

VIŠJA STROKOVNA ŠOLA ACADEMIA

MARIBOR

DIPLOMSKO DELO

**VIDEONADZORNI SISTEM POŠTE SLOVENIJE
D.O.O.**

Kandidat: Dominik Škorjanc

Študent izrednega študija

Številka indeksa: 11190350025

Študijski program: Varovanje

Mentor: mag. Boris Grilc

Maribor, 2014

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Podpisani Dominik Škorjanc z vpisno št. 11190350025 sem avtor diplomskega dela z naslovom Videonadzorni sistem Pošte Slovenije d.o.o., ki sem ga napisal pod mentorstvom g. Borisa Grilca, mag. javne uprave.

S svojim podpisom zagotavljam, da:

- je predloženo diplomsko delo izključno rezultat mojega dela,
- sem poskrbel, da so dela in mnenja drugih avtorjev, ki jih uporabljam v predloženi nalogi, navedena oz. citirana skladno s pravili Višje strokovne šole Academia,
- se zavedam, da je plagiatorstvo – predstavljanje tujih del oziroma misli kot moje lastne kaznivo po Zakonu o avtorskih in sorodnih pravicah; UL št. 16/2007; (v nadaljevanju ZASP), prekršek pa podleže tudi ukrepom Višje strokovne šole Academia skladno z njenimi pravili,
- skladno z 32. členom ZASP-a dovoljujem Višji strokovni šoli Academia objavo diplomskega dela na spletnem portalu šole.

Maribor, september 2014

Podpis študenta:

ZAHVALA

Iskreno se zahvaljujem mentorju g. Borisu Grilcu, mag. javne uprave za strokovno pomoč, nasvete in usmeritve pri izdelavi diplomskega dela.

Za nasvete in pomoč pri pridobivanju potrebnih podatkov za izdelavo diplomskega dela se zahvaljujem g. Mitji Štampferju, direktorju Področja korporativne varnosti in nadzora Pošte Slovenije d.o.o., in g. Sebastijanu Petku, vodji Nadzornega centra Pošte Slovenije d.o.o.

Zahvaljujem se tudi Tini Janžekovič, univ.dipl.prof.slov., za lektoriranje.

Posebna zahvala moji družini za pomoč in podporo pri študiju.

POVZETEK

V diplomskem delu sem predstavil videonadzorni sistem Pošte Slovenije d.o.o., ki je po obsegu eden večjih v regiji in je bil vzpostavljen za potrebe varovanja ljudi in premoženja Pošte Slovenije d.o.o.

V začetku diplomskega dela na kratko predstavljam videonadzor, ki omogoča spremljanje dogajanj na varovanih območjih oz. lokacijah, zajem, prenos, zapisovanje, pregledovanje in arhiviranje slikovnih informacij ter s tem zagotavlja širok spekter uporabnih informacij. Sledi predstavitev zakonskih določil pri izvajanju videonadzora, predstavitev delovnega okolja, v katerem deluje videonadzorni sistem Pošte Slovenije d.o.o. ter podajanje razlogov za njegovo postavitev.

Osrednji del diplomskega dela je namenjen tehnični predstavitvi, delovanju in upravljanju z videonadzornim sistemom Pošte Slovenije d.o.o. Sledi predstavitev prednosti in ekonomski vidik izbire videonadzornega sistema Pošte Slovenije d.o.o.

V zaključku pa sledi še analiza dosedanjega delovanja videonadzornega sistema Pošte Slovenije d.o.o., ugotovitve in sklepi.

Ključne besede: videonadzor, videonadzorne kamere, centralizirano upravljanje z videonadzornim sistemom, obdelava in hranjenje videoposnetkov, nadzorni center.

ABSTRACT

Video Surveillance System at the Post of Slovenia

In the research paper I have presented the video surveillance system at the Post of Slovenia which is one of the largest in the region and was set up in order to protect the people and the assets of the Post of Slovenia.

In the beginning of my Diploma paper I have briefly presented the video-surveillance system which enables monitoring the action in the surveyed areas or locations, gathering information, transmitting, recording, examining data also archiving visual data which provides a wide range of useful information. Following is the presentation of statutory provisions which the video surveillance system is based on, presentation of the working environment in which the video surveillance system at the Post of Slovenia is set up and the reasons for its establishment are also explained.

The main part of the Diploma paper is dedicated to technical analysis, functioning and operating of the video surveillance system at the Post of Slovenia. Then the advantages of the video surveillance system at the Post of Slovenia are presented and the economic perspective of selecting video surveillance system is explained.

In the end the analysis of the so far operating video surveillance system at the Post of Slovenia is given along with the latest findings and a final conclusion.

Key words: video surveillance, video surveillance cameras, centralized video surveillance system, data analysis, data processing, control center.

KAZALO VSEBINE

1	UVOD	9
1.1	OPIS PODROČJA IN OPREDELITEV PROBLEMA	9
1.2	NAMEN, CILJI IN OSNOVNE TRDITVE.....	9
1.3	PREDPOSTAVKE IN OMEJITVE	10
1.4	UPORABLJENE RAZISKOVALNE METODE	10
2	VIDEONADZOR.....	11
2.1	SPLOŠNO O VIDEONADZORNIH SISTEMIH	11
2.2	ZAKONSKA UREDITEV IZVAJANJA VIDEONADZORA	14
3	PREDSTAVITEV DELOVNEGA OKOLJA	17
3.1	PREDSTAVITEV PODJETJA POŠTA SLOVENIJE D.O.O.....	17
3.1.1	<i>Poslanstvo in vizija Pošte Slovenije d.o.o.</i>	18
3.1.2	<i>Področje korporativne varnosti in nadzora na Pošti Slovenije d.o.o.</i>	19
3.2	NADZORNI CENTER POŠTE SLOVENIJE D.O.O.....	24
3.2.1	<i>Tehnična opremljenost Nadzornega centra Pošte Slovenije d.o.o.</i>	25
3.2.2	<i>Delo operaterjev v Nadzornem centru Pošte Slovenije d.o.o.</i>	27
4	VIDEONADZORNI SISTEM POŠTE SLOVENIJE D.O.O.	31
4.1	ODLOČITEV ZA VZPOSTAVITEV VIDEONADZORA	31
4.2	ZAHTEV POŠTE SLOVENIJE D.O.O. ZA VIDEONADZORNI SISTEM	32
4.3	TEHNIKA VIDEONADZORNEGA SISTEMA POŠTE SLOVENIJE D.O.O.	34
4.3.1	<i>Videonadzorne kamere</i>	37
4.3.2	<i>Vmesnik oziroma MX-ExtIO modul</i>	43
4.4	PRIMER POSTAVITVE KAMER (POKRITOST PROSTORA Z VIDEONADZOROM).....	44
4.5	GLOBALNO KOMUNIKACIJSKO OMREŽJE POŠTE SLOVENIJE D.O.O.....	45
5	PREDNOSTI VIDEONADZORNEGA SISTEMA POŠTE SLOVENIJE D.O.O....	49
5.1	PREDNOSTI PRI OBDELAVI PODATKOV	49
5.2	CENTRALIZACIJA PODATKOV	50
5.3	HITER DOSTOP DO PODATKOV	51
5.4	VELIKOST ZBRANIH PODATKOV	52
5.5	MOŽNOST UPORABE VIDEONADZORNEGA SISTEMA ZA MARKETING	52
6	EKONOMSKI VIDIK IZBIRE VIDEONADZORNEGA SISTEMA POŠTE SLOVENIJE D.O.O.	54

