REPUBLIKA SLOVENIJA
MINISTRSTVO ZA NOTRANJE ZADEVE
POLICIJA

60 LET INFORMACIJSKO-TELEKOMUNIKACIJSKEGA SISTEMA POLICIJE

60 LET INFORMACIJSKO-TELEKOMUNIKACIJSKEGA SISTEMA POLICIJE

POLICIJA

Izdalo: Ministrstvo za notranje zadeve Republike Slovenije, Policija
Priprava: GPU, Uprava za informatiko in telekomunikacije
Oblikovanje naslovnice: SUPG, Matjaž Mitrović
Oblikovanje besedila: SUPG, Mirsada Dželadini
Tisk: Tisk Žnidarič, d. o. o.
Naklada: 300 izvodov
Ljubljana 2017

KAZALO VSEBINE

1 NAGOVOR GENERALNEGA DIREKTORJA POLICIJE

V policiji smo se že zgodaj zavedali koristi informacijsko-komunikacijske tehnologije (IKT) in pomena njenega obvladovanja za naše uspešno delovanje. Letos zato praznujemo že 60. obletnico Informacijsko-telekomunikacijskega sistema policije - ITSP. Sodelavci iz Urada za informatiko in telekomunikacije so pomemben del slovenske policije in skrbijo za uspešno delovanje ITSP, njegovo prilagajanje potrebam policije in njegov stalen razvoj. V letošnjem letu je veljavo stopila nova policijska zakonodaja: Zakon o organiziranosti in delu v policiji in Zakon o nalogah in pooblastilih policije. Tudi te spremembe zakonodaje bodo omogočile učinkovitejše izvajanje policijskih pooblastil s pomočjo novih informacijsko-komunikacijskih rešitev.

Varnostni problemi in s tem povezani izzivi se vse bolj selijo v spletno okolje, zato si v teh časih ni mogoče predstavljati učinkovitega odziva na varnostne probleme brez ustrezne podpore s tega področja. Globalizacija sveta, migrantska kriza, stopnjevanje terorističnih groženj in kibernetska kriminaliteta so le nekateri od aktualnih izzivov za delovanje policije. Prav ITSP je eden ključnih sistemov za uspešno odzivanje slovenske policije na te izzive in eden temeljev mednarodnega policijskega sodelovanja. Nedavno, ob sprejetju uredbe o sistematični mejni kontroli, je tako npr. informacijsko-komunikacijski sistem za mejno kontrolo omogočil uspešno preverjanje potnikov po nacionalnih in nadnacionalnih podatkovnih bazah, čeprav se je število vseh preverjanj povečalo kar 10x. V času migrantske krize leta 2015 pa je bil ITSP z aplikacijo za registracijo in preverjanje migrantov eden ključnih elementov za uspešno obvladovanje migrantskega vala. Zagotovljen je bil hiter in human postopek registracije, ki je bil prijazen do migrantov, hkrati pa policija ni odstopala od dogovorjenih varnostnih standardov. Tudi na EU nivoju je prav uporaba informacijsko-komunikacijskih rešitev eden ključnih elementov zagotavljanja varnosti. EU na informacijsko-komunikacijski tehnologiji gradi nove rešitve za zagotavljanje varnosti, boj proti terorizmu in organiziranemu kriminalu. Med drugim načrtuje vključitev AFIS funkcionalnosti v SIS, vpeljujejo se nove metode kontrole letalskih potnikov (API in PNR), pripravlja se rešitev za registracijo državljanov tretjih držav, ki vstopajo v prostor EU, t.i. Vhodno

– izhodni sistem (Entry-exit system) in še bi lahko naštevali. Izpostaviti je potrebno še radijske komunikacije, ki so eden temeljev uspešnega delovanja policije. Danes se radijske govorne storitve dopolnjujejo oz. nadgrajujejo z lokacijskimi storitvami (GPS), mobilnim prenosom podatkov, tudi mobilnim prenosom video posnetkov in nujno je, da policija sledi razvoju tehnologije tudi na področju brezžičnih komunikacij: s Tetro, LTE in 5G komunikacijami. Z vse bolj pomembno vlogo kibernetskega prostora se mora biti policija sposobna ustrezno odzivati tudi na kibernetske grožnje in pri vpeljevanju novih informacijsko-komunikacijskih rešitev še prav posebno skrb nameniti varovanju varovanih podatkov policije in zaščiti osebnih podatkov. Na nivoju EU bosta kmalu veljavni dve pomembni uredbi. Uredba o omrežni in informacijski varnosti (NIS) in Splošna uredba o zaščiti podatkov (GDPR). Slednja za varstvo osebnih podatkov med drugim predpisuje določitev pooblaščenca za varstvo osebnih podatkov, ki ga imamo v slovenski policiji že vrsto let.

Za zaključek naj vsem, ki so gradili ITSP oz. sodelujejo pri njegovem razvoju še danes, zaželim uspešno delo in čestitam za 60. obletnico! Policiji in UIT izzivov gotovo ne bo zmanjkalo, s skupnimi močmi, ustreznim angažiranjem in sodelovanjem pa bomo gotovo uspešno uresničevali naše poslanstvo v korist vseh državljanov.

Marjan Fank
generalni direktor policije

2 NAGOVOR DIREKTORJA URADA ZA INFORMATIKO IN TELEKOMUNIKACIJE

V letu 2017 praznujemo že 60. obletnico začetkov strojne obdelave podatkov v policiji. Za področje informacijsko-komunikacijske tehnologije (IKT) še prav posebej velja, da je edina stalnica sprememba. Tudi minulih 10 let je zaznamoval hiter razvoj tehnologije, ki je področje informacijsko-komunikacijske tehnologije bistveno spremenil.

Med najpomembnejšimi informacijsko-komunikacijskimi rešitvami je potrebno izpostaviti enormen porast uporabe socialnih omrežij, kar ni spremenilo le načina komuniciranja ljudi in organizacij, temveč je bistveno vplivalo na celoto medčloveških odnosov. Informacijsko-komunikacijska tehnologija nas spremlja na vsakem koraku. K temu so pripomogle mobilne komunikacije, predvsem pametni telefoni, tablice in brezžična WiFi, 4G in LTE omrežja. Prihaja t.i. Internet stvari (IoT- Internet of things) in tehnologije 5G, kar prinaša nove možnosti, pa tudi nove izzive. Vse skupaj pomeni, da je na razpolago neskončna množica podatkov, z analizo katerih lahko pridemo do pomembnih informacij, in nam omogočajo, da z njihovo pomočjo usmerjamo naše delovanje in odločitve. Govorimo o t.i. velikih podatkih (big data). S pojavom računalništva v oblaku (cloud computing) se je bistveno spremenil model zagotavljanja informacijsko-komunikacijskih storitev. Danes so na voljo informacijsko-komunikacijske storitve v oblakih, ki uporabnikom omogočajo, da lahko kadarkoli, od koderkoli, s katerokoli napravo dostopajo do informacijsko-komunikacijskih storitev in podatkov.

V slovenski policiji se zavedamo, da je uporaba sodobne informacijsko-komunikacijske tehnologije nujna za uspešno spopadanje z novimi varnostnimi izzivi. V zadnjem obdobju sta le-te zaznamovala migrantska kriza in naraščajoče teroristične grožnje. Republika Slovenija je od leta 2004 članica Evropske unije (EU) in v okviru EU z drugimi državami članicami sodeluje pri oblikovanju in uporabi novih informacijsko-komunikacijskih rešitev. Med drugim se je na ta način uspešno vključila v Schengenski informacijski sistem II. generacije (SIS II), se tesneje povezala z Europolovim informacijskim sistemom EIS in z Interpolovim informacijskim sistemom I24/7. Vse našteto nam omogoča dostop in izmenjavo informacij,

pomembnih za zagotavljanje varnosti. Izpostaviti je potrebno tudi naše sodelovanje v Prümski izmenjavi podatkov, ki je pomembno pripomogla k odkrivanju in identifikaciji storilcev kaznivih dejanj. Pri razvoju informacijsko-komunikacijskih rešitev nadaljujemo s prakso samostojnega razvoja operativnih rešitev. Glavne prednosti takšnega pristopa so zmožnost hitrega odzivanja na potrebe policije, lažje prilagajanje potrebam in pričakovanjem uporabnikov in izgradnja celovitega, integriranega Informacijsko - telekomunikacijskega sistema policije (ITSP). Na ta način smo med drugim pripravili nove rešitve za potrebe delovanja Operativno-komunikacijskega centra (OKC) Dnevnik dogodkov OKC za sprejem klicev na interventno številko 113 in razvili rešitev za mobilno delo policije e-Policist, ki bo temelj za razvoj in širitev novih mobilnih rešitev. Pripravili smo rešitev TravelDocMigrant za registracijo in preverjanje migrantov in razvili rešitev za spremljanje podatkov o letalskih potnikih (API - Advanced passenger information system), če naštejem le nekatere. Poleg tega smo vpeljali nov sistem za področje varovanja oseb in objektov Infranet in začeli s pospešeno digitalizacijo videonadzornih sistemov. Gre za zelo hitro razvijajoče se področje in tudi nove načine uporabe, saj pospešeno vpeljujemo tudi video snemanje postopkov policistov s pomočjo kamer nameščenih na uniformah. S pomočjo digitalnega videa tako prispevamo k transparentnosti policijskega dela, hkrati pa na ta način povečujemo varnost policistov. Rešitev ima tudi preventivni učinek na potencialne storilce kaznivih dejanj. Več podatkov o informacijsko-komunikacijskih projektih slovenske policije boste našli v brošuri, ki je pred vami.

Še eno področje je potrebno izpostaviti. Razvoj informacijsko-komunikacijske tehnologije, ki je vedno bolj vseprisotna, prinaša seveda tudi izzive na področju kibernetske varnosti. Policija nastopa v različnih vlogah. Zadolžena je za preiskovanje kaznivih dejanj s področja kibernetskega kriminala, hkrati pa skrbi za varovanje lastnega ITSP. Oboje je tudi del lani sprejete Strategije kibernetske varnosti Republike Slovenije. Slovenska policija se zaveda pomena IKT tehnologij in nujnosti ustreznih vlaganj v to tehnologijo.

Za konec je potrebno izpostaviti predvsem vlogo ljudi, IKT strokovnjakov. Brez njih in brez ustreznih vlaganj v njihovo znanje si ni mogoče zamišljati uspešne IKT podpore, brez nje pa uspešnega delovanja policije. Tega se je potrebno zavedati in si prizadevati za zagotovitev pogojev za pridobivanje, razvoj in zadržanje IKT strokovnjakov.

Ob 60. obletnici ITSP čestitam vsem sodelavcem!

mag. Andrej Bračko
direktor Urada za informatiko in telekomunikacije

3 RAZVOJ APLIKACIJ

V letu 2017 praznujemo 60. obletnico razvoja informacijsko-telekomunikacijskega sistema policije - ITSP. Kaj se je spremenilo v 10 letih?

Kljub znatnim finančnim omejitvam v zadnjih nekaj letih je delo potekalo nemoteno in večina programskih rešitev je bila plod znanja lastnega kadra. V času pred schengenskim informacijskim sistemom smo lahko govorili o relativno zaprtem sistemu ITSP, v današnjem času pa skrbimo za komunikacije z vsemi možnimi partnerji, pridobivamo podatke iz vseh, z zakonom določenih virov. V prvih letih po osamosvojitvi smo zagotavljali osnovno infrastrukturo preko evidenc, sedaj pa ustvarjamo celovite rešitve, aplikacije, ki so usmerjene v celovito reševanje problemov, ne le v evidentiranje.

3.1 Mobilne aplikacije

V zadnjem obdobju je v slovenski policiji dozorelo spoznanje, da bi lahko uvedba ustreznih in celovitih mobilnih rešitev pomembno pripomogla k povečanju uspešnosti in učinkovitosti dela na posameznih področjih policijskega dela. Tako smo z močno podporo vodstva Policije ter s pomočjo evropskih sredstev izvedli prvi pravi projekt mobilne rešitve ePolicist. V tem projektu je bila v sodelovanju z zunanjim izvajalcem leta 2016 razvita prva sodobna mobilna aplikacija v Policiji - ePolicist.

Aplikacija je razvita za različne platforme (Windows, Android, iOs), različne naprave (7-10 palčna tablica, pameten telefon) in prilagodljiva različnim velikostim zaslona (responsive design). Omogoča preverjanje po evidencah (Interpol, Fonetični indeks oseb (FIO), Schengenski informacijski sistem (SIS), Vizumski informacijski sistem (VIS), RISK- register prebivalstva in vozil) s prikazom podrobnosti zadetka, prav tako pa tudi izvedbo določenih policijskih postopkov.

Glavni cilj projekta je bil razviti celovito mobilno rešitev, ki bi policistom omogočala ne le preverjanje, ampak tudi izvedbo postopka izdajanja plačilnega naloga ter drugih postopkov s področja prometne varnosti na prenosni mobilni napravi na terenu.

Slovenska policija je s projektom ePolicist pričela tudi z aktivnim sodelovanjem v ENLETS delovni skupini (European Network of Law Enforcement Technology Services). Še posebej smo aktivni v podskupini ENLETS Mobile, v sklopu katere smo tudi organizirali

in gostili konferenco na temo mobilnih rešitev v evropskih policijah. ENLETS nas je tudi uvrstil med t.i. »forerunners« na področju mobilnih projektov.

Podrobneje je ta rešitev predstavljena v drugem delu te publikacije.

3.2 Področje mejne kontrole

TravelDoc - preverjanje prehodov meje

Leta 2001 smo z nabavo prvih čitalcev za branje potovalnih dokumentov razvili prvo aplikacijo za hitro preverjanje oseb na mejnih prehodih - aplikacijo TravelDoc. S to aplikacijo je mogoče preverjati vse potne listine (osebne izkaznice, potne liste, vize, nekatera dovoljenja), ki vsebujejo strojno berljiv zapis (MRZ - Machine Readable Zone) in ki ustrezajo ICAO standardu. Aplikacija je sprva za svoje delo uporabljala čitalce dokumentov IDStar 4048 ter za povezavo z zaledjem avtomatiziran dostop do IBM Personal Communication in transakcije MISK (mejna kontrola).

Aplikacija se je razvijala skladno s spremembami v IT, strojni opremi ter spremembami zakonodaje. Sedaj uporablja dve različni vrsti čitalcev dokumentov (ARH PRMC in DESKO Penta). Čitalci so poleg strojno berljivega zapisa (MRZ) sposobni brati tudi RFID čip, ki se nahaja na potovalnih dokumentih ter s tem zmanjševati možnost uporabe ponarejenih dokumentov za prehajanje meje. Poleg čitalcev dokumentov aplikacija uporablja tudi čitalec prstnih odtisov za potrebe preverjanja oseb po centralni evropski vizni evidenci ter naši interni bazi prstnih odtisov AFIS migrant. Za povezljivost z zalednimi sistemi (Interpol, FIO, SIS, VIS) se uporabljajo spletni servisi.

14

eMigrant – registracija migrantov

Ob begunski krizi v letu 2015 smo se soočili s kar nekaj problemi, tako na naši severni meji, predvsem pa na naši južni meji, ki je hkrati tudi zunanja schengenska meja. Čeprav so bili dogodki delno pričakovani, je vse presenetilo veliko število oseb, ki so prečkale mejo in jih je bilo potrebno registrirati v skladu z migrantsko zakonodajo. Potrebovali smo odgovarjajočo rešitev za preprečitev humanitarne krize in zagotavljanja varnosti državljanov.

Zaradi res velikega števila oseb smo potrebovali rešitev, ki bo sposobna hitro obdelati veliko število oseb v čim krajšem času in zajeti čim več podatkov o teh osebah. V ta namen je bila na temelju obstoječe aplikacije TravelDoc razvita aplikacija eMigrant.

Omogočila je hitro preverjanje oseb po policijskih evidencah, zajem osebnih podatkov posameznih oseb in družin, vključno z obrazno fotografijo in prstnimi odtisi, njihovo shranjevanje v policijske evidence, ter izdajanje potrebnih dokumentov.

Podrobneje je ta rešitev predstavljena v drugem delu te publikacije.

PNR (Passenger Name Record) / API (Advanced Passenger Information)

Evropski parlament je podprl direktivo o izmenjavi podatkov o rezervacijah letalskih potnikov (PNR), direktiva Sveta 2004/82/ES o izmenjevanju podatkov o potnikih v letalskem prometu (API) pa je veljavna že več let. V skladu z direktivo API lahko policija obravnava letalske potnike, ki prihajajo v Slovenijo iz držav, ki niso članice Evropske unije ali schengenskega območja.

Za pridobivanje podatkov iz evidenc letalskih potnikov in njihovo obdelavo smo v policiji razvili platformo za računalniško podprto presojo varnostnega tveganja letalskih potnikov z namenom:

- učinkovite in razumljive obdelave podatkov o potnikih,
- hitrejšega prehoda meje zaradi predhodne obdelave,
- boljšega odkrivanja varnostnih tveganj,
- preprečevanja posledic tveganja z ustreznimi ukrepi,
- zagotavljanja zasebnosti potnikov,
- boljše informacijske varnosti.

Želeli smo vzpostaviti platformo oziroma orodje, ki omogoča dovolj preprosto ustvarjanje procesov presoje, da lahko analitiki to storijo samostojno, brez pomoči razvijalcev programske opreme. Tako se lahko temeljito posvečajo merilom presoje in manj tehnologiji. S procesi presoje varnostnih tveganj je možno odkriti morebitne nevarnosti, preprečiti možne posledice in doseči, da se policija primerno odzove z ustreznimi ukrepi.

Platformo za presojo varnostnega tveganja smo v slovenski policiji razvili sami, ker želimo obdržati določeno stopnjo avtonomnosti, natančno poznati mehanizme presoje in platformo vključiti v sam sistem policije. Za pripravo kompleksnih pravil smo uporabili odprtokodno analitično orodje KNIME. To je programsko orodje, namenjeno analizi in organizaciji podatkov. Uporablja se z grafičnim vmesnikom, v katerem posamezne module povezujemo v podatkovne procese.

Podrobneje je ta rešitev predstavljena v drugem delu te publikacije.

3.3 Statistično poročanje

Prejšnja leta je potekala prenova statističnega poročanja, v sklopu katerega so bili z zunanjim izvajalcem pripravljeni temelji za preselitev celotnega podatkovnega

skladišča na distribuirano platformo, za področje mejnih zadev pa so bili izdelani tudi statistični pregledi.

Zdaj pa se nam uresničuje načrt pridobivanja lastnega kadra za področje statističnega poročanja, izdelava novih statističnih pregledov, migracija s centralnega računalnika in dokončna ukinitev programa SAS, kar bo zmanjšalo stroške. Veliko obeta novo BI (Business Intelligence) orodje, omogoča boljšo storitev in manj vnaprej pripravljenih poročil, hkrati pa več možnosti za analiziranje podatkov.

3.4 Elektronsko izobraževanje na daljavo (EIDA)

V letu 2009 smo ponovno obudili v življenje zamisel o elektronskem izobraževanju na daljavo. V sodelovanju s Policijsko akademijo smo postavili portal EIDA in v letu 2010 že izvedli usposabljanje na intranetu za vse delavce policije. Kmalu zatem je sledil še portal za zunanje uporabnike EIDAZ, namenjen delavcem policije, ki dostopajo do izobraževanja preko spletnih strani.

3.5 Področje kriminalitete

Informacijski sistem za področje kriminalitete (ISPK) je bilo treba uskladiti z zakonodajnimi spremembami in ga prilagoditi uporabniškim zahtevam. Med drugim je bila dvignjena raven varnosti dostopa do podatkov, poenostavljeno je bilo evidentiranje bagatelne kriminalitete, izboljšano evidentiranje podatkov po 149. b členu ZKP in uvedena računalniška podpora vodenju finančnih preiskav.

V glavnem podprojektu prenove ISPK sta bili pripravljeni dve programski rešitvi za pisanje kriminalističnih obrazcev na terenu z avtomatiziranim prenosom podatkov v evidence in za analiziranje velikih količin podatkov. Osnovna evidenca kaznivih dejanj je bila nadgrajena s funkcijami pisarniškega poslovanja v aplikaciji Beležka policista.

Seveda je v izdelavi in prenavljanju še kopica drugih aplikativnih rešitev in projektov, kot so:

- Krim sledi - v okviru katerega je bila pripravljena aplikativna rešitev za primerjavo in analizo sledi obuval;
- OKCP - razvoj integriranega preverjanja po vseh virih podatkov;
- GIS Policije - Geografsko informacijski sistem;

- RIS4I - Registracija delovnega časa;
- E-dostavnica - omogoča poslovanje vložišč s fizičnimi dokumenti;
- DDOKC - nova verzija dnevnika dogodkov Operativno komunikacijskega centra;
- Face Trace - programska rešitev za avtomatizacijo obrazne prepoznave;
- Prüm - obdelava osebnih podatkov iz nacionalnih zbirk podatkov - preverjanje po prstnih odtisih in profilih DNK.

3.6 Prednosti in slabosti lastnega razvoja

Jack Welch: Če je stopnja sprememb zunaj vaše organizacije večja od stopnje sprememb znotraj nje, prihodnost ni rožnata.

Najprej je potrebno ugotoviti, ali dobro obvladamo posamezne procese - ali smo pri njih odlični, povprečni ali pa morda celo slabi. Za procese, ki jih ne opravljamo niti izvrstno niti stroškovno učinkovito, je smiselno poiskati zunanje izvajalce, ki bodo to opravljali boljše in hitrejše.

Včasih je smiselno objektivno razmisliti, če je »outsourcing« ustrezen za določeni del sistema IT; za velike in ključne poslovne procese je tvegano preiti na popolno zunanje izvajanje. Strokovnjaki ugotavljajo, da je obvladovanje ravni storitev pri nosilcih tovrstne podpore še bolj izpostavljeno operativnim tveganjem, kot pa če se storitve že postavljenih rešitev IT izvajajo znotraj.

Predvsem na področju razvoja aplikacij za podporo operativnega dela policije, kljub nekaterim težavam, večinoma uspešno sledimo potrebam. Lasten razvoj nam omogoča hitro odzivanje na potrebe in pripravo dobro integriranih rešitev. Hkrati pa je obvladovanje informacijsko-komunikacijske tehnologije z lastnimi strokovnjaki pomembno tudi z vidika varovanja podatkov in informacijsko-komunikacijskih sistemov. Ključni faktor za uspešno delo so ljudje. Zato je še posebej pomembno v policiji zagotoviti ustrezne pogoje za zaposlovanje in zadržanje kvalitetnih strokovnjakov za IKT. Z vidika njihovega razvoja pa je nujno zavedanje o pomenu izobraževanja in vlaganja v znanje.

Charles Darwin: Ne preživijo najmočnejši ali najpametnejši, ampak tisti, ki se najbolje prilagajajo spremembam.

4 INFORMACIJSKO-TELEKOMUNIKACIJSKA INFRASTRUKTURA

Za zadnje desetletno obdobje na področju informacijsko-telekomunikacijske infrastrukture je značilno, da je bilo zelo turbulentno.

Finančna sredstva namenjena temu področju so se skozi obdobje zelo spreminjala. Če je bilo na začetku še v redu, je sledila velika kriza, ko smo se znašli v situaciji, da razvoj praktično ni bil več mogoč. Prisiljeni smo bili iskati rešitve v zmanjševanju obsega storitev, ki jih Policija nujno potrebuje za uspešno delo. Položaj lepo ilustrira dejstvo, da smo v informacijsko-telekomunikacijski sistem Policije (ITSP) vključevali osebne računalnike, ki so jih v drugih državnih organih odpisali, saj so bili še vedno bistveno boljši od tistega, kar smo imeli. Proti koncu obdobja pa nam je država spet namenila več sredstev, tako da smo IKT infrastrukturo večinoma že dvignili na ustrezen nivo.

V tem obdobju, leta 2010, smo izpeljali tudi nekaj organizacijskih sprememb in med drugim, v isti sektor združili vsa pomembnejša delovna področja, ki se nanašajo na IKT infrastrukturo. Osebni računalniki in namizna strojna oprema, strežniški sistemi in centralni računalnik, lokalna omrežja in medomrežne povezave, fiksna in mobilna telefonija, vsa ta področja so zdaj združena v enem sektorju. Ta sprememba je prinesla pomembne sinergijske učinke ter zelo izboljšala sodelovanje, notranji prenos znanja in informacij, omogočila hitrejši bolj koordiniran razvoj in vzdrževanje infrastrukture.

4.1 Distribuirana informacijska strojna oprema

Obdobje od 2008 do 2015 je zaznamovala finančna kriza in s tem veliko pomanjkanje nabav terminalne informacijske opreme. Nabave so bile tako okrnjene, da smo si morali pomagati z donacijami odpisane računalniške opreme iz gospodarstva in javne uprave. Svetla točka so bili projekti financirani iz sklada za zunanje meje, s katerimi smo redno posodabljali vsaj lokalno informacijsko opremo na zunanji schengenski meji. Kljub temu smo v tem obdobju vse lokalne strežnike končno nadgradili iz Windows NT na Windows Server 2003 ali 2008 R2 in osebne računalnike z Windows 2000 na Windows XP.

V zadnjem letu je investicijski krč popustil in posledično smo nabavili več informacijske opreme. To nam je omogočilo, da smo dokončno opustili zastarel in varnostno zelo sporen operacijski sistem Windows XP na osebnih računalnikih in Windows 2003 na lokalnih strežnikih.

Pomembno spremembo smo uvedli tudi pri zagotavljanju storitve tiskanja, kjer bomo namesto lastnih tiskalniških naprav imeli tiskalniške naprave v najemu.

Nameščanje programske opreme

V letu 2006 smo pripravili infrastrukturno okolje za uvajanje namiznih operacijskih sistemov »Windows XP«, namesto prejšnjih, takrat že zastarelih »Windows 2000«. V naslednjem letu smo uvedli še nadzorna in upravljavska orodja »System Center Configuration Manager 2007« za Windows okolje. Infrastrukturno okolje za uvajanje namiznih operacijskih sistemov »Windows 7« smo pripravili leta 2011. Zatem smo uvedli sistem za avtentikacijo dostopa do internetnih storitev. V zadnjih dveh letih

smo zamenjali verzijo nadzornih in upravljavskih orodij »System Center Configuration Manager« na naprednejšo in zmogljivejšo verzijo SCCM 2012. V zadnjem letu smo pričeli s pripravami infrastrukturnega okolja za uvajanje namiznih operacijskih sistemov »Windows 10« in sodelovali pri uvajanju nove kriptografske tehnologije za zaščito podatkovnih medijev »BitLocker«.

4.2 Centralni računalniški sistem

Leta 2006 smo vzpostavili rezervni računalniški center v Novem mestu in implementirali storitev GDPS/XRC, ki omogoča asinhrono kopiranje vseh podatkov iz primarnega podatkovnega centra v Ljubljani v rezervni center. Za varnostno kopiranje podatkov iz vseh strežnikov in pomembnejših delovnih postaj smo vpeljali rešitev »Tivoli Storage Manager«. Rešitev se je ob vpeljavi izvajala na z/OS operacijskem sistemu centralnega računalnika. Avtomatizirali smo delo na centralnem računalniku z vpeljavo podsistema »System Automation for z/OS«, ki omogoča avtomatizirano obdelavo podatkov, zagon in zaključevanje sistema, ter avtomatizirano odzivanje na sporočila operacijskega sistema in vseh ostalih podsistemov. Namestili smo zadnjo verzijo IMS baze, na kateri se je takrat še izvajal Centralni register prebivalstva, ki je bil kasneje prenesen na Ministrstvo za javno upravo. V produkcijo smo postavili aplikativni strežnik »WebSphere« verzije 5.1. Prva aplikacija, ki se je na njem izvajala je bil »eRISK«.

