice posameznikov, kadar so njihovi podatki ali sistemi predmet vdora brez njihove krivde?

Vprašanje odgovornosti v primeru kibernetskega napada se nikoli ne konča pri hekerju, ki največkrat niti ni odkrit. Pri nedavnem vdoru v bazo podatkov hotelske verige Marriott International je govora predvsem o dolgoletnih nepravilnostih pri ravnanju s podatki več sto milijonov gostov. Pristojne organe in oškodovance bo zanimalo, ali je upravljavec podatkov te ščitil z zadostno skrbnostjo in po odkritju varnostnega incidenta sprejel vse ukrepe, ki so minimalizirali škodo, ter izpolnil ostale dolžnosti, ki jih nalaga zakonodaja.

Pravno past za podjetja lahko predstavljajo tudi pogodbe ali splošni pogoji, saj podjetja strankam pogosto obljubijo: »Zavarovali bomo vaše podatke pred vdori.« To se po jezikovni metodi lahko interpretira kot iztožljiva pogodbena obveznost (obligacija rezultata), ki je povsem drugačna od dikcije: »Sprejeli bomo ustrezne ukrepe za varovanje vaših podatkov.« To ne pomeni, da se podjetje ne zavezuje k varovanju. Gre za obligacijo prizadevanja, saj absolutna varnost ni mogoča. Kot lahko vidimo na predstavljenem primeru, mora pravna analiza konkretne rešitve presegati zgolj preverjanje, ali je pristop k varnosti v okviru standarda »razumne kibernetske varnosti« in skladen z zakonodajo.

Pojem »razumna kibernetska varnost« morata sodna praksa in praksa regulatorjev zapolnjevati v skladu s trenutnim stanjem tehnike, ki se hitro spreminja. Meniva, da »razumna kibernetska varnost« ne pomeni popolne varnosti; sprejeti ukrepi pa morajo biti sorazmerni tveganosti in občutljivosti varovanih podatkov in sistemov.[9] Najboljše prakse v industriji, mednarodno priznani standardi (ISO 27001, ki določa sisteme vodenja varovanja informacij) in smernice ter praksa nadzornih organov (informacijskih pooblaščencev) bodo zelo pomembni pri oblikovanju standarda skrbnosti zagotavljanja kibernetske varnosti (*standard of care*).

[1] <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>.

[2] Osredotočava se na problematiko, zanimivo za gospodarske družbe in organizacije s področja javnega in zasebnega prava. Drugi vidiki, predvsem kazenski in mednarodnopravni, presegajo domet prispevka.

[3] <https://pro.finance.si/TRIGLAV/8942377/Kaj-lahko-v-podjetju-storite-za-upravljanje-kibernetskih-tveganj>.

[4] Zaradi izgube dobrega poslovnega imena ali zaupanja uporabnikov lahko vdor pomeni takšno izgubo posla, da družba postane insolventna. Primer nizozemske certifikacijske družbe Diginotar in primer ameriške družbe 21st Century Oncology, ki se ukvarja z zdravljenjem raka. Ta se je za las izognila stečaju: <https://phoenixnap.com/blog/business-deterioration-after-a-data-breach>.

[5] Angleški nazivi tipov napadov (trenutno še ni ustaljenih prevodov): Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, Man-in-the-middle (MitM) attack, Phishing and spear phishing attacks, Drive-by attack, Password attack, SQL injection attack, Cross-site scripting (XSS) attack, Eavesdropping attack, Birthday attack, Malware attack <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Eavesdropping%20attack>.

[6] <https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/>.

Zakonodaja in zagotavljanje skladnosti poslovanja

V nadaljevanju navajava najbolj relevantno zakonodajo s področja kibernetske varnosti.[10]

Poslovne skrivnosti

Poslovne skrivnosti so v skladu z 39. členom Zakona o gospodarskih družbah (ZGD-1)[11] podatki, za katere tako določi družba s pisnim sklepom, ali podatki, za katere je očitno, da bi nastala občutna škoda, če bi zanje izvedela nepooblaščena oseba. Gre za zelo široko kategorijo podatkov, ki po najini oceni predstavljajo eno od največjih (poslovnih) tveganj za organizacijo.[12] Poslovna škoda, ki lahko družbam ali organizacijam nastane zaradi vdora, je odvisna od konkretnih okoliščin in kritičnosti podatkov. Za škodo, ki nastane družbi zaradi nezadostnega zagotavljanja kibernetske varnosti, po najinem mnenju pride v poštev pravni standard skrbnosti vestnega in poštenega gospodarstvenika, ki ga morajo skladno z drugim odstavkom 263. člena ZGD-1 dokazati člani organa vodenja ali nadzora gospodarske družbe. Skrbnost vestnega in poštenega gospodarstvenika je nadalje konkretizirana s pravnim pojmom poštenega in vestnega izpolnjevanja dolžnosti, ki v informacijski dobi pomeni tudi skrb za ustrezno raven kibernetske varnosti.