7	UGOTOVITVE IN SKLEPI	57
8	UPORABLJENA LITERATURA IN VIRI.....	62
8.1	LITERATURA	62
8.2	VIRI	62
8.3	SPLETNI VIRI	63

KAZALO SLIK

SLIKA 1:	SHEMA SODOBNIH VIDEONADZORNIH SISTEMOV	13
SLIKA 2:	ORGANIGRAM PKVN-JA	24
SLIKA 3:	NADZORNI CENTER POŠTE SLOVENIJE D.O.O.	26
SLIKA 4:	PROGRAM MxCC	28
SLIKA 5:	DIAGRAM POTEKA DELA OPERATERJA V NC-JU OB SPROŽITVI ALARMA V POŠTNI POSLOVALNICI	29
SLIKA 6:	SHEMATSKI PRIKAZ PRENOSA ALARMA IZ LOKACIJE V NC	36
SLIKA 7:	PRIMER PRIKAZA AKTIVIRANEGA ALARMA V POŠTNI POSLOVALNICI V PROGRAMU MxCC	36
SLIKA 8:	PRIMER OBDELAVE SLIKE OD ZAJEMA DO OBDELAVE (KODIRANJA) IN SHRANITVE V MOBOTIXOVI KAMERI	38
SLIKA 9:	MOBOTIXOVI KAMERI Q24M IN Q25M	39
SLIKA 10:	MOBOTIXOVI KAMERI M24M IN M25M	40
SLIKA 11:	MOBOTIXOVI KAMERI D14D IN D15D.....	41
SLIKA 12:	MOBOTIXOVI KAMERI D24M IN D25M	41
SLIKA 13:	MOBOTIXOVA IP MEGAPIKSEL VIDEODOMOFONA T24M IN T25M	42
SLIKA 14:	PRIKAZ NOTRANJOSTI MX-EXTIO MODULA	44
SLIKA 15:	PRIMER POKRITOSTI PROSTORA POŠTNE POSLOVALNICE S ŠTIRIMI KAMERAMI	45
SLIKA 16:	GLOBALNO KOMUNIKACIJSKO OMREŽJE POŠTE SLOVENIJE D.O.O.	46
SLIKA 17:	SHEMA HRBTENIČNEGA IN PRISTOPNEGA OMREŽJA	48
SLIKA 18:	PRIKAZ »PLAYER« NAČINA V MxCC.....	51
SLIKA 19:	FUNKCIJI »COUNTING LINE« IN »HEATMAP« V PROGRAMU MxCC	53

KAZALO TABEL

TABELA 1:	MODELI IN ŠTEVILO KAMER V VIDEONADZORNEM SISTEMU POŠTE	43
TABELA 2:	ENERGETSKI IZRAČUN PORABE ELEKTRIČNE ENERGIJE MED PRIMERLJIVIMA VIDEONADZORNIMA SISTEMOMA V PRVIH 10-ih LETIH DELOVANJA.....	56

KAZALO GRAFIKONOV

GRAFIKON 1: ŠTEVILO KAZNIVIH DEJANJ NA POŠTI MED LETI 2004 IN 2012	31
GRAFIKON 2: ŠTEVILO OBDELANIH IN SHRANJENIH POSNETKOV OD AVGUSTA 2012 DO JULIJA 2014.....	58
GRAFIKON 3: PRIKAZ ŠTEVILA ROPOV IN VLOMOV NA POŠTI OD LETA 2010 DO JULIJA 2014	60

1 UVOD

1.1 *Opis področja in opredelitev problema*

V diplomskem delu bom predstavil postavitve, delovanje in upravljanje videonadzornega sistema Pošte Slovenije d.o.o. (v nadaljevanju: Pošta), kateri s svojimi 1282-imi videonadzornimi kamerami v 438-ih poštnih poslovalnicah na območju Republike Slovenije (v nadaljevanju: RS) spada med večje v regiji. Ugotavljal bom, ali je v praksi izvedljivo hipno upravljanje in dostopanje do oddaljenih podatkov na snemalnem mediju v kamerah ter ali je te podatke mogoče tudi takoj preusmeriti na centralni snemalni medij. Dokazoval bom, da je možno nadzirati enako velike prostore, čeprav so nekateri opremljeni z videonadzornim sistemom z manjšim številom kamer (manjši stroški). Opravil bom tudi analizo videonadzornega sistema po dveh letih operativnega delovanja (koliko je bilo zavarovanih posnetkov, pomoč pri odkrivanju kaznivih dejanj, število posredovanih posnetkov policiji, hitrost obdelave podatkov itd.). Glede na velikost me zanima tudi ekonomski vidik stroškov vzdrževanja videonadzornega sistema, zato bom opravil analizo porabe električne energije videonadzornih kamer.

1.2 *Namen, cilji in osnovne trditve*

Namen diplomskega dela je predstavitev in analiza prednosti in uporabnosti decentraliziranega videonadzornega sistema s centralnim dostopom do kamer in podatkov po dveh letih operativnega delovanja. Ob izdelavi diplomskega dela pa sem želel hkrati nadgraditi znanje o videonadzornih sistemih.

Cilji diplomskega dela so:

- kratka predstavitev podjetja in delovnega okolja (tj. Nadzornega centra Pošte),
- predstavitev videonadzora (na splošno) in zakonskih določil za izvajanje videonadzora,
- predstavitev videonadzornega sistema Pošte in upravljanja s sistemom,
- analiza delovanja videonadzornega sistema Pošte (hitrost obdelave podatkov, količina podatkov, snemanje na različne medije itd.),
- ekonomski porabe električne energije videonadzornega sistema Pošte.

Osnovne trditve diplomskega dela so:

- slikovni zajem prostora z manjšim številom kamer,
- hipen dostop do podatkov na lokaciji kamere ali centralnega strežnika, na katerem se hranijo podatki – enostavno in hitro upravljanje s tako obsežnim videonadzornim sistemom,
- postaviti kvaliteten videonadzorni sistem za sprejemljivo ceno in majhno porabo električne energije,
- možnost uporabe videonadzornega sistema za ekonomske potrebe podjetja.

1.3 *Predpostavke in omejitve*

Predpostavljam, da mi bodo nadrejeni v podjetju zagotovili sodelovanje in pomoč ter točnost podatkov, saj bodo le-ti pridobljeni iz predstavljenega videonadzornega sistema.

Pri omejitvah bi izpostavil, da bodo vse analize in podatki vezani na časovno obdobje zadnjih dveh let, saj je videonadzorni sistem Pošte operativen šele od leta 2012. Nekateri podatki ne bodo uporabljeni zaradi varovanja poslovne skrivnosti ali varovanja osebnih podatkov.

1.4 *Uporabljene raziskovalne metode*

Diplomsko delo bo izdelano na primeru videonadzornega sistema Pošte, s katerim upravljam tudi sam. Za izdelavo teoretičnega dela diplomskega dela bom uporabil interno gradivo in literaturo, internetne strani, zbrano slovensko in tujo literaturo, revije in lastno znanje. Podatki bodo pridobljeni iz konkretnih primerov pri delovanju videonadzornega sistema Pošte v zadnjih dveh letih ter bodo predstavljeni tabelarno in grafično.

