V prvem delu prispevka[1] sva predstavila ključna pravna vprašanja o zagotavljanju kibernetske varnosti in podala kratek pregled zakonodaje. V drugem delu pa na namišljenem primeru vdora obravnavava ukrepe za zagotavljanje kibernetske varnosti in pojasnjujeva, zakaj mora pri njihovi implementaciji, delovanju in odpravljanju posledic sodelovati ustrezno podučen pravnik.

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

Pravni vidiki kibernetske varnosti (2. del)

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

Primer vdora in posledic

Dežurni informatik (namišljene)[2] bolnišnice v nedeljo pri kosilu prejme klic zdravnika, ki ne more odpreti elektronske kartoteke tujega, premeščenega pacienta. Kot vedno v takšnih primerih se na daljavo poveže na informacijski sistem klinike in začne reševati problem. Hitro ugotovi, da sistem ne dovoli odpiranja datoteke, saj protivirusni program javlja grožnjo. Ker mu je zdravnik po telefonu omenil, da gre za pacienta iz tuje bolnice in ker ima datoteka podobno končnico kot njihove e-kartoteke, informatik izklopi protivirusni program in datoteko z omogočenimi makri odpre na svojem računalniku. Izpis je sicer drugačen od tistih, ki jih pozna, vendar verjame, da si bo zdravnik lahko pomagal z njim, zato datoteko shrani na strežnik bolnišnice in zdravniku pošlje sporočilo, da je rešil problem. Rutinsko preveri še parametre delovanja informacijskega sistema bolnišnice in prekine oddaljeno povezavo.

Zgodaj zjutraj prejme klic vodje informacijske tehnologije (IT), naj nujno takoj pride v službo. Po prihodu brž opazi, da so sprejemne ambulante prazne. Sliši zgolj medicinsko sestro, kako teka po oddelku z neurejenim šopom papirjev v roki in daje navodila: »Računalniki ne delujejo, zato zavračamo vse paciente. Na papir si zapišite vse podatke pacientov, ki se jih spomnite.« Obenem v bolnišnico pripelje rešilni avtomobil. Varnostnik ga že na vhodu preusmeri v drugo bolnišnico. V vsem tem kaosu informatiku pogled uide na velik zaslon, namenjen obveščanju pacientov. Na zaslonu je obvestilo: »Imate 24 ur časa, da nakažete 500 bitcoinov na: 1aa5cmQmvTq8YQTEqcTmW7dfBNuFwgdDG.«

Oddelek IT se sestane z vodstvom bolnišnice. Direktor nemirno postopa po pisarni in mrmra, da se ne bo pustil izsiljevati, vodja informatike mu zagotavlja, da bodo problem rešili z obnovitvijo sistema s kopij (backup) iz oddaljenih shramb podatkov. Oddelek po navodilih direktorja začne s postopki obnove sistema. Kmalu ugotovijo, da so tudi podatki obeh varnostnih kopij kriptirani (zaklenjeni s šifro). Vodja informatike takoj pokliče kolege, ki se ukvarjajo s kibernetsko varnostjo. Svetujejo mu, naj poskusijo s specializiranim protivirusnim programom. Kljub vsemu trudu in plačilu precej visokega zneska za namestitev programa tudi ta poskus ni uspešen. Ob poteku 24-urnega roka se obvestilo na zaslonu spremeni. Prikaže se povezava na spletno stran *place-direktorja.onion* in napis: »Če v 24 urah ne nakažete 500 bitcoinov, bomo objavili vse podatke.« Ko preverijo spletni naslov z grozo ugotovijo, da so na strani objavljeni vsi dohodninski podatki direktorja. Informatiki se kljub temu ne vdajo in poskusijo z uporabo še enega programa ter uspejo delno povrniti dostop do e-kartotek in informacijskega sistema. Ko poteče dodaten rok, se ne zgodi nič, zato menijo, da so bili njihovi napori uspešni.

Čez dobro uro jih pokliče vodja službe za odnose z javnostjo, ki pove, da so se v medijih pojavili naslovi, kot so: »Kje je predsednik vlade dobil sifilis?« Ker mediji ne objavijo vira, piarovci zanikajo, da so podatki prišli od njih. Direktor zaradi objav izgubi zaupanje v svoje informatike in angažira tuje strokovnjake za informacijsko tehnologijo. Ti zagotovijo, da bodo v treh dneh vzpostavili delovanje sistema. V trenutku, ko tuji informatiki vkorakajo v bolnišnico, začnejo ena za drugo ugašati najnovejše medicinske naprave, ki so povezane v splet. Osebje začne z rešilnimi avtomobili kritične bolnike takoj pošiljati v druge bolnišnice. Kljub upoštevanju triažnih pravil in izjemni odzivnosti medicinskega osebja dva pacienta umreta.

