poročilo

INFORMATIKA V JAVNI UPRAVI 2016

Konferenca Informatika v javni upravi je potekala 5. in 6. decembra 2016 v Kongresnem centru Brdo pri Kranju. Rdeča nit konference je bila Digitalna preobrazba javne uprave – GaaS.

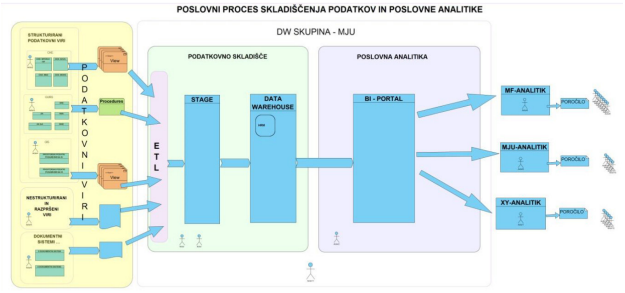
Konferenca je postala že tradicionalna in je priložnost za predstavitev primerov dobre prakse v javni upravi. Pomembno sporočilo konference je, da je informatizacija javne uprave ključna za celotno državo, ne le za javno upravo. Javna uprava kot informacijski sistem razpolaga z velikim bogastvom podatkov in tisti podatki, ki so javno dostopni, lahko zainteresiranim omogočijo razvoj novih storitev, s tem pa tudi poslovni zagon in konkurenčno prednost.

Soočanje z najpogostejšimi ranljivostmi spletnih aplikacij državnih organov

Anže Mihelič in Simon Vrhovec s Fakultete za varnostne vede Univerze v Mariboru sta v svojem prispevku predstavila identificiranje in analiziranje varnostnih tveganj, ki so jim izpostavljene spletne aplikacije državnih organov. Pri tem sta se osredotočila na najbolj kritične ranljivosti, kot so vrivanje SQL, nedelujoče upravljanje avtentikacije in sej ter napad XSS. Zaradi visoke občutljivosti podatkov, ki se shranjujejo in pretakajo po kanalih spletnih aplikacij državnih organov, javnost pričakuje zagotavljanje visoke stopnje varnosti pri komunikaciji ter pri hrambi in obdelavi osebnih in drugih podatkov, kar v splošnem razumemo kot varovanje sredstev informacijskega sistema in zagotavljanje nadzora nad dostopom do informacij. Med najpogostejša varnostna tveganja, ki so jim izpostavljene vse spletne aplikacije, med drugim tudi aplikacije državnih organov, spadata vrivanje SQL in napad XSS. Omenjeni ranljivosti sta izbrani predvsem zaradi pogostosti in preprostosti zaznavanja. V povprečju je omenjenim tveganjem izpostavljenih kar 81,6 odstotkov digitaliziranih javnih uprav vseh analiziranih držav. V Evropi je ta delež nekoliko višji, saj znaša 90 odstotkov. Vrivanje SQL (angl. *SQL injection*) je napad na spletno aplikacijo in zbirko podatkov, pri katerem napadalec med podatke, ki jih aplikaciji posreduje uporabnik, vrine del poizvedbe (angl. *SQL query*) in s tem spremeni osnovno delovanje ukaza. Napad je možno izvesti pri aplikacijah, ki ne preverjajo vhodnih podatkov, temveč jih neposredno prenesejo v dinamične poizvedbe. Napad XSS (angl. *Cross-Site Scripting*) je napad na spletno aplikacijo, pri katerem napadalec v aplikacijo vstavi ukaze JavaScript, ki se izvedejo v brskalniku uporabnika. Gre za spreminjanje spletne aplikacije, tako da ob obisku strani spletni brskalnik obdela vstavljeno zlonamerno programsko kodo kot del spletne strani. Z napadom XSS lahko napadalci spreminjajo in poneverjajo podatke spletne strani ter pridobijo najrazličnejše podatke – od osebnih podatkov do podatkov o kreditnih karticah. (Mihelič in Vrhovec, 2016)

Izzivi pri vzpostavitvi sistema podatkovnega skladišča in poslovne analitike v državni upravi