V letu 2007 smo implementirali sporočilno platformo »WebSphere MQ« s katero še danes izmenjujemo podatke z zunanjimi partnerji in sistem »CICS Transaction Gateway«, ki aplikativnim strežnikom Websphere omogoča dostop programov CICS transakcijskih strežnikov. Leta 2009 smo dvignili verzijo transakcijskega strežnika CICS iz verzije 3.1 na 3.2 in verzijo aplikativnega strežnika »Websphere« na verzijo 6.1. Leta 2010 smo zamenjali obstoječa diskovna sistema IBM ESS 2105 z 5 TB uporabne kapacitete in EMC 5200 s 125 GB uporabne kapaciteta za diskovni sistem IBM System Storage DS8100 z 10 TB uporabne kapacitete. Izboljšali smo tudi način kopiranja podatkov v rezervni center z vpeljavo rešitve »Tivoli Productivity Center for Replication«.

V produkcijsko rabo smo v 2011 implementirali virtualizacijsko okolje »z/VM« in nanj preselili »Tivoli Storage Manager« na z/Linux operacijski sistem, s čimer smo izboljšali njegovo delovanje in hkrati znižali stroške varnostnega kopiranja. Razvojno okolje »Visual Age Generator« smo zamenjali z novejšim »Rational Business Developer EGL«. Naslednje leto smo nadgradili verzijo transakcijskega strežnika CICS TS na 4.1. V letu 2013 pa smo z uporabo DB2 »Data sharing« funkcionalnosti

implementirali souporabo podatkov med več medsebojno povezanimi DB2 strežniškimi instancami združenimi v računalniško gručo, kar nam v primeru izvajanja vzdrževalnih del na podatkovni bazi omogoča krajše izpade oz. le teh sploh ni. V računalniško gručo »SYSPLEX« smo implementirali tudi transakcijski strežnik CICS. Aplikativni strežnik »WebSphere« smo leta 2014 nadgradili na verzijo 8.

V zadnjih desetih letih smo zaradi povečanja obremenitev dvakrat zamenjali centralni računalnik. Trenutno je v uporabi IBM zServer z12 model 2828-H13 X03. Ob koncu desetletnega obdobja v 2016 smo zamenjali še diskovno polje, tako da sedaj uporabljamo IBM System Storage DS8884 z 80 TB uporabne kapacitete. Hkrati smo implementirali sodobnejšo rešitev za asinhrono kopiranje podatkov iz primarnega v rezervni podatkovni center »IBM Copy Services Management«. Razvojno okolje »Rational Business Developer EGL« pa smo zamenjali s sodobnejšim »Urban Code Deploy«.

Fotografije iz aplikacije »Digitalna fotografija« smo prenesli iz diskovnega sistema centralnega računalnika na cenejše diskovno polje s področja odprtih sistemov.

Oprema v računalniškem centru

4.3 Pisarniško poslovanje in elektronska pošta

Nadgradili in poenotili smo sistem pisarniškega poslovanja, ter poslovanja z dokumentarnim gradivom z uporabo zadnje verzija programske rešitve SPIS. Združili smo sistema »zunanje« in »notranje« elektronske pošte v Domino/Notes okolju in ob začetku predsedovanja Slovenije EU-ju uvedli mobilni dostop do pošte. Konec leta 2015 smo hkrati z ostalo državno upravo uvedli sistem elektronskih računov »eRačuni«. Domino/Notes okolje smo na strežniški strani dvignili na verzijo 9, na strani odjemalcev pa dvig verzije še poteka.

4.4 Sistemi za podporo operativnemu delu

Schengenski sistem prve generacije SISone4All smo uspešno vpeljali leta 2007. V letu 2012 smo vzpostavili sistem EUROSUR, ki omogoča državam članicam in agenciji Frontex sodelovanje na področju mejne kontrole. Leta 2013 smo zamenjali SISone4All sistem s schengenskim informacijskim sistemom druge generacije. SIS II z vsemi vmesniki deluje na centralnem računalniku, ki zagotavljajo tako sinhrono, kot asinhrono komunikacijo s centralnim sistemom SIS II. Istega leta smo v sodelovanju z Ministrstvom za zunanje zadeve vpeljali programsko rešitev za podporo izdaje viz. Sodelovali pa smo tudi pri vzpostavitvi lastne rešitve za klicne centre 113 »DDOKC«.

4.5 Računalništvo v oblaku

V letu 2013 smo uvedli odprtokodno virtualizacijo v DMZ območju. Leta 2015, ob zamenjavi dotrajanega strežniškega sistema GPU z novim, smo zamenjali tudi VmWare virtualizacijsko okolje z virtualizacijskim okoljem Hyper-V. V prenovljenem in leta 2016 razširjenem strežniškem sistemu deluje preko 100 različnih logičnih strežnikov.

4.6 Lokalna in prostrana omrežja

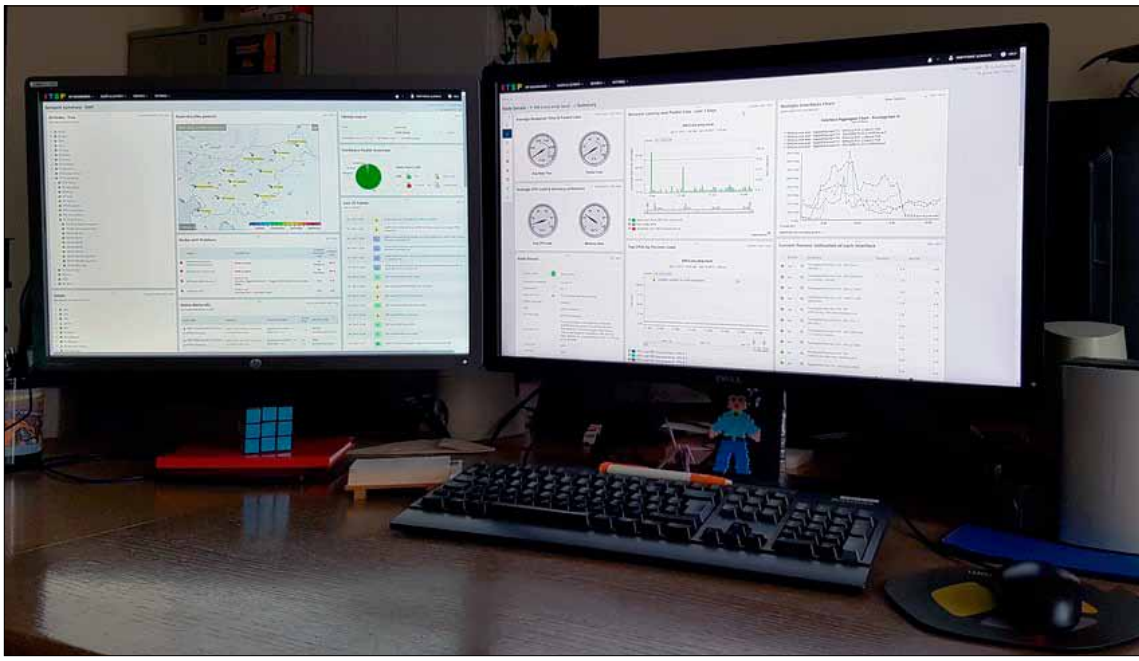
V zadnjih desetih letih, natančneje leta 2010, smo organizacijsko združili področji lokalnih (LAN) in prostranih (WAN) omrežij, kar je povečalo učinkovitost našega dela.

Zmogljivosti povezav širokopasovnega omrežja smo povečali na policijskih upravah iz 1-2 Mbit/s na 100 Mbit/s, iz 256-512 kbit/s na 40 Mbit/s na policijskih postajah in na maksimalno možne tehnično izvedljive na manjših enotah (najmanjša uradna hitrost

je 2048/384 kbit/s). Sodelovali smo pri povezavah v schengenski informacijski sistem, najprej z rešitvijo SISone4All, nato povezavo do SIS II, sistema druge generacije. Trenutno pa smo v pripravi prehoda na omrežje nove generacije (TESTA NG).

V tem času smo poenotili tehnologije, ukinili TDM (Time-Division Multiplexing) najete vode, izvedli prehod v IP okolje in integracijo prenosa podatkov, govora (delno videa). Konsolidirali smo topologije širokopasovnega omrežja policije na dvonivojsko centralizirano omrežje in ga pripravili na uvedbo oblačnih storitev.

Pridobili smo lastni naslovni prostor v internetu in dual-homing - ločeni povezavi do dveh avtonomnih sistemov internetnih ponudnikov in implementirali ustrezno zmogljivo opremo (usmerjevalniki, stikala, požarne pregrade). Uredili smo povezavo rezervnega računalniškega centra z zmogljivo redundantno optično povezavo s sistemi DWDM. Vzpostavili smo varna in ločena brezžična omrežja za službeno uporabo in goste ter vpeljali nove mobilne tehnologije (širokopasovne mobilne komunikacije, pametne naprave). Izvedli smo še implementacijo sistema za nadzor in upravljanje omrežja (Slika 4), v omrežje vključenih sistemov (strežniki, DDOKC) in upravljanje IP naslovnega prostora, ki ga uporabljamo v Uradu za informatiko in telekomunikacije in kolegi v Oddelku za informatiko in telekomunikacije na policijskih upravah.



Nadzorni sistem omrežja

Prenovljena je bila tudi oprema podatkovnega centra (datacenter stikala s kapacitetami 40 Gbit/s), ki sedaj omogoča vključitev zmogljivih virtualiziranih strežniških sistemov.

4.7 Fiksno govorno omrežje

Fiksno govorno omrežje oziroma telefonske storitve v omrežju MNZ RS in Slovenske policije, je že od začetka eno od temeljev ITSP.

Moderno govorno omrežje z več kot 150 lokacijami po državi sodi med največje zaprte sisteme v državi in prinaša prednosti tako za upravljavce oziroma vzdrževalce omrežja, kot končne uporabnike. V času zamenjave starih sistemov z novimi sistemi, so bile uporabljene v omrežju najnovejše, takrat dostopne tehnološke rešitve na trgu. O sposobnosti tehničnega osebja Policije govori tudi dejstvo, da sta v prehodnem obdobju paralelno delovali dve omrežji, ki sta bili povezani - v času »zamenjave« je imel uporabnik zato le nekaj minut onemogočeno uporabo telefonskega aparata.

V skladu s tehnološkim razvojem, smo omrežje nadgrajevali in posodabljali (danes sta na različnih delih omrežja v uporabi H.323 in SIP protokola), tako da govorno omrežje MNZ/Policije še vedno sodi med sodobnejše sisteme v državi in omogoča široko paleto možnosti oziroma storitev (prikaz imena kličočega, izbiranje po imenu, telefonski asistent, ...). Sodoben sistem (Slika 5) je omogočil tudi razširitev govornega omrežja preko državne meje (CPS Megvarje) in znatne finančne prihranke.

Koncept omrežja zagotavlja delovanje govornega omrežja v skladu z zahtevami po robustnem in zanesljivem delovanju v najrazličnejših razmerah. To nesporno dokazujejo tudi primeri iz preteklosti - ko so v različnih izrednih razmerah (npr. poplave) delovali govorni sistemi Policije nemoteno. Ne smemo pozabiti tudi na dejstvo, da govorno omrežje MNZ/Policije sodi s stališča finančne učinkovitosti med najugodnejše v državi.

Tehnološkemu razvoju na področju govornega omrežja so sledile tudi druge tehnološke rešitve, ki poleg učinkovitejšega delovnega procesa prinašajo pogosto tudi finančne učinke.

Namizne telefaks naprave zamenjuje centralizirana storitev (E-fax), ki omogoča sprejem in pošiljanje telefaks sporočil preko Lotus Notes pošte. Za lažje in učinkovitejše delo operativnih enot na terenu, je bila vzpostavljena storitev - Sklic, ki

omogoča avtomatsko obveščanje uporabnikov o sklicu enote, kar pomeni bistveno hitrejši in učinkovitejši sklic enote kot v preteklosti, ko se je sklic izvajal ročno. Vpeljali smo sistem obveščanja uporabnikov preko pošiljanja SMS sporočil - SMS poštar, ki je uporaben za različne namene, za obveščanje o alarmnih/stanjih delovanja sistemov kritične infrastrukture ali kot pomemben element sistema obveščanja operativnih služb.

Detajl telefonske centrale

4.8 Oprema klicnih centrov 113

Širša javnost ocenjuje delo Policije po različnih elementih. Med najpomembnejše sodi delo klicnih centrov za sprejem interventnih klicev na številko 113. Telekomunikacijsko opremo različnih proizvajalcev smo v preteklosti nadomestili s sodobnejšo in zmogljivejšo ter jo hkrati poenotili. Kljub zavedanju dejstva, da gre pri rešitvi klicnih centrov za zelo kompleksno okolje (saj se prepletajo različne tehnologije in so zato potrebna znanja različnih področij na nivoju sistemskega integratorja), smo v UIT z lastnimi viri razvili rešitev za vse klicne centre, ki sprejemajo interventne klice na številko 113 v državi. Sistem redno posodabljamo glede na potrebe uporabnikov in morebitne spremembe zakonodaje. Lastna rešitev nam omogoča lažjo vpeljavo novih funkcionalnosti (npr. lociranje uporabnikov v primeru klica na interventno številko 113 z mobilnega telefona) in hitrejšo odpravo morebitnih napak, kar je pri tovrstnih centrih vitalnega pomena. Za potrebe lastnega razvoja novih rešitev in morebitna testiranja, smo vzpostavili tudi razvojno/testno IKT okolje.

4.9 Mobilne storitve

V letu 2007 smo uvedli prve mobilne storitve v Policiji: potisne pošte na »BlackBerry« platformi. Leta 2014 smo sodelovali pri postavitvi strežniške in komunikacijske infrastrukture za pilotsko aplikacijo »ePolicist«. V letu 2015 pa smo uvedli sistem za upravljanje mobilnih naprav (»Enterprise Mobility Management«) na MobileIron platformi in s tem Policiji omogočili varno uporabo pametnih mobilnih naprav. Kasneje pa smo sodelovali še pri postavitvi strežniške in komunikacijske infrastrukture za projekt »ePolicist«.

Konfiguriranje in prenos podatkov na telefon

Kadar je potrebno, lastno omrežje dopolnjuje uporaba komercialnih mobilnih omrežij, pa naj bo to za potrebe, kot so recimo prenos govora, dostop do elektronske pošte in evidenc ali prenos multimedijskih vsebin.

V primeru podatkovnih komunikacij se zagotavlja zasebnost komunikacije z vzpostavitvijo šifrirane povezave med uporabnikom na terenu in ITSP omrežjem. Tehnološki razvoj od EDGE do LTE se zdi skoraj neverjeten. Hitremu tehnološkemu razvoju pa sledijo tudi naprave končnih uporabnikov. Zaradi racionalizacije in širšega

nabora storitev različnim končnim uporabnikom, se je v zadnjem letu začel izvajati prehod na »standardno« terminalno opremo.

Podrobneje so rešitve za mobilno delo predstavljene v drugem delu te publikacije.

4.10 Posodobitev snemalnega sistema

Policija dokazuje zakonitost in strokovnost svojega dela tudi s pomočjo posnetkov na snemalnih napravah. Dotrajane snemalne naprave smo nadomestil z novim snemalnim sistemom. Snemanje na trakove oziroma kasete, smo nadomestili s snemanjem pogovorov in beleženjem prometnih podatkov na računalniške diske. Do posnetkov je omogočen dostop tudi iz centralne lokacije, namesto izključno lokalnega dostopa, kar bistveno olajša delo. Tehnološki napredek je bistveno pospešil tudi dostop in poslušanje želenega posnetka. Nove tehnološke rešitve omogočajo lažje vključevanje snemanja, saj za snemanje večjega dela terminalne opreme govornega omrežja ITSP, ni več potreben poseg na terenu.

Namesto priklopa snemalnega vmesnika, se uporabi mehanizem izločanja kanalov na namenskem vmesniku med govornim strežnikom in snemalno napravo. Brez težav je mogoče snemati telefonske priključke na oddaljeni lokaciji.

5 INFORMACIJSKO TELEKOMUNIKACIJSKA PODPORA

Razvoj računalništva je v zadnjem desetletju bliskovit. Nihče si pred desetimi leti ni predstavljal, da bo danes možno izvajati policijsko delo na mobilnih napravah in da bo večina policijskih postopkov avtomatiziranih. Zaradi hitrega razvoja računalništva, programske opreme ter uporabe ne samo računalnikov, ampak tudi mobilnih naprav, se je prav tako razvijala podpora IKT storitvam.

Razvoj sodobnih tehnologij je narekoval razvoj tudi podpori za te napredne tehnologije. Pred desetimi leti je bila podpora organizirana v Oddelku za statistiko in podporo uporabnikom. Začela se je oblikovati skupina ljudi, ki so nudili osnovno IKT podporo. Podpora je temeljila bolj na sprejemu napak in ne tudi sami odpravi le teh. Ni bilo vzpostavljene enotne točke za prijavo napak, napake so se sprejemale po vseh oddelkih informatike, ni bilo nadzora nad zahtevki in odprava težav je bila dolgotrajna.

Podpora vsem IKT storitvam je danes oblikovana v Sektorju za IKT podpro. V sektorju je združena celotna podpora za informacijsko-komunikacijske sisteme in procese. Del sektorja je Storitveni center Policije (v nadaljevanju SC), ki je enotna vstopna točka za prijavo napak in težav s področja IKT sistemov in storitev. V SC smo združili skupino zaposlenih, ki so delali na help desku in skupino zaposlenih, ki so skrbeli za 24/7/356 nadzor centralnega računalnika. Z združitvijo smo vzpostavili enotno vstopno točko za prijavo vseh IKT napak in zahtev. Storitven center je sodobno opremljen center, ki pri delu uporablja napredno tehnologijo za sprejem, beleženje in reševanje težav. V aplikaciji se beležijo vse napake in težave, ki jih zaznajo končni uporabniki. S to rešitvijo smo na področju podpore zelo povečali učinkovitost SC. SC skrbi za reševanje težav na prvem nivoju podpore. V podpori smo združili tudi uvajanje novih aplikativnih rešitev razvitih v Policiji. Zaposleni SC izvajajo celoten postopek uvajanja aplikacij, od izvedbe testiranj aplikacij do izdelave navodil in priprave načrta za uvedbo aplikativnih rešitev v Policiji. Pri uvajanju aplikacij izvaja tudi šolanje končnih uporabnikov po Sloveniji. Delavci SC veliko sodelujejo z UUP GPU in UKP GPU pri izobraževanju sodelavcev na PP.

V sektorju je tudi skupina, ki rešuje zahtevnejše naloge s področja prekrškovnih zadev in ažuriranja baze podatkov na centralnem računalniku. Skupina se je skozi leta gradila in spreminjala. Začelo se je, ko je skupina sodelavk začela vnašati podatke za kreiranje baze podatkov za Fonetični indeks oseb (FIO). Sodelavke so

vnašale in ažurirale podatke (prometne nesreče, kazniva dejanja, javni red in ostalo). Vzpostavile so evidenco prstnih odtisov, vnos prstnih vtisov v sistem AFIS. V tej skupini so se izdelovale tudi mesečne in letne analize podatkov policijskega dela. Analize so se delale v obliki biltena, ki je bil namenjen ministru in generalnemu direktorju. V zadnjih desetih letih se je močno spremenilo delo te skupine, nekaj dela je odpadlo ali zamrlo, nastajalo je drugo. Danes skupina skrbi za zahtevnejše naloge s področja prekrškovnih zadev in ažuriranja baze podatkov na centralnem računalniku. Skupina sedaj rešuje zahtevnejše primere reklamacij plačilnih nalogov, vsakodnevno sodeluje s Finančno Upravo RS, Banko Slovenije, Ministrstvom za finance ter strankami v postopku. Prav tako organizira, usklajuje in kontrolira reševanje teh reklamacijskih zahtevkov med Policijo in ostalimi državnimi organi, ki so navedeni zgoraj. Sodelavke poleg ostalega skrbijo tudi za izmenjavo podatkov o prometnih nesrečah z zavarovalniškim združenjem. Skupina dnevno sodeluje z Centrom za prekrškovne zahteve, Uprave uniformirane policije, Generalne policijske uprave, s katerim skupaj rešuje najbolj zahtevne prekrškovne primere.

V Sektorju za IKT podporo smo v celoti združili podporo za končne uporabnike s področja IKT storitev. Smo vstopna točka za prijavo informacijsko-komunikacjskih zahtev in težav končnih uporabnikov v Policiji. Prav tako smo prvi nivo podpore, ki želi večino napak odpraviti že kar neposredno v kontaktu z uporabniki, s tem smo podporo spravili na višji nivo učinkovitosti.

6 OPERATIVNO TEHNIČNI SISTEMI

Obletnice, kot je na primer 60 let obstoja neke organizirane strukture na področju informatike in telekomunikacij, je primerno obeležiti in opravljeno delo prikazati s konkretnimi podatki in če je komu bližje, tudi z zgodbami o življenju ljudi, ki so pri delu sodelovali.

6.1 Laboratorij merilnikov

V zadnjem desetletju se je UIT GPU srečeval z vrsto strokovno tehničnih nalog na različnih delovnih področjih. Eno izmed njih je področje elektronskih naprav, ki obsega širok nabor opreme in sredstev za delo Policije. Pred 10 leti je takratni minister za notranje zadeve podpisal sistemizacijo delovnih mest, v kateri so bila na novo določena delovna mesta strokovnjakov v laboratoriju merilnikov, hkrati se je oddelek preimenoval v Oddelek za elektronske naprave in laboratorij merilnikov. Sledila so 3

leta vztrajnega strokovnega dela, katerega rezultat je bila podelitev akreditacije za kontrolo merilnikov po standardu SIST EN ISO/IEC 17020 v začetku januarja 2010. Kaj v stroki dejansko pomeni prejeti priznanje za strokovno usposobljenost za izvajanje strokovno tehničnih nalog – kontrol merilnikov za ugotavljanje skladnosti s predpisi, najbolje vedo tisti, ki so pri projektu aktivno sodelovali. Akreditacija je bila podeljena po strogem ocenjevalnem ciklusu, ki ga določajo mednarodni predpisi in zaveze akreditacijskih organov. V oddelku smo bili na dosežek upravičeno ponosni. Laboratorij je pričel z aktivnim izvajanjem kontrol merilnikov, upravne postopke, ki sledijo kontrolam merilnikov, pa je izvajal Urad RS za meroslovje. Tudi tuji strokovni ocenjevalci so v okviru rednih letnih presoj laboratoriju podeljevali laskave ocene in priznanja. Žal ima vsaka zgodba o uspehu lahko na poti tudi kakšen kamenček spotike. Urad RS za meroslovje je pričel prevzemati kontrole merilnikov pod svoje okrilje z navajanjem različnih razlogov, vezanih predvsem na racionalizacijo poslovanja. Konec leta 2015 je Urad RS za meroslovje izdal nova pravilnika za merilnike hitrosti v cestnem prometu in etilometre. V pravilnika so zapisali določilo, da postopke overitev, katerih sestavni del so kontrole merilnikov za merilnike, ki so v lasti države, izvaja Urad RS za meroslovje. Praktično izvajanje kontrol se je na uradu pričelo z januarjem 2016, ko je laboratorij z vednostjo vodstva Policije in MNZ prenehal izvajati akreditirane kontrole merilnikov. Konec leta 2016 je Policija tudi uradno preklicala akreditacijo in s tem zaključila strokovno zelo uspešno obdobje na področju umer-

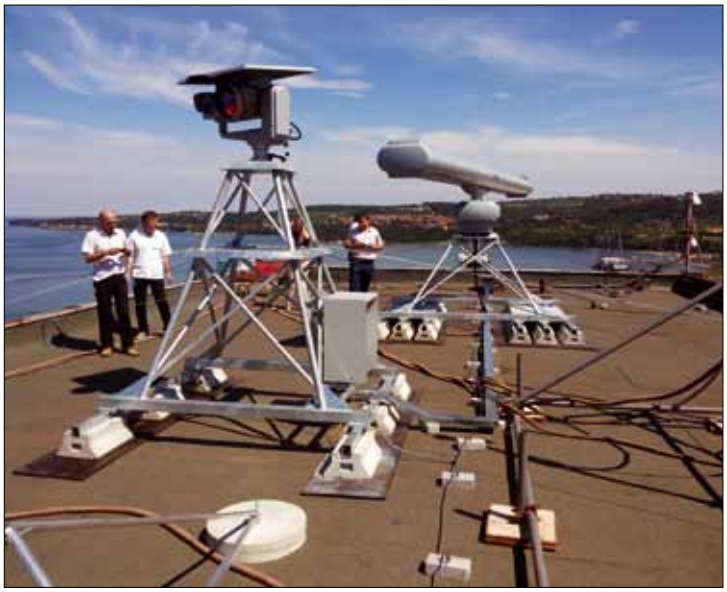
janja merilnikov hitrosti in etilometrov. Osebje laboratorija bo delo nadaljevalo na servisiranju merilnikov, načrtovanju uporabe novih merilnikov v policiji, logističnih nalogah med policijskimi enotami in uradom ter izvajalo druge naloge v oddelku.

6.2 Oprema za nadzor državne meje

Zahtevno področje predstavlja oprema za nadzor državne meje na morju. Poleg prenosnih in mobilnih naprav za nadzor mejnih področij na kopnem, ima Policija tudi radarski sistem za nadzor morja. Do sredine 2015 je v ta namen deloval radar na hotelu Bernardin v Portorožu, ki je le delno pokrival področje nadzora. Zaradi novih varnostnih okoliščin je bil sistem nadgrajen in dopolnjen z novo opremo. Celoten sistem danes sestavljata dva radarja, prvi je še vedno v Portorožu na Grand hotelu Bernardin, drugi pa v luki Koper. Pomemben dodatek k predhodnemu sistemu je sistem dnevno nočnih kamer, ki jih je mogoče usmerjati po podatkih iz radarjev. To omogoča natančno lociranje in videonadzor ter shranjevanje podatkov o raznovrstnih varnostno občutljivih dogodkih na morju. Celoten projekt je bil voden po sistemu »na ključ«, z zagotovitvijo optimalnih možnosti izbranemu ponudniku za pripravo takšnega sistema, ki bo Policiji v dejansko pomoč.

Pri večjih projektih radi kdaj rečemo, če le ne bi bilo »Murphyja«, s čimer poskušamo povedati, da se lahko tudi kaj zalomi. In res ni šlo vse gladko. Pri vzpostavitvi sistema smo se srečali z nepredvidenimi kompleksnimi tehničnimi vprašanji in reševanjem problematike skupaj s ponudnikom. Urad za informatiko in telekomunikacije je aktivno pristopil k reševanju. Povečane so bile prenosne zmogljivosti omrežja, izvedeni pregledi opreme na naši strani in njene tehnične zmogljivosti. Ponudnik je sodeloval in po različnih tehničnih prilagoditvah je sistem danes tehnično in operativno uporaben. Pričakujemo še nadaljnje aktivnosti, ki jih bodo narekovale praktične izkušnje policistov, ki s sistemom upravljajo. To sodi med običajno aktivnosti, ki so pomembne za razvoj IKT storitev ter opreme v Policiji. Dodati je potrebno še sodelovanje s Fakulteto za pomorstvo in promet ter Upravo RS za pomorstvo, ki za potrebe njunih aktivnosti uporabljata podatke iz sistema pomorskega radarja. Sodelovanje med temi deležniki je zgledno in v duhu dobrega sodelovanja in dobrih poslovnih praks.

To je le eden od sistemov za nadzor državne meje in sicer morske meje, ki smo ga uspeli nadgraditi in posodobiti v zadnjem obdobju. Za nadzor kopenske meje se uporablja ustaljene in preskušene sisteme ter naprave.