Intelektualna lastnina

Intelektualna lastnina in *know-how* sta marsikdaj razlog za kibernetske napade na organizacije, saj zlasti v nejavni in neregistrirani obliki (predvsem *know-how* in avtorske pravice, kot je npr. programska koda) predstavljata bistveno konkurenčno prednost organizacij. Področje urejajo Zakon o avtorski in sorodnih pravicah (ZASP),[13] Zakon o industrijski lastnini (ZIL-1)[14] in mnogi mednarodnopravni akti in akti EU.

Osebni podatki

Hiter razvoj internetnih tehnologij, družbenih omrežij in medijev omogoča, da se osebni podatki posameznika izjemno hitro širijo. Zato so posledice vdora v zasebnost za posameznike lahko zelo hude. Podatkovna analiza in povezovanje raznovrstnih baz podatkov o posamezniku razkrivata informacije, ki se jih včasih ne zavedajo niti posamezniki sami.[15] Splošna uredba o varstvu podatkov (GDPR)[16] že v 5. členu določa, da se morajo osebni podatki obdelovati na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo z ustreznimi tehničnimi ali organizacijskimi ukrepi. Z vidika kibernetske varnosti sta pomembna tudi 24. in 25. člen, ki določata obveznost upravljavca, da izvaja ustrezne tehnične in organizacijske ukrepe ter zagotovi, da obdelava poteka v skladu z GDPR. V 32. členu GDPR predpisuje »ustrezne ukrepe« varnosti obdelave osebnih podatkov, ki je odvisna od tveganj, ki jih predstavlja obdelava. V praksi pa zagotavljanje šifriranja, zagotavljanje zaupnosti, celovitosti, dostopnosti in odpornosti sistemov in storitev ter zmožnost povrniti razpoložljivost tudi na osnovni ravni predstavljajo precejšen tehnološki izziv. Zagotavljanje odpornosti sistema in informacijske varnosti osebnih podatkov pred kibernetskimi napadi je dolžnost upravljavcev, ki jih lahko ob vdoru doleti globa v višini štirih procentov letnih globalnih prihodkov oziroma 20 milijonov evrov. Dodatno obveznost za upravljavce določata 33. in 34. člen, ki predpisujeta obveščanje nadzornega organa (in posameznikov), kar pomeni, da mora organizacija v primeru vdorov načrtovati in izvajati postopke obveščanja in dokumentirati vse kršitve varstva osebnih podatkov. Uporaba novih tehnologij je za ohranitev konkurenčnosti nujna, zato morajo organizacije izvajati tudi ocene učinkov v zvezi z varstvom podatkov (35. člen). Oblikovanje prakse glede ustreznih ukrepov je kontinuiran proces, ki je odvisen od tehnološkega razvoja. Tudi zato je GDPR napisan tehnološko nevtralno – ne določa, kateri tehnološki ukrep mora biti izveden. Trenutno sta v praksi najpogostejši oporni točki pri tehničnih ukrepih standarda ISO 27001 in 27002.[17] Zaradi hitrega razvoja kibernetskega prostora je problem standardov v tem, da težko sledijo vsem tehničnim novostim.

Kritična infrastruktura

Zakon o informacijski varnosti (ZInfV)[18] za zagotavljanje visoke ravni varnosti omrežij in informacijskih sistemov v vseh varnostnih razmerah določa merila za določitev različnih kategorij zavezancev (izvajalci bistvenih storitev, ponudniki digitalnih storitev, organi državne uprave) ter predpisuje ukrepe, ki jih morajo izpolnjevati. V praksi gre predvsem za vzpostavitev varnostno operativnih centrov. Zakon o kritični infrastrukturi (ZKI)[19] je bil sprejet za sistemsko ureditev neprekinjenega delovanja kritične infrastrukture energetike, prometa, prehrane, preskrbe s pitno vodo, zdravstva, financ, varovanja okolja ter informacijsko-komunikacijskih omrežij in sistemov.