Predavatelji so bili Aleš Veršič in Karmen Kern Pipan z Direktorata za informatiko ter Samo Dečman iz podjetja 3 GEN, d. o. o. Ugotavljajo, da slovenska javna uprava na področju razvoja poslovne analitike, podatkovnih skladišč in masovnih podatkov ne izkorišča vseh potencialov, ki jih ponuja digitalni način poslovanja, in to tako v smislu povečevanja učinkovitosti poslovanja kot tudi boljšega prilagajanja uporabnikom. Na Ministrstvu za javno upravo so začeli projekt za vzpostavitev skladišča podatkov in sistema poslovne analitike, ki bosta v naslednjih letih na voljo kot horizontalna storitev na državnem računalniškem oblaku (DRO) za organe državne uprave. Poseben izziv predstavljata tudi anonimizacija osebnih podatkov pri prenosu v podatkovno skladišče in njihova uporaba v poslovni analitiki. Odpira se veliko vprašanj glede lastništva podatkov ter varstva osebnih podatkov in podatkovnega vira, ki bi bil lahko uporaben za vse uporabnike sistema. Tak primer je lahko register prostorskih enot, v katerem so med drugim naslovi in seznam občin. Pomembno vprašanje je vprašanje odgovornosti pri zagotavljanju delovanja podatkovnega toka. Treba bo dovolj jasno opredeliti matriko odgovornosti za posamezno aktivnost v procesu.



Slika 1: Predvidena shema za poslovni proces skladiščenja podatkov in poslovne analitike (Vir: Veršič, et al., 2016)

Poseben izziv predstavljata tudi anonimizacija osebnih podatkov pri prenosu v podatkovno skladišče in njihova uporaba v poslovni analitiki. Vsako zbiranje podatkov mora biti predhodno utemeljeno z nekim namenom in ciljem. Iz obojega namreč izhaja nabor podatkov, ki je potreben za dosego cilja. Povedano drugače, zbiranja podatkov na zalogo ne sme biti, temveč mora biti nabor podatkov najmanjši možen, ki še zadošča za dosego cilja. Ob upoštevanju te smernice je v mnogih letih v državni upravi nastala množica podatkovnih zbirk. Vsaka namenska podatkovna zbirka spada pod okrilje natanko ene inštitucije, ki se v tem kontekstu imenuje upravljalec podatkovne zbirke. Medtem ko je vsebina podatkovne zbirke unikatna za neki namen, tega ne moremo trditi za podatke, saj je lahko neki podatek istočasno v več podatkovnih zbirkah. Govorimo o neke vrste preseku podatkov oziroma skupnem imenovalcu, na podlagi katerega je mogoče določene podatkovne zbirke povezati, kar je dober temelj za izgradnjo centralnega podatkovnega skladišča, ki bi služilo kot vir za različne statistične analize večine državnih inštitucij in za nova znanja, ki bi bila pridobljena z uporabo naprednih orodij za analizo vzorcev pri podatkih. Anonimizacija ne sme ogroziti namena centralnega podatkovnega skladišča. To pomeni, da nekateri deli podatkovne zbirke ne bodo anonimizirani ali pa ne bodo anonimizirani v celoti. Takšne segmente bodo dodatno zaščitili z revizijsko sledjo. (Veršič, A., et al., 2016a)