LJ Z6-38V

6.3 Oprema za nadzor prometa

Poleg običajne opreme za nadzor prometa, kot so merilniki hitrosti in alkohola, ki sodijo v našo pristojnost, so tudi video naprave za spremljanje varnostno občutljivih dogodkov na terenu z mobilnimi sistemi. Za ta namen smo preuredili kombinirano vozilo, ki smo ga uporabljali za številne aktivnosti. V vozilo smo vgradili robustno kamero, sisteme za prenos videa preko mobilnih omrežij, opremo za sprejem videa

s helikopterja. To vozilo se je izkazalo kot nepogrešljivo tehnično sredstvo policije, skupaj s strokovnjaki, ki z opremo aktivno upravljajo. Pomembnosti te opreme se je zavedalo tudi vodstvo Policije v protestih 2012/13. Na predlog generalnega direktorja policije smo se vključili v operativno delo policistov pri nadzoru prometa. Še posebej tovornega prometa, ki ga je težje nadzorovati s klasičnimi metodami dela in izvajati ustrezne ukrepe po Zakonu o pravilih cestnega prometa, Zakonu o motornih vozilih, Zakonu o voznikih in Zakonu o cestah. Aktivnosti so bile na začetku omejene na poskusno delo v smeri ugotavljanja, ali je izvajanje takšnega nadzora sploh primerno ali ne. Praksa je pokazala, da je bila ideja na mestu, znanje in usposobljenost naših sodelavcev za delo v tekočem prometu pa tudi. Danes je nadzor prometa na avtocestah redna oblika dela UIT GPU skupaj s policijskimi enotami. Še več! Zaradi uspešnosti je bilo v 2016 izvedeno javno naročilo za nakup dveh novih kombiniranih vozil, s katerima bomo nadomestili obstoječe vozilo, ki je

bilo v začetku aktivnosti ponovno aktivirano iz odpisanih vozil. Novi vozili bosta v primerjavi s starim sodobneje opremljeni, imeli bosta novo, moderno opremo za različne namene dela na terenu. Ob tem je pomembno dejstvo, da je tudi letalska enota policije izvedla posodobitev helikopterja z novo video kamero visoke ločljivosti, kar bo omogočalo kvalitetnejšo sliko za spremljanje dogodkov v operativnih štabih in sprejemanje odločitev.

6.4 Osebna video oprema

Zaradi potreb po rekonstrukciji postopkov policistov z občani - policisti so pri delu z občani v določenih primerih zelo izpostavljeni - in usmerjanja Posebne policijske enote (PPE) v primerih dogodkov s povečanim varnostnim tveganjem, je bilo potrebno zagotoviti primerno opremo. Izvedli smo testiranja video opreme za osebno rabo policistov. Rezultati so pokazali, kaj je potrebno šteti kot nujne in nepogrešljive lastnosti tovrstne opreme za delo policistov. To je nato vodilo v pripravo tehnične specifikacije za nakup opreme, ki je bila prvič praktično uporabljena že v času protestov 2012/13. Zaradi izjemne uporabne vrednosti opreme je bila obstoječa oprema dopolnjena in predana v redno uporabo v PPE. V času masovnih migracijskih tokov

konec 2015 je tako policija uporabila vsa razpoložljiva sredstva, ki so omogočala, da so policijske enote lahko delale v boljših pogojih. Zaradi izredne uporabnosti pri različnih policijskih postopkih se opremljanje operativnih enot nadaljuje, kolikor dopuščajo razpoložljivi viri.

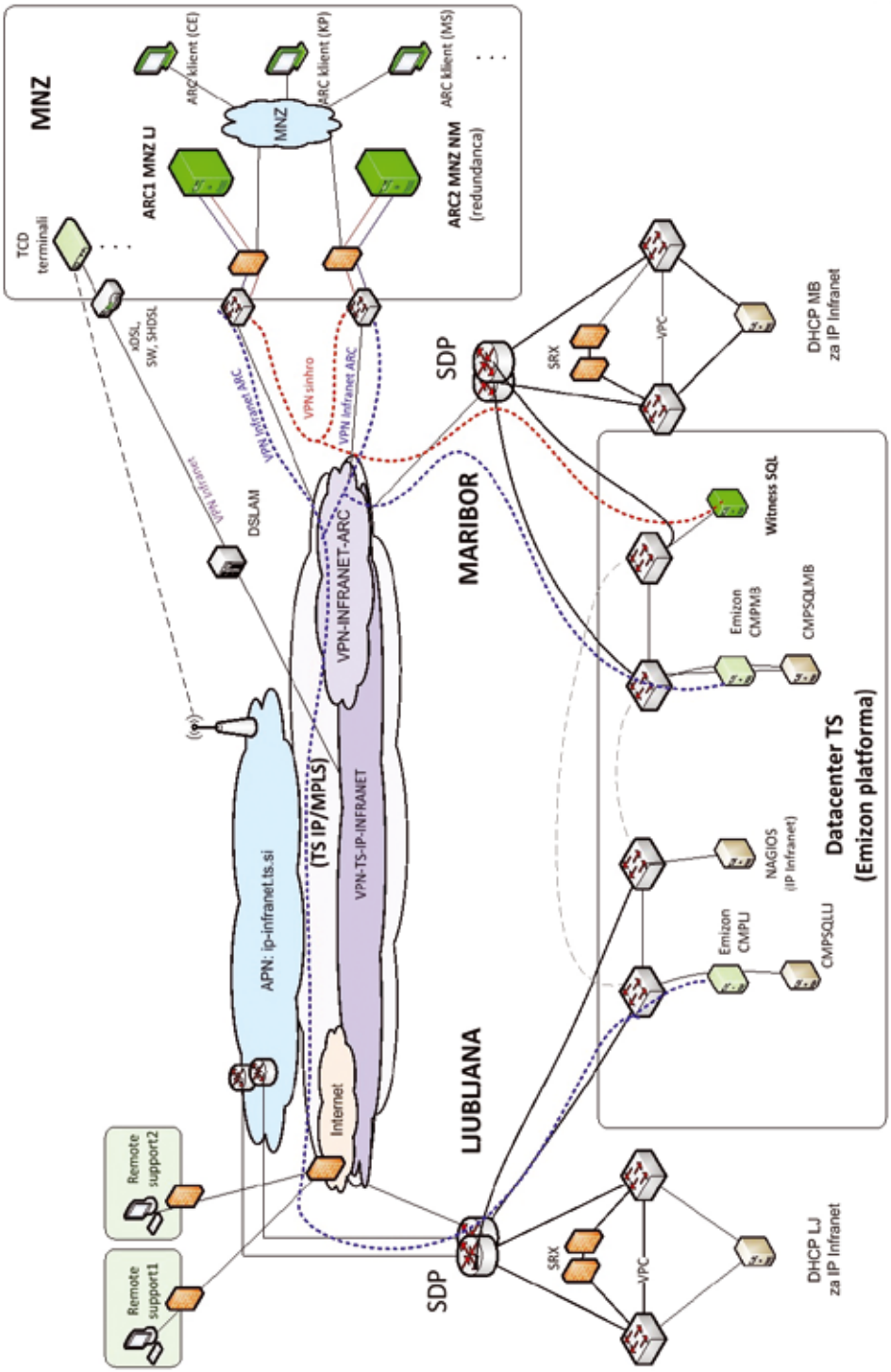
6.5 IP infranet – sistem za prenos alarmnih sporočil (2016 - 2017)

Obstoječi sistem za prenos alarmnih sporočil infranet je bil postavljen l. 2003, najprej na območju Generalne policijske uprave in Policijske uprave Ljubljana kot zamenjava za zastareli TUS sistem. V naslednjih letih smo sistem dograjevali po posameznih policijskih upravah in dokončali leta 2007. Po letih uspešnega delovanja, je prišel čas za zamenjavo. Razlogi so bili naslednji:

- obstoječi sistem ni več omogočal širitve (racionalizacija dežurne službe policije, varovane in ogrožene osebe, nepredvideni dogodki),
- leta 2010 smo od proizvajalca ASCOM prejeli obvestilo o prenehanju podpore za obstoječ sistem,
- znatno se je zmanjšala podpora pri vzdrževanju obstoječega sistema,
- zastarela tehnologija (DOS aplikacija); težave operaterjev z zagotavljanjem bakrenih povezav do mikrolokacij,
- znižanje stroškov.

Osnova za začetek iskanja ustrezne rešitve je bil predpisan standard za sisteme za prenose alarmnih sporočil Standard SIST EN 50136, ki predpisuje stalno 24/7 nadzorovano povezavo s časovnimi omejitvami glede hitrosti in zakasnitve prenosne poti za prenos alarmnega sporočila. Za ustrezno se je izkazala tehnologija, ki temelji na IP protokolu, ki zaradi zagotavljanja stalnega nadzora prenosne poti (zanesljivost), vzporedno uporablja še prenosno pot preko GPRS (GSM). Poleg tega je bila zaradi varnosti ena od glavnih zahtev tudi ta, da naš del sistema upravljamo in nadziramo ter določamo konfiguracijo sami. Omogočena je tudi integracija in uporaba obstoječega ITS policije.

Glavni del IP sistem se nahaja na lokaciji Telekoma Slovenije. ARC (Advanced Resource Connector) strežnika na strani naročnika se povezujeta v sistem preko VPN (Virtual Private Network) / APN (Access Point Name) Telekoma Slovenije. Izvedena je bila rešitev z dvema strežnikoma, ki imata vsak svojo podatkovno bazo. Operater poskrbi za kreiranje uporabnika Policija na portalu IP infranet, s katerim se dostopa do njemu dodeljenih terminalov ter pripadajočih ARC sprejemnikov. V administra-


MNZ
TCD terminali
ARC1 MNZ LJ
ARC2 MNZ NM (redundanca)
ARC klient (CE)
ARC klient (KP)
ARC klient (MS)
MNZ
xDSL SW, SHDSL
DSLAM
VPN Infranet ARC
VPN sinhro
VPN Infranet ARC
VPN Infranet ARC
SDP
SRX
VPC
DHCP MB za IP Infranet
MARIBOR
Witness SQL
Emizon CMPM3
CMPSQLMB
VPN-INFRANET-ARC
(TS IP/MPLS)
VPN-TS-IP-INFRANET
APN: ip-infranet.ts.si
Internet
NAGIOS (IP Infranet)
Emizon CMPLJ
CMPSQLLJ
Datacenter TS (Emizon platforma)
LJUBLJANA
Remote support2
Remote support1
SDP
SRX
VPC
DHCP LJ za IP Infranet

torskem portalu IP infraneta bo operater Policije upravljal in administriral pripadajoče priključke z vsemi želenimi parametri ter preko klientov nastavil usmerjanje signalov na izbrane lokacije nadzornih centrov. Vsi alarmi se pošiljajo na centralni ARC strežnik z bazo v redundanci. Posamezne lokacije (Operativno-komunikacijski centri) preko klientov sprejemajo le tiste alarme, ki se jih določi s konfiguracijo. Za povezavo med IP infranet strežniki na lokaciji operaterja in nadzornim strežnikom se vzpostavi namenski VPN.

Na ta način je Policija dobila moderen sistem za prenos alarmnih sporočil, ki deluje na IP protokolu, kar je osnova podatkovnega komuniciranja večine omrežij. Zagotovljena je možnost širitve priključkov, redundantna zgradba zagotavlja zanesljivost, sistem ima ustrezno tehnično podporo in zanj je zagotovljeno vzdrževanje.

6.6 Videonadzorni sistemi visoke ločljivosti

V letu 2009 smo s sredstvi Sklada za mejo izvedli prvo nadgradnjo oz. zamenjavo obstoječega analognega videonadzornega (VN) sistema s sodobnim sistemom visoke ločljivosti. Do leta 2012 smo opremili vse mejne prehode s sodobnimi VN sistemi. Ključni cilj je bila zamenjava zastarelih in dotrajanih videonadzornih sistemov na objektih Policije s sodobnimi videonadzornimi sistemi z IP tehnologijo visoke ločljivosti. Takšni videonadzorni sistemi omogočajo visoko kvaliteto posnetkov, ki v praksi ni primerljiva s slabo kvaliteto PAL videonadzornih sistemov. To dejstvo predstavlja veliko »dodano« vrednost, saj je v primeru varnostnih dogodkov te lažje analizirati, rekonstruirati, opraviti morebitno prepoznavo oseb ali stvari. Predvideni sistemi omogočajo tudi oddaljen dostop (centralni nadzor), ki ne prihrani le stroškov (potni stroški, stroški uporabe vozil, delovne ure zaposlenih, morebitne dnevnice), temveč tudi skrajša čas izdelav kopij videoposnetkov. Kopije lahko delamo na daljavo, ne da bi bilo pri tem potrebno obiskati posamezno lokacijo. Omogočeno je tudi daljinsko pregledovanje posameznih parametrov delovanja (delovanje kamer, snemanje oz. velikost arhiva), kar prav tako predstavlja nižanje stroškov. Na žalost nam zaradi pomanjkanja finančnih sredstev v zadnjih desetih letih na objektih v notranjosti ni uspelo izvesti nobene posodobitve oz. zamenjave obstoječih analognih videonadzornih sistemov.

6.7 Zadnjih 10 let radijskih sistemov Policije

Telekomunikacije predstavljajo hitro razvijajočo tehnologijo in glede na svetovne smernice in napovedi bo napredek v prihodnosti še hitrejši. Poudarek dela na podro-

čju radijskih komunikacij zadnjih 10-tih let je bil na dokončanju sistema digitalnega radia TETRA, ki se je začel graditi že v letu 2003. Zaradi finančnih omejitev nam ni uspelo vzpostaviti nacionalnega sistema in zato ostaja to še naprej najpomembnejša naloga za prihodnja leta. Sistem TETRA je tehnološko še vedno najoptimalnejša rešitev za govorne komunikacije po radijskem sistemu, saj druge tehnologije (npr. LTE, DMR) trenutno ne dosegajo zahtevanih funkcionalnosti. Potrebno je namreč upoštevati specifičnosti uporabnikov javne varnosti glede zanesljivosti, razpoložljivosti, zmožnosti in varnosti telekomunikacijskih sistemov. Prav sistem TETRA nam je omogočil, da smo v preteklem obdobju lahko vpeljali nove funkcionalnosti, ki so olajšale policijsko delo. Predvsem bi tu omenili novo dispečersko aplikacijo, ki se uporablja v operativno-komunikacijskih centrih in aplikacijo avtomatskega lociranja vozil (GPS/AVL).

Zadnje desetletje predstavlja velik tehnološki preskok v celotni zgodovini radijskih zvez policije, saj se je izvajala obsežna digitalizacija sistemov. Toda razvoj gre z nezmanjšanim tempom naprej in nova omrežja prihodnosti bodo nudila bistveno hitrejše prenose podatkov, kar bo povečalo nabor možnih funkcionalnosti. Trend modernizacije je zaznati tudi v svetovnem merilu, vendar je potrebno imeti določeno mero previdno-

sti. Trenutno namreč še niti ena država na nacionalnem nivoju ne uporablja le širokopasovnih radijskih sistemov za vse vrste komunikacij, ki jih potrebujejo uporabniki javne varnosti.

Z operativnega stališča so bile radijske komunikacije Policije v zadnjem desetletju postavljene pred velike izzive. Kot najpomembnejši operativni akciji lahko navedemo predsedovanje Slovenije Evropski Uniji in migrantsko krizo. Oba dogodka sta bila časovno daljša, potekala sta na velikem geografskem področju in tudi potrebe po prometnih kapacitetah so bile velike. Poleg omenjenih aktivnosti, je bilo realizirano tudi veliko število drugih operativnih akcij in varovanj. Kljub omejitvam radijskega pokrivanja obstoječega sistema TETRA, so bile vse akcije uspešno realizirane.

Vsekakor moramo v tem sklopu omeniti tudi hudo preizkušnjo, ki je doletela vse delavce policije - žledolom v začetku leta 2014. Veliko škode je bilo takrat povzročene tudi na radijskih sistemih policije. V začetni fazi omenjene naravne nesreče je prišlo do najobširnejšega izpada oskrbe določenih področij z električno energijo. Zaradi dolgotrajnega izpada elektrike tudi akumulatorski sistemi na gorskih objektih niso zdržali. Delavci s področja radijskih komunikacij smo se skupaj s predstavniki drugih služb trudili v največji možni meri zagotavljali ustrezno delovanje sistemov. Pri tem smo uporabljali vse razpoložljive agregate in rezervne antenske sisteme ter s tem dosegli,

da naši uporabniki na terenu niso imeli večjih težav s komuniciranjem po radijskih sistemih. Aktivnosti so potekale v zelo težkih pogojih, vendar smo bili kljub temu pri našem delu uspešni. V obdobju, ki je sledilo žledolomu, je bilo potrebno sanirati nastalo škodo, predvsem na komponentah, ki so instalirane na antenskih stolpih. Delavci Oddelka za radijske komunikacije so z zavzetim in strokovnim pristopom prispevali rešitve, ki so omogočale policijskim uporabnikom realizacijo operativnih nalog.

Zgodovina radijske tehnologije je zelo dolga, med največjimi imeni na tem področju pa je tudi izumitelj, ki je začel svojo pot v naši bližini. V lanskem letu je namreč minilo 160 let od rojstva Nikole Tesle, ki so mu šele po smrti priznali izumiteljstvo na radijskem področju. Današnja vrsta izumov je sicer drugačna, toda brez teh dosežkov preteklosti, ne bi imeli tehnologije, ki nam danes lajša življenja.

6.8 Sodelovanje pri migrantski problematiki

Urad za informatiko in telekomunikacije (UIT) je bil v drugi polovici leta 2015 močno vpet v reševanje migrantske problematike v prvi vrsti s tehničnega vidika. V sprejemnih centrih je bilo nujno čim prej zagotoviti vse pogoje za izvajanje registracije migrantov. Taki centri so bili vzpostavljeni v Stari livarni v Dobovi, v bivšem objektu Beti v Dobovi, na železniškem mejnem prehodu (ŽMP) Dobova, na mejnem prehodu Obrežje, v šotorišču v Središču ob Dravi, na mejnem platoju v Šentilju, v Integralu Lendava, na Vrhniki in v sejmišču v Celju. Določene lokacije je bilo potrebno za čas mirovanja centra tudi protivlomno varovati. Vsa dela je UIT izvedel strokovno in učinkovito. Kot velik dosežek ocenjujemo, da smo na ŽMP Dobova v prostorih fito-veto, v slabem dnevu vzpostavili 25 registrirnih mest in to tik pred 1. novembrom, kar je drastično zmanjšalo število migrantov v Dobovi. Iz lastnih virov smo zagotovili strojno opremo in s pomočjo operaterjev vzpostavili omrežne povezave v ITSP. Ob prihodu hrvaškega vlaka z več kot 1000 migranti - bili so tudi po štirje taki vlaki na dan - je bilo potrebno izvesti registracijo migrantov in jih na različne načine s slovenskimi prevoznimi sredstvi prepeljati na drugo lokacijo v Sloveniji. Naslednji pomemben dosežek je bil, da smo v sodelovanju z Oddelkom za informatiko in telekomunikacije, Službe za operativno podporo, Policijske uprave Novo mesto in zunanjimi izvajalci vzpostavili in zagotovili delovanje 35 registrirnih mest v šotorišču Livarna v Dobovi v roku manj kot 20 ur. Tako opremljen registracijski center je omogočil boljše pogoje za delo policistov.

Vključili smo se tudi v sistem nudenja kadrovske pomoči. Enota UIT je štela 10 policistov. Vsi policisti so delovali v delovnih uniformah z vsemi prisilnimi sredstvi. Delovali so na območju Policijske uprave Novo mesto, najprej na Policijski postaji

Brežice, kasneje pa v stalnem sestavu na Dobovi. Operativno delo so opravljali v oktobru, novembru in decembru 2015. V teh mesecih so policisti UIT opravili nadpovprečno veliko varnostnih pregledov oseb tudi z vidika policistov na lokalni ravni. To je več kot zgovoren podatek o zahtevnem delovanju.

Za konec lahko navedemo, da je bilo v zadnjem desetletju veliko uspešnih zgodb, več kot neuspešnih. Zato velja delo nadaljevati in sodelovanje med enotami Policije okrepiti. Varnostni izzivi, ki so pred nami upravičujejo naše aktivnosti in jih skozi preteklo prakso potrjujejo.

7 ZAŠČITA INFORMACIJSKO TELEKOMUNIKACIJSKIH SISTEMOV IN PODATKOV

Sektor za zaščito IKT storitev in podatkov (v nadaljevanju SZP) deluje na vsaj treh vsebinsko zaokroženih področjih. Področje informacijske varnosti in normativno področje zaokrožujeta tretje specialno tehnično področje, to je protiprisluškovalne preglede in TEMPEST meritve.

Skrb za stalno zagotavljanje primernega nivoja informacijske varnosti vsekakor izpostavlja nujnost vlaganja v posodobitve strojne in programske opreme ter zagotavljanje usposobljenega kadra. Kader mora poleg ustrezne izobrazbe in želje po stalnem usposabljanju, izkazovati tudi ustrezen nivo lojalnosti do ustavne ureditve in demokratičnih vrednot.

Nujnost vlaganja v informacijsko varnostno infrastrukturo je odziv na stalno prisotne grožnje Informacijskemu sistemu policije in zbranim varovanim podatkom, zato so prisotne tudi zahteve po posodabljanju, nagrajevanju sistema varovanja.

V letu 2011 smo pričeli z nabavo varnostne pregrade nove generacije, ki smo jo uspeli zaključiti v letu 2014. Požarne pregrade nove generacije imajo možnosti vpogleda in nadzora nad aplikacijami (prejšnje požarne pregrade so imele nadzor samo nad IP naslovom in portom), uporabljajo kategorizacijo spletnih strani, imajo možnost blokiranja dostopa do nevarnih kategorij spletnih strani, možnosti povezovanja dostopa uporabnikov s pravilnikom ter možnosti pregledovanja prometa za različnimi grožnjami. Pregledajo tudi promet zaradi odkrivanja in blokiranja različnih virusov, vohunske programe, črve in druge vrste zlonamerne programske opreme. Ravno tako delajo dekripcijo SSL in SSH šifriranega prometa in zagotavljajo, da se šifriran promet ne uporablja za prikrivanje neželene dejavnosti ali nevarne vsebine. S tem se zmanjša možnost uporabe dostopov in aplikacij, ki jih za svoje delo ne potrebujejo vsi uporabniki. To pripomore k zmanjšanju prometa v omrežju in zniža možnost potencialne okužbe.

V začetku leta 2017 smo v omrežje postavili nove požarne pregrade z dodatno funkcionalnostjo, ki bo v omrežju preprečevala napredno usmerjene napade v realnem času. Tovrstne napade antivirusni programi ne zaznajo. Z sistemom bomo

tako analizirali omrežni promet in datoteke, ki se prenašajo po omrežju. Na tako imenovanim peskovniku (angl. sandbox) teče virtualni operacijski sistem, v katerem orodje spremlja procese izvršljive kode in na podlagi teh vzorcev obnašanja se orodje odloči, ali je promet okužen ali ne. Tako lahko poleg znanih ranljivosti, z spremljanjem procesov na peskovniku, odkrije tudi neznane grožnje.

Orodje za upravljanje varnostnih dogodkov (SIEM) nam takoj (v realnem času) poda celovit pregled nad stanjem varnosti informacijskega sistema. Na enem mestu zbiramo vse zapise beleženja (log). Z zbiranjem in analiziranjem vseh podatkov iz strežniških, mrežnih in ostalih naprav omogoča učinkovito upravljanje varnostnih tveganj (sprotno alarmiranje in ukrepanje ob varnostnih kršitvah v realnem času) in ne šele takrat, ko je incident že napravil škodo. S SIEM sistemom sprejemamo boljše varnostne odločitve.

V letih 2015/16 smo sistema za enotno prijavo in upravljanje uporabniških identitet vzpostavili na novo. Kljub začetnim težavam postaja IDM orodje, ki nam omogoča vse več avtomatizacije pri upravljanju uporabniških identitet in s tem prihranek pri kadrovskih resursih, kar je v času varčevanja s kadri izjemnega pomena.

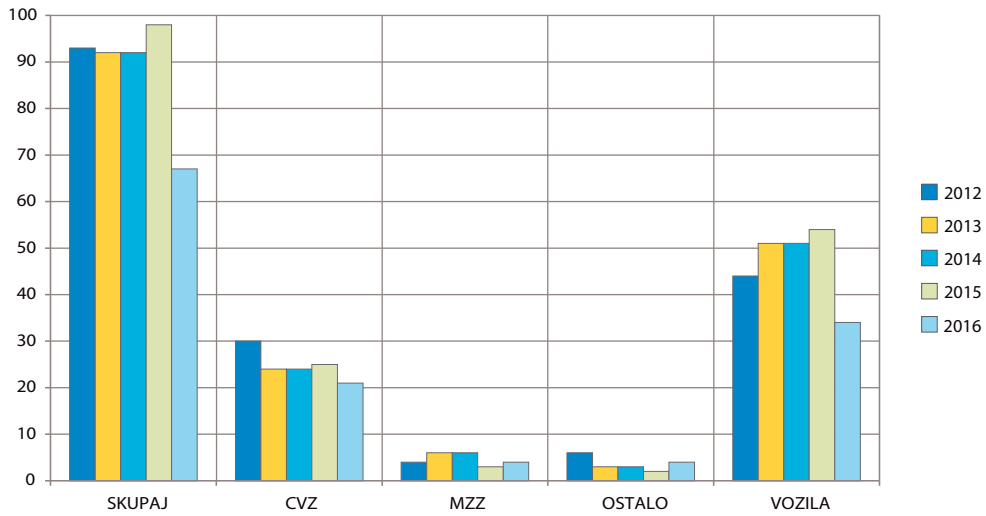
Z vpeljavo sistema za upravljanje uporabniških identitet smo na enem mestu združili upravljanje vseh uporabnikovih računov, kar je zmanjšalo čas potreben za administracijo teh podatkov in razbremenilo nekatere delavce. V enem koraku se tako uporabniku lahko dodeli več računov ali pa se istočasno zapre vse dostope do sistema. Zelo pomembna je tudi sledljivost in zgodovina sprememb podatkov, ki je v sistemu vidna in takoj dosegljiva za vse spremembe. V sistem ažurno uvažamo tudi razne evidence o dodatnih uporabnikovih dostopih in tako smo pridobili centralno evidenco, iz katere se pravilni podatki kopirajo na ostale podrejeno povezane sisteme. Vpeljali smo tudi možnost izpisa poročil, kar lokalnim skrbnikom sistemov omogoča, da hitro pridobijo želene podatke o vseh uporabnikih svoje enote. Ne nazadnje pa smo s povečanjem zmožnosti e-poslovanja sistema zmanjšali tudi obseg papirnatih obrazcev za več kot 20%.

Že skoraj desetletje na Policiji deluje tudi strežnik za izdajo uporabniških in strežniških certifikatov (Certifikatna agencija Policije), s katerim omogočamo svojim zaposlenim varno prijavo v sistem ITSP. Zaradi vedno močnejših računalnikov se algoritmi za računanje in ščitenje ključev spreminjajo in z ažurnimi posodobitvami opreme skrbimo, da so naši izdani certifikati skladni s priporočljivo varnostno politiko izdajanja certifikatov. Z novim sistemom bomo v kratkem omogočili tudi avtomatsko izdelavo certifikatov, kar bo zmanjšalo čas od uporabnikove zahteve za dostop do odobritve dostopa in predvsem skrajšalo administrativne postopke.

Informacijsko telekomunikacijski sistem policije za obravnavo tajnih podatkov višjih stopenj (ITSPTP) je deležen posodobitve zaščite in to z nacionalnimi rešitvami. Leta 2016 smo pridobili nacionalno opremo za ščitenje tajnih podatkov višjih stopenj in smo jo v začetku leta 2017 tudi implementirali. Pri tem izpostavljamo, da je oprema slovenskega izvora, kar pomeni, da je verjetnost posega tujih služb v delovanje opreme manjša. Dodatne prednosti so še bistveno nižja cena, hiter odziv v primeru napak ali okvar, možnost razvoja.