Elektronske komunikacije in elektronsko poslovanje

Ti področji urejata Zakon o elektronskih komunikacijah (ZEKom-1)[20] in Zakon o elektronskem poslovanju na trgu (ZEPT).[21] Prvi določa pogoje za zagotavljanje elektronskih komunikacijskih omrežij in izvajanje elektronskih komunikacijskih storitev ter nadzor nad delom operaterjev, ki zagotavljajo delovanje komunikacijskih omrežij. Drugi določa način in obseg elektronskega poslovanja na trgu. Za kibernetsko varnost je pomembna ureditev odgovornosti ponudnikov storitev za podatke, ki jih posredujeta tako prejemnik kot ponudnik storitve.

Sektorske zakonodaje

Javni sektor in gospodarske panoge, kot so bančništvo, zavarovalništvo, zdravstvo, telekomunikacije in druge, urejajo področne zakonodaje z različnimi zahtevami po odpornosti sistemov in informacijski varnosti podatkov. Pri načrtovanju skladnosti poslovanja je pomembno upoštevati konkretne zahteve, temeljni tehničini in organizacijski ukrepi pa so zaradi vključenosti v kibernetski prostor skupni vsem.

Kriminalitetna politika

Kazenski zakonik (KZ-1)[22] v specialnem delu inkriminira naslednja kazniva dejanja: zloraba osebnih podatkov, napad na informacijski sistem, zloraba informacijskega sistema, izdelovanje in pridobivanje orožja in pripomočkov, namenjenih za kaznivo dejanje.

[7] <https://www.prnewswire.com/news-releases/class-action-lawsuit-filed-on-behalf-of-plaintiffs-whose-sensitive-personal-information-was-stolen-in-breach-of-marriott-servers-300758440.html>.

[8] <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>.

[9] Podobno usmeritev ima tudi GDPR v členu 32.

[10] Obseg prispevka ne dopušča podrobnejše analize, saj je potencialno uporabljivih pravnih virov zelo veliko; npr. v Sloveniji velja več kot 20.000 zakonov in podzakonskih predpisov. Poleg tega so tu še uredbe, direktive in drugi akti EU, sodna praksa in mednarodne konvencije.

[11] Ur. l. RS, št. 65/09 – UPB in nasl.

[12] V DZ je obravnavi predlog Zakona o poslovni skrivnosti (EPA: 368-VIII), ki bo pojme opredelil drugače.

[13] Ur. l. RS, št. 16/07 – UPB in nasl.

[14] Ur. l. RS, št. 51/06 – UPB in nasl.

[15] **Hildebrandt, M.**, in **Gutwirth, S.**: Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer, New York, 2008.

[16] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), UL L 119 z dne 4. maja 2016.

[17] <https://www.iso.org/isoiec-27001-information-security.html>.

[18] Ur. l. RS, št. 30/18.

[19] Ur. l. RS, št. 75/17.

[20] Ur. l. RS, št. 109/12 in nasl.

[21] Ur. l. RS, št. 96/09 – UPB in nasl,

[22] Ur. l. RS, št. 50/12 – UPB in nasl.

Sklep

Finančne in pravne posledice zaradi nezadostne skrbnosti pri zagotavljanju kibernetske varnosti so zaradi tehnološkega napredka vsak dan večje in se merijo v milijonih ali celo milijardah. Vdori in njihove posledice so kljub naporom specializiranih IT-oddelkov in strokovnjakov s področja kibernetske varnosti neizogibno dejstvo. Pravniki morajo organizacijam pojasniti tveganja in obveznosti, ki jim jih nalaga zakonodaja, ter svetovati, katere tehnološke in organizacijske ukrepe naj sprejmejo, da bodo ravnale z zadostno skrbnostjo. Le z ustreznim sodelovanjem tehnoloških in pravnih strokovnjakov lahko organizacije obvladujejo tveganja zaradi motenega delovanja svojih informacijskih sistemov ali posega v zaupnost, celovitost in razpoložljivost svojih podatkov, kot so poslovne skrivnosti, intelektualna lastnina in osebni podatki.