V diplomskem delu bom uporabil naslednje metode:

- deduktivno metodo pri razlagi dejstev in zakonov,
- deskriptivno metodo za opisovanje posameznih pojmov in pojavov ob uporabi in interpretaciji literature,
- induktivno metodo pri uporabi dejstev in podatkov iz prakse, ko bom v zaključku povzemal vsebino le-teh,
- metodo analize in sinteze,
- metodo klasifikacije pri definiranju posameznih pojmov,
- metodo kompilacije pri navajanju izpiskov, navedb in citatov različnih avtorjev.

2 VIDEONADZOR

2.1 *Splošno o videonadzornih sistemih*

Videonadzorni sistemi oz. sistemi videonadzora so medsebojno funkcijsko povezana namenska tehnična sredstva oz. naprave, ki omogočajo zajem videopodatkov s kamerami (analogne kamere¹, IP kamere², IP megapiksel kamere³ itd.), shranjevanje in obdelavo podatkov na razne snemalne medije (DVR⁴, HDVR⁵, NVR⁶ itd.), prenos podatkov preko prenosnih poti oz. omrežij (kabli za prenos podatkov, brezžični prenos) ter prikaz in upravljanje z njimi s pomočjo nameščenih programov na raznih monitorjih, računalnikih, delovnih postajah, mobilnih telefonih, tabličnih računalniki itd. (Potokar in Welzer Družovec, 2013, str. 2; povz. po Golob, 1997).

»Videonadzorni sistemi nam omogočajo pregled dogajanj na objektih s pomočjo kamer v »živo« ali pregledovanje videoposnetkov o dogodkih, ki so se zgodili v preteklosti, ter tako služijo za obveščanje o izrednih dogodkih, odkrivanje napak na objektih, nadzor fizičnih oseb, nadzor nad premoženjem, preprečevanje poškodb, dokumentiranje dogodkov, analiziranje itd.« (http://www.varnost.si/videonadzorni_sistem).

Pri izbiri videonadzornega sistema je potrebno upoštevati njegov namen, potrebno je vedeti, za kakšen objekt gre, kje je lociran, kdo so uporabniki, kdo bo nadzorovan, koliko denarja imamo na razpolago itd. Pri dokončni izbiri je bistvenega pomena posvetovanje s strokovnjaki s področja videonadzora ter na koncu podrobna proučitev vseh ponudb, kajti ni nujno, da bo najcenejša ponudba na dolgi rok tudi najugodnejša (npr. nezmožnost nadgradnje videonadzornega sistema, v kolikor se v prihodnosti pokaže potreba po nadgraditvi oz. razširitvi le-tega, neizkoriščenost vseh razpoložljivih tehnologij, predimenzioniran videonadzorni sistem glede na njegovo namembnost, poraba električne energije in posledično veliki stroški delovanja itd.).

¹ Analogne kamere potrebujejo dodatno napravo za pretvorbo analognih signalov v digitalne signale.

² IP je kratica za internetni protokol, ki omogoča prenos podatkov preko računalniškega omrežja. IP kamere imajo enake resolucije (ločljivosti) kot analogne kamere ter vgrajen pretvornik analognih signalov v digitalne videosignale.

³ IP visoko resolucijske oz. ločljivostne kamere.

⁴ DVR (angl. Digital Video Recorder) – digitalni videosnemalnik.

⁵ HDVR (angl. Hybrid Digital Video Recorder) – hibridni videosnemalnik.

⁶ NVR (angl. Network Video Recorder) – omrežni videosnemalnik.

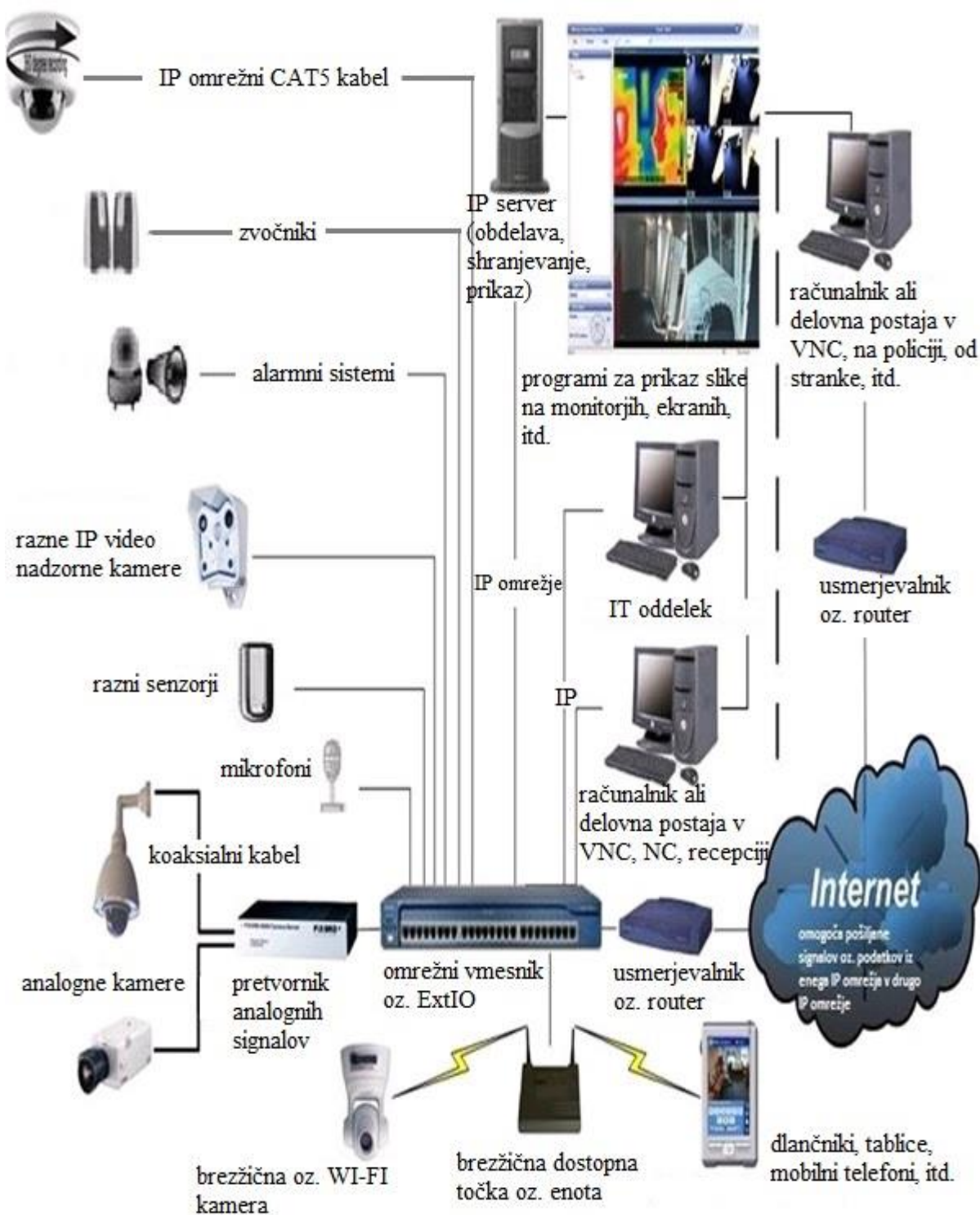
Videonadzorne sisteme lahko glede na tehnične lastnosti delimo v tri skupine:

- klasične analogne videonadzorne sisteme (kamere z analognim prenosom videosignala),
- IP videonadzorne sisteme (razne IP kamere z digitalnim prenosom videosignala preko računalniškega omrežja po protokolu TCP⁷/IP),
- hibridne videonadzorne sisteme, ki so kombinacija analognih in IP videonadzornih sistemov.