Eno od področij dela SZP je tudi izvajanje TEMPEST meritev - določanje t.i. TEMPEST con, kar izvajamo že od leta 2010, ko smo pridobili ustrezno opremo. Pojem TEMPEST zajema raziskave in proučevanje neželenega elektromagnetnega sevanja, pa tudi vrsto ukrepov za njegovo preprečevanje oziroma zmanjšanje. Meritve se izvajajo skladno z določenimi zakoni in uredbami. Kot metodologija za določitev con se uporabljajo NATO in EU standardi. Sama izvedba meritve se opravi na zaprosilo naročnika, predvsem ob vzpostavljanju varnostnih območij, v katerih se bodo obravnavali tajni podatki stopnje zaupnosti ZAUPNO ali višje, saj je opravljeno določanje TEMPEST con eden od pogojev za pridobitev dovoljenja, ki ga izda Urad Vlade Republike Slovenije za varovanje tajnih podatkov (UVTP).

Meritve izvajamo za državne organe kot tudi za zunanje uporabnike. V teh letih se je z razvojem tehnologije pojavila potreba po razširitvi frekvenčnega pasu, v kate-



Protiprisluškovalni pregledi v obdobju od 01.01.2012 do 30.11.2016

rem se opravljajo meritve. Posledično so se pojavili novi standardi EU in NATO, ki so za nas zavezujoči. Zato bo predvidoma v letu 2017 posodobljena tudi ta oprema. S tem bodo implementirani tudi posodobljeni NATO in EU standardi za izvajanje TEMPEST meritev.

Dotaknimo se še izvajanja protiprisluškovalnih pregledov. V preteklih petih letih je bilo izvedenih kar 467 različnih pregledov.

Investicije v posodobitev opreme za protiprisluškovalne preglede so bile izvedene v letih 2015 in 2016. V letu 2015 je bila izvedena nabava motilcev radiofrekvenčnega (RF) spektra. V letu 2016 pa nabava opreme ESMD s programsko opremo RAMON in NESTOR ter Orion. Poleg tega je bila izvedena nabava različnih prenosnih anten in dodatne opreme. Zaradi zahtev oz potrebe po večji mobilnosti v okviru izvajanja policijskih protiprisluškovalnih pregledov je bilo nabavljeno tudi kombinirano vozilo. Nove tehnologije zahtevajo tudi ustrezna znanja, zato je bila skupina za izvajanje protiprisluškovalnega pregleda tudi ustrezno usposobljena.

Izboljšanju zavedanja uporabnikov o nevarnostih povezanih s prisluškovanjem je bilo namenjeno usposabljanje o možnosti prisluha. V zadnjih petih letih smo v okviru medresorskega sodelovanja med Ministrstvom za notranje zadeve (MNZ) in Ministrstvom za zunanje zadeve (MZZ) izvedli 17 predavanj s področja prisluškovalne zaščite. Vsa predavanja so se odvijala na MZZ-ju in na različnih veleposlaništvih RS. Predavanja so bila izvedena tudi na prošnjo Banke Slovenije za guvernerja in ostale vodstvene delavce in šolsko skupino Centra za varnost in zaščito (CVZ), saj so protiprisluškovalno zaščito umestili v program za usposabljanje Policist specialist - varnostnik CVZ.

Področje informacijske varnosti, varstva osebnih podatkov, obravnave tajnih podatkov obravnavanih znotraj informacijskih sistemov in protiprisluškovalnih pregledov je bilo tudi predmet normativnega urejanja. Posodobljeno je bilo poglavje o zbiranju in obdelavi podatkov, tako v Zakonu o organiziranosti in delu v policiji kakor tudi v Zakonu o nalogah in pooblastilih policije. Tudi področje protiprisluškovalnih pregledov se je v specialni policijski zakonodaji ustrezno uredilo. Pri tem bi omenili tudi uvedbo novega pravnega pojma t.i. varovanega podatka, ki ga je opredelil Zakon o nalogah in pooblastilih policije. Spremembam področne zakonodaje je sledila dopolnitev tudi vseh podzakonskih predpisov.

V zadnjih letih je bil na področju policijskega informacijskega prava, kot svojstveno »dopolnilo« uveden koncept internih aktov s področja informacijske varnosti. Informacijske varnostne politike pomenijo dinamičen pristop k reševanju perečih informacijsko varnostnih vprašanj.

8 IZPOSTAVLJENI PROJEKTI

8.1 Integracije v mednarodne informacijske sisteme

Z vključitvijo Republike Slovenije v EU so se tudi za Policijo začeli projekti postopne integracije v različne nadnacionalne informacijske sisteme oz. intenzivnejše izmenjave podatkov z drugimi partnerskimi državami. Prvi mejnik je bilo leto 2007, ko smo se uspešno vključili v Schengenski Informacijski sistem prve generacije, temu dogodku pa je sledilo desetletje intenzivnih povezovanj.

8.1.1 SIS II – Schengenski informacijski sistem II. generacije

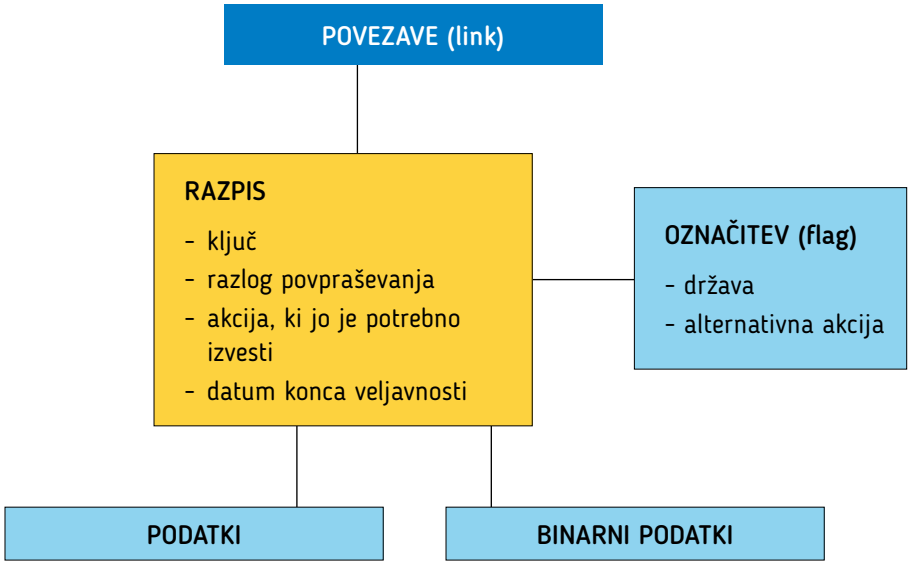
SIS II je bil projekt s katerim so bila povezana velika pričakovanja, vendar se je pri njegovi izvedbi pojavilo ogromno težav. Aprila leta 2013 so države uspešno izvedle migracijo iz SIS I na SIS II. Projekt je prinesel predvsem možnosti razširitve nabora podatkov, ki so na voljo članicam, vključno s fotografijami, prstnimi odtisi in relacijami med podatki. Projekt je bil tako formalno zaključen, izkušnje deset letnega sodelovanja v tej nalogi pa bodo koristne tudi za nove evropske IKT projekte.

SIS II je sestavljen iz:

- centralnega sistema (tehnično podprti del CS-SIS, kjer se hrani podatkovna zbirka in enotni nacionalni vmesnik NI.SIS),
- nacionalnega sistema (NS-SIS je vsaki državi lasten; predstavljajo ga nacionalni podatkovni sistemi, ki komunicirajo s centralnim sistemom; lahko vsebuje tudi celotno ali delno kopijo centralne podatkovne zbirke. Slovenija se je odločila, da nacionalne kopije SIS II ne bo implementirala pri svoji različici integracije) in
- komunikacijske infrastrukture (navidezno šifrirano omrežje, namenjeno podatkom v SIS II in izmenjavi podatkov med uradi SIRENE).

V schengenskem informacijskem sistemu se hranijo podatki o osebah, za katere je bil izdan razpis ukrepa in predmetih, ki se iščejo zaradi zasega (ukradeni predmeti) ali kot dokaz na sodišču v kazenskih postopkih.

Shema schengenskega razpisa



Sam katalog podatkov in vseh pripadajočih šifrantov je kar zajetna knjiga, ki obsega cca 200 strani zelo natančnih specifikacij in opisov po posameznih entitetah. Poleg same informacijske rešitve je v tem segmentu ena najkompleksnejših nalog tudi poenotenje šifrantov, saj je entitetni model kar bogat z atributi, ki so večinoma podprti z ustreznimi šifranti.

Vpogled v SIS II imajo poleg policije še druge inštitucije:

- Ministrstvo za zunanje zadeve pri postopku izdajanja vizumov (prepoved vstopa v Schengensko območje),
- Finančna uprava Republike Slovenije - Carina (kontrola vozil, plovil in izvenkrmnih motorjev, kontejnerjev, industrijske opreme in letal),
- upravne enote pri postopku izdajanja dovoljen za bivanje (kontrola na prepoved vstopa v Schengensko območje), pri izdaji orožnih listov (ukradeno orožje), izvajajo tudi razpise za ukradene listine seveda preko urada SIRENE,
- Enote za registracijo vozil (tehnični pregledi - ukradena vozila) in
- Azilni dom (vloge za azil).

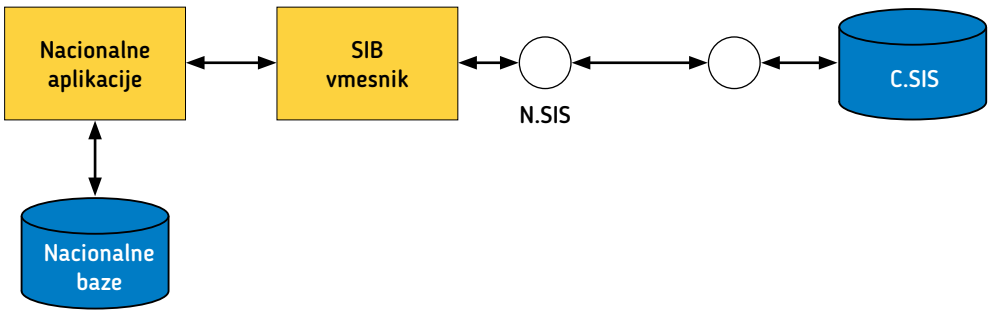
Razlika med SIS I in SIS II

SIS I je bil v svojem bistvu zelo enostaven sistem, ki je vseboval samo nekaj ključnih podatkov in je deloval po principu je/ni zadetka (hit/no hit). Vseboval je le osnovne podatke o osebah (priimek, ime, datum in kraj rojstva, državljanstvo, identifikacijo o nevarnosti osebe, vzrok razpisa in akcijo, ki jo je potrebno izvesti), kategorije razpisov so bile enake, prav tako je obstajala funkcija označevanja razpisov.

Pri predmetih so se evidentirali le podatki o vozilih in registrskih tablicah, listinah (izdanih in bianco), registriranemu denarju in orožju. Tudi o predmetih so se evidentirali samo ključni podatki (identifikacijske številke in nekaj drugih podatkov za lažjo identifikacijo). Vse ostale informacije so se hranile samo v uradih SIRENE in so se v primeru zadetka posredovale državi, kjer je do zadetka prišlo.

Nove funkcionalnosti so predvsem bistveno večji obseg podatkov, možnost pripenjanja biometričnih podatkov in dokumentov (EAW), možnost izvajanja povezav med razpisi ter bolj natančno je opredeljeno in implementirano zbiranje informacij o zlorabljenih identitetah. Poleg tega pa v tehničnem pogledu SIS II omogoča državam članicam tudi direktno preverjanje po centralni bazi podatkov tako, da nacionalna kopija sistema ni več obvezna. Za to različico implementacije integracije se je odločila tudi Slovenija, saj se je pričakovalo, da bi na ta način lažje, cenejše in enako kvalitetno zadostili vsem zahtevam.

Shema delovanja SIS II v RS



Namesto zaključka - kdaj se občani srečamo s tem sistemom

Schengenski informacijski sistem je v ozadju pri kar nekaj postopkih, s katerimi se kot državljani redno srečujemo.

Vsakič, ko potujemo v tretje države (države, ki niso del schengenskega pravnega red, npr. Hrvaška) se izvede mejna kontrola. Ob vsaki taki akciji se izvede povpraševanje tako po nacionalnih bazah kot tudi po schengenskem sistemu. V takih primerih se izvaja kontrola tako po bazah oseb kot tudi po bazi listin (ukradene listine).

Pogosto se dogajajo zadetki pri postopku registracije vozila. Tudi tu se izvede preverjanje po SIS in sicer po registrski tablici in številki šasije. Predvsem pri nakupu rabljenih vozil, ki so prišla iz tujine in zgodovina vozila ni bila ustrezno preverjena, je bilo kar nekaj primerov, ko je šlo za dobrovernega kupca pri ukradenem vozilu.

Če zgubimo ali nam je kako drugače odtujen osebni dokument, sami sprožimo akcijo v SIS in sicer ob vsaki prijavi na upravni enoti - avtomatično se izvede razpis listine v SIS. Enako se zgodi tudi za druge predmete, če so bili odtujeni s kaznivim dejanjem in je ob tem nastal policijski zapisnik. Seveda smo v tem primeru morali poznati ključne identifikacijske številke posameznih predmetov, saj brez tega izvedba ukrepa ni možna.

8.1.2 VIS – vizumski informacijski sistem

Sistem za podporo izdajanja vizumov je nastajal kot sestrski sistem SIS II. Infrastrukturno je precej podoben, v njem pa se hranijo na centralni lokaciji vse vloge prosilcev za vizume. Preko tega sistema se izvaja preverjanje veljavnosti in verodostojnosti vizuma ob prehodu preko schengenske meje ali ob ugotavljanju identifikacije osebe na ozemlju schengenskih držav. Je pa ta sistem v pristojnosti Ministrstva za zunanje zadeve, Policija v njem sodeluje kot eden ključnih uporabnikov.

Ključne funkcije sistema so:

- evidentiranje vseh vlog za izdajo vizuma (vključno z biometričnimi podatki),
- izvedba preverjanja prosilcev po operativnih evidencah,
- posvetovanje z drugimi državami v primeru, da je to zahtevano, o morebitnih zadržkih (rizične države) in
- iskanje po centralni bazi vseh vizumom (po osebi, listini ali prstnih odtisih).

Pred uvedbo VIS je policija na mejnih prehodih izdajala vizume preko lastne aplikativne rešitve, v ozadju pa se je prosilce preverjalo po nacionalni bazi in tudi po SIS bazah. Ker pa je VIS precej kompleksna aplikativna rešitev, ki zahteva tudi ustrezno nacionalno komponento in ker policija izda relativno malo vizumov je bil sprejet sklep, da ne bomo razvijali lastne rešitve, temveč se bomo pri postopku izdajanja vizuma povezali z MZZ in uporabili njihovo rešitev na enak način, kot jo uporabljajo

na diplomatsko konzularnih predstavništvih (DKP). Z dnem 1.9.2014 smo začeli za izdajo vizumov uporabljati novo aplikacijo VIZIS (last MZZ). Seveda pa smo morali razviti integracijske komponente in lastne rešitve za preverjanje po VIS.

Aplikacija **TravelDoc** - Preverjanje potnih listin je grafični uporabniški vmesnik za avtomatsko preverjanje oseb, listin in vozil pri prehodu meje z uporabo spletnih servisov za mejno kontrolo (eMisk) in preverjanje po VIS (SiVis). Avtomatsko branje potnih listin je mogoče z čitalci potnih listin ARH PRMC in DESKO Penta. Preverjati je mogoče vse potne listine (osebne izkaznice, potne liste, vize, nekatera dovoljenja), ki vsebujejo strojno berljiv (MRZ) zapis in ki ustrezajo ICAO standardu.

Ključna novost: Preverjanje viznih potnikov in ugotavljanje njihove istovetnosti preko prstnih odtisov v centralni VIS bazi, kar omogoča primerjavo v realnem času.

S čitalci dokumentov je možno preverjati tudi biometrične potne liste. To so potni listi z vgrajenim RFID čipom, na kateremu so shranjeni osebni podatki (MRZ (Machine Readable Zone) zapis, fotografija, prstni odtisi). Biometrični potni list je na sprednji strani označen z oznako (simbol čipa).

Biometrični potni listi se trenutno pojavljajo v različnih razvojnih fazah:

- BAC (basic access control) so potni listi, ki imajo na RFID čipu shranjene podatke o MRZ zapisu, fotografijo ter imajo možnost pasivne in aktivne avtentikacije.
- EAC (extended access control) so potni listi, ki imajo poleg vsega, kar imajo BAC potni listi, shranjene informacije o prstnih odtisih in/ali šarenici (angl. iris) ter imajo dodatne možnosti avtentikacije.

Naša aplikacija omogoča preverjanje obeh vrst biometričnih potnih listov. Tako lahko na zaslonu dobite izpisane naslednje podatke iz RFID čipa:

- fotografijo,
- 2 prstna odtisa,
- uspešnost posamezne avtentikacije.

Dostop do EAC podatkov (prstni odtis, šarenica) je mogoč le ob uspešni avtentikaciji. Za uspešnost le teh je potrebno imeti od države izdajateljice potnega lista pridobljene ustrezne certifikate. Ker izmenjava certifikatov med državami še ni popolnoma dorečena, je dostop do teh podatkov omejen.

Osnovno preverjanje vizumske nalepke po evidencah

Predpogoj ugotavljanje istovetnosti oseb preko prstnih odtisov po centralni evidenci VIS je strojno prebrana vizumska nalepka ali ročni vnos podatkov o vizumski nalepki.

Le ta se najprej preveri po nacionalni bazi (Fonetični indeks oseb - FIO), Interpolovi bazi (I24*7), centralni evidenci izdanih vizumov (VIS) in v SIS evidencah.

Če je številka nalepke najdena v centralni evidenci VIS se poleg obarvanja iskalnih polj, zastavic in semaforjev zeleno obarva tudi okno INFORMACIJA O ZADETKU, v katerem se izpišejo osnovni podatki o vizi in osebi iz centralne evidence VIS.

Zajem prstnega odtisa

Najprej s čitalcem prstnih odtisov zajamemo prstne odtise osebe, nato zaženemo modul za zajem prstnih odtisov, rezultat preverjanja je prikazan na spodnji sliki.

Namesto zaključka

Pri razvoju tako kompleksnih aplikativnih rešitev vedno skušamo najti najbolj optimalno različico implementacije. Zaradi korektnega sodelovanja z Ministrstvom za zunanje zadeve so bili stroški integracije v VIS in razvoja aplikativnih rešitev

bistveno nižji. Predvsem pa bi pomanjkanje kadrovskih resursov lahko vplivalo na kvaliteto in pravočasnost izvedbe vseh nalog. Vsekakor pa ta in podobne rešitve v veliki meri olajšajo izvajanje posameznih operativnih nalog policistom, ki morajo pri svojem delu imeti vedno več specialnih znanj.

8.1.3 INTERPOL

Generalni sekretariat INTERPOLA v Lyonu (IPSG), Francija, upravlja z globalnim policijskim komunikacijskim sistem I-24/7 in podatkovnimi zbirkami organizacije v katerih so razpisani ukrepi za iskane osebe in predmete (vozila, listine in orožje) na podlagi zahtev Nacionalnih centralnih uradov INTERPOLA iz 187 držav članic in mednarodnih organizacij s katerimi ima IPSG sklenjen poseben sporazum.

Razpisani ukrepi v I-24/7 so po vsebini tipizirani za izvajanje ukrepa prijetja iskane osebe in njene izročitve določeni državi, za pogrešane osebe, za sporočanje naslova bivališča, za zavrnitev vstopa v državo, za fotokopiranje listin in za izsleditev iskanih predmetov (enako kot SIS).

Interpol ima okvir svojega delovanja precej širši kot SIS II, predvsem pa je to edini kanal preko katerega se lahko izvaja sodelovanje z ne-EU državami. Gre tudi za najstarejši tovrstni informacijski sistem, članice so tako rekoč vse države. Tehnološko je drugače zastavljen od SIS II (starejši, neprestano se modificira, ne gre pa v celovito prenovo). Svoje baze je za on line preverjanje po ključnih iskalnih parametrih odprl relativno pozno. Tudi servisi, ki so na razpolago, so precej enostavni in zahtevajo logično dodelavo na nacionalni ravni. Kljub tem pomanjkljivostim, predvsem pa zaradi t.i. 'balkanske problematike', je bilo ključno, da smo izvedli v naših aplikacijah za preverjanje oseb, vozil in listin tesno integracijo tudi z I-24/7 sistemom (metoda FIND).

Končnim uporabnikom - policistom je tako omogočeno, da v skladu z nacionalno zakonodajo simultano preverjajo obstoj razpisov - ukrepov v centralnem računalniku policije za iskane osebe in predmete (listine in vozila):

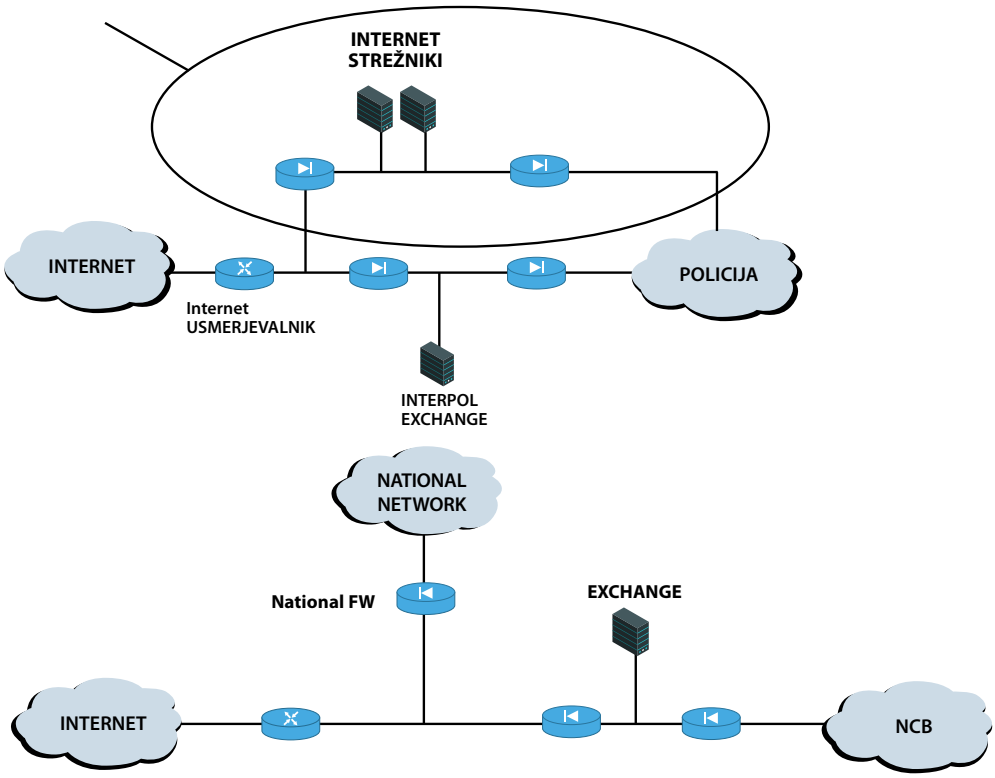
- na nacionalnem nivoju,
- v SIS in
- v podatkovnih zbirkah INTERPOLA.

V primerih, ko bo pri preverjanju prišlo do zadetka v I-24/7, bo policist v nacionalni aplikaciji dobil vpogled v status razpisa in njegove detajlne podatke. O vseh zadetkih policist z depešo obvesti pristojno službo. Trenutno delamo na optimizaciji tega obveščanja (popolna avtomatizacija pisanja poročila o zadetku).

Dvojnost zadetkov

Posebnost izvedbe takih aplikativnih integracij je pojav DVOJNIH ZADETKOV (države, ki so članice SIS in Interpol razpisujemo iskanja v obeh sistemih). Zaradi tega je potrebno zelo natančno urediti hierarhijo razpisov in temu prilagoditi tudi operativne akcije na terenu. Tako se v primeru, ko je za osebo razpisan ukrep v I-24/7 in v SIS, ima zadetek v SIS prednost pred zadetkom v I-24/7. Ker imajo nacionalni zadetki najvišjo prioriteto so integrirana iskanja implementirana na način, da se nacionalne zadetke prikazuje izključno na osnovi nacionalnih baz (čeprav so izvedeni vpisi v SIS in I-24/7, jih med temi zadetki ne prikažemo).

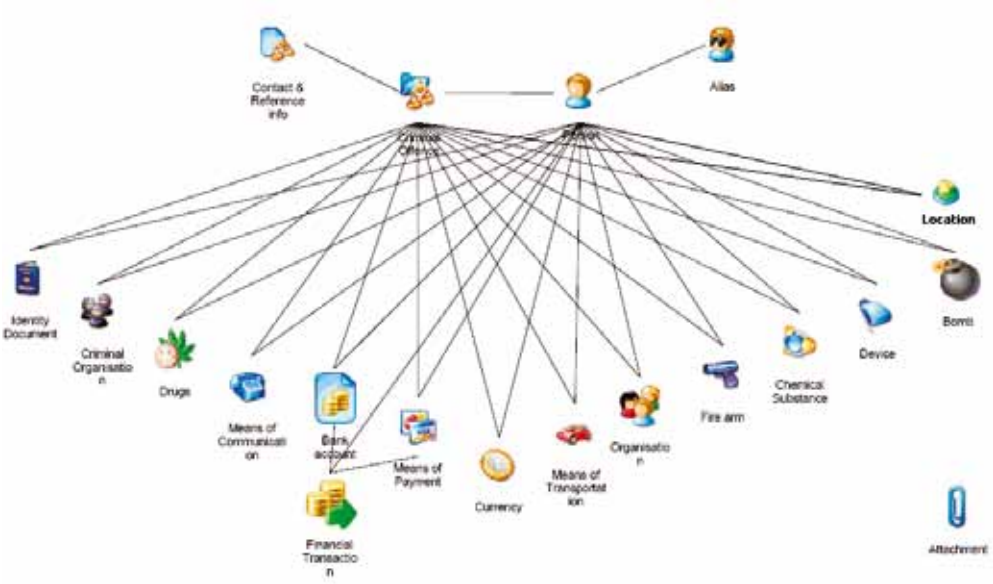
Shema izvedbe integracije v I-24/7



8.1.4 EUROPOL

Evropski policijski urad - Europol je 1. januarja 2010 postal agencija Evropske unije, pristojna za organizirani kriminal, terorizem in druge hujše oblike kriminala, ki prizadenejo dve ali več držav članic, tako da je zaradi obsega, pomena in posledic kaznivih dejanj potrebno skupno delovanje držav članic. Za vključitev Europola v preiskavo zadeve morajo biti izpolnjeni naslednji predpogoji: področje kriminalitete, obseg nalog, za katere je bil Europolu dodeljen mandat, vpletene so organizirane kriminalne združbe, zaradi kriminalne dejavnosti pa sta prizadeti ali povezani vsaj dve ali več držav članic. Ena od nalog nacionalne enote EUROPOLA pa je vnašanje in preverjanje informacij v Europolovem informacijskem sistemu (EIS). Za potrebe teh nalog smo pristopili k implementaciji t.i. SI data loaderja za EIS.

Entitetni modeli za potrebe kriminalistične analitike so bistveno bolj kompleksni kot evidence, ki služijo preverjanju oz. razpisom iskanih oseb ali predmetov. To nakazuje tudi skica EIS modela podatkov.