Projekt E-občina in informatizacija javne uprave

Dare Korać iz podjetja Sigmateh je predstavil projekt E-občina in informatizacija javne uprave. Meni, da v sodobnem svetu informacijske tehnologije spletno poslovanje ne predstavlja več poslovne prednosti, temveč pričakovano funkcionalnost. E-poslovanje z državo je del našega vsakdana. Tudi občine morajo svojim občanom ponuditi dostopnost lastnih storitev na spletu. Občani ob obisku spletne strani pričakujejo e-vloge in tudi spletno plačevanje taks. Če občina navedenih storitev ne ponuja, so pripombe občanov vedno bolj neposredne in vedno jasneje izražene. Informatizacija poslovanja slovenskih občin je bila v primerjavi z drugimi področji v preteklih letih v precejšnjem zaostanku, saj je še pred tremi leti na svetovnem spletu e-vloge s spletnim plačevanjem taks ponujalo le sedem od 212 občin. Še pred dobrima dvema letoma je le okoli 17 % občin ob prenovi občinske spletne strani od izvajalca zahtevalo tudi uvedbo elektronskih vlog in spletnega plačevanja taks. Danes sta zahteva po uvedbi e-vlog in spletno plačevanje taks ob prenovi občinskih spletnih strani že praksa, saj e-poslovanje zahteva že nekaj več kot polovica občin. Projekt E-občina je nastal kot pilotni projekt uvajanja elektronskih vlog v slovenske občine. Sprva so se v okviru tega projekta osredotočili na razvoj centralnega portala za vse slovenske občine; na tem portalu bi občine imele možnost objaviti lastne elektronske vloge. Portal je bil ločen od občinskih spletnih strani, občine pa so na svoji spletni strani objavile le povezavo do vlog na portalu E-občina. Omogočeni so bili odprtje vloge v formatu word ali pdf, oddaja e-vlog (z digitalnim certifikatom ali brez njega) in spletno plačevanje taks (plačilne kartice, Moneta, spletna banka). Predvidevali so, da se bo v dveh letih v portal vključilo vsaj trideset občin, vendar je bilo zanimanje za to rešitev precej manjše od pričakovanj. Želje, potrebe in zahteve občin so bile usmerjene v razvoj spletnih strani, ki omogočajo vse navedene funkcionalnosti na enem mestu, saj so bili občani ob preusmeritvi na drugo spletno stran zmedeni in nezaupljivi ter so spletno stran dokaj hitro zapustili. Razvoj portala se je leta 2014 usmeril v izdelavo spletnih strani za občine z vključenim celovitim e-poslovanjem in komuniciranjem občine z občani (projekt E-občina 2.0). E-občina 2.0 predstavlja novo generacijo poslovanja slovenskih občin, saj občine z aktivacijo nove spletne strani v eni informacijski rešitvi zagotovijo komuniciranje občine z občani po več kanalih in celovito dostopnost storitev občine na svetovnem spletu. Omogočajo e-vloge s spletnim plačilom takse, vprašanja občanov in odgovore občine, anonimne predloge in pobude ter deljenje objav z občinske spletne strani na družbenih omrežjih. Tudi komunikacija med občino in občani ter obveščanje občanov potekata po več kanalih: z objavo novic na spletni strani, deljenjem vsebine spletne strani na družbenih omrežjih ter pošiljanjem SMS-obvestil in e-sporočil (na katera se občani naročijo sami). E-storitve so občanom dostopne na vseh napravah in ne zahtevajo posebne naprave, namestitve ali drugih prilagoditev.

Prednosti e-poslovanja v primerjavi s konvencionalnim poslovanjem so predvsem naslednje:

- manj dela s sprejemanjem vlog v glavni pisarni;
- manj dela z dopolnitvami vlog zaradi popolnejših podatkov ob oddaji vloge;
- učinkovitejše obveščanje občanov o poslovanju lokalne samouprave (občan na spletni strani izbere kategorije obvestil, ki jih želi prejemati);
- vključevanje občanov, društev in javnih zavodov pri

objavljanju dogodkov in spodbujanju lokalnega utripa;
- nižje takse za občane v primeru oddaje e-vloge, ki je podpisana z digitalnim certifikatom.

Nenehen razvoj poslovanja in odlično poznavanje poslovanja občin predstavljata osnovno gonilo razvoja in rasti. E-občina že nekaj let presega funkcionalnosti klasičnih spletnih strani, nenehen razvoj portala pa zagotavlja širitev funkcionalnosti na sorodna področja. Predlogi in želje občin so začrtali razvoj projekta E-občina 3.0, ki je že v razvoju in bo zaživel predvidoma v letu 2017. Obstoječe funkcionalnosti bodo še nadgrajene, saj je predvideno, da se bo poslovanje razširilo na javne zavode in društva v občini ter turistično ponudbo občin. Spletna stran občine bo predstavljala centralno spletno točko v občini – tako na področju e-poslovanja kot tudi na področju družbenega življenja. (Korać, 2016)