Bolnišnico kmalu obiščejo kriminalisti in nadzorni organi. Revizija, ki jo izvedejo skupaj z varnostnimi strokovnjaki, pokaže, da se je zgodil kibernetski vdor s krajo podatkov (ang. *phishing*)[3] in izsiljevalskim programom (ang. *ransomware*).[4] Elektronska pošta, ki jo je prejel informatik, je bila v resnici poslana z računalnika hekerja, ki se je izdajal, da je zdravnik, zaradi česar je informatik na svojem računalniku z administratorskimi pravicami zagnal okuženo datoteko in jo na koncu odložil na strežniku. Heker je s tem pridobil kontrolo nad vsemi informacijskimi sistemi bolnišnice, hkrati pa se je zaradi odložene datoteke po sistemu razširil virus, ki je kriptiral (zaklenil) vse datoteke. Ob odpiranju kartoteke »tujega pacienta« je prišlo do vdora izsiljevalske kode,[5] ki je zaklenila vse podatke bolnišnice, hkrati pa hekerju omogočila dostop do repozitorija administratorskih gesel, ki so omogočala neomejeni dostop do vseh sistemov bolnišnice. Kriminalistom hekerja ni uspelo izslediti. Nadzorni organi hitro ugotovijo, da je bila bolnišnica kljub sodobnemu informacijskemu sistemu organizacijsko povsem nepripravljena za odziv na kompleksen kibernetski napad. Zaradi neustreznih organizacijskih in tehničnih ukrepov ter neobveščanja pristojnih organov je prišlo do javne objave zdravstvenih podatkov mnogih pacientov bolnišnice. Zaradi kršitev dolžnosti in hudega posega v zasebnost pacientov je bolnišnici izrečena visoka globa. Mnogi pacienti se odločijo za vložitev odškodninskih zahtevkov zoper bolnišnico. Zaradi enormnega povečanja izdatkov za plačilo glob in odškodnin

[1] **Planinšek, J.**, in **Skok, T.**: Pravni vidiki kibernetske varnosti (1. del), PP, št. 7/2019, str. 16–18.

[2] Primer je sicer izmišljen, a temelji na mnogih podobnih napadih, ki so že ohromili delovanje bolnišnic. Glej npr.: <https://www.scmagazine.com/home/security-news/cyberattack-forces-health-sciences-north-to-place-systems-on-downtime-at-24-hospitals/>

[3] Vsem oblikam kibernetskega napada s t. i. »phishingom« je skupno, da se kraja podatkov izvede s prevaro hekerja, ki se predstavlja preko na prvi pogled preverjene in varne povezave. Izraz *phishing*, ki zaenkrat nima slovenske ustreznice, omenja tudi slovenski nacionalni odzivni center za kibernetsko varnost SI-CERT, <https://www.cert.si/si/varnostne-groznje/phishing/>.

[4] Gre za zlonamerno programsko kodo (ang. *malware*), ki prevzame nadzor nad računalnikom ali podobno napravo in onemogoči dostop do shranjenih podatkov. Podprta z grožnjami snovalca je namenjena izsiljevanju. <https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html>.

[5] Izsiljevalski program je vrsta zlonamerne programske opreme, ki grozi, da bo objavila podatke o žrtvi vdora ali za vedno onemogočila dostop do podatkov, če žrtev ne bo plačala odkupnine.

oškodovanim bolnišnica zaide v rdeče številke in konča v stečaju, saj ni imela sklenjenega zavarovanja za primer kibernetskega napada.

Navedeni primer je seveda ekstremen. Predstavlja zgolj enega od neskončnih možnih scenarijev, ki so se že zgodili[6] ali se šele bodo. Zato se morajo organizacije na kibernetske napade ustrezno pripraviti s tehničnimi in organizacijskimi ukrepi.

Ukrepi zagotavljanja kibernetske varnosti

Na prvi pogled se zdi, da bi se bilo zgoraj navedenemu primeru kibernetskega napada zelo težko izogniti. Kaj torej lahko storijo organizacije in katere pravne vidike je pri tem treba upoštevati?

Osnovni ukrepi zagotavljanja kibernetske varnosti so predvsem:

- uporaba močnih gesel in politika upravljanja z gesli,
- nadzor dostopov do podatkov in aplikacij (uporabniške pravice), nadzor prenosa podatkov ter dostopa do informacijske opreme (dostop do prostorov),
- požarni zidovi (*firewalls*) in protivirusni programi (*security software*),
- redno posodabljanje programov.