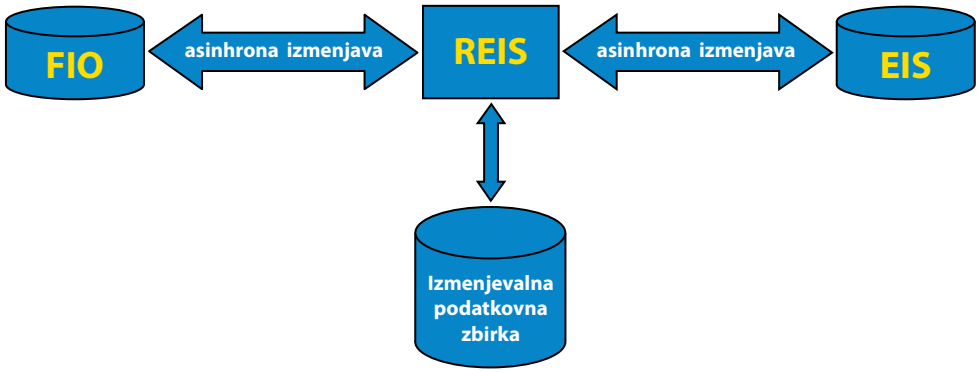


Prav zaradi kompleksnosti modela in postopkov sinhronizacije je bil projekt razdeljen na tri sklope:

- Sinhronizacija med nacionalno evidenco kaznivih dejanj in operativnih informacij (Fonetični indeks oseb - FIO) in EIS_SI.

- EIS_SI, ki je vmesni člen med FIO in EIS (middleware) in je sestavljen iz izmenjevalne podatkovne zbirke, podatkovno-procesne logike in grafičnega uporabniškega vmesnika.
- Sinhronizacija med EIS_SI in EIS (Europolov informacijski sistem).

Shema delovanja sistema



Takšna modularna zasnova z vmesnim členom je bila potrebna tudi zato, ker izmenjava podatkov med FIO in EIS temelji na asinhroni komunikaciji.

REIS je spletna aplikacija namenjena upravljanju razpisov v Europolovem informacijskem sistemu. Predstavlja osrednji del večjega sistema, ki skrbi za sinhronizacijo med policijskimi evidencami in Europolovim informacijskim sistemom. REIS zajema grafični uporabniški vmesnik ter poslovno logiko za upravljanje z razpisi. Shranjevanju stanj oz. sprememb, ki jih opravimo v aplikaciji, pa služi izmenjevalna podatkovna zbirka.

Uporabniki, ki so zadolženi za vnos podatkov v EIS dobijo preko namenske aplikacije na seznam kandidate, ki ustrezajo formalnim pogojem za vpis v EIS. Vendar se šele uporabnik odloči ali je posredovanje podatkov upravičeno ali ne. Na podlagi te odločitve se izvedejo vse zaledne funkcije.

Primer kompleksnejšega razpisa o obravnavanem kaznivem dejanju EIS:

Iskalni pogoji: Dogodek

Nazaj

Kontaktne informacije

Naziv	Tip
SIRENE 1	POLICIJSKE SLUŽBE

Dogodek [EIS]:

Nacionalna oznaka	KDT001_399159	Številka datoteke	399159
Vrsta dogodka	TERORIZEM	Nacionalni ustreznik	
Zadeva	FINANCIRANJE TERORIZMA		
Lokacija	ČRNA VAS,BRGLEZOV ŠTRADON 3		
Država	SLOVENIJA		
Datum	13.12.2011 07:15	Št. vpletenih oseb	4
Opombe	Ni opomb!		
Koda obravnave			
Pojasnilo za kodo HO	Ni pojasnila!		
Zanesljivost			
Zaupnost			
Vir			
Storjeno v prihodnosti?	NE		
Datum vpisa	23.01.2013 12:38:39	Datum zadnje spremembe	23.01.2013 12:38:39
Datum brisanja			
Podaljšanje razpisa	NE		
Utemeljitev podaljšanja	Ni utemeljitve!		
Trenutni status [akcija]	USPEŠNO [VNOS]		

Podrejene entitete

Povezana entiteta	Tip povezave
Bomba [LPTORO_198117]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Bomba [LPTORO_198118]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Bomba [LPTORO_198119]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Valuta [LPTDEN_100]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Valuta [LPTDEN_101]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Valuta [LPTDEN_102]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Valuta [LPTDEN_103]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Droga [LPTMAM_49]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Droga [LPTMAM_50]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA
Strelno orožje [LPTORO_198078]	UPORABLJENO ZA STORITEV KAZNIVEGA DEJANJA

Kot je razvidno iz entitetnega modela sistema EIS, je lahko vsaka entiteta del večje celote (drevesa) med seboj povezanih entitet. Aplikacija REIS nam v tem delu ponuja možnost »sprehajanja« po takšnem drevesu medsebojno povezanih entitet. Povezave so namreč tudi ključni del entitetnega modela sistema EIS.

Namesto zaključka

Čeprav to integracijo direktno uporablja zelo malo uporabnikov v policiji, pa brez posredovanja nacionalnih podatkov v EIS ni mogoče pričakovati EUROPOLOVIH asistenc pri preiskovanju hudih mednarodnih kaznivih dejanj. Le na ta način so našim preiskovalcem odprti dodatni viri podatkov, asistence na področju analitične dejavnosti in tesno sodelovanje z drugimi državami, ki preiskujejo iste osebe ali podobna dejanja.

8.1.5 PRÜM

S podpisom PRÜMSKE konvencije so bili vzpostavljeni pravni temelji za čezmejno izmenjavo podatkov o vozilih, DNK profilih in prstnih odtisih za pomoč pri preiskovanji hujših kaznivih dejanj. Nosilec izmenjave za DNK in prstnih odtisov je Policija, izmenjavo podatkov o vozilih pa upravlja MNZ.

Vozila

EUCARIS je komunikacijsko omrežje, ki omogoča sodelujočim državam izmenjavo podatkov o motornih vozilih. EUCARIS omogoča on-line preverjanje podatkov motornih vozil iz nacionalnih registrov držav, pridruženih v EUCARIS.

Za preverjanje v EUCARIS je narejena spletna aplikacija, ki nam omogoča preverjanje po nacionalnih registrih drugih držav. Dostop do te rešitve ima Urad SIRENE (Uprava kriminalistične policije, Sektor za mednarodno policijsko sodelovanje) ki za potrebe celotne policije izvede ustrezno preverjanje.

DNK profili

Rešitev za DNK profile je bolj avtorsko zasnovana. Že vzpostavitev centralne nacionalne evidence vseh profilov in integracija z analizatorjem je bila kar kompleksna naloga. Razvoj nacionalnega iskalnega modula, ki omogoča iskanje po nacionalni bazi DNK profilov po različnih kriterijih ujemanja (točno, srednje, mehko) je bil svojevrsten izziv, saj je bilo sodelovanje s forenziki izredno intenzivno, testno obdobje pa zelo dolgo.

Z implementacijo prümske izmenjave pa smo evidenco nadgradili še v mednarodno izmenjavo podatkov. Pri tej rešitvi smo tesno sodelovali z nekaterimi partnerskimi državami, ki so ponudile v uporabo zaključene komponente po posameznih funkcionalnostih (komunikacijski modul, iskalni modul), vendar je rešitev uporabna le, če so moduli vključeni v lastno aplikativno rešitev kot celoto.

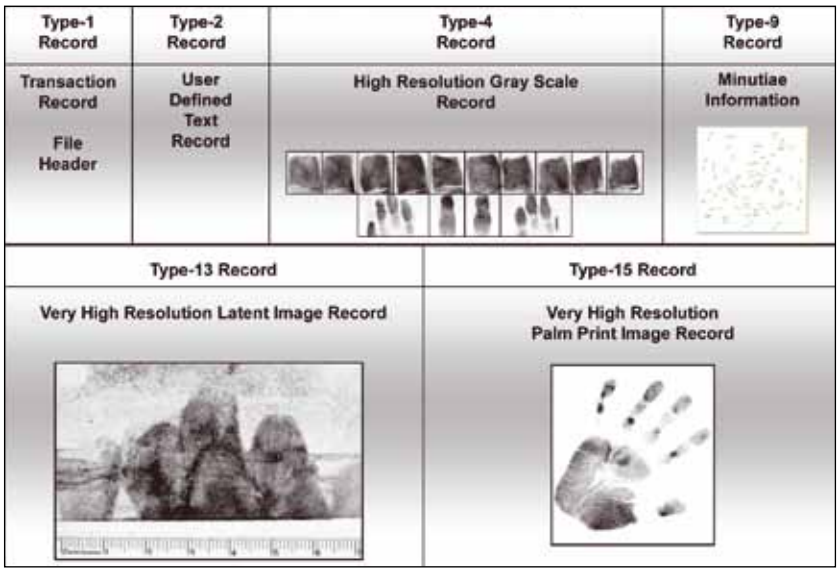
Rezultati te izmenjave so odmevni, saj je bilo na podlagi teh podatkov raziskanih kar nekaj hudih kaznivih dejanj tako v Sloveniji, kot tudi v tujini. So pa nadaljnje aktivnosti na tem področju usmerjene predvsem v širitev izmenjave podatkov proti balkanskim državam.

Delovno mesto forenzika

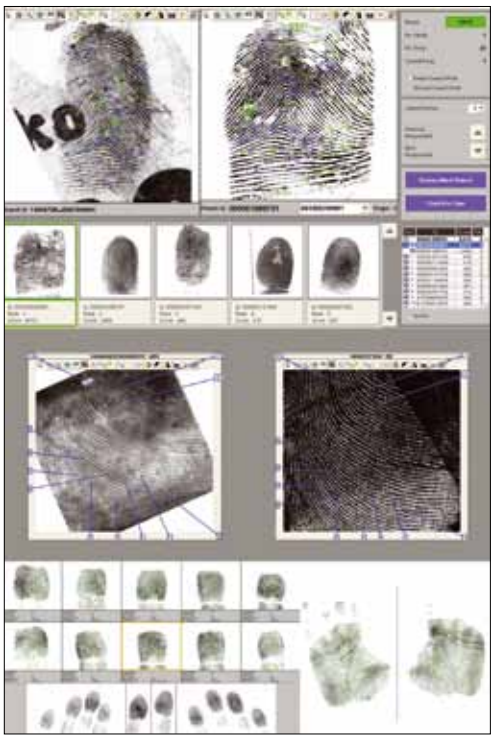
Prstni odtisi

Pri izmenjavi prstni odtisov je bilo potrebno pripraviti »work flow« aplikacijo (aplikacijo delovnega procesa), preko katere se izmenjujejo informacije o zadetkih, v ozadju pa je sistem za hrambo in prepoznavo prstnih odtisov (AFIS). Pri implementaciji tega sklopa izmenjav so bile aplikativne naloge bolj v ozadju. Z operativnega zornega kota sicer prstni odtisi zgubljajo na pomenu, vendar je kljub vsemu to še vedno pogosto uporabljena kriminalistično-tehnična preiskava predvsem pri preiskovanju klasičnih kaznivih dejanj.

Primer sheme Prümske daktiloskopske baze podatkov



Obrazec za zajem prstnih odtisov



Delovno mesto izvedenca za daktiloskop

8.2 Rešitev za sprejem klicev na številko 113

Klicni centri za sprejem interventnih klicev sodijo med najbolj kritične in kompleksne sisteme. Policija sprejema interventne klice na telefonsko številko 113. Državljani pričakujejo od policije hiter sprejem klicev in nemoteno delovanje še posebej v primeru izrednih okoliščin. Zaradi dotrajanosti opreme in stroškov povezanih z vzdrževanjem klicnih centrov, je bila sprejeta odločitev o lastnem razvoju aplikacije za podporo delu klicnega centra.

Na letnem nivoju na klicnih centrih sprejmejo preko pol milijona klicev, od katerih jih je med 35-40 % interventnih. Interventni klici so tisti, zaradi katerih je potrebna napotitev policijskih sil na kraj dogodka. Statistike kažejo, da pomeni vsak interventni klic za OKC še vsaj sedem dodatnih klicev. Zavedati pa se je potrebno, da se za temi podatki skrivajo zgodbe ljudi, ki potrebujejo in pričakujejo pomoč policije.

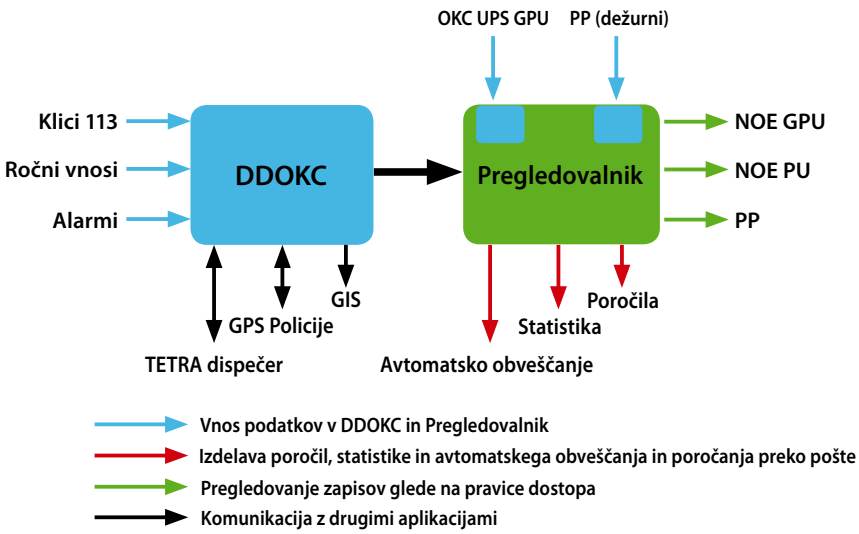
Okolje klicnega centra je kompleksno in narejeno po zahtevah naročnika oziroma potrebi uporabnikov klicnega centra. Glede na vse pridobljene izkušnje s klicnimi centri različnih generacij, smo se v policiji dobro zavedali dejstva, da načrtovanje in izdelava okolja klicnega centra zahteva širok spekter znanj s področja telekomunikacij in informatike. Skozi leta uporabe ter rešitve različnih proizvajalcev se je pokazalo, kakšne rešitve dejansko potrebujemo.

Tako smo si zastavili cilj posodobiti telekomunikacijsko infrastrukturo klicnih centrov ter razviti in uvesti novo aplikacijo za celovito upravljanje z interventnimi klici v operativno komunikacijskih centrih Policije. S tem smo dosegli boljšo podporo delovnemu procesu in nižje stroške vzdrževanja. Pri tem je potrebno poudariti, da gre za kritično storitev, od katere so posredno odvisna človeška življenja, materialne dobrine, stopnja varnosti v državi ter ugled policije v javnosti.

Ključne komponente sistema so:

- Telefonska centrala;
- Aplikacija DDOKC za podporo operaterjem;
- Aplikacija KC113 za vpogled v zadeve ustrezno pooblaščenim drugim delavcem policije;
- Integracije z drugi aplikativnimi rešitvami in zalednimi sistemi.

Shema sistema DDOKC in Pregledovalnika



8.2.1 Podpora telefonski centrali

Zaradi nezadostnih praktičnih izkušenj pri razvoju modulov povezanih s CTI (Computer Telephony Integration) aplikacijami, je bila aktualna dilema glede razvoja potrebnih komponent povezanih s funkcionalnostimi CTI strežnika. Posledica konkretnih uporabniških zahtev (npr. fleksibilnost določanja minimalnega števila prijavljenih agentov klicnega centra) je pripeljala do odločitve, da upravljanje s klici in celoten nadzor nad delom agentov klicnega centra prevzame CTI strežnik (značilnost modernih CTI rešitev). Za ta namen smo uporabili odprto kodno platformo za razvoj telekomunikacijskih storitev Asterisk oziroma distribucijo Elastix. Zaradi specifične uporabe Asterisk-a, je bil potreben lasten razvoj programskih modulov, ki omogočajo upravljanje Asteriska v skladu z informacijami, ki jih pridobi preko vmesnika CSTA (Computer Supported Telecommunications Applications).

Pri razvoju potrebnih modulov nove rešitve (CTI strežnika in odjemalcih na delovnih postajah), so bila uporabljena standardna orodja. Veliko pozornosti smo namenili tudi segmentom vzdrževanja (jasno definiranje odgovornosti in mejne kontrolne točke) ter vključitvi v krovni nadzorni sistem (informacije dostopne tudi agentom storitvenega centra za pomoč uporabnikom - Help Desk), v katerem je mogoče nadzorovati stanje ključnih modulov.

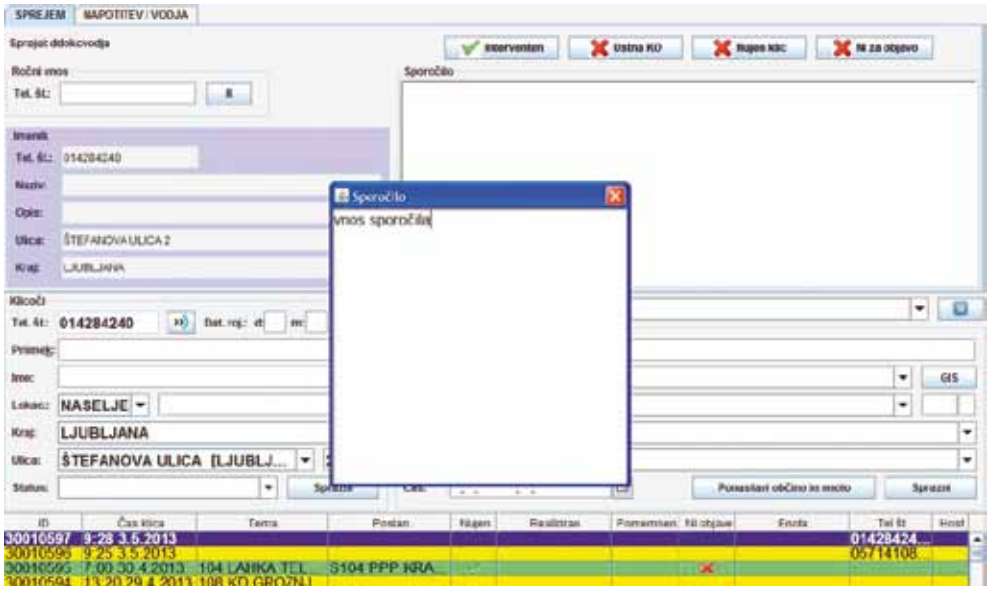
8.2.2 Monitoring

Funkcionalnost, ki omogoča hiter pogled uporabnika ali upravljavca na glavne komponente sistema (Linux, Asterisk, DB2, CTI aplikacija, Strežnik (osnovno »zdravje«), itd.) in je ključnega pomena pri zagotavljanju hitrega odzivanja na morebitne probleme.

8.2.3 Dnevnik dogodkov DDOKC

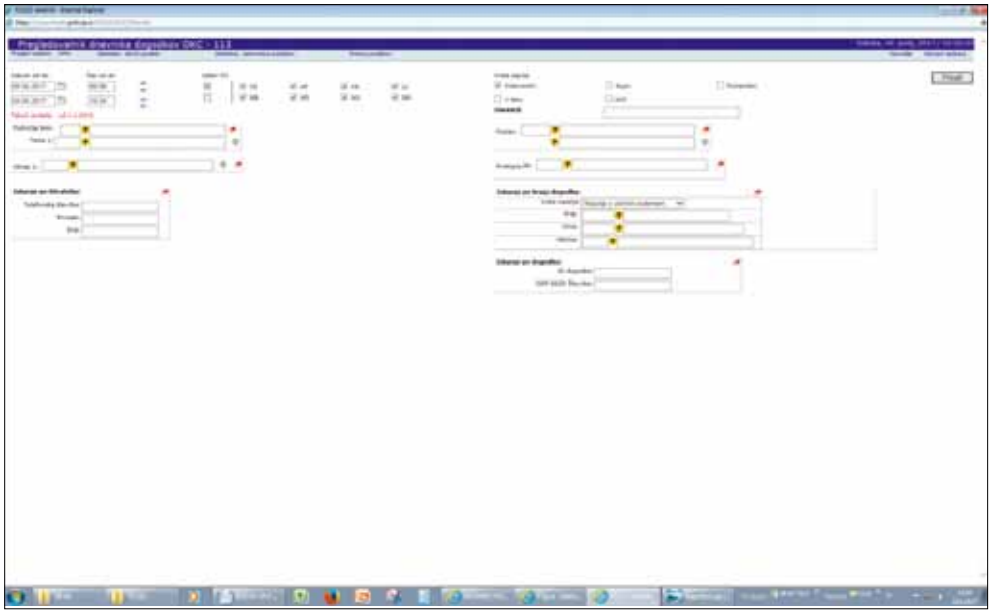
Dnevnik dogodkov je računalniška aplikacija, namenjena delavcem Operativno-komunikacijskega centra (OKC) in omogoča celovito beleženje klicev občanov na številko 113.

Po funkcionalnostih je aplikacija razdeljena na naloge vodje izmene in operaterja. Beležijo se vsi prispeli klici na 113, njihova vsebina, izvedene napotitve policijskih sil, izvedeni ukrepi, obveščanje pristojnih organov služb in oseb ter druge dejavnosti OKC. Ob klicu na 113 se podatki o kličočem in njegovi lokaciji pridobijo preko spletnih servisov pri ponudnikih telefonskih storitev, lokacija se prikaže tudi v GIS komponenti. Ob zaključku akcije se vpišejo zaključne ugotovitve/poročilo in zaključni časi. Poleg tega so podprte osnovne telefonske funkcionalnosti: digitalna tipkovnica, hitro klicanje, obravnava čakalnih vrst, povratni klici, zgrešeni klici, ročni vnosi v primeru izpada, snemanje pogovorov, poslušanje posnetkov pogovorov (na telefonu ali zvočniku), omogočeno je tudi pogovorno okno med operaterji za interno komunikacijo.

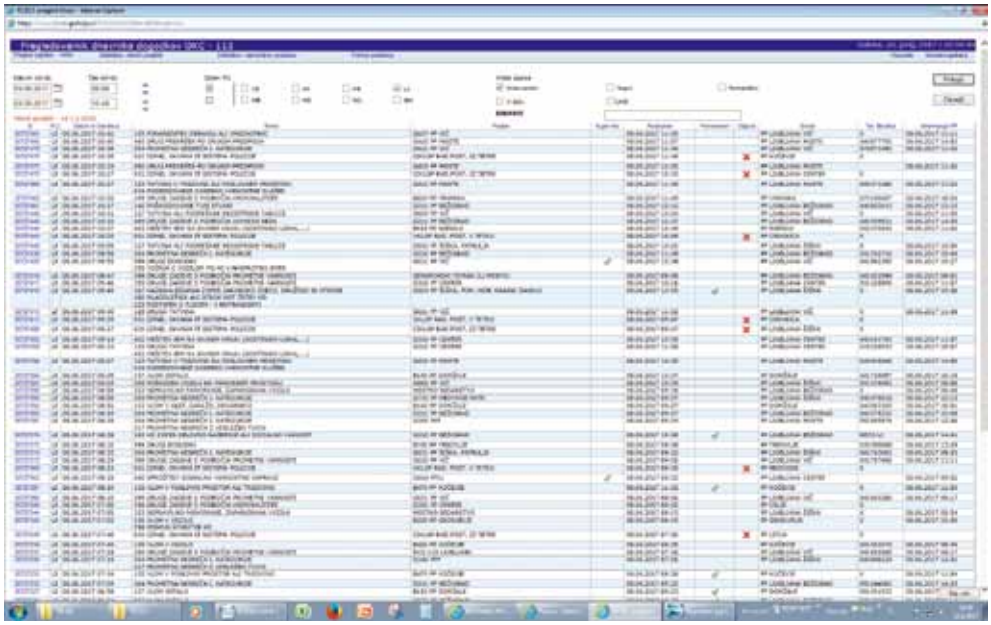


8.2.4 Pregledovalnik KC113

Podatki iz aplikacije DDOKC se sproti prepisujejo tudi na centralni računalnik, kjer so dostopni preko Pregledovalnika KC113 tudi drugim, ustrezno pooblaščenim delavcem policije. S tem konceptom smo razbremenili osnovno aplikativno rešitev vseh



sekundarnih funkcionalnosti, ki bi lahko vplivale na zanesljivost njenega delovanja in odzivne čase. Že iz imena je razvidno, da služi predvsem vpogledom v aktualno dogajanje, omogoča sicer vnos dodatnih opisov in poročil, ko posamezni dogodek prevzamejo v obravnavo druge službe policije in s tem zaokrožitev vseh informacij o dogodku na enem mestu. V tem sklopu je tudi izvedena integracija s podatkovnim skladiščem in podpora statističnemu poročanju ter dodatno obveščanje.



Zaključek

S projektom prenove rešitve za podporo delu OKC smo po poslovni plati z lastnim in zunanjimi kadri (zagotovljena kontinuiteta razvoja) postavili popolnoma nove aplikativne rešitve (uvedli smo nekaj novih uporabniških funkcionalnosti, ki jih še dodajamo). S tem smo dosegli neodvisnost od zunanjih ponudnikov storitev in povečali zanesljivost delovanja sistema kot celote (sedaj podpora 24*7). V tehnološkem smislu so vse ključne komponente zamenjane z novejšimi, zmogljivejšimi in zanesljivejšimi (telefonske centrale, strežniki, uporabljeno standardno razvojno orodje) in zvedene so bile integracije z drugimi lastnimi aplikativnimi rešitvami (GPS, Dispečer, ISPP).

8.3 Mobilne rešitve

8.3.1 Uporabljene mobilne rešitve

V policiji obstajajo mobilne rešitve že več let.

- General Dynamics Itronix – Duotouch

Za izvedbo mobilnega preverjanja na schengenski meji na vlakih so bile uvedene naprave General Dynamics Itronix - Duotouch. Gre za popolnoma samostojne naprave z zaslonom za dotik. V okviru priprav na prvo schengensko evalvacijo je bilo za potrebe Postaje mejne policije Dobova nabavljenih 5 naprav. Predvidena je bila uporaba za mejno kontrolo z vzpostavitvijo VPN povezave preko GSM omrežja. Te naprave so se v letu 2011 nadomestile z napravami Datastrip.

Prejšnje rešitve: Itronix Duotouch za schengensko preverjanje na vlakih

- Datastrip

V letu 2011 je bilo v uporabo predanih 50 naprav Datastrip (nabava iz Sklada za meje). To so popolnoma samostojne naprave, katerih prednosti so integrirani čitalci (OCRB zapisa in RFID) ter namensko razvita mobilna aplikacija za mejno kontrolo (oz. druga preverjanja). Tako je policistom omogočeno praktično popolnoma avtomatizirano preverjanje pri mejni kontroli, vključno z možnostjo preverjanja biometričnih podatkov (npr. v viznem informacijskem sistemu VIS). Aplikacije so bile razvite z lastnimi viri. Celotna rešitev je prav gotovo primer dobre prakse v evropskih policijah.

Obstoječe rešitve: Datastrip za schengensko preverjanje na vlakih ter PPIU

- specialni prenosniki Bormann

Že nekaj časa so v Specializirani enoti za nadzor državne meje (SENDM) GPU in Policijskih postajah za izravnalne ukrepe (PPIU) v uporabi posebni prenosniki Bormann. Nabava 50-ih naprav je bila izvedena s pomočjo Sklada za meje. Osnovni namen je mobilni dostop do ITSP zaradi preverjanja. Dodatne, posebej mobilnemu načinu dela prilagojene aplikacije, torej ni. Posebnost je robustnost naprav ter certifikat za varno uporabo naprave med vožnjo.

Obstoječe rešitve: Bormann za schengensko preverjanje med vožnjo SENDM ter PPIU

- mobilni dostop do ITSP (običajni prenosniki)

Med mobilne rešitve spadajo tudi druge (npr. storitev potisne pošte Blackberry, Tetra radijske postaje pa omogočajo enostavno preverjanje s pomočjo kratkih sporočil sistema Tetra).

8.3.2 ePolicist

V slovenski policiji je že dalj časa prisotna potreba po rešitvah za delo policistov v mobilnih pogojih. Rešitve za dostop do informacijsko telekomunikacijskega sistema Policije (ITSP) so že v uporabi, a je s tem omogočena zgolj uporaba obstoječih aplikativnih rešitev ter nekaj drugih rešitev, predvsem namenjenih za izvajanje mejne kontrole.

ePolicist
Tretji partner v patrulji

Večje pozitivne učinke si že ves čas obetamo z uvedbo prave mobilne rešitve, ki bi policistom omogočala izvedbo postopkov v mobilnih pogojih v celoti. Informacijska

podpora izvajanja določenih policijskih postopkov v mobilnih pogojih dela je vsekakor smiselna. ePolicist ne pomeni le preverjanja po evidencah, pač pa popolno oz. delno izvedbo postopka. Predvsem gre za nekatere postopke s področja prometa, kjer bi bili učinki vidni zelo hitro.