Kibernetska varnost v praksi

Franci Mulec in Franc Močilnar z Ministrstva za zunanje zadeve ter Samo Maček z Generalnega sekretariata Vlade RS so predstavili kibernetsko varnost v praksi. Ugotavljajo, da število varnostnih incidentov in njihova kompleksnost v zadnjih letih vztrajno rasteta. Kibernetska varnost je postala sestavni del nacionalne varnosti držav in mednarodne skupnosti. V svojem prispevku so predstavili zbirko orodij, politik, konceptov, zaščitnih ukrepov, smernic in pristopov, s katerimi lahko ta tveganja obvladujemo. Obravnavali so tudi usmeritve in ukrepe na področju kibernetske varnosti ter izpostavili konkretna tveganja in zaščitne ukrepe pri obravnavanju elektronskih dokumentov. Odmevna razkritja zaupnih dokumentov v zadnjih letih so spremenila dojemanje groženj, ki smo jim izpostavljeni pri uporabi informacijsko-komunikacijske tehnologije. Struktura virov tveganja se širi z interesnih skupin posameznikov na geostrateški nivo; vse bolj je povezana z interesi, ki izhajajo iz globalizacije in širših družbenih sprememb. Poglavitni viri kibernetskih groženj so hektivizem, interesi nacionalnih držav in organizirani kriminal. Z odkritjem črva Stuxnet je postalo jasno, da lahko kibernetske grožnje presežejo meje virtualne sfere in imajo uničujoče posledice v realnem svetu. Razvili so zlonamerna orodja, usmerjena v infrastrukturo in namenjena vohunjenju. Dodelanost navedenih orodij ponazarja dejstvo, da jih pogosto odkrijejo, ko so že zelo razširjena in je njihov namen v veliki meri že dosežen. Evropska unija in Slovenija sta aktivno pristopili h krepitvi kibernetske varnosti in zagotavljanju nemotenega delovanja informacijsko-komunikacijskih sistemov, od katerih je odvisno delovanje celotne družbe. Evropska agenda za varnost kot varnostno grožnjo izpostavlja kibernetski kriminal ter njegovo povezanost s terorizmom in organiziranim kriminalom. V nadaljevanju bodo predstavljene nekatere aktivnosti evropskih institucij in naše države na področju obvladovanja navedenih varnostnih groženj. Leta 2013 je Evropska komisija objavila strategijo za kibernetsko varnost Evropske unije z naslovom "Odprt, varen in zavarovan kibernetski prostor" (An Open, Safe and Secure Cyberspace; https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security) ter predlog direktive o varnosti omrežij in informacij (Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security accross the Union; https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security). Strategija predstavlja celostno vizijo EU, kako najučinkoviteje preprečiti kibernetske motnje in napade. Direktiva je ključni del splošne strategije, na podlagi katere bi morale države članice, ponudniki interneta in upravljavci kritične infrastrukture (kot so platforme za e-trgovanje, družabna omrežja) ter upravljavci na področju energije, prevoza, bančništva in zdravstvenih storitev zagotoviti varno in zaupanja vredno digitalno okolje v celotni Evropski uniji.

Direktiva določa naslednje ukrepe:

- države članice morajo sprejeti strategijo za varnost omrežij in informacij ter določiti nacionalni organ, ki bo pristojen za varnost omrežij in informacij ter bo imel ustrezne finančne in človeške vire;
- vzpostaviti je treba sistem sodelovanja med državami članicami in sistem s Komisijo za pošiljanje zgodnjih opozoril o tveganjih in zapletih prek varne infrastrukture ter za sodelovanje in organizacijo rednih medsebojnih strokovnih pregledov;
- upravljavci kritičnih infrastruktur v nekaterih sektorjih (finančne storitve, prevoz, energetika, zdravstvo), ponudniki storitev informacijske družbe (zlasti trgovine z aplikacijami, platforme za e-trgovanje, internetna plačila, računalništvo v oblaku, iskalniki, družabna omrežja) in javne uprave morajo prilagoditi postopke za obvladovanje tveganj in poročati o večjih zapletih glede varnosti svojih temeljnih storitev.