Ti osnovni ukrepi[7] so običajno določeni v obliki pravilnikov in se praviloma izvajajo izključno s strani službe za IT. Pravniki so običajno vključeni v sestavo internih pravil organizacij in pomembni pri pregledu licenčnih in storitvenih pogodb, vezanih na naročilo in nabavo programske in strojne opreme.

V praksi se je pokazalo, da kombinacija organizacijskih in tehničnih ukrepov ne zagotavlja več ustrezne kibernetske varnosti. Velikost in kompleksnost informacijskih sistemov organizacij se je namreč tako povečala, da zagotavljanje varnosti ne more temeljiti na premisi, da bomo lahko napadalce zadržali izven sistema. Ukrepi so bili zadostni, ko organizacije niso uporabljale nešteto aplikacij, oblačnih storitev in zaposlenim preko interneta niso omogočale oddaljenega dostop do podatkov in aplikacij – npr. dostop do elektronske pošte z mobilnimi telefoni in uporaba drugih tehnik, ki omogočajo delo na daljavo.

Treba je sprejeti dejstvo, da absolutne varnosti ni in da morajo ukrepi temeljiti na premisi, da je heker že uspel vdreti v sistem (kot v zgoraj opisanem primeru vdora v bolnišnico). Pri tem opozarjava, da je praktično nešteto načinov, kako lahko heker vdre v informacijski sistem.

Novo premiso kibernetske varnosti, da absolutne varnosti ni**,** potrjujejo tudi novejši zakonodajni akti.[8] Tako so predpisane zahteve po ukrepih, kot so:

- določanje bistvenih storitev in sistemov,
- postopki rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov (za zagotavljanje varnosti obdelave),
- vzdrževanje dokumentarnega sistema upravljanja varovanja informacij ter sistem upravljanja neprekinjenega poslovanja (analiza tveganj, politika neprekinjenega poslovanja, popis bistvenih elementov sistema, načrt obnovitve, načrt odzivanja na incidente in ponovne vzpostavitve delovanja sistema, obveščanje regulatorjev),
- načrt ukrepov za zagotavljanje celovitosti, zaupnosti in razpoložljivosti omrežja in informacijskih sistemov, ki upoštevajo podrobnosti in posebnosti sistema,
- omogočanje poznejšega ugotavljanja, kdaj so bili podatki preneseni, uporabljeni ali drugače obdelani in kdo je to storil (revizijska sled),
- izvajanje ocen učinkov in posvetovanje z regulatorji glede implementacije novih ukrepov.

Zakonodajalec poleg sprejetja osnovnih ukrepov predpisuje tudi aktivno spremljanje delovanja sistema, ozaveščanje uporabnikov in zbiranje podatkov o vdorih (incidentih) ter njihovo analizo. V zgoraj opisanem primeru bi ustrezno implementiran sistem bolnišnice (Varnostno operativni center) zaznal nenavadno aktivnost (kriptiranje podatkov pacientov), zato bi se služba za IT lahko pravočasno odzvala in preprečila najhujše posledice.

Vzpostavitev modernih varnostno operativnih centrov zahteva tudi aktivno sodelovanje pravnikov, zlasti pri:

- definiranju zahtev, ki so odvisne od konkretne organizacije. Če organizacijo (npr. zavarovalnico) zavezujejo specialni predpisi, morajo biti ustrezno definirane tudi storitve, potrebne za zagotavljanje ustrezne stopnje kibernetske varnosti. V praksi se konkretne zahteve in odgovornosti ponudnikov določijo v dodatkih k storitvenim pogodbam (ang. *service-level agreements*),
- spremljanju delovanja sistema in ozaveščanju uporabnikov, ki se izvaja v obliki rednih pregledov in revizij ter izvedbi ustreznih izobraževanj uporabnikov;
- načrtovanju sistemov – GDPR npr. v členu 35 zahteva izvedbo ocen učinkov in v nekaterih primerih tudi posvet z regulatorji,
- pripravi načrtov odziva na incidente in pri samih odzivih – v zgornjem primeru je bila bolnišnica na incident nepripravljena, zato ni pravočasno obvestila pristojnih institucij in posameznikov, kar bi zmanjšalo posledice vdora,[9]
- obvladovanju tveganj – predvsem načrtovanju tehničnih in organizacijskih tveganj ter pri odločanju, kakšno zavarovanje naj organizacija sklene za potencialno škodo, ki lahko nastane kljub sprejetim ukrepom.