Cilji projekta:

- razviti celovito mobilno rešitev, ki bo policistom omogočala izvedbo preverjanj oseb, listin in vozil v evidencah na prenosni mobilni napravi na terenu,
- razviti celovito mobilno rešitev, ki bo policistom omogočala izvedbo celotnega postopka izdajanja plačilnega naloga ter drugih postopkov s področja prometne varnosti na prenosni mobilni napravi na terenu v stoječem policijskem vozilu oz. njegovi neposredni okolici,
- v rešitev vključiti še ustrezno ovrednotene postopke z drugih področij policijske dejavnosti (javni red, kriminaliteta, ...).

Obseg:

- Razvoj in vzdrževanje programske opreme (aplikacije) za mobilne delovne postaje, prilagoditev centralne programske opreme (centralna baza za sprejem dokumentov in podatkov iz mobilnih delovnih postaj ter vmesniki), vzpostavitev povezav, integracija in upravljanje uporabniške programske opreme ter zaščita;

74

ePolicist v praksi

- Najem mobilnih storitev (mobilne naprave in prenos podatkov za vsako delovno postajo);
- Usposabljanje policistov za delo z mobilno rešitvijo;
- Promocija in druge aktivnosti informiranja in obveščanja;
- Nakup strojne opreme.

Predvideni rezultati projekta

Predvideni rezultat projekta je izvajanje identificiranih in potrjenih postopkov s prekrškovnega področja (prometna varnost, ...) na mobilni napravi v vozilu in njegovi neposredni bližini ter posledično izdajanje plačilnih nalogov ter možnost plačila globe na kraju tudi z uporabo POS terminala. Predvideni rezultat projekta je tudi izvajanje postopkov s področja preiskovanja kaznivih dejanj in drugih področij policijskega dela s pomočjo mobilne informacijske rešitve.

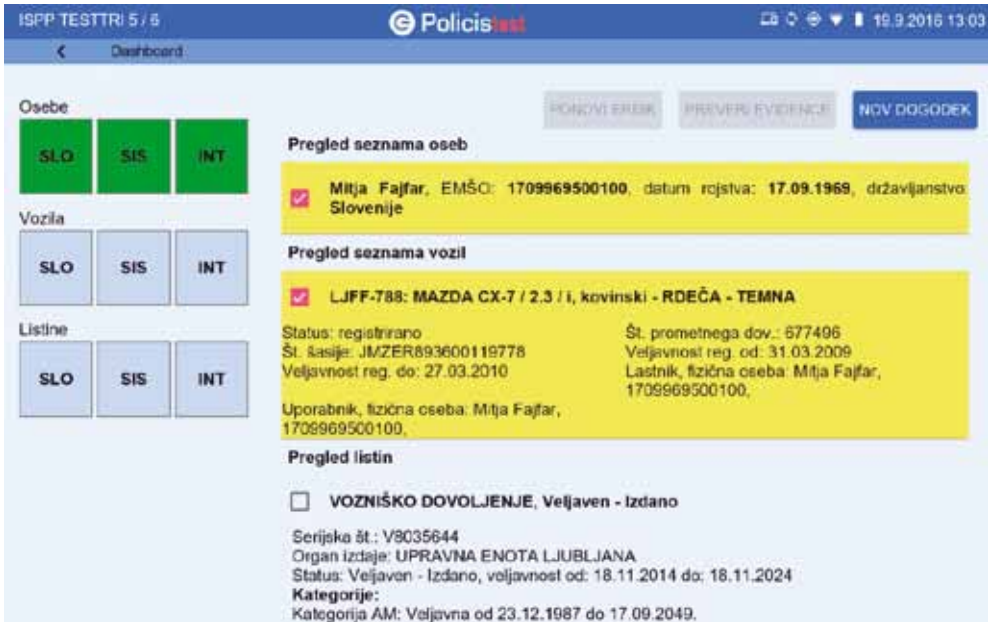
Izvedba je bila pogojena z izvedbo pilotskega projekta in njegovo pozitivno oceno.

ePolicist oprema

V okviru projekta je bilo izvedenih precej aktivnosti:

- Razvoj aplikacije ePolicist:
  - Razvoj mobilne verzije aplikacije ePolicist;
  - Razvoj vmesniških integracijskih storitev/aplikacij;
  - Razvoj in prilagoditev zalednih aplikacij;
  - Razvoj storitve mobilne analitike;
  - Vzpostavitev ustrezne vmesniške platforme.
- Pridobitev ustrezne mobilne opreme (nakup/najem);

- Uvedba sistema za upravljanje in nadzor mobilnih naprav:
  - Vzpostavitev ustrezne platforme;
  - Integracija storitve z zahtevanimi obstoječimi rešitvami.



Preverjanje

Rezultat projekta pa je poleg nabave in uvedbe mobilnih naprav predvsem aplikativna mobilna rešitev, ki zajema naslednje komponente:

- portal ePolicist,
- integrirano preverjanje,
- plačilni nalog,
- podprti štirje splošni postopki,
- podprtih enajst postopkov s področja prometa,
- pregledovanje izdanih obrazcev/dokumentov,
- izdelava dnevnega poročila policista,
- prikaz operativnih obvestil,
- spletni servis za iskanje možnih geolokacij v šifrantih policije na osnovi GPS geokoordinat prebranih na napravi.

Podprti postopki s področja prometa

Poleg navedenega so kot ločene aktivnosti izvedene še:

- izvedba mednarodne konference ePolicist v sodelovanju z evropsko mrežo EN-LETS Mobile,
- uvedba sistema za upravljanje mobilnih naprav,
- storitev vpogleda v prekrškovne zadeve za državljane preko portala e-uprava.

ePolicist v praksi

77

8.3.3 Mobilna mejna kontrola

Uredba o sistematičnemu nadzoru na Schengenski meji je kljub opozorilom Republike Slovenije stopila v veljavo 7. aprila 2017. Dodatnih tehničnih sredstev za sistematični nadzor na meji ni bilo zagotovljenih. Tako je nastala izjemna situacija, ki je postala evidentna med velikonočnimi prazniki v letu 2017, ko Policija kljub brezhibno delujočim sistemom za preverjanje identitete na mejnih prehodih in dodatnemu kadru na meji, ni uspela zagotoviti normalnega prehoda preko Schengenske meje. Še posebej izraziti so bili problemi pri izvajanju kontrole potnikov na avtobusih in pri izvajanju mejne kontrole na maloobmejnih mejnih prehodih. Ocenili smo, da bi lahko izvajanje mejne kontrole bistveno pohitrili in na ta način povečali pretočnost na mejnih prehodih, oz. potnikom zagotovili ustreznejše potovalne pogoje, z uvedbo mobilne rešitve za mejno kontrolo. Urad za informatiko in telekomunikacije in Upra-

va uniformirane policije sta takoj pristopila k iskanju rešitev in potrebnih specifikacij za javno naročilo. Ustrezna mobilna rešitev za izvajanje mejne kontrole, ki bi bila priročna, hitro delujoča, zanesljiva in sodobna bi zelo olajšala oz. pohitrila delovni

proces predvsem v primeru potnikov na avtobusih, vlakih ter maloobmejnih mejnih prehodih. Dodatno pa bi lahko s takšnim načinom dela z določeno prilagoditvijo delovnega procesa izvedli bistveno več mejnih kontrol, in s tem neposredno skrajšali čakalne dobe, tudi na drugih točkah (steze mejnih prehodov, ...) ter na področju izvajanja izravnalnih ukrepov.

Kot rešitev, ki jo je bilo edino mogoče izvesti v danih časovnih okvirih smo izbrali rešitev s pametnim telefonom Samsung S7 in Grabba čitalcem. Poleg tega dejstva pa se rešitev odlikuje s prilagodljivostjo, sodobnostjo, zelo hitrim delovanjem ter možnostjo kasnejšega lastnega vzdrževanja aplikacije, saj se konceptualno rešitev sklada z novimi načini razvoja aplikacij v Policiji.

Ključni del rešitve je razvoj sodobne mobilne aplikacije za mobilno mejno kontrolo na pametnem telefonu (Samsung S7) s pomočjo naprave Grabba za strojno branje potovalnih listin in prstnih odtisov.

Potrebna strojna oprema so naprave, ki skupaj z namensko mobilno aplikacijo in pametnim telefonom omogočajo izvajanje mobilne mejne kontrole. Naprave se namestijo na obstoječe pametne mobilne telefone in tako razširijo napravo s potrebnimi čitalci za strojno branje potovalnih listin (MRZ, RFID, fingerprint, smartcard ...) za potrebe izvajanja mejne kontrole v mobilnih pogojih dela. Namenska mobilna aplikacija na pametnem telefonu je integrirana z napravo za potrebe strojnega branja listin in prstnih odtisov in na drugi strani z zalednimi servisi, preko katerih se izvede preverjanje v nacionalnih in nadnacionalnih zbirkah za potrebe mejne kontrole.

Pripravljena rešitev je v celoti izpolnila pričakovanja naročnika ter uporabnikov. Na podlagi zelo pozitivnih izkušenj pilotnega projekta predlagamo proučitev možnosti razširitve uporabe mobilnih naprav na ostale mejne prehode (mednarodne in za obmejni promet) ter na mobilne enote SENDM in PPIU.

8.3.4 Informacijski sistem za preiskovanje kriminalitete (ISPK) – mobilna pisarna

Znotraj projekta ISPK smo razvili tudi rešitve za mobilno poslovanje kriminalistov.

8.3.5 Upravljanje mobilnih naprav – MDM (Mobile Device Management)

Cilji vzpostavitve sistema za varovanje in upravljanje mobilnih naprav so tesno povezani s poslovno mobilnostjo:

- upravljanje velikega števila različnih mobilnih naprav,
- povezovanje v obstoječe okolje,
- varen dostop do pomembnih podatkov kjerkoli in kadarkoli,
- varen dostop do aplikacij za obdelavo podatkov,
- hitra in enostavna distribucija aplikacij na vse naprave,
- ločevanje službenih in privatnih podatkov ter aplikacij.

Izvedene so bile naslednje aktivnosti:

- nakup in namestitev strojne in programske opreme za upravljanje mobilnih naprav,
- konfiguracija programske opreme za upravljanje mobilnih naprav,
- integracija programske opreme za upravljanje mobilnih naprav z obstoječo infrastrukturo,
- testiranje rešitve in izdelava priprave tehnične dokumentacije projekta,
- uvajanje naročnika v upravljanje sistema.

Uvedena je rešitev MobileIron, ki je ena od vodilnih MDM oz. EMM rešitev.

8.3.6 Storitev vpogleda v prekrškovne zadeve za državljane preko portala e-uprava

Na portalu eUprava lahko državljani pogledajo v svoje aktivne prekrške, ki so zavedeni v policijskih evidencah. Vpogled je možen le z uporabo digitalnega potrdila, saj gre za osebne podatke. Novo storitev smo pripravili v sodelovanju z Ministrstvom za javno upravo ter registriranim uporabnikom portala eUprava omogočili vpogled v njihove aktivne prekrške v evidencah policije. Državljan lahko pogleda v vse podatke, ki so navedeni na zapisniku prekrška: od datuma in lokacije do podatkov v zvezi s postopkom in plačilom. Ob vpogledu se podatki pridobijo neposredno iz policijskih evidenc.

8.4 eMigrant

S prihodom velikega števila migrantov na našo južno mejo, ki je hkrati tudi zunanja Schengenska meja, smo se soočili z velikimi humanitarnimi, kakor tudi varnostnimi problemi. V zelo kratkem času je bilo potrebno zagotoviti:

- Preverjanje oseb po operativnih evidencah;
- Hitro evidentiranje oseb;
- Izdajo potrebne dokumentacije;
- Sprotno poročanje o problematiki;
- Evidentiranje vseh nastalih finančnih posledic.

eMigrant aplikacija na zaslonu

Pred uporabo te aplikacije je evidentiranje ene osebe vzelo 20 minut in več (brez zajema prstnih odtisov), po uvedbi aplikacije se je čas obravnave ene osebe zmanjšal na 3-5 minut.

Nadgradnja obstoječe aplikacije za mejno kontrolo TravelDoc, ki vključuje zajem podatkov iz potovalnega dokumenta preko optičnega čitalca dokumentov in preverjanje listine in osebe po operativnih evidencah. Nadgradili smo jo z naslednjimi elementi:

- Zajem prstnih odtisov s čitalcem prstnih odtisov;
- Zajem fotografije s spletno kamero;
- Možnost ročnega vnosa osebe (veliko število oseb brez dokumenta);
- Izdaja in tiskanje odločb (identifikacija, zadržanje, zavrnitev ...);

eMigrant – Preverjanje preko čitalca dokumentov in informacija o zadetku

- Prenos podatkov o osebi, dokumentu, prstnem odtisu in sliki v centralno evidenco podatkov;
- On-line in Off-line način delovanja;
- Naknaden vnos »import« iz excel ali CSV datotek ter originalne strukture na disku (XML, NIST, JPG, PDF datoteke).

Aplikacija eMigrant je z našimi evidencami povezana preko spletnih servisov:

- Servis za prijavo in journal;
- Servis za vnos dogodka in osebe v Fonetični Indeks Oseb (FIO) (evidentiranje);
- Servis za izrek mejnega ukrepa zavrnitve/zadržanja;
- Servis za registracijo/štetje migrantov.

eMigrant – Zajem prstnega odtisa

Izdelani so bili posebni statistični pregledi za redno poročanje štabu in operativno delo (dva zbirnika za komulativo po operativnih zadevah in drugi za finančne resurse). Končno smo dodali tudi AFIS funkcionalnost.

8.5 Elektronska izmenjava podatkov

Informacijski sistem policije smo dolga leta obravnavali kot zaprt sistem. V zadnjem desetletju pa so trendi povezovanja sistema z raznimi zunanjimi inštitucijami v porastu. Poleg integracij v mednarodne informacijske sisteme s policijskimi vsebinami je vedno več operativnih potreb po izmenjavi podatkov tudi z drugimi državnimi organi, v zadnjem času pa tudi drugimi poslovnimi subjekti in v nekaterih primerih celo posamezniki. Prav zaradi tovrstnih potreb in zahtev postajajo ustrezno zaščitene aplikativne rešitve ključne za uspešno delovanje nekaterih specialnih služb, ki s svojimi aktivnostmi vplivajo na učinkovitejše delo policije kot celote.

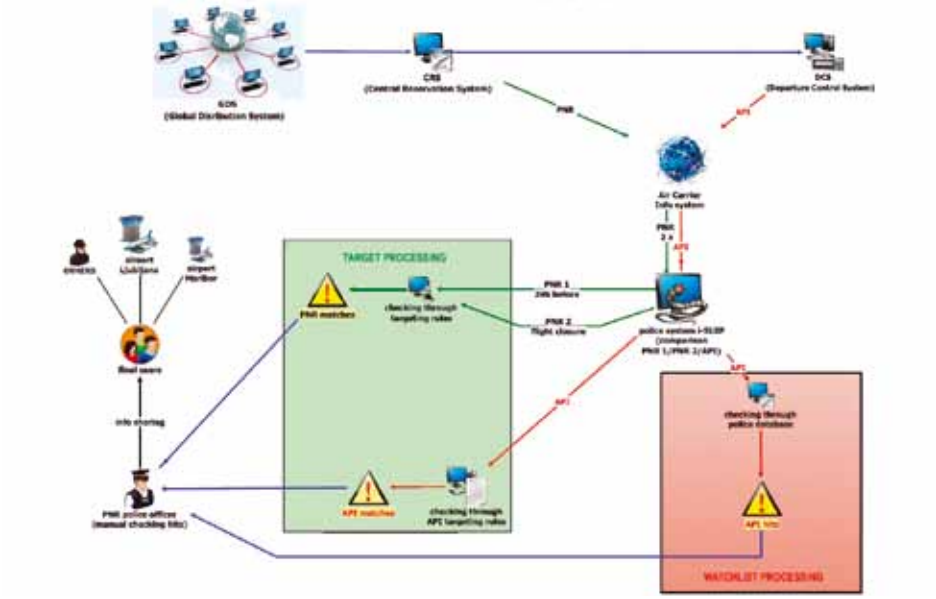
8.5.1 PNR (Passenger Name Record) / API (Advanced Passenger Information)

S sprejetjem ustrezne zakonodaje je v Sloveniji omogočeno sistematično zbiranje podatkov o letalskih potnikih. Predvsem zaradi razmaha terorističnih groženj je to eden od ukrepov, s katerim policija skuša slediti sodobnim izzivom na področju obvladova-

nja varnostih tveganj. Z namenom, da bi pravočasno prišli do ustrezne aplikativne rešitve, je bila ustanovljena projektna skupina (trajanje projekta 1.3.2014 – 31.7.2016), katere glavni cilj je bil vzpostavitev nacionalne enote za informacije o potnikih (Oddelek za ocenjevanje varnostnih tveganj v Upravi kriminalistične policije GPU), določitev delovnih procesov v tej enoti in razvoj sistema za obdelavo podatkov (i-SUIP).

V tehničnem smislu so bili ključni izzivi predvsem pri sodelovanju z letalskimi prevozniki in njihovo pripravljenostjo (zavezo) za posredovanje podatkov. Komunikacija z zunanjim svetom mora biti ustrezno zaščitena, zato smo prvič kot ključno varnostno komponento uporabili Data Power. Drugi izziv je bila obdelava velike količine podatkov (letalski prevozniki so znani po »razvajanju« svojih potnikov, zato beležijo tudi njihove posebne želje) v EDIFACT formatu, ki je v današnjem času prava redkost.

Shema sistema



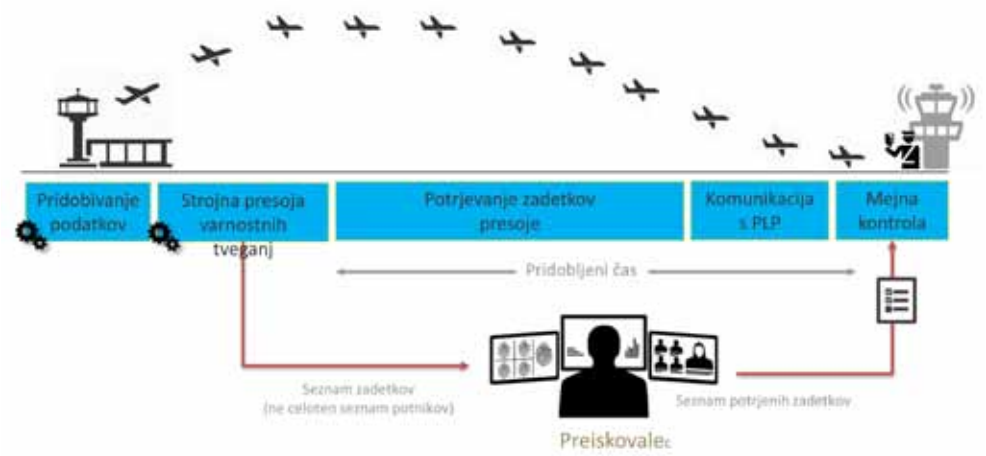
V okviru projekta so bile uspešno razdelane vse potrebne funkcionalnosti in tudi ustrezno implementirane. Nastal je lastni produkt, ki v celoti pokriva vse zahteve in želje končnih uporabnikov.

Postopki obdelave podatkov so avtomatizirani, ključne funkcije pa so:

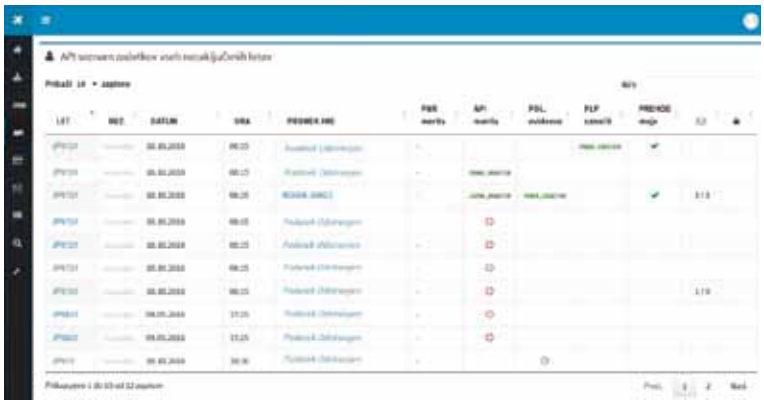
- pridobivanje podatkov,

- strojna presoja varnostnega tveganja:
  - preverjanje po evidencah (nacionalnih, SIS in Interpola) in
  - implementacija preprostih pravil v postopku ocenjevanja tveganja,
- potrjevanje zadetkov,
- usmerjanje mejnih policistov in
- mejna kontrola.

Shematični prikaz aktivnosti na časovni premici je prikazan na skici



Naš namen je tudi zavarovati zasebnost potnikov, zato analitik nima vpogleda v celoten seznam letalskih potnikov, oziroma ima to možnost le takrat, ko so izpolnjeni zakonski razlogi. Namesto njega varnostno presojo opravi računalniški sistem in izloči potnike, ki so v določenih policijskih evidencah ali ustrezajo vnaprej določenim merilom presoje. Ker so analitiku podatki na voljo takoj po vzletu letala, ima za



PNR/API seznam potnikov (zadetkov)

varnostno presojo več časa - posledično jo lahko opravi temeljiteje ter tako pomaga policistom na letališkem mejnem prehodu, da so na izvedbo mejne kontrole bolje pripravljeni in se osredotočijo na sumljive potnike.

Namesto zaključka

V okviru projekta se je razvilo dobro sodelovanje med IT strokovnjaki in uporabniki sistema, kar je bilo ključno za uspešen zaključek projekta. Z lastnim razvojem in uporabo odprtokodnih tehnologij smo uspeli zagotoviti cenejšo izgradnjo sistema, cenejše in hitrejše prilagajanje in nadgrajevanje sistema, hkrati pa tudi njegovo odlično poznavanje (izboljševanje algoritmov za izdelavo ocene tveganja), pridobljena znanja in izkušnje pa bomo lahko s pridom izkoristili tudi pri drugih projektih in nalogah, ki so še pred nami.

8.5.2 Slovensko zavarovalniško združenje (SZZ) in Zavod za zdravstveno zavarovanje Slovenije (ZZZS)

Slovensko zavarovalniško združenje in Policija sodelujeta že vrsto let. Zaradi optimalnega obravnavanja škodnih zahtevkov v zvezi s prometnimi nesrečami sta sklenila sporazum o posredovanju podatkov o prometnih nesrečah, ki jih je obravnavala policija (plačilo po posredovanem zapisniku). Za te potrebe smo razvili nekaj spletnih servisov, preko katerih zavarovalnice lahko pogledajo v evidenco policije, ali je bil njihov zavarovanec udeležen v prometni nesreči kot trdi (datum, ura, lokacija in osebni podatki oz. podatki o vozilu). V kolikor policija poseduje zapisnik o takem dogodku, ga lahko elektronsko naročijo. Nekajkrat dnevno se podatki s paketno obdelavo posredujejo na SZZ, kje so na razpolago članicam združenja. Komunikacijo smo v preteklem letu nadgradili še s funkcijo posredovanja »foto albuma« s kraja ogleda prometne nesreče (FTP protokol), v kolikor ga je policijska enota izdelala.

Izmenjava podatkov s ZZZS še ni bila predmet prenove na sodobnejšo tehnologijo. ZZZS se kot »državni instituciji« posreduje podatke o prometnih nesrečah, kjer je bila ugotovljena telesna poškodba ali smrt vsaj enega od udeležencev. Tu se podatki posredujejo še preko Lotus Notes replikacije.

Namesto zaključka

S to izmenjavo podatkov smo razbremenili enote policije administrativnih postopkov v zvezi s pripravo in posredovanjem zapisnikov v papirnati obliki. Predvsem pa sta to storitvi, ki bistveno olajšata postopke tudi državljanom.

8.5.3 Vrhovno državno tožilstvo (VDT)

V letošnjem letu nam je uspelo vzpostaviti tudi elektronsko izmenjavo podatkov z Vrhovnim državnim tožilstvom (VDT) (sporazum o izmenjavi podatkov). S to izmenjavo sta policija in VDT dogovorila elektronsko pošiljanje določenih podatkov policije na VDT:

- meta podatkov o zaključnih dokumentih v zvezi s preiskovanji kaznivih dejanj (kazenska ovadba, dopolnitev kazenske ovadbe ali poročilo po 10. odstavku 148. člena ZKP),
- zaključnih dokumentov v PDF formatu, ko so za to izpolnjeni pogoji (elektronski podpis, če je zaključni dokument: poročila po 10. odstavku 148. člena, ki jih ne spremlja predmet, ovadba zoper neznane storilce, ki jih ne spremlja predmet in ki jim ni priložena pobuda za kako preiskovalno dejanje (recimo pobuda za izpis prometa), ali ovadbe zoper znane storilce, kadar je oškodovanec že na policiji podal izjavo o umiku predloga za pregon).

V obratni smeri VDT posreduje policiji:

- podatke in dokumente o zavrženju kaznivega dejanja oz. posameznega osumljenca v kaznivem dejanju.

Namesto zaključka

Racionalizacije poslovanj na nivoju državne uprave temeljijo na dobri informacijski podpori znotraj organov. Ko dve partnerski organizaciji posedujeta informacijski sistem z ustreznim nivojem storitev, se lahko odločita za dodatno racionalizacijo pri medsebojnem sodelovanju. Dokler temelji znotraj organa niso trdni, se rešitev izmenjav podatkov ni možno uspešno lotiti. Za prehod na e-poslovanje se dogovarjamo tudi z Vrhovnim sodiščem.

8.5.4 Finančna uprava RS (FURS), aplikacija Uprave RS za javna plačila (UJPnet), Evidenca kazenskih točk (EKT), Cross-Border Exchange (CBE)

Področje prekrškov je v policiji s spremembo zakonodaje v leti 2005 dobilo na pomenu. V bistvu je to edino področje delovanja policije, kjer v celoti in samostojno odloča. S to odgovornostjo za pravilno in kvalitetno vodenje postopkov po Zakonu o prekrških, ki se zelo pogosto spreminja (2016 – ZP1J), se je poskušalo kar nekaj

postopkov avtomatizirati do te mere, da bi se enote razbremenile določenih administrativnih opravil, hkrati pa postopki ne bi bili odvisni od človeškega faktorja.

Vzpostavljena je bila centralna evidenca vseh prekrškovnih zadev, v katero enote vnašajo osnovne podatke o prekrškovnih postopkih, v ozadju pa se izvajajo izmenjave podatkov s ključnimi akterji v masovnih postopkih:

- prevzem podatkov o osebah iz RSP (pravne osebe preko AJPESa),
- za tujce se izvede pridobivanje podatkov po CBE kanalu (čezmejna izmenjava informacij),
- redno dnevno pridobivanje podatkov o vseh prilivih na račun policije za izrečene globe, stroške postopkov ali takse preko aplikacije UJPnet,
- redno dnevno pridobivanje podatkov o prilivih za ugotovljene kršitve tujcev, ki jim je bilo omogočeno plačilo preko POS terminalov (poslovanje z Banko Koper),
- redno dnevno posredovanje izvršljivih neplačanih terjatev v izterjavo na FURS in
- redno dnevno posredovanje pravnomočno izrečenih kazenskih točk v EKT.

Namesto zaključka

Čeprav popolnoma neatraktivno področje, tako dela policije kot poslovanja, je za obvladovanje teh postopkov ključna ustrezna IT podpora. Pri letnem obsegu dela nad 300.000 zadev je ročno spremljanje postopkov popolnoma nemogoče in nesmiselno. To so rešitve, ki se nam zdijo že popolnoma same po sebi umevne, vendar predvsem zaradi hitrega spreminjanja zakonodaje zahtevajo redno posodabljanje vseh zalednih algoritmov.