Usmeritvam EU na področju zagotavljanja kibernetske varnosti sledi tudi Slovenija. Ustanovljen bo nacionalni organ za kibernetsko varnost. Pri udejanjanju ciljev bosta ključna dejavnika tudi vloga in usklajeno delovanje drugih državnih organov, telekomunikacijskih operaterjev ter številnih organizacij, združenj, gospodarskih subjektov in tujih partnerjev.

Izhodišče za opredeljevanje kriterijev predstavljajo posledice, ki bi jih imelo nedelovanje za državo, gospodarstvo

in nekatere druge dejavnosti. Osnovni kriteriji obsegajo kritično infrastrukturo, ki zaradi nedelovanja:

- povzroči ali ima za posledico smrt več kot 50 oseb;
- pomembno vpliva na zdravje prebivalstva, in to v takšni meri, da je treba hospitalizirati več kot 100 oseb za več kot teden dni;
- vpliva na izvajanje gospodarske ali druge dejavnosti v obsegu povzročene škode ali izpada dohodka več deset milijonov evrov na dan;
- vpliva na prekinitev preskrbe s pitno vodo ali hrano za več kot teden dni za preko 100.000 prebivalcev;
- vpliva na prekinitev preskrbe z električno energijo za tri dni ali z zemeljskim plinom za več kot teden dni za preko 100.000 prebivalcev;
- vpliva na izpad oskrbe z naftnimi derivati za več kot teden dni za preko 100.000 prebivalcev.

Glede na prioritete delovanja oziroma neposreden vpliv na delovanje drugih sektorjev je kritična infrastruktura razvrščena po naslednjem prioritetnem vrstnem redu:

- zagotavljanje električne energije,
- informacijsko-komunikacijska podpora,
- preskrba s pitno vodo,
- preskrba s hrano,
- zagotavljanje zdravstvene oskrbe,
- preskrba z naftnimi derivati,
- zagotavljanje železniškega prometa,
- zagotavljanje letalskega prometa,
- delovanje pristaniške dejavnosti,
- preskrba s plinom,
- delovanje plačilnega prometa,
- zagotavljanje oskrbe z gotovino,
- delovanje državnega proračuna in
- varovanje zdravega okolja.

V vladnih informacijskih sistemih in na področju zunanjih zadev je bilo tveganje obravnavano glede na posledice razkritja podatkov ali težav v delovanju sistemov. V nadaljevanju so bili v središču zanimanja predvsem ukrepi varovanja na dveh nivojih varnosti:

- srednji nivo varnosti (angl. *medium level security*) – podatki brez določene stopnje tajnosti in stopnja INTERNO; njihovo razkritje bi lahko škodovalo delovanju ali izvajanju nalog organa;
- visoka stopnja varnosti (angl. *high level security*) – obravnavanje tajnih podatkov višjih stopenj; njihovo razkritje bi lahko škodovalo varnosti ali interesom države.

Primer referenčnega okvira je dokument The CIS Critical Security Controls for Effective Cyber Defense Version 6.0. Osnovni dokument opisuje 20 kontrol. Poleg tega je na voljo tudi metrika za opisane kontrole. Gre za naslednje kontrole, od katerih naj bi s prvimi petimi kontrolami dosegli največji učinek z najmanjšimi stroški:

- popis pooblaščenih in nepooblaščenih naprav v omrežju;
- popis dovoljene in nedovoljene programske opreme v sistemu;
- vzpostavitev in upravljanje varnih konfiguracij strojne in programske opreme na mobilnih napravah, prenosnikih, delovnih postajah, strežnikih;
- stalno spremljanje in ugotavljanje ranljivosti in ukrepanje;
- nadzorovana uporaba administrativnih privilegijev v sistemu;
- spremljanje in analiziranje sistemskih dnevniških zapisov;
- zaščita elektronske pošte in spletnega brskalnika;
- obramba pred škodljivo programsko opremo;
- omejevanje in nadzor mrežnih vrat, protokolov in storitev;
- zmožnost obnove podatkov;
- vzpostavitev in upravljanje varnih konfiguracij mrežne opreme, kot so požarne pregrade, usmerjevalniki in stikala;
- mejna obramba (na robu omrežja);
- zaščita podatkov;
- nadzorovan dostop, ki temelji na potrebi po vedenju;
- nadzor nad brezžičnimi omrežji;
- spremljanje in nadzor nad računi;
- usposabljanje uporabnikov;
- nadzor nad varnostjo aplikacijske programske opreme;
- odzivanje na incidente in upravljanje incidentov ter
- testiranje ranljivosti in izvajanje vaj.

Manj tipična tveganja in ukrepi so:

- uporaba opreme TEMPEST (zaščita pred neželenimi elektronskimi emisijami);
- fizični ukrepi varovanja (ključne sestavine sistema se namestijo v varnostnih območjih);
- preprečevanje optičnih napadov;
- namensko šifrirane rešitve;
- uporaba informacijske opreme.

Komunikacijsko-informacijske sisteme povezujemo tako, da v neki sistem uvozimo podatke iz drugega sistema oziroma omrežja. S tem se zmanjšajo operativni stroški, izboljša funkcionalnost in poveča učinkovitost; poleg tega se omogoči centraliziran dostop do podatkov itd. Omrežij z zelo občutljivimi podatki ne povezujemo z javnimi omrežji, npr. z internetom. Če že, jih povežemo preko diodnih naprav, ki poskrbijo, da pretok podatkov poteka samo v eno smer, npr. za posredovanje podatkov o vremenu ali o natančnem času (prek protokola NTP) iz javnega omrežja v zasebno omrežje. Kopiranje podatkov preko USB-naprav

je visokotvegano. Podatki se lahko prenašajo preko CD-ja (pri snemanju CD-ja mora biti izbrana možnost Read only/ Samo za branje). Pri napravah mejne zaščite ne smemo pozabiti na ustrezno fizično varovanje, prav tako moramo poskrbeti za upravljanje teh naprav, za nadzor dostopa do teh naprav, za ustrezne dnevniške zapise in za neprekinjeno delovanje teh naprav, odvisno od poslovnih in varnostnih zahtev. (Mulec, F., et al., 2016)

Reference

Korać, D., 2016. Projekt E-občina in informatizacija javne uprave. V: Schlamberger, N., et al. ur. *Informatika v javni upravi 2016: zbornik, 5.–6. december 2016, Kongresni center Brdo pri Kranju.* Ljubljana: Slovensko društvo Informatika.

Mihelič, A. in Vrhovec, S., 2016. Soočanje z najpogostejšimi ranljivostmi spletnih aplikacij državnih organov. V: Schlamberger, N., et al. ur. *Informatika v javni upravi 2016: zbornik, 5.–6. december 2016, Kongresni center Brdo pri Kranju.* Ljubljana: Slovensko društvo Informatika.

Mulec, F., Močilnar, F. in Maček, S., 2016. Kibernetska varnost v praksi. V: Schlamberger, N., et al. ur. *Informatika v javni upravi 2016: zbornik, 5.–6. december 2016, Kongresni center Brdo pri Kranju.* Ljubljana: Slovensko društvo Informatika.

Veršič, A., Kern Pipan, K. in Dečman, S., 2016. *Izzivi poslovne analitike v državni upravi.* [pdf] Dostopno na: http://iju2016.iju-konferenca.si/Upload/Predstavitve/A.Versi%C4%8D-K.Kern%20Pipan-S.De%C4%8Dman.pdf [20. 5. 2017].

Veršič, A., Kern Pipan, K. in Dečman, S., 2016a. Izzivi pri vzpostavitvi sistema podatkovnega skladišča in poslovne analitike v državni upravi. V: Schlamberger, N., et al. ur. *Informatika v javni upravi 2016: zbornik, 5.–6. december 2016, Kongresni center Brdo pri Kranju.* Ljubljana: Slovensko društvo Informatika.

Boštjan Krajnc