Kibernetska zavarovanja

Kibernetski vdori so postali eno največjih poslovnih tveganj.[10] Glede na to, da tehnični in organizacijski ukrepi ne morejo zagotoviti absolutne varnosti, je eden od načinov obvladovanja tveganj tudi sklenitev kibernetskega zavarovanja. Vloga pravnikov je, da upravi pojasnijo, kakšne vrste odgovornosti (škode) lahko nastanejo organizaciji, in skrbno preverijo, ali zavarovalne police, vključno s splošnimi pogoji ponujenih zavarovanj, krijejo predvidljiva tveganja in potencialno škodo.

Kibernetska zavarovanja običajno nudijo:

- odziv na incident ter ponovno vzpostavitev delovanja sistema – npr. v obliki povrnitve stroškov zunanjih strokovnjakov in nove programske ter strojne opreme,
- kritje odgovornosti za kršitve zaupnosti in zasebnosti v primeru vloženih odškodninskih zahtevkov tretjih oseb in glob nadzornih organov,
- kritje odgovornosti za omrežno varnost v primeru odškodninskih zahtevkov tretjih oseb,
- odpravo posledic obratovalnega zastoja s prekinitvijo poslovanja,
- kritje nezakonitega odvzema sredstev s kibernetskim izsiljevanjem (*ransomware*, kot v zgornjem primeru) in drugimi oblikami kibernetskega kriminala.

[6] Zdravstvene ustanove se vse pogosteje znajdejo med žrtvami kibernetskih napadov, glej npr.: <https://healthitsecurity.com/news/united-hospital-district-reports-june-2018-breach-from-phishing-attack>.

[7] Več o osnovnih ukrepih: <https://www.nibusinessinfo.co.uk/content/common-cyber-security-measures>.

[8] Predvsem npr. GDPR (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; GDPR), UL L 119 z dne 4. maja 2016, ZInfV (Ur. l. RS, št. 30/18) in ZKI (Ur. l. RS, št. 75/17).

[9] Predvsem za »kritično infrastrukturo« že zakonodajalec predpisuje pripravo dokumentarnega sistema upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja.

[10] Po podatkih študije 2017 *Global Risk Management Survey*, ki jo je pripravila zavarovalnica Aon, se kibernetski napadi uvrščajo med deset največjih tveganj, kjer na lestvici zasedajo 5. mesto. Povzetek dostopen na: <https://www.visualcapitalist.com/the-changing-landscape-of-business-risk/>.

Glede na potrebe zavarovanca so možne ustrezne prilagoditve. Pri tem je bistveno, da razumemo odnos kibernetskega zavarovanja do drugih (običajno že sklenjenih) zavarovanj, kot je npr. zavarovanje odgovornosti. Pri sklepanju zavarovanj bodo zavarovalnice zanimali predvsem splošni podatki o zavarovancu (dejavnost, promet, število zaposlenih), podatkovna struktura informacijskega sistema (velikost, količina in vrsta podatkov, lastnosti pogodbene obdelave podatkov), podatki o ukrepih zagotavljanja omrežne in podatkovne varnosti (obstoj pooblaščene osebe za varstvo osebnih podatkov, spoštovanje minimalnih varnostnih standardov), podatki o potrebnem zavarovanju nevarnosti in potrebnem zavarovalnem kritju (zavarovalna vsota, odbitna franšiza, želene oblike kritij). Na podlagi zbranih podatkov o zavarovancu, vključno z vpogledom v zavarovalno zgodovino, zavarovalnica ponudi ustrezno kritje zavarovanja škodnega primera. Naloga pravnikov je, da podajo mnenje, ali so konkretna kritja ustrezna glede na zahteve zakonodaje, že sklenjena zavarovanja ter organizacijske in tehnične ukrepe, ki jih je že implementirala organizacija.

Sklep

V prispevku sva predstavila ključne ukrepe za zagotavljanje kibernetske varnosti v obliki organizacijskih in tehničnih ukrepov. Gre za ukrepe, ki jih običajno izvaja specializiran oddelek za IT, ki mora pri implementaciji in izvajanju ukrepov sodelovati tudi s pravniki. Sodelovanje je ključnega pomena, zlasti za zagotovitev pravilnega spremljanja delovanja sistema, osveščanje uporabnikov o nevarnostih in pripravi načrtov ravnanj ob vdorih. Sodelovanje pravnikov je zelo pomembno tudi pri sklepanju kibernetskih zavarovanj, ki morajo kriti predvidljiva tveganja (globe in različne oblike škode), ob upoštevanju realnosti, da absolutne varnosti pred kibernetskimi vdori ni.