Največji napredek na področju varovanja je bil v zadnjih letih storjen prav na področju videonadzornih naprav oz. same tehnike videonadzornih sistemov. Vendar zaradi velikega števila prodanih analognih kamer v prejšnjih letih še vedno prevladujejo v osnovi klasični analogni videonadzorni sistemi, ki pa so danes že zastareli in večinoma že nadgrajeni v sodobnejše hibridne videonadzorne sisteme, ki so v večini opremljeni z IP kamerami brez megapiksel tehnologije. Oba videonadzorna sistema pa zaradi nenehnega razvoja informacijskih tehnologij (v nadaljevanju: IT), računalniške opreme in programov ter trenutnih prodajnih trendov prodaje IP megapiksel kamer (najsodobnejše imajo vgrajene mikrofone, zvočnike, razne senzorje gibanja, toplotne senzorje ter programe za obdelavo in upravljanje z videopodatki ter lastne snemalne medije) izpodrivajo sodobni IP megapiksel videonadzorni sistemi. Le-ti zaradi vseh sodobnih tehnologij niso več prostorsko, podatkovno in dostopno omejeni ter so z možnostjo priključitve več vrst drugih naprav v sam videonadzorni sistem (kot je razvidno iz Slike 1, na kateri je prikazana shema sodobnih videonadzornih sistemov) uporabni še za druge namene (npr. za odpiranje vrat na daljavo, pogovarjanje, videokonference) in preprostejši za uporabo (npr. nadzor in upravljanje preko mobilnega telefona ali dlančnika).

Glavne pomanjkljivosti IP megapiksel videonadzornega sistema so še vedno sorazmerno visoka cena IP megapiksel kamer, varnost podatkov in nedelovanje sistema v primeru izpada internetnega omrežja.

⁷ TCP (angl. Transmission Control Protocol) je protokol za nadzor prenosa. Sporočila preko protokola TCP se zaradi vzpostavljene povezave med odjemalcem in prejemnikom prenašajo zanesljivo v obe smeri, so brez napak, podvajanja in v pravilnem vrstnem redu.



Slika 1: Shema sodobnih videonadzornih sistemov

Vir: Prirejeno po: <http://www.technoriya.in/images/CCTV%20IP%20diagram.png>

2.2 Zakonska ureditev izvajanja videonadzora

V RS ureja uporabo videonadzora več zakonov, med katere spadajo Zakon o varstvu osebnih podatkov⁸ (v nadaljevanju: ZVOP-1), Kazenski zakonik⁹, Zakon o nalogah in pooblastilih policije¹⁰ (v nadaljevanju: ZNPPol), Zakon o zasebnem varovanju¹¹ (v nadaljevanju: ZZasV-1), Zakon o spremembah in dopolnitvah Zakona o igrah na srečo¹² (Potokar, 2012, str. 6).

Sodoben način življenja, potreba po varnosti ljudi in premoženja ter hiter razvoj videonadzornih sistemov prispevajo k vedno večji uporabi in nameščanju videonadzornih sistemov na vseh področjih družbenega življenja. Ker pa je videonadzor eden od načinov pridobivanja osebnih podatkov (z zadnjo generacijo videonadzornih sistemov lahko le-ti prepoznajo starost, spol, obraze, določene gibe ipd. ter s tem že posegajo na področje biometrije), ga je bilo potrebno dobro zakonsko urediti. Tako je pri odločanju o nujnosti in potrebnosti uvedbe videonadzora potrebno upoštevati načelo namembnosti, ki je temeljno načelo varstva osebnih podatkov; osebni podatki se lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače (16. člen ZVOP-1). Potrebnost pa je potrebno presoati v odvisnosti od posameznega primera, kar pomeni, da mora biti osnovno vodilo pri uvedbi videonadzora načelo, da se le-ta uvede, kadar ni na razpolago drugega milejšega ukrepa za zagotovitev varnosti ljudi in premoženja (Potokar in Welzer Družovec, 2013, str. 2).

Najpodrobneje področje videonadzora ureja ZVOP-1:

- oseba javnega ali zasebnega sektorja lahko izvaja videonadzor dostopa v uradne službene oz. poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oz. poslovnih prostorov in ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih (prvi odstavek 75. člena ZVOP-1),
- videonadzor znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov

⁸ Zakon o varstvu osebnih podatkov – uradno prečiščeno besedilo (ZVOP-1-UPB1). Ur. l. RS, št. 94/2007, z dne 16. 10. 2007.

⁹ Kazenski zakonik (KZ-1). Ur. l. RS, št. 55/2008, z dne 4. 6. 2008.

¹⁰ Zakon o nalogah in pooblastilih policije (ZNPPol). Ur. l. RS, št. 15/2013, z dne 18. 2. 2013.

¹¹ Zakon o zasebnem varovanju (ZZasV-1). Ur. l. RS, št. 17/2011, z dne 11. 3. 2011.

¹² Zakon o spremembah in dopolnitvah Zakona o igrah na srečo (ZIS-E). Ur. l. RS, št. 108/2012, z dne 29. 12. 2012.

ter poslovne skrivnosti in če tega namena ni možno doseči z milejšimi sredstvi (prvi odstavek 77. člena ZVOP-1). Ne sme pa se videonadzor izvajati izven delovnega mesta, zlasti v garderobah, dvigalih in sanitarnih prostorih. Prav tako morajo biti zaposleni pred začetkom izvajanja videonadzora vnaprej pisno obveščeni o njegovem izvajanju, delodajalec pa se mora pred uvedbo videonadzora posvetovati z reprezentativnim sindikatom pri delodajalcu,

- oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, mora izdati obvestilo, da se izvaja videonadzor (74. člen ZVOP-1), katero mora biti vidno in razločno objavljeno tako, da omogoča posamezniku seznanitev o njegovem izvajanju najkasneje, ko se nad njim začne izvajati videonadzor. Vsebovati mora naslednje informacije: da se izvaja videonadzor, naziv osebe javnega ali zasebnega sektorja, ki ga izvaja, telefonsko številko za pridobitev informacije kje in koliko časa se shranjujejo posnetki iz videonadzornega sistema,
- videonadzorni sistem mora biti zavarovan pred dostopom nepooblaščenih oseb (74. člen ZVOP-1),
- oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, mora v svojih aktih predpisati organizacijske, tehnične in logično-tehnične ukrepe za zavarovanje osebnih podatkov (24. in 25. člen ZVOP-1) ter zagotoviti varovanje osebnih podatkov (24. člen ZVOP-1). Prav tako mora v notranjih aktih določiti tudi osebo, ki je odgovorna za evidenco videonadzornega sistema, ter osebe, ki lahko zaradi narave njihovega dela obdelujejo podatke v evidenci videonadzornega sistema (25. člen ZVOP-1),
- oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, mora zagotoviti evidenco, iz katere je mogoče pozneje ugotoviti, kdaj so bili posamezni osebni podatki iz evidence videonadzornega sistema uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je možno zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov (24. člen ZVOP-1),
- izvajalec videonadzora mora za evidenco videonadzornega sistema vzpostaviti tudi katalog zbirke osebnih podatkov (26. člen ZVOP-1) ter podatke iz kataloga zbirke osebnih podatkov posredovati nadzornemu organu za varstvo osebnih podatkov (27. člen ZVOP-1). Izjeme so upravljavci osebnih podatkov, ki imajo manj kot 50 zaposlenih, katerim za zbirko videonadzora ni potrebno izdelati internega akta o zavarovanju osebnih podatkov, katalogov zbirk osebnih podatkov in vnašati podatke iz katalogov v register zbirk osebnih podatkov (4. odstavek 7. člena ZVOP-1). Izjema

pa so naslednji upravljavci: javni sektor, notarji, odvetniki, detektivi, izvršitelji, izvajalci zasebnega varovanja, zasebni zdravstveni delavci, izvajalci zdravstvenih storitev, upravljavci, ki vodijo zbirke, ki vsebujejo občutljive osebne podatke in je obdelava občutljivih osebnih podatkov del njihove registrirane dejavnosti (peti odstavek 7. člena ZVOP-1),