8.5.5 Poškodbeni listi

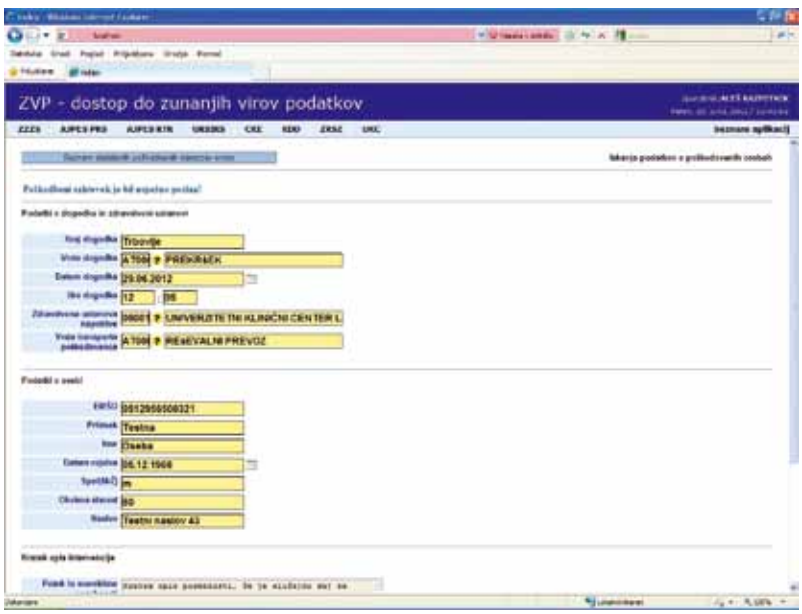
Ob vsaki obravnavi dogodka s telesno poškodbo morajo policisti pridobiti od ustrezne zdravstvene organizacije najprej preliminarno informacijo o poškodbi, od katere so odvisni preiskovalni ukrepi, kasneje pa še končni izvid o poškodbi, ki služi za dokončanje obravnave takega dogodka (prometne nesreče, delovne nesreče, itd.). Torej vsakič, ko se je poškodovanec odpeljal v zdravstveno ustanovo na zdravniško »obdelavo«, se je moral policist, ki je dogodek obravnaval, zglasiti v tej ustanovi, da so mu izročili preliminarni rezultat pregleda. Kasneje se je moral v tej inštituciji zglasiti ponovno ali pa je moral počakati pošto s končnimi rezultati zdravniških ugotovitev. To je botrovalo precejšnji izgubi časa, nepotrebnemu čakanju v zdravstvenih ustanovah in vožnjam s kraja dogodka do urgentnega centra in nazaj.

Na pobudo Ljubljanskega Univerzitetnega kliničnega centra (UKC) in Postaje prometne policije (PPP) Ljubljana smo z ministrstvom za zdravje podpisali sporazum o izmenjavi podatkov – poškodbenih listov. Pripravili smo aplikativno rešitev preko katere lahko enota policije odda povpraševanje v bolnišnične sisteme (različne bolnišnice uporabljajo različne sisteme, vstopna točka pa je poenotena prav za te potrebe). Enota vnese kraj in čas dogodka, podatke o osebi, če so znani (pri hudih poškodovancih to včasih ni možno ugotoviti) ter povpraševanje usmeri na zdravstveno inštitucijo, kamor je bila oseba odpeljana. Zdravstveni sistem preveri med sprejetimi pacienti ali že vodi podatke o osebi. Ko zdravniško osebje vnese za tako osebo preliminarni izvid, se ta avtomatično posreduje v aplikativni predal policijske enote. Enako se zgodi tudi, ko vnesejo končno diagnozo za tako osebo. Enota podatke lahko hrani v sistemu ter jih po potrebi izpiše in priloži drugim poročilom. Dosegli smo, da se tako posredovani poškodbeni listi obravnavajo kot verodostojni v vseh nadaljnjih postopkih.

Namesto zaključka

Čeprav je bilo implementiranje te rešitve kompleksno predvsem zato, ker je morala partnerska organizacija izvesti precej prilagoditev znotraj svojega sistema, so prihranki občutni (predvsem razbremenitev policistov s čakanjem na prve rezultate). Vse to ne bi uspelo brez zagnanosti nekaterih posameznikov na obeh straneh končnih uporabnikov.

Primer oddaje zahtevka



8.6 Redundantno komunikacijsko omrežje Policije

Preko širokopasovnega komunikacijskega omrežja informacijsko-telekomunikacijskega sistema policije (ITSP) dostopajo uporabniki iz vseh enot policije do vsebin, aplikacij in storitev v podatkovnih centrih na GPU in v sekundarnem računalniškem centru v Novem mestu. Preko tega omrežja se povezuje ITSP tudi z nacionalnimi in mednarodnimi organizacijami (Ministrstvo za obrambo RS, Ministrstvo za javno upravo, Nacionalni center kriznega upravljanja (NCKU), Prüm, SISI/II, Europol, Interpol, VIS, Eurosur).

Namen projekta je zagotavljanje dovolj zmogljive, varne in razpoložljive infrastrukture za operativno delo policije. Omrežje predstavlja temelj za delovanje obstoječih in novih aplikacij, ki potrebujejo bodisi zmogljivejšo infrastrukturo, bodisi morajo biti zaščitene in ločene od ostalih informacijskih tokov. Komunikacije izven upravnih območij policije morajo biti šifrirane.

Nekaj razlogov za izvajanje projekta:

- oprema se stara, končuje se njena življenjska doba in podpora,
- povečuje se možnost odpovedi, ki se pojavljajo pogosteje in so težavnejše,
- zmogljivost opreme je premajhna za uvedbo novih aplikacij in storitev in jo je nemogoče povečevati, saj ni več razvoja,
- ne podpira močnejših varnostnih mehanizmov,
- ima zelo omejeno možnost implementacije programskih in varnostnih popravkov.

Projekt sestavljata dva glavna segmenta, posodabljanje dostopovnega in jedrnega dela omrežja.

Lastnosti jedrnega dela omrežja:

- združuje povezave vseh oddaljenih enot policije,
- povezuje centralni računalnik, strežnike, shranjevalne sisteme, varnostne naprave in sistem za varnostno kopiranje,
- omogoča dostop policistom, delavcem policije in zunanjim upravičenim uporabnikom do vsebin, aplikacij in storitev ITSP,
- povezavo do omrežij SIS, Europol, Interpol, Eurosur, FADO, Hkom, NCKU, Internet, ...
- nadzorovano ločuje interna omrežja.

Pred prenovo je imelo omrežje relativno nizke hitrosti povezav prostranega omrežja, velikostnega reda od < 1Mbit/s do največ 100 Mbit/s v centru. Glavne lokacije so bile v primeru izpada dosegljive preko ISDN klicne rezervne povezave, kapacitete 128 kbit/s.

V lokalnih omrežjih so bili tipični vmesniki ethernet (10M) in fastethernet (100M) ter gigabitni za povezavo strežnikov, shranjevalnih sistemov in ostale opreme v podatkovnem centru.

Nove zmogljivosti prostranega omrežja se praviloma začno s hitrostmi 10 Mbit/s, razen na lokacijah, kjer ni tehničnih možnosti za izvedbo hitrejših. Zmogljivosti povezav do policijskih uprav in večjih policijskih postaj ter glavnih schengenskih mejnih prehodov so 100 Mbit/s, oz. 40 Mbit/s.

V dvajsetih letih je bila zmogljivost prostranega omrežja povečana kar 100-krat.

Poudariti je potrebno, da so pomembne lokacije do dveh centralnih sistemov (primarni in sekundarni računalniški center) povezane redundantno. Fizično gre za povezavo preko dveh ponudnikov omrežnih storitev (Telekom in T-2), logično pa imajo na voljo štiri komunikacijske kanale.

Lokalna omrežja praktično ne poznajo več vmesnikov slabših od fast oz. gigaethernet (100M, 1G), medtem ko pri podatkovnih centrih govorimo o 10G in 40G povezljivosti.

Nova oprema je tudi temelj za uvedbo brezžičnih omrežij, ki jih je možno vzpostaviti na vseh policijskih lokacijah, kjer že deluje klasično, žično omrežje.

Izhodišča projekta:

- podpora obstoječim informacijskim sistemom ITSP,
- povečanje zmogljivosti in varnosti,
- podvojena konfiguracija,
- skladnost s svetovnimi trendi,
- razširljivost in možnost uvajanja novih tehnologij in storitev,
- možnost implementacije nove IKT opreme,
- optimizacija obstoječih rešitev,
- možnost gradnje namenskih, varno ločenih omrežij.

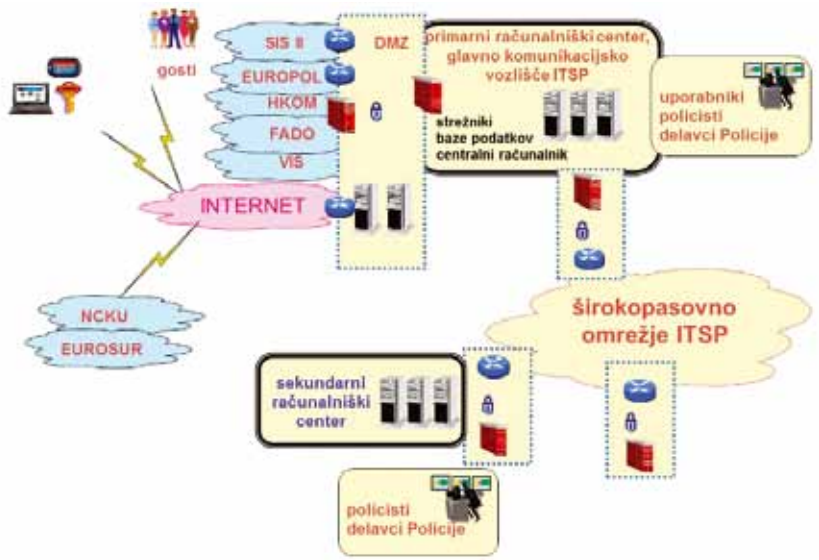
Izdelan je bil koncept rešitve nadgradnje omrežja. Pri pripravi so sodelovali strokovnjaki UIT, ki so raziskali tehnične rešitve, dobre prakse drugih organizacij in spremljali tehnološke novosti. Sledila je priprava tehničnih specifikacij in izvedba javnih naročil. Dinamika posodabljanja omrežja je letna.

Hkrati z izborom opreme so potekali dogovori s ponudniki telekomunikacijskih storitev za pridobivanje omrežnih povezav višjih hitrosti. Sledila je dobava, instalacija, konfiguracija, integracija, preizkus, vključitev v omrežje in prevzem opreme.

Nekaj glavnih poslovnih učinkov: boljša podpora operativnemu delu policije, možnost uvedbe novih zahtevnejših aplikacij, večja razpoložljivost omrežja (manj izpadov in motenj poslovnih procesov), možnost več hkratnih poizvedb v bazah podatkov ...).

S stališča UIT, kot strokovne službe, je pomembna možnost centralnega upravljanja in nadzora celotnega omrežja in opreme, kar posledično zmanjšuje stroške intervencij in povečuje hitrost odprave napak.

Poenostavljena shema ITSP s ključnimi elementi



Povzetki 2006-2016

- Zmogljivosti povezav policijskih lokacij so bile povečane na policijskih upravah iz 1-2 Mbit/s na 100 Mbit/s, iz 256-512 kbit/s na 40 Mbit/s na policijskih postajah in na maksimalno možne tehnično izvedljive na manjših enotah;

- Vključitev v schengenski informacijski sistem, po SISone4All, preko SIS II je v pripravi prehod na omrežje nove generacije (TESTA NG);
- Poenotenje tehnologij, ukinjanje TDM, prehod v IP okolje in integracija prenosa podatkov, govora (delno videa);
- Konsolidacija topologije širokopasovnega omrežja policije: dvonivojsko / centralizirano omrežje, pripravljeno na »oblačne« storitve;
- Pridobljen lastni naslovni prostor v internetu in dual-homing - ločeni povezavi do dveh avtonomnih sistemov internetnih ponudnikov;
- Implementirana ustrezno zmogljiva oprema (usmerjevalniki, stikala);
- Vzpostavitev rezervnega računalniškega centra - zmogljiva redundantna optična povezava s sistemi DWDM;
- Vzpostavitev varnih in ločenih brezžičnih omrežij za službeno uporabo in goste;
- Vpeljava mobilnih tehnologij (širokopasovne mobilne komunikacije, pametne naprave);
- Prenovljena oprema podatkovnega centra (datacenter stikala s kapacitetami 40 Gbit/s), omogoča vključitev zmogljivih virtualiziranih strežniških sistemov;
- Organizacijsko smo združili področji lokalnih (LAN) in prostranih (WAN) omrežij;
- Implementiran sistem za nadzor in upravljanje omrežja, v omrežje vključenih sistemov (strežniki, DDOKC) in upravljanje IP naslovnega prostora, ki ga uporabljamo v UIT (SITI, SRA, SITP, ...) in kolegi OIT PU.

8.7 GPS Policije in TETRA dispečer

8.7.1 GPS Policije

Namen projekta

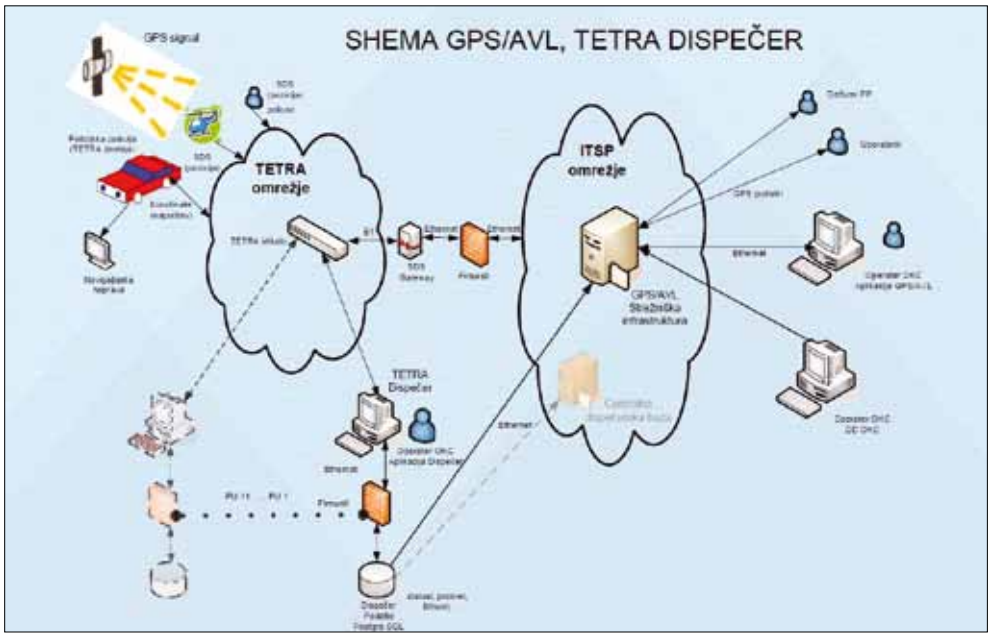
Namen izvedbe aplikacije GPS (Global Positioning System) Policije je uporabniku omogočiti spremljanje in upravljanje policijskih patrulj na terenu za izvajanje operativnih del in nalog Policije. Z implementacijo aplikacije smo v Uradu za informatiko in telekomunikacije izboljšali učinkovitost delovnega procesa in posledično skrajšali čas realizacije posameznih del in nalog. Hkrati s skrajšanjem časa se je skrajšal čas pretoka informacij za realizacijo posamezne naloge. Bistveni element delovanja in uporabe aplikacije gre iskati predvsem v povečanju zagotavljanja varnosti policistov na terenu. Shranjevanje operativnih podatkov uporabniku omogoča kasnejšo analizo o gibanju policijske patrulje.

Prejšnje in novo stanje

Ker v prvih letih delovanja DRO TETRA večina TETRA terminalov ni imela vgrajenih GPS modulov, se je problem rešil z nabavo zunanjih GPS modulov (razvila firma XE-TRA), ki so (tako kot TETRA terminali z vgrajenimi GPS moduli) pošiljali lokacijske podatke vozil preko TETRA omrežja na poseben sprejemni stacionarni TETRA terminal (GPU OKC), od koder so ga zajemale aplikativne rešitve, razvite znotraj Policije.

Leta 2006 se je pričelo uporabljati aplikacijo GpsWin proizvajalca Sledenje, Informacijski sistemi d.o.o. Le-ta je za prikaz lokacij vozil poleg lokacijskih podatkov, poslanih iz TETRA avtomobilskih terminalov, uporabljala tudi lokacijske podatke iz avtomobilskih modulov proizvajalca aplikacije. Za prenos slednjih se je uporabljalo omrežje mobilnega operaterja (GPRS). Ker se je v času delovanja aplikacije pokazala potreba po dodatnih funkcionalnostih, pogodba pa se je iztekla novembra 2007 (uporaba pa je bila omejena pretežno na OKC Ljubljana), se je pojavila potreba po novi nadgrajeni aplikativni rešitvi, ki bo dostopna policijskim enotam po vsej Sloveniji.

Shema GPS Policije



Aplikacija GPS Policije je spletna aplikacija, ki jo je za potrebe Policije razvila firma CVS Mobile. Dostopna je na delovnih postajah, ki so del ITSP. Uporabnik do aplikacije lahko dostopa le preko svojega uporabniškega računa. Podatki o lokacijah vozil se

prenašajo izključno preko lastnega TETRA omrežja. V skladu z idejami oz. poprejšnjimi zahtevami operativnih enot aplikacija podpira zahtevane funkcionalnosti, ki tako omogočajo boljši pregled ter hitrejše in bolj učinkovito upravljanje s patruljami. Omogočena je naknadna analiza oz. rekonstrukcija poti. Vgrajen je tudi sistem uporabniški profilov, tako da je vsakemu posameznemu uporabniku možno definirati nivo dostopa do funkcionalnosti aplikacije. Omogočena je povezava do drugih aplikacij (DDOKC, GUI TETRA) za sprejem podatkov. V nekaterih policijskih avtomobilih so nameščene navigacijske naprave (Garmin), ki poleg navigacije omogočajo dodatno funkcionalnost (SDS sporočila iz/v TETRA omrežje, statusi, sprejem lokacij).

Operativni vidik:

- optimalno razporejanje policijskih patrulj,
- povečanje varnosti policistov na terenu,
- analiziranje izvedenih ukrepov s pomočjo shranjenih podatkov,
- ocena potrebnega časa za prihod policista,
- statistična obdelava podatkov,
- spremljanje lokacije in gibanja policijskih patrulj,
- povezljivost aplikacije GPS Policije in aplikacije Dispečerski sistem GUI TETRA,
- uvid v lastnosti policijske patrulje.

8.7.2 Dispečerski sistem GUI TETRA

Namen projekta

Namen izvedbe aplikacije Dispečerski sistem GUI TETRA je bil izvajanje govornih in podatkovnih komunikacij med policistom – operaterjem Operativno-komunikacijskega centra (OKC) in uporabniki - policijskimi patruljami na terenu, torej operativnemu vodenju zvez in policijskih patrulj na terenu.

Prejšnje in novo stanje

Leta 2005 je bil po OKC-jih nameščen analogni dispečerski sistem RAKOS (nadomestil je stari COMPAD), a je bil podvržen možnosti prisluškovanja ter ni omogočal novih funkcionalnosti; izjema sta bila OKC Koper z digitalnim sistemom ASTRO (Dispatch Elite Consol) ter OKC Krško z digitalnim sistemom TETRA, kjer je bil nameščen dispečerski grafični sistem proizvajalca. Ker le-ta ni izpolnjeval nekaterih zahtev uporabnikov (dnevnik dogodkov, pregled zgodovine, možnost snemanja in poslušanja zadnjih klicev, prilagodljivost izgleda aplikacije, možnost povezovanja do drugih aplikacij...), se je izkazala potreba po izboljšani, nadgrajeni aplikaciji, ki jo je realiziralo podjetje ZASLON Telekom z novo aplikacijo dispečerskega sistema digitalnega radijskega omrežja TETRA (GUI TETRA). Le-ta nudi poleg bistveno izboljšanega grafičnega vmesnika uporabnikom tudi temeljno podatkovno podporo aplikaciji GPS Policije preko SQL podatkovnih baz.

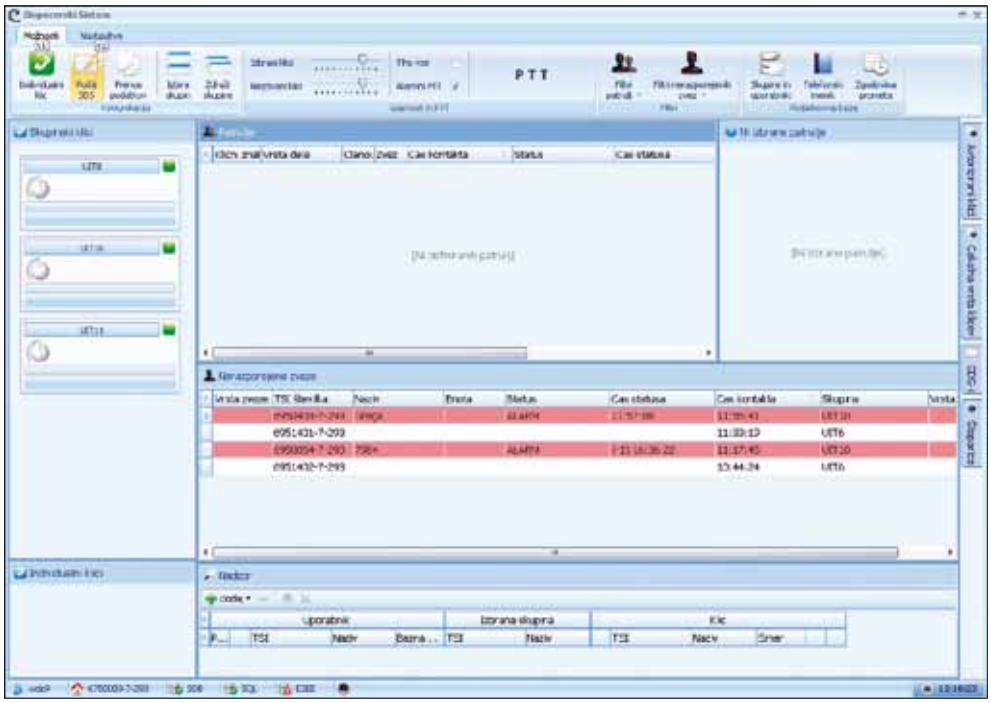
Kratek povzetek izvedenih aktivnosti

Ustanovitev delovne skupine za izvedbo vzpostavitve grafičnega vmesnika dispečerske funkcije sistema TETRA (2005) s sledečimi nalogami:

- 1. faza:
  - pregled in analiza možnih tehničnih rešitev,
  - priprava razpisne dokumentacije (tehnični del).
- 2. faza:
  - sodelovanje pri javnem razpisu,
  - razpis in podpis pogodbe (2008),
  - sodelovanje s ponudnikom pri izdelavi aplikacije,
  - testiranje funkcionalnosti,
  - končni prevzem strojne in programske opreme (2009).

- 3. faza:
  - instalacija strojne in programske opreme,
  - šolanje končnih uporabnikov.

Shema Dispečerski sistem GUI TETRA



Operativni vidik:

- izvajanje skupinskih in individualnih klicev,
- operativno vodenje zvez in patrulj,
- pošiljanje SDS sporočil,
- pregled zgodovine klicev,
- pregled posnetih govornih komunikacij,
- nadzor uporabnika,
- povezljivost z aplikacijo GPS Policije,
- kreiranje dinamičnih govornih skupin,
- izklop uporabnika iz omrežja DRO TETRA.

8.8 Varovanje ITSP (poudarek na ogroženosti – internet) in novi pravni vidiki zavarovanja osebnih podatkov

8.8.1 Varovanje ITSP na vstopnih točkah

60-letnica neke organizacijske enote praviloma izzove željo po prikazu njenega razvoja oziroma prikazu pomembnih mejnikov, ki naj bi po oceni pomenila korak oziroma bolje preskok v njenem delovanju. Glede na naslovno temo bi se seveda ta dejstva nanašala na področje varnosti ali bolje informacijske varnosti. Toda tako dolgo dobo je izredno težko ocenjevati predvsem z današnjega vidika, vidika informacijske družbe in njenega kibernetsko-varnostnega podsistema.

Zato raje začnimo s sprejemom Strategije kibernetske varnosti RS in letom 2016.

Strategija ni spregledala pomena Policije za zagotavljanje slovenske kibernetske varnosti. Poudarja pomen preiskovanja računalniškega kriminala, izrecno pa omenja tudi informacijsko-telekomunikacijski sistem policije (v nadaljevanju ITSP). Razlog za tako pomembno vlogo ITSP je v njegovem pomenu, v okvir zagotavljanja nacionalne varnosti Republike Slovenije.

Učinkovitost izvedbe nalog policije je pogojena z dobrim delovanjem ITSP. Njegovo okrnjeno delovanje ali celo nedelovanje pomeni prekinitev izvajanja ključnih nalog. Posledice takega dogodka so lahko kritične in povezane s povečanim tveganjem za varnost. Če želi policija zagotoviti neprekinjeno delovanje informacijskega sistema mora poskrbeti za ustrezno raven njegove varnosti, zato je glavni cilj informacijske varnosti zagotavljanje razpoložljivosti (dostop do podatkov, v vsakem trenutku, ko jih potrebujejo pooblaščeni uporabniki), celovitosti (preprečevanje nepooblaščenih sprememb) in zaupnosti (preprečevanje nepooblaščenega dostopa) informacijskega sistema ter njegovih storitev in podatkov. Naraščajoča medsebojna povezanost informacijskih sistemov, omrežij in različnih tipov naprav je povzročila naraščanje števila možnih točk vdorov ter izpostavljenost širšemu spektru in večjemu številu groženj.

Varovanje internetne vstopne točke

Povezovanje ITSP in zunanjega omrežja predstavlja potencialno nevarnost nepooblaščenega pretoka podatkov, zato je na izpostavljenih točkah potrebno zagotoviti visoko stopnjo varovanja podatkov in komunikacijske infrastrukture. Povezava ITSP s svetovnim spletom izpostavlja sistem kibernetskim napadom.

Ne glede na izpostavljenost ITSP je zahteva uporabnikov potreba po uporabi čim več informacijskih storitev. Uporabniki dejansko dajejo prednost funkcionalnosti in lažji uporabi, kot pa zahtevam varne obdelave podatkov. S tem pa se povečuje tudi varnostno tveganje.

Napadalci postajajo vedno bolj izurjeni v svojih sposobnostih izkoriščanja ranljivosti informacijskih sistemov. Skrbniki, ki so zadolženi za varnost, potrebujejo veliko smiselnih podatkov s sistemov beleženja. Na ta način lahko zaznajo napredne napade. Današnji napadalci že rutinsko obidejo običajne zaščitne sisteme, zato so potrebni dodatni viri podatkov poleg klasičnega prometa o napadih. Posamezne varnostne rešitve, kot je proti virusna zaščita, se velikokrat zaobidejo z različnimi tehnikami. Zato so potrebne več nivojske zaščite, da se prepreči kar največ različnih groženj. Pomembno je, da imajo organizacije ogromno podatkov z različnih naprav, da lahko zaznajo potencialne okužbe.