- v kolikor videonadzorni sistem ne snema in se opravlja videonadzor v »živo«, ne nastane zbirka osebnih podatkov, zato ZVOP-1 takšnega videonadzora ne ureja. Je pa upravljavec, ki se odloči za takšno obliko videonadzora, lahko podvržen odškodninski tožbi ali uvedbi kazenskega postopka. Priporoča se, da upravljavci tudi v takšnem primeru obvestijo posameznike z obvestilom, ki vsebuje vse elemente iz 74. člena ZVOP-1, ki mora biti izobešeno na vidnem mestu in trajno oz. dokler se izvaja videonadzor,
- videonadzor za izključno osebno uporabo, družinsko življenje ali druge domače potrebe ni podvržen določilom ZVOP-1 o videonadzoru (7. člen ZVOP-1). Kljub temu posameznik, ki bi snemal npr. sosedovo parcelo ali druge posameznike, tvega odškodninsko tožbo ali uvedbo kazenskega postopka,
- videonadzor v večstanovanjskih stavbah se lahko izvaja le, kadar je to potrebno za varnost ljudi in premoženja (drugi odstavek 76. člena ZVOP-1),
- videoposnetki pridobljeni z videonadzorom se v primeru dostopa v službene ali poslovne prostore lahko shranjujejo tako dolgo kot to določa interni akt o varovanju osebnih podatkov ali drug podoben akt, vendar največ eno leto po nastanku, nato jih je treba izbrisati oz. uničiti. Za vse ostale videoposnetke (tudi javnih površin) pa velja splošni rok hrambe, ki določa, da se osebni podatki shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali in nadalje obdelovali. Priporoča se čim krajši rok hranjenja (Informacijski pooblaščenec, 2008, str. 6–13).

3 PREDSTAVITEV DELOVNEGA OKOLJA

3.1 *Predstavitev podjetja Pošta Slovenije d.o.o.*

Pošta je bila ustanovljena ob razdružitvi nekdanjega skupnega PTT podjetja Slovenije 1. januarja 1995 z Aktom o ustanovitvi družbe Pošta Slovenije d.o.o. (v nadaljevanju: Akt o ustanovitvi) na podlagi Zakona o poštnih storitvah. Od julija 2002 deluje kot gospodarska družba v 100-odstotni lasti RS, ki jo upravlja skladno z Zakonom o gospodarskih družbah ter uresničuje ustanoviteljske pravice preko Slovenske odškodninske družbe. Organa družbe sta nadzorni svet in poslovodstvo.

Pošta je pomemben gospodarski objekt v RS, kar se kaže v obsežnem naboru storitev, visokih prihodkih, investicijah in nabavah, dolgoletni tradiciji, velikem številu zaposlenih in velikem številu poštnih objektov. Pošta trenutno zaposluje približno 6.000 uslužbencev, ki delo opravljajo v 550-ih poštnih poslovalnicah s približno 1.350-imi poštnimi okenci.

Dejavnost

Primarna dejavnost je izvajanje univerzalne poštne storitve¹³ (pisemske storitve, paketi, direktna pošta, hitra pošta, publikacije), denarne storitve (poštne nakaznice, plačilni promet, poslovne banke, Poštna banka Slovenije), velik pomen pa imajo tudi druge poštne in kurirske storitve (telegrami, elektronske storitve: E-Arhiv Pošte Slovenije, moja.posta.si, certifikacijska agencija POŠTA@CA itd.), direktni marketing, Pošta na Petrolu, razvijanje fotografij, prodaja srečk, športne stave, znamke, osebne znamke. Pošta poleg navedenih dejavnosti opravlja tudi druge posle, ki so potrebni za njen obstoj in opravljanje dejavnosti, ne pomenijo pa neposrednega opravljanja dejavnosti, ki so določene v Aktu o ustanovitvi.

Organiziranost

Pošta je sestavljena iz poslovodstva, strokovnih služb in poslovnih enot (v nadaljevanju: PE), ki so organizirani tako, da je omogočeno uspešno in racionalno izvajanje vseh dejavnosti in

¹³ Univerzalne poštne storitve so poštne storitve, ki morajo biti zagotovljene vsem uporabnikom po dostopni ceni ne glede na njihov kraj bivanja ali poslovanja. Z univerzalnimi poštnimi storitvami se zagotavlja vsem uporabnikom poštnih storitev vsak delovni dan, vendar ne manj kot petkrat tedensko, najmanj en sprejem in ena vročitev poštnih pošilk do mase 2 kg, poštnih paketov do mase 20 kg, priporočenih in vrednostnih poštnih pošilk ter poštnih pošilk za slepe in slabovidne. Zakon o poštnih storitvah določa tudi mehanizme za financiranje univerzalnih poštnih storitev. Stroške za izvajanja univerzalnih poštnih storitev pokrivajo izvajalci poštnih storitev, ki spadajo v sklop univerzalnih poštnih storitev (Petek, 2011, str. 14).

funkcij podjetja po naslednjih kriterijih: vrsta in obseg dejavnosti, medsebojna povezanost dejavnosti, strokovna sorodnost dela, tehnične in kadrovske možnosti.

Strokovne službe opravljajo strokovna dela za potrebe družbe, zagotavljajo pogoje za enotno delovanje družbe kot celote ter skrbijo za povezovanje in sodelovanje z mednarodnimi institucijami.

Poslovodstvo in strokovne službe družbe sestavljajo: poslovodstvo družbe, pooblašenci poslovodstva, svetovalci poslovodstva, štabne službe, Področje globalne logistike, Področje trženja, Področje informacijske tehnologije, Področje računovodstva, Področje financ, Področje investicij in nabave, Področje kadrovskih in pravnih zadev, Področje mednarodnih odnosov, Področje razvoja in tehnologije storitev ter Področje korporativne varnosti in nadzora.

Poslovne enote opravljajo dejavnosti družbe, ki so določene v Aktu o ustanovitvi, ter strokovne operativne naloge, potrebne za opravljanje dejavnosti na teritorialno zaokroženem območju. PE je z vidika svoje dejavnosti odgovorna za smotrno poslovanje s sredstvi, ki jih uporablja za svoje delovanje. Pri izvajanju svoje dejavnosti mora PE ravnati skladno s postavljenimi normativi, standardi in planskimi nalogami. Vodi jo direktor PE ter jo lahko sestavljajo oddelki v strokovnih službah in poštne poslovalnice. Pošta ima devet poslovnih enot: PE Celje, PE Koper, PE Kranj, PE Ljubljana, PE Poštni logistični center Ljubljana (v nadaljevanju: PLC Ljubljana), PE Maribor, PE Murska Sobota, PE Nova Gorica in PE Novo mesto.

3.1.1 Poslanstvo in vizija Pošte Slovenije d.o.o.

Poslanstvo

Poslanstvo Pošte je zagotavljati razvoj ter kakovostno, konkurenčno in zanesljivo izvajanje poštnih, logističnih in varnih elektronskih poštnih storitev, storitev uporabe globalnega poštnega informacijskega in komunikacijskega omrežja ter prodaje trgovskega blaga prebivalstvu in pravnim subjektom v domačem in mednarodnem okolju, ob vsem tem pa prispevati k nacionalnemu razvoju tudi na demografsko ogroženih območjih, zadovoljstvu državljanov kot uporabnikov storitev, večanju konkurenčnosti in poslovne učinkovitosti podjetij in drugih poslovnih subjektov.

Vizija

Vizija Pošte je biti najpomembnejši in največji izvajalec poštnih in z njimi povezanih logističnih storitev v RS tudi po liberalizaciji poštne trga v Evropski uniji, razvijati

pripadnost in lojalnost zaposlenih, vlagati v njihovo znanje ter zagotavljati njihovo socialno varnost, dolgoročno plačilno sposobnost in optimalno donosnost vloženega kapitala (<http://www.posta.si/opis-storitve/551/Poslanstvo-in-vizija>).

3.1.2 Področje korporativne varnosti in nadzora na Pošti Slovenije d.o.o.

Področje korporativne varnosti in nadzora (v nadaljevanju: PKVN) je bilo ustanovljeno leta 2008 kot Sektor za korporativno varnost in nadzor ter leta 2011 preimenovano v PKVN.

PKVN sestavljajo Oddelek korporativne varnosti (pododdelek Nadzorni center), Oddelek notranje kontrole, Oddelek informacijske varnosti in Pooblaščenec za pranje denarja.

PKVN je organizacijska enota v sklopu strokovnih služb Pošte in je neposredno podrejen njenemu poslovodstvu. Osnovne naloge PKVN-ja so pripravljanje in nadzorovanje izvajanja varnostne politike ter internih predpisov v najširšem pomenu (notranja kontrola) ter tako celovito obravnavanje vseh relevantnih varnostnih pojavov in poslovanja Pošte kot gospodarskega subjekta.

PKVN zagotavlja in vodi varnostne politike pri:

- organizaciji fizičnega in tehničnega varovanja ljudi in premoženja,
- obvladovanju poslovnih in drugih varnostnih tveganj,
- ogroženosti zaradi požarov in naravnih nesreč,
- delovnih nesrečah,
- industrijskem vohunjenju ter drugih oblikah ogrožanja,
- informacijski varnosti.

Pošta spada med zavezanke, ki jih je Vlada RS s sklepom zavezala k organiziranju obveznega varovanja na podlagi Uredbe o obveznem organiziranju varovanja¹⁴, ki je bila izdana na podlagi tretjega odstavka 69. člena ZZasV-1. Tako se varovanje ljudi in premoženja ter ostale oblike zasebnega varovanja izvajajo na podlagi navedenih pravnih aktov in internih aktov Pošte (Pravilnik o zagotavljanju varnosti v Pošti Slovenije d.o.o.¹⁵, Navodilo za gibanje v poštah objektih in postopke poštne delavcev ob izrednih dogodkih¹⁶, Navodilo o nalogah, dolžnostih in načinu izvajanja dela receptorsko-vratarske službe v upravni stavbi Pošte Slovenije d.o.o. Maribor, Slomškov trg 10 (št. 0/20-2187/1-2007), Pravilnik o poslovnih

¹⁴ Uredba o obveznem organiziranju varovanja. Ur. l. RS, št. 80/2012 z dne 26. 10. 2012.

¹⁵ Uradno glasilo Pošte Slovenije d.o.o., št. 1/2004.

¹⁶ Uradno glasilo Pošte Slovenije d.o.o., št. 1/2006.

skrivnosti¹⁷, Zadrževanje v poštnih objektih izven delovnega časa¹⁸, Požarni red¹⁹, Pravilnik o pisarniškem poslovanju²⁰).

Pošta z izbranim pogodbenim izvajalcem varovanja oz. družbo za zasebno varovanje fizično in tehnično s protitropnimi (sistem za klic v sili) in protivlomni sistemi varuje svoja območja, objekte, prostore in ljudi, pri čemer mora pogodbeni izvajalec izpolnjevati naslednje pogoje (Petek, 2011, str. 42–44):

- izvajalec ali njegov zakoniti zastopnik ne sme biti pravnomočno obsojen zaradi naslednjih kaznivih dejanj, ki so opredeljena v Kazenskem zakoniku Republike Slovenije:
 - hudodelsko združevanje,
 - sprejemanje podkupnine pri volitvah (velja za fizične osebe), nedovoljeno sprejemanje daril, nedovoljeno dajanje daril, jemanje podkupnine (velja za fizične osebe), dajanje podkupnine, sprejemanje daril za nezakonito posredovanje in dajanje daril za nezakonito posredovanje,
 - goljufija, poslovna goljufija, preslepitev pri pridobitvi posojila ali ugodnosti in zatajitev finančnih obveznosti ter goljufija zoper finančne interese Evropskih skupnosti v smislu 1. člena Konvencije o zaščiti finančnih interesov Evropskih skupnosti,
 - pranje denarja,
- izvajalec mora biti vpisan v sodni register. V primeru, da je ponudnik samostojni podjetnik, mora biti vpisan v poslovni register Republike Slovenije, ki ga izdaja Agencija Republike Slovenije za javnopravne evidence in storitve (AJPes), in mora imeti registrirano dejavnost zasebnega varovanja,
- izvajalec ne sme biti v postopku prisilne poravnave, stečaja ali likvidacije, v preteklosti pa ni smel opustiti poslovne dejavnosti v takšnem ali podobnem položaju,
- izvajalec ne sme imeti blokirane svojega transakcijskega računa v zadnjih šestih mesecih poslovanja pred začetkom izvajanja fizičnega varovanja,
- izvajalec mora imeti veljavno licenco za varovanje ljudi in premoženja, licenco za načrtovanje varnostnih sistemov, licenco za upravljanje z varnostno-nadzornim

¹⁷ Uradno glasilo Pošte Slovenije d.o.o., št. 2/2006.

¹⁸ Uradno glasilo Pošte Slovenije d.o.o., št. 5/1998.

¹⁹ Uradno glasilo Pošte Slovenije d.o.o., št. 2/2003.

²⁰ Uradno glasilo Pošte Slovenije d.o.o., št. 2/2006.

centrom (v nadaljevanju: VNC), licenco za prevoz denarja in drugih vrednostnih pošilk v skladu z ZZasV-1, pred pričetkom izvajanja fizičnega varovanja pa ne sme biti v postopku odvzema katere koli licence s področja zasebnega varovanja, prav tako pa mu v preteklosti ni smela biti nikoli začasno ali stalno odvzeta licenca,

- izvajalec mora imeti lastni oz. najeti VNC,
- izvajalec mora imeti v vsaki intervencijski skupini vsaj enega varnostnika, ki je opravil usposabljanje iz samoobrambe in borilnih veščin pri enem izmed izvajalcev samoobrambe po programu, ki je predpisan za pridobitev nacionalne poklicne kvalifikacije varnostnik,
- izvajalec mora zagotavljati 15-minutni intervencijski čas od trenutka sprejema informacije o alarmu do prihoda na objekt, in sicer 24 ur dnevno vse dni v letu,
- izvajalec mora imeti ustrezne reference pri varovanju bank ali drugih finančnih institucij, ki izvajajo gotovinsko poslovanje s fizičnimi ali pravnimi osebami.

Osnovni namen fizičnega varovanja na Pošti je varovanje oseb in premoženja Pošte pred uničenjem, poškodovanjem, kriminalnimi in drugimi škodljivimi pojavi ter se izvaja z varnostniki izbranih pogodbenih izvajalcev varovanja. Fizična varovanja na Pošti se opravljajo v obliki stalne prisotnosti varnostnika na varnostni točki, občasnega fizičnega varovanja pri izvajanju posameznih delovnih procesov, varnostno-receptorskih služb, obhodnih varovanj, intervencij in varovanj pri prevozu denarja in drugih vrednostnih pošilk ter se vedno opravljajo v kombinaciji s tehničnim varovanjem. Osnovni namen tehničnega varovanja je nadzor in omejitev gibanja v objektu, na območju ali v prostoru, odkrivanje in obveščanje o posameznih dogodkih na varovanem območju ter prenos, obdelava in arhiviranje prenesenih sporočil.

Tehnično varovanje oseb in premoženja v objektih in poslovnih prostorih Pošte zajema naslednje sisteme:

- mehanska zaščita poslovnih prostorov in delovnih mest,
- sistem kontrole pristopa pred vstopom v objekt ali prostor,
- sistem kontrole pristopa z uporabo biometričnih naprav,
- sistem za javljanje vloma,
- sistem za klic v sili (protiropni sistemi),
- videonadzorni sistem (Petek, 2011, str. 46).

Vse oblike varovanj, ki se izvajajo za potrebe Pošte in jih opravljajo pogodbeni izvajalci varnostnih storitev, so koordinirane iz njihovih VNC-jev. Za koordinacijo izvajanja nalog na področju zasebnega varovanja pa skrbi PKVN v sodelovanju s poslovodstvom pogodbenega izvajalca storitev zasebnega varovanja (Petek, 2011, str. 45).

Pogodbeni izvajalec varnostnih storitev mora varovanje opravljati skladno s pravili stroke tako, da je zagotovljeno varovanje premoženja, naprav in objekta pred uničenjem, poškodovanjem, tatvino in drugimi oblikami škodljivih pojavov, in sicer z načini in oblikami, ki jih določajo veljavni predpisi (Petek, 2011, str. 44).

Oddelek korporativne varnosti

Primarno se s področjem zagotavljanja korporativne varnosti Pošte ukvarja Oddelek korporativne varnosti, ki na podlagi celovite obravnave vseh relevantnih varnostnih pojavov načrtuje, vodi in usmerja storitve zasebnega varovanja ter v posameznih primerih tudi poslovne procese družbe v smeri zagotavljanja najvišje stopnje varnosti za zaposlene in za premoženje Pošte glede na dane možnosti in razmere. Poleg navedenega preventivnega delovanja, ki predstavlja osrednji del delovanja, se zaposleni v tej službi zaradi izkušenj pri odkrivanju storilcev kaznivih dejanj vključujejo tudi v postopke odkrivanja storilcev (tako med zaposlenimi kot drugimi), pri čemer tesno sodelujejo z organi odkrivanja.

Oddelek korporativne varnosti v sodelovanju z drugimi organizacijskimi enotami izvaja naslednje naloge:

- oblikuje smernice na varnostnem področju,
- izvaja analize s področja korporativne varnosti in pripravlja poročila, ki predstavljajo podlago za načrtovanje, izbiro in uvajanje novih sredstev ter ukrepov varovanja,
- organizira, spremlja in sodeluje pri pripravi izobraževalnih programov usposabljanja zaposlenih na varnostnem področju,
- sodeluje z institucijami s področja varnosti in izvaja druge naloge z varnostnega področja, ki jih opredeljujejo zakoni in drugi predpisi ali jih določi poslovodstvo Pošte v skladu s pristojnostmi (Petek, 2011, str. 15-16).

Oddelek notranje kontrole

Oddelek notranje kontrole s stalno kontrolo in ukrepi, odrejenimi za odpravo nepravilnosti in pomanjkljivosti, sodeluje pri zagotavljanju nemotenega, pravilnega in kakovostnega delovanja poštne prometa v vseh fazah tehnološkega procesa v notranjem in mednarodnem prometu (Petek, 2011, str. 16). V ta namen inšpektorji notranje kontrole izvajajo kontrole

poslovanja pošt, PLC-ja Ljubljana in drugih organizacijskih enot družbe. Pri tem preverjajo izvajanje zakonov in drugih predpisov ter tehnoloških navodil, izvajanje navodil in usmeritev generalnega direktorja družbe, direktorja sektorja, preverjajo pravilnost in smotrnost organiziranosti dela, spremljajo strokovno usposobljenost poštnih delavcev ter dajejo predloge in pobude za izboljšanje kakovosti poslovanja. V primerih pritožb uporabnikov ali suma, da je bilo storjeno kaznivo dejanje, opravljajo poizvedbe in zbirajo dokaze ter obvestila (<http://www.intranet.si/predstavitev-sektorjev/23570/Podrocje-korporativne-varnosti-in-nadzora>).

Oddelek informacijske varnosti

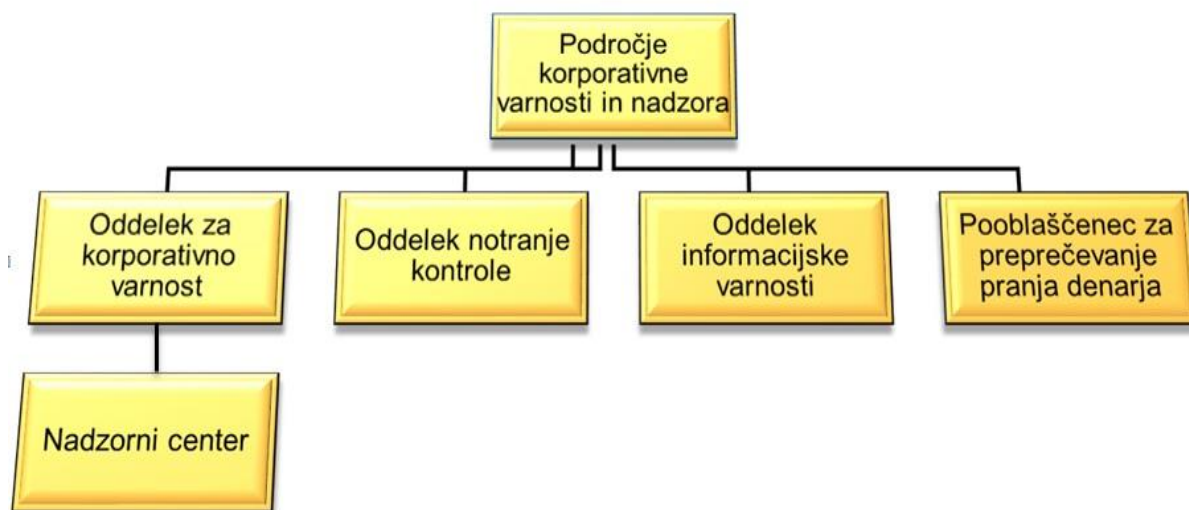
Oddelek informacijske varnosti skrbi za varovanje podatkov, informacij in informacijskih virov. Izvaja ocene informacijskih tveganj (t. i. IT tveganj), sodeluje pri izdelavi načrtov neprekinjenega poslovanja in skrbi za njihovo ažurno dopolnjevanje, nadzoruje njihovo izvajanje ter nadzira dodeljevanje dostopov do posameznih informacijskih virov. Na dalje razvija in vzdržuje politike, navodila, postopke, priročnike s področja varovanja informacij ter skrbi za program izobraževanja in vzpostavitev ustreznega nivoja varnostne kulture vseh zaposlenih. V sodelovanju s Področjem informacijske tehnologije vpeljuje varnostne mehanizme, ki zagotavljajo varno delovanje informacijskega sistema (<http://www.intranet.si/predstavitev-sektorjev/23570/Podrocje-korporativne-varnosti-in-nadzora>).

Pooblaščenec za preprečevanje pranja denarja

Osnovno delovno področje pooblaščenca za preprečevanje pranja denarja predstavlja skrb za vzpostavitev, delovanje in razvoj sistema odkrivanja in preprečevanja pranja denarja in financiranja terorizma, skrb za pravilno in pravočasno sporočanje podatkov Uradu za preprečevanje pranja denarja, sodelovanje pri pripravi in spremembah operativnih postopkov ter pri pripravi določb notranjih aktov, ki se nanašajo na preprečevanje in odkrivanje pranja denarja in financiranja terorizma, sodelovanje pri izdelavi smernic za opravljanje kontrole v zvezi s preprečevanjem in odkrivanjem pranja denarja in financiranja terorizma, spremljanje in koordiniranje dejavnosti na področju odkrivanja in preprečevanja pranja denarja in financiranja terorizma, sodelovanje pri vzpostavitvi in razvoju informacijske podpore za izvajanje dejavnosti v zvezi z odkrivanjem in preprečevanjem pranja denarja in financiranja terorizma, poslovodstvu daje pobude in predloge za izboljšanje sistema odkrivanja in preprečevanja pranja denarja in financiranja terorizma, sodelovanje pri pripravi programov

strokovnega usposabljanja in izobraževanja zaposlenih na področju preprečevanja in odkrivanja pranja denarja in financiranja terorizma (<http://www.intranet.si/predstavitev-sektorjev/23570/Podrocje-korporativne-varnosti-in-nadzora>).

Za nazornejšo predstavitev je na Sliki 2 predstavljen organigram PKVN-ja:



Slika 2: Organigram PKVN-ja

Vir: Prirejeno po: internem viru Pošte Slovenije d.o.o.

3.2 Nadzorni center Pošte Slovenije d.o.o.

Nadzorni center (v nadaljevanju: NC) velja za enega najobčutljivejših in najpomembnejših členov v sistemu varovanja. Iz sistemov tehničnega varovanja se v NC stekajo vsi varnostno relevantni podatki, tam se jih obdela in arhivira ter z njimi seznanja pristojne službe. Zato je nujno potrebna njegova varnostna brezhibnost, tehnična dovršenost in ne nazadnje organizacijska učinkovitost (Petek, 2012, str. 8–9).

NC Pošte (katerega operativne delovne naloge spadajo v PKVN) je pododdelek Oddelka za korporativno varnost in se nahaja v prostorih Poštnega logističnega centra Maribor (v nadaljevanju: PLC Maribor). Zaradi občutljivosti dela, možnih zlorab, pritiskov ali morebitnih groženj, predvsem pa zaradi varovanja osebnih podatkov je bila prostorom in operaterjem NC-ja namenjena posebna obravnava, kar v praksi pomeni, da so prostori in operaterji NC-ja v največji možni meri ločeni od ostalih vhodov, prostorov in delavcev v PLC-ju Maribor. Tako je NC dodatno tehnično varovan z videonadzorom pred vhodom v NC, ima pa tudi posebno elektronsko-mehansko varovalno ključavnico na vratih NC-ja, ki

omogoča kontrolo vstopa le pooblaščenim osebam in operaterjem, ki delajo v njem. Na opisan način se zagotavlja varnost in nemoteno delovanje NC-ja. Le-to je nujno potrebno, saj je opremljen z najsodobnejšo informacijsko tehnologijo, ki omogoča nemoteno in kvalitetno operativno izvedbo delovnih nalog, katere v osnovi zajemajo sledenje vozil in nadzor poštnih poslovalnic z videonadzornim sistemom (Petek, 2012, str. 9).

Potrebno je poudariti, da je Pošta zgradila NC izključno za lastne potrebe. Zato le-ta ni grajen in tehnično opremljen po predpisih o VNC-ju v zasebnem varovanju ter ne ustreza vsem določilom, ki so s standardi predpisani v ZZasV-1 in določeni v Odredbi o določitvi standardov, ki so obvezni na področju zasebnega varovanja²¹ za VNC (SIST EN 50518²², SIST EN 50131²³, SIST EN 50132²⁴, SIST EN 50133²⁵, SIST EN 50134²⁶, SIST EN 50136²⁷, SIST EN 54²⁸, SIST EN 1522:2000²⁹).

NC je začel z operativnim izvajanjem nalog in del povezanih z dejavnostjo NC-ja v začetku avgusta 2012. Trenutno lahko za potrebe varovanja ljudi in premoženja spremlja, obdeluje, posreduje in arhivira videopodatke iz 438-ih poštnih poslovalnic in drugih lokacij Pošte ter preko vzpostavljenega sistema GPS³⁰ za sledenje vozil nadzira 331 poštnih vozil, od katerih jih ima 170 stikalo za klic v sili (t. i. panik stikalo). Poštna vozila so razporejena po vsej RS ter operativno delujejo v vseh poslovnih enotah Pošte.

3.2.1 Tehnična opremljenost Nadzornega centra Pošte Slovenije d.o.o.

Kot že omenjeno je NC opremljen z najsodobnejšo opremo in programsko podporo na področju računalništva in informacijske tehnologije. Vsa ta tehnika omogoča 24-urni nadzor in snemanje aktualnih dogajanj ter neprekinjeno, učinkovito in hitro pošiljanje in obdelavo

²¹ Izdana na podlagi četrtega odstavka 13. člena ZZasV-1 (Ur. l. RS, št. 17/11), dne 15. 2. 2012.

²² SIST EN 50518 – Nadzorni in sprejemni centri za alarme, 2011.

²³ SIST EN 50131 – Alarmni sistemi – Sistemi za javljanje vloma in rop, 2005.

²⁴ SIST EN 50132 – Alarmni sistemi – Nadzorni sistemi CCTV za uporabo v aplikacijah varovanja, 2010.

²⁵ SIST EN 50133 – Alarmni sistemi – Sistemi za nadzor dostopa za uporabo v aplikacijah varovanja, 2010.

²⁶ SIST EN 50134 – Alarmni sistemi – Socialni alarmni sistemi, 2010.

²⁷ SIST EN 50136 – Alarmni sistemi – Sistemi in oprema za prenos alarma, 2008.

²⁸ SIST EN 54 – Sistemi za odkrivanje in javljanje požara in alarmiranje, 2010.

²⁹ SIST EN 1522:2000 – Okna, vrata, polkna in rolete – Odpornost proti izstrelkom iz strelnega orožja – Zahteve in klasifikacija, 2010.

³⁰ GPS (angl. Global Positioning System) je globalni sistem pozicioniranja ali sistem globalnega pozicioniranja.

podatkov, ki se stekajo v NC. Vse morebitne tehnične težave se hitro in učinkovito rešujejo z učinkovitim sodelovanjem s Področjem informacijske tehnologije.

Za nemoteno delovanje NC-ja sta opremljeni dve delovni mesti, vsaka s svojim računalnikom in dvema monitorjema ter centralno videosteno³¹.

Tehnična opremljenost NC-ja obsega tri