Ogroženost je posledica sledečih dejstev:

- Neznana orodja - najbolj učinkovita orodja za zlorabe so tista, ki jih varnostni mehanizmi ne zaznajo. Posledično kibernetski kriminal sloni pretežno na izkoriščanju ranljivosti in orodjih, ki jih varnostni mehanizmi še ne poznajo. Vsa ta orodja so javnosti neznana in običajno njihov obstoj zaznamo šele takrat, ko pride do odkritja posledic njihove uporabe.
- Kibernetski kolonializem - praktično vsa informacijska oprema sloni na tehnologiji, ki je v veliki meri razvita v nekaj državah.
- Kadrovska problematika - kibernetska varnost je visokotehnološko področje. Za upravljanje kibernetskih varnostnih mehanizmov so potrebni kadri z ustrezno izobrazbo in izkušnjami. Takih kadrov primanjkuje tudi v tehnološko razvitejših državah z bistveno večjo populacijo. Nerealno je pričakovati, da lahko državni organi pridobijo in zadržijo potrebne kadre. Posledica je slabša izkoriščenost potenciala varnostnih mehanizmov, ki jih imamo na voljo.

Na nadzornih strežnikih zbiramo sledilne zapise, jih avtomatizirano pregledujemo in na podlagi določenih dogodkov ustrezno ukrepamo. Beležijo se tudi vsi poskusi vdorov. Nadzorni strežniki tudi skrbijo, da so vse potrebne storitve ves čas delujoče. Če se zgodi, da določena storitev ne deluje, jo nadzorni strežnik poskuša ponovno vzpostaviti. Ob neuspeli vzpostavitvi sistem avtomatsko obvesti skrbnika preko elektronske pošte. Integriteto sistemskih datotek preverjamo na vsakem strežniku posebej. Ob zaznavi kršitve integritete, sistem obvesti skrbnika, ki v sledilnih zapisih preveri dogajanje na strežniku in samo datoteko.

Varnostni incidenti so nizi dogodkov, ki vplivajo na varnost omrežja, naprave ali podatkov. Preprečujemo jih z ustrezno zaščito in preventivnimi ukrepi. Odzivanje na incidente temelji na pripravi nanje. Ko incident zaznamo, se najprej opravi analiza in klasifikacija, nato pa sledi preiskovanje. To lahko pripelje do novih ugotovitev, na podlagi katerih se pripravijo ukrepi za zamejitev posledic, odstranitev nastale škode in povrnitev sistema v prvotno stanje. Aktivnosti po incidentu so velikokrat zelo pomembne, da jih lahko povežemo z drugimi obravnavanimi incidenti, zaznavamo trende in opazimo nove ranljivosti. Razvoj različnih poročil in alarmov za zaznavanje incidentov je postopen. Najprej so izdelani enostavni alarmi, ki se jih nato povezuje v kompleksnejše, da se zazna kar največ sumljivih dejavnosti v sistemu.

V policiji imamo trenutno pretežno ustrezno sodobno in vzdrževano opremo (različne tipe varnostnih pregrad IPS, SIEM, ...). Na strežnikih za dostop do interneta in poštnih strežnikih imamo postavljene protivirusne pregrade, s katerimi ustavimo vse znane viruse na poti iz interneta v lokalno omrežje. Spisek znanih virusov redno osvežujemo in tako zagotavljamo varnost pred okužbo uporabniških delovnih postaj. V omrežju imamo IBM ISS (SiteProtector), ki na ključnih vstopnih točkah opravlja funkcijo IDS/IPS in pregleduje promet za detekcijo in blokiranje sumljivega prometa. Omogoča nam zaščito v realnem času, dodatnega uveljavljanja varnostnih politik (ročna nastavitev zaprtosti sistema), izvaja se analiza vsebine na nivoju aplikacij, proaktivno posodabljanje za nove ranljivosti s strani razvojnega tima proizvajalca in natančno analizo internetnega prometa. Tako že sam sistem prepreči širjenje velike količine groženj z interneta, ki so nato še dodatno onemogočene z rednim posodabljanjem operacijskih sistemov na strežnikih in delovnih postajah.

Veliko napadov je izvršenih z orodji, ki jih klasični sistemi ne zaznajo, zato je nujno implementirati orodje za zaznavanje neznanih zlorab.

V statistiki so združeni podatki dostopov do interneta vseh uporabnikov s katerimkoli načinom.

Primerjava uporabe interneta po letih

Leto	2008	2009	2010	2011	2012
Število zahtevkov	1.284.317.213	2.438.576.325	3.274.251.895	4.492.753.986	5.148.274.952
Preneseni podatki (TB)	20,93	49,17	76,71	88,85	103,47
Leto	2013	2014	2015	2016	
Število zahtevkov	4.985.838.897	4.913.840.256	5.651.407.434	53.61.454.909	
Preneseni podatki (TB)	136,27	271	401,72	642,12	

Stanje varnosti internetnih odjemalcev

Napadi na končne uporabnike so ena izmed najbolj učinkovitih metod uspešnih vdorov. Namesto da se napadalec loti storitev na strežniku, je napad na uporabnika mogoč tako, da uporabnik dostopa do okužene vsebine iz različnih virov. Način okužbe so ranljivosti v aplikacijah ali operacijskem sistemu uporabnika, ki pride v kontakt s kontaminirano vsebino. Ker je tak računalnik avtoriziran v zaščitenem internem omrežju, lahko napadalec nato poskuša dostopati še do drugih virov znotraj tega omrežja.

Na delovnih postajah uporabnikov ITSP je nameščena protivirusna programska oprema, ki se redno posodablja. Na delovnih postajah, ki dostopajo v naše omrežje preko klicnih linij ali VPN povezav, pa je poleg tega nameščena še dodatna programska oprema za zaščito povezave. Na računalnike, ki niso pod 24 urnim nadzorom policistov, se namešča programska oprema za zaščito podatkov na pomnilniških medijih. Prav tako se namešča zaščita na prenosne USB medije.

Protivirusna programska oprema se uporablja za preprečevanje, odkrivanje in odstranjevanje zlonamerne programske opreme. Protivirusni sistem Sophos centralno skrbi za zaščito delovnih postaj in strežnikov v ITSP. Sistem je zabeležil več poskusov okužb računalnikov, okuženih računalnikov, okuženih datotek in opozoril na sumljivo obnašanje posameznih programov (od teh niso vsi škodljivi). Ključnega pomena za hiter odziv in preprečevanje širjenja okužb je centralna postavitev sistema. Stanje se z vseh računalnikov pošilja na centralno lokacijo, kar omogoča, da imamo ves čas pregled nad anomalijami v sistemu, pa naj gre za okužbo z spleta ali lokalno (USB, CD, ...). Hkrati pa se popravki in posodobitve distribuirajo hitro vsem odjemalcem hkrati.

V letu 2016 je bilo zabeleženih 206.762 opozoril.

Sophos AV	2013	2014	2015	2016
Število opozoril	5.122	10.268	9.834	206.762

Enormno povečanje je posledica ponavljajočega javljanja iste grožnje. Avtomatično čiščenje je na sistemu onemogočeno, vendar pa možnosti širjenja ni bilo. Zelo pereč problem so tudi virusi, črvi in trojanci, ki se razširjajo kot priponke elektronske pošte. Računalnik pa se lahko okuži že samo z brskanjem po internetu. Večino teh sistem zazna in onemogoči nadaljnjo okužbo, vedno pa je mogoča okužba pred objavo posodobitve (zero-day attack).

Razvoj nas je pripeljal do točke, da se informacijska varnost širi tudi na področje mobilne telefonije, saj se dostop do delov informacijskega sistema seli tudi na pametne telefone. Zaradi tega pa je lahko takšna naprava tudi vstopna točka za zlonamerne vdore v informacijske sisteme.

V policiji smo za potrebe dostopa uporabnikov mobilnih naprav do ITSP, v letu 2016 implementirali sistem za upravljanje mobilnih naprav MobileIron. Osnovni ukrep varovanja podatkov v sistemu MibileIron je šifriranje podatkovnih komunikacij in uporaba ti. kontejnerskih storitev. Podatki se na strežnikih nahajajo v nešifrirani obliki, pri prenosu podatkov na mobilne naprave pa se uporabljajo postopki šifriranja. Mobilni uporabniki se v ITSP povezujejo preko varovanih povezav z uporabo šifriranega tunela in dodatne avtentikacije na samih napravah. Terminalne naprave morajo biti zaščitene tako, da ob morebitni nepooblaščeni uporabi terminala ni možen nepooblaščen dostop do ITSP ali do podatkov ITSP. Na terminalnih napravah ne sme biti tajnih podatkov.

Govorna komunikacija, kot osnovna storitev mobilnih operaterjev, ni ustrezno zaščitena pred prestrezanjem, zato je za varno komunikacijo potrebno uporabiti druge storitve. Ena od možnosti je prenos govora preko podatkovnega omrežja, z uporabo aplikacij, ki vsebino šifrirajo. Te aplikacije so Signal, Viber, idr. ... pri čemer je naše priporočilo uporaba aplikacije Signal. Dostop do aplikacij je glede na varnostni profil uporabnika omejen na nabor odobrenih aplikacij internetne tržnice ali pa aplikacij dostopnih v spletni trgovini Google Play.

Navkljub visokim standardom ščitenja službenega dela naprave, pa zasebni del ostaja pod močnim vplivom nezaželenih dejavnikov iz okolja. Varnost podatkov je tako odvisna od uporabnika samega in njegovih dejanj, osveščenosti in znanja. Prav zaradi slednjega UIT opravlja redna usposabljanja s področja informacijske varnosti na enotah znotraj policije.

Izboljševanje varnosti sistema

Napadalci vseskozi iščejo nove načine za uspešne vdore v informacijske sisteme. Načini okužb se razvijajo tako na strežniški, kot na uporabniški strani. Zaradi tega potrebujejo skrbniki ogromno različnih virov podatkov, da lahko poiščejo indice o okužbi. Zbiranje in analiza teh podatkov s celotnega sistema je zahteven proces. Zaznati grožnjo in se uspešno obraniti pred njo, je izziv današnjega časa.

Skrb za ustrezno raven informacijske varnosti bi moral biti eden izmed primarnih ciljev vsake organizacije, predvsem pa policije. Za dosego tega cilja je potrebno, da

se varovanje prilagaja spremembam v okolju informacijskih sistemov. Samo pristop, ki sledi tako razvoju tehnologije kot groženj, lahko zagotavlja učinkovito zaščito.

Največji informacijski varnostni problem so zaposleni. Raziskave kažejo, da so več kot polovico kibernetskih vdorov posredno ali neposredno povzročili zaposleni v organizaciji. Te kršitve so najpogosteje posledica malomarnosti ali nevednosti. Implementacija varnostnih mehanizmov ni zadosten pogoj za zaščito podatkov in informacijskih sredstev, v kolikor se uporabniki v zunanje omrežje povezujejo preko nedovoljenih načinov komunikacije, kot so obhodni neavtorizirani dostopi. Usposabljanja za zaposlene so zelo pomembna, da se krepi ozaveščenost uporabnikov in poudarja njihova odgovornost za varnost informacijskega sistema.

Izkušnje po svetu kažejo, da je za ustrezno in pravočasno reakcijo ob varnostnih dogodkih v informacijsko telekomunikacijskih sistemih potrebno oblikovati ustrezno ekipo strokovnjakov, ki redno spremljajo dogajanje in po potrebi strokovno reagirajo. Strokovnjaki morajo biti ustrezno opremljeni in organizirani.

Delo zahteva različne profile ljudi s področja informatike in komunikacij, ki izvajajo delovne naloge s področja analitike delovanja informacijskega sistema, specialističnih pregledov in forenzike. Poleg zahtev po interdisciplinarnosti, se pojavlja tudi zahteva po ustreznem številu tako usposobljenih delavcev. Glede na trenutno količino napadov je potrebno analizirati veliko število alarmov (cca 7000/mesec). To pa pomeni, da bomo rabili tudi zadostno število delavcev.

Zaključek

Področje informacijske varnosti je vedno kompleksnejše, varovanje sistemov pa vse zahtevnejše. To pomeni, da se moramo dobro zavedati, da obstajajo nevarnosti na vseh področjih delovanja informacijsko telekomunikacijskih sistemov. V ITSP imamo zgrajen kompleksen sistem varovanja, v katerega so vključene različne tehnične in organizacijske rešitve. Vse navedene aktivnosti zahtevajo od skrbnikov sistema širok nabor znanj, časa in dostop do najnovejših informacij. Zagotoviti je potrebno tudi sodelovanje na namenskih izobraževanjih, kjer se lahko strokovnjaki seznanijo z novimi tehnikami napadov in obrambe.

8.8.2 Varovanje osebnih podatkov

Evropska unija mora ostati gonilna sila razvoja in spodbujanja mednarodnih standardov na področju varstva osebnih podatkov (VOP). Ta misel je sprožila dolgotrajen

proces priprave nove zakonodaje varstva osebnih podatkov, ki v vsebinskem smislu temelji na interakcijah oziroma pravnih razmerjih znotraj digitalnega prostora. Le-ta temeljijo na osebnih in drugih podatkih, ki nastanejo, ko npr. posamezniki kupujejo blago in storitve, vzpostavljajo ali ohranjajo stike z drugimi ali npr. dajejo svoje ideje na svetovni splet. Poleg nespornih koristi nastajajo tudi nova tveganja. Posameznik je izpostavljen kraji identitete, lahko je žrtev diskriminacijskega profiliranja, izpostavljen je stalnemu nadzoru ali »računalniški« goljufiji, itn. Tveganja prinašajo tudi odgovornosti upravljavcev, npr. dolžnost spoštovanja pravil o varstvu osebnih podatkov. Omenimo, da se osebni podatki lahko uporabljajo za različne namene, le v kolikor je to pravno dopustno.

Razlogi, ki so pripeljali do uveljavitve novega pravnega reda varstva osebnih podatkov so:

- Vpliv novih tehnologij (Nujnost uporabe načel varstva osebnih podatkov, ne glede na to, katera tehnologija se uporabi za obdelavo. Pričakovati je, da se upravljavci popolnoma zavedajo posledic uporabe novih tehnologij);
- Krepitev razsežnosti notranjega trga pri varstvu podatkov (Zahtevana je bila potreba po večji pravni varnosti, zmanjšanju upravnih bremen ter zagotovitvi enakih pogojev za gospodarske subjekte in druge upravljavce podatkov);
- Obravnavanje globalizacije in izboljšanje mednarodnih prenosov podatkov (Zaradi pogostih obdelav osebnih podatkov zunaj EU prihaja do različnih težav v povezavi s pravom, ki velja za obdelavo. Glede mednarodnih prenosov podatkov veliko organizacij zagovarja zahtevo po enostavnejši ureditvi prenosa podatkov);
- Zagotovitev trdnejše institucionalne ureditve za učinkovito izvrševanje predpisov o varstvu podatkov (Zahteva se nanaša predvsem na potrebo po okrepitvi organov za varstvo osebnih podatkov) in
- Večja usklajenost pravnega okvira na področju varstva podatkov (Zahteva se nanaša predvsem na potrebo po okrepitvi organov za varstvo osebnih podatkov).

Zato je morala Evropska unija oblikovati celovit in skladen pristop, ki bo med drugim zagotovil popolno spoštovanje pravice posameznika do varstva osebnih podatkov in, ki kot svoje glavne cilje postavlja:

- krepitev pravic posameznikov in
- krepitev razsežnosti notranjega trga.

Nova ureditev varstva osebnih podatkov v EU

Osrednji del trenutno še veljavne zakonodaje Evropske unije o varstvu osebnih podatkov (Direktiva 95/46/ES) je bil sprejet leta 1995 z dvema ciljema, in sicer zagotoviti varstvo temeljne pravice do varstva osebnih podatkov ter zagotoviti prosti pretok osebnih podatkov med državami članicami. Področje je bilo sicer naknadno dopolnjeno z več pravnimi akti, delno pa je bilo urejeno tudi policijsko področje in sicer s posebnimi pravili, ki so zagotovila varstvo podatkov na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah (Okvirni sklep 2008/977/PNZ).

Tehnološke spremembe, globalizacija, zahteve po pravnih spremembah varstva osebnih podatkov, širitev digitalnega trga, itn. so pripeljale do ugotovitev, da je pravni okvir varstva osebnih podatkov neustrezen. Slovenski Informacijski pooblaščenec opredeljuje razloge za spremembe oz. sprejem uredbe z nujno reformo določbe direktive iz leta 1995. Leto predstavlja obdobje »pred digitalno dobo«, EU pa je treba pripraviti na uresničevanje zahtev »digitalne ere«. »Tehnologije« kot so Google, FB, CCTV, internet stvari, pametni telefoni, pametna mesta, internetno bančništvo, kognitivne tehnologije, umetna inteligenca, itn. vodijo v uveljavljanje novosti na področju pravnega podsistema – prava informacij. Na to področje se navezujejo tudi nove oblike osebnih podatkov, nevarnost zlorabe funkcionalnosti (function creep), profiliranja, posegov v lokacijsko zasebnost, itd.. Kot posledica navedenega se postavljajo zahteve po večji unifikaciji varstva osebnih podatkov, na področju javne varnosti pa se je pojavila zahteva po višji stopnji harmonizacije predpisov oz. udejanjenju vsaj minimalnih standardov varstva osebnih podatkov.

Uredba temelji na 2. odstavku 16. člena Pogodbe o delovanju EU (PDEU). Določba je nova, posebna pravna podlaga uvedena z Lizbonsko pogodbo, predstavlja pa osnovo za sprejetje novega pravnega okvirja varstva osebnih podatkov. Pravni okvir sicer predstavljata:

- 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) in
- Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ.

Uredba namesto dosedanjih 28 ureditev, prinaša pravno poenotenje in nekatere druge novosti:

- velja za vse upravljavce osebnih podatkov, čim obdelujejo osebne podatke državljanov EU, četudi imajo sedež izven EU,
- koncept osebnih podatkov se ne oži - uredba, primeroma, kot osebne podatke določa tudi spletne identifikatorje, identifikatorje naprav, ID piškotkov, RFID oznake, IP naslove; občutljivi osebni podatki so tudi genetski in biometrični podatki,
- kot novost se za osebne podatke štejejo tudi psevdonimni podatki,
- »One Stop Shop Principle« - če poteka obdelava osebnih podatkov v več državah članicah, je vodilni informacijski pooblaščenec tisti, kjer je glavna poslovna enota upravljavca,
- uvaja se Evropski odbor za VOP,
- uvajajo se »pooblaščenci za varstvo osebnih podatkov«, t.i. DPO-ji,
- poudarek se daje presoji vplivov na zasebnost (PIA),
- poudarja se koncept vgrajene zasebnosti (Privacy by Design),
- vzpostavlja se pravica do pozabe (izbris rezultatov iskanja),
- molk ni nikoli privolitev, privolitev je informirana in svobodna, nedvoumna izjava volje, pri občutljivih osebnih podatkih pa mora biti privolitev celo izrecna,
- obveznost poročanja o varnostnih incidentih (Informacijskemu pooblaščencu in prizadetemu posamezniku),
- visoke kazni.

Preden predstavimo izbrane določbe direktive o VOP opozorimo na Mnenje DS ustanovljene na osnovi 29. člena Direktive 95/46/ES (mnenje iz april 2016), da je treba vedno, torej tudi pri obveščevalno varnostnih aktivnostih, katere lahko štejemo tudi kot del javne varnosti, zagotoviti štiri elemente, in sicer: 1. pravila o obdelavi osebnih podatkov morajo biti jasna, natančna, dostopna (informiran posameznik); 2. nujnost in sorazmernost obdelave in za zakonite namene; 3. obstajati mora neodvisen nadzorni mehanizem, le-ta mora biti učinkovit in nepristranski in 4. posamezniku morajo biti na voljo učinkovita pravna sredstva.

Direktiva o VOP v »policijskem sektorju«

Pravica do varstva osebnih podatkov je določena v 8. členu Listine EU o temeljnih pravicah (LEUTP) in 16. členu PDEU. Kot je poudarilo Sodišče EU, pravica do varstva osebnih podatkov ni absolutna, temveč jo je treba obravnavati glede na vlogo, ki jo ima v družbi s tem, da je varstvo podatkov tesno povezano s spoštovanjem zasebnega in družinskega življenja, varovanega v 7. členu LEUTP, ki določa, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. V skladu z 52. členom

LEUTP se lahko omejitve uresničevanja pravice do varstva podatkov uvedejo samo, če so predpisane z zakonom, če spoštujejo bistveno vsebino pravice in svoboščin ter so ob upoštevanju načela sorazmernosti potrebne in dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Evropska unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.

Sam namen obdelave osebnih podatkov je služiti človeku in s tem zagotavljati spoštovanje njegovih temeljnih pravic in svoboščin, v danem primeru predvsem zagotavljati uresničevanje pravice do varstva osebnih podatkov. Tako stališče bi moralo prispevati k oblikovanju oz. izboljšanju območja svobode, varnosti in pravice.

Za učinkovito varstvo osebnih podatkov v Uniji ni potrebna samo krepitev pravic posameznikov, na katere se nanašajo osebni podatki, ter dolžnosti tistih, ki osebne podatke obdelujejo, ampak so potrebna tudi enakovredna pooblastila za spremljanje in zagotavljanje skladnosti s pravili varstva osebnih podatkov v državah članicah.

Direktiva je v normativnem delu razdeljena na enajst poglavij: splošne določbe; načela; pravice posameznika, na katerega se nanašajo osebni podatki; upravljavec in obdelovalec; prenos osebnih podatkov v tretje države ali mednarodne organizacije; nacionalni nadzorni organ; sodelovanje; pravna sredstva, odgovornost in sankcije; delegirani in izvedbeni akti in končne določbe.

Poglejmo si nekaj konkretnih predlogov ureditve.

Direktiva vsebuje pravila v povezavi z obdelavo osebnih podatkov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij ter dva cilja: zaščito temeljnih pravic in svoboščin fizičnih oseb in zlasti njihove pravice do varstva osebnih podatkov, pri čemer se zagotavlja visoka raven javne varnosti ter zagotovitev izmenjave osebnih podatkov med pristojnimi organi. Področje uporabe Direktive ni omejeno na čezmejno obdelavo podatkov, ampak se uporablja za vse postopke obdelave, ki jih za namene Direktive izvajajo pristojni organi. Direktiva se ne uporablja za obdelavo v sklopu dejavnosti zunaj področja uporabe zakonodaje Unije niti za obdelavo s strani institucij, organov, uradov in agencij Unije, ki je predmet druge uredbe in druge posebne zakonodaje.

Med splošne določbe spada tudi opredelitev temeljnih pojmov. Nekateri so sicer povzeti po dosedanji ureditvi, drugi so spremenjeni, dopolnjeni z dodatnimi ali na novo uvedenimi elementi. Nove opredelitve pojmov določajo »kršitev varnosti osebnih podatkov«, »genetske podatke« in »biometrične podatke«, »pristojne organe« in »otroka« na podlagi Konvencije ZN o otrokovih pravicah.

Države članice morajo zagotoviti spoštovanje vsaj sledečih načel. Osebni podatki so obvezno obdelani pošteno in zakonito; zbrani za določene, jasne in zakonite namene ter se ne smejo naprej obdelovati na način, ki je nezdružljiv s temi nameni. Podatki morajo biti primerni, ustrezni in ne pretirani glede na namene, za katere se obdelujejo. Zahteva se, da so podatki točni in po potrebi posodobljeni. Sprejeti je treba vse primerne ukrepe za zagotovitev, da se netočni osebni podatki nemudoma izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo. Podatki morajo biti shranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, vendar le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo. Obdelani morajo biti v okviru pristojnosti in odgovornosti upravljavca, ki zagotovi skladnost z določbami predpisov, sprejetih v skladu s to direktivo.

Direktiva izpostavlja zahtevo po razlikovanju med različnimi vrstami posameznikov (kategorije posameznikov), na katere se nanašajo osebni podatki. Za to morajo države članice zagotoviti, da upravljavec v največji možni meri jasno razlikuje med osebnimi podatki različnih vrst posameznikov, na katere se nanašajo osebni podatki.

Glede različne stopnje točnosti in zanesljivosti osebnih podatkov države članice zagotovijo, da se različne vrste osebnih podatkov, ki se obdelujejo, v največji možni meri razlikujejo glede na njihovo stopnjo točnosti in zanesljivosti. Prav tako države članice zagotovijo, da se osebni podatki, ki temeljijo na dejstvih, v največji možni meri razlikujejo od osebnih podatkov, ki temeljijo na osebnih mnenjih (mehki podatki).

Države članice prepovejo obdelavo osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično prepričanje, vero ali prepričanje, članstvo v sindikatu, genetske podatke ali podatke v povezavi z zdravstvenim ali spolnim življenjem. Ta prepoved se ne uporablja, kadar: je obdelava dovoljena z zakonom, ki zagotavlja ustrezne zaščitne ukrepe; ali je obdelava potrebna za varstvo življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge osebe; ali je obdelava povezana s podatki, ki jih posameznik, na katerega se nanašajo osebni podatki, objavi.

Poleg tega države članice zagotovijo tudi:

- Pravico posameznika, na katerega se nanašajo osebni podatki, do dostopa do svojih osebnih podatkov (dodani so novi elementi informiranja posameznikov, na katere se nanašajo osebni podatki: o roku shranjevanja, pravicah do popravka, izbrisa ali omejitve in vložitve pritožbe);
- Možnost sprejema zakonodajnih ukrepov za omejitev pravice do dostopa, če to zahteva posebna narava obdelave podatkov na področjih policije in kazenskega pravosodja, in zagotavlja, da se posameznik, na katerega se nanašajo osebni podatki, obvesti o omejitvi dostopa;

- V primerih, kadar je neposreden dostop omejen, posamezniku, na katerega se nanašajo osebni podatki, obvestiti o možnosti posrednega dostopa prek nadzornega organa, ki uveljavi pravico v njegovem imenu in mora posameznika, na katerega se nanašajo osebni podatki, obvestiti o izidu preverjanj;
- Pravico do popravkov sledi ali pravico do izbrisa sledi;
- Pravico do označitve obdelave.

Poglavje IV določa splošne obveznosti upravljavca in obdelovalca, varnost podatkov in uradno osebo za varstvo podatkov. Med splošnimi obveznostmi omenimo pristojnost upravljavca, da ravna v skladu s to direktivo in zagotovi skladnost, vključno s sprejetjem politik in mehanizmov za zagotavljanje skladnosti. Države članice morajo zagotoviti skladnost dela upravljavca z obveznostmi, ki izhajajo iz načel vgrajenega varstva podatkov.

Uvaja se dolžnost obveščanja o kršitvi varnosti osebnih podatkov.

Direktiva, na osnovi splošne uredbe, uvaja tudi pooblaščeno osebo za varnost osebnih podatkov. Podobno ureditev v Sloveniji že poznamo in je implementirana v policiji, vendar bo treba njen položaj in pristojnosti okrepiti.

Ocenjeno je, da direktiva zagotavlja dosledno in visoko raven varstva podatkov ter tako krepi medsebojno zaupanje med policijo in pravosodnimi organi različnih držav članic ter spodbuja prost pretok podatkov med njimi. Ob tem je direktiva, kot oblika pravnega predpisa, po mnenju Komisije, najboljši pravni akt, saj državam članicam dopušča potrebno prožnost pri izvajanju načel, pravil in njihovih izjem na nacionalni ravni.

Zaključek

Kaj čaka policijo ob tako spremenjenem pravnem okvirju?

Prva naloga bo temeljita preučitev vseh novosti in spremenjenih dosedanjih določb. Nedvomno bo treba pripraviti ali samo popraviti zakon, ki bo prenesel določbe direktive v nacionalni pravni red. Sicer je to vprašanje v pristojnosti Ministrstva za pravosodje, vendar bo sodelovanje policije pri pripravi predpisa nedvomno potrebno, po obsegu pa pravno in informacijsko zahtevno. Poleg zakona pa bo potrebno poseči tudi v podzakonske akte.

9 VIZIJA URADA ZA INFORMATIKO IN TELEKOMUNIKACIJE

Zagotavljati napredne, zanesljive in varne informacijsko – telekomunikacijske storitve in druge elektronske sisteme ter naprave za potrebe Policije ter z uvajanjem novih in stalnim prilagajanjem obstoječih IKT rešitev prispevati k večji učinkovitosti in uspešnosti njenega delovanja.


PC 02


POLICIJA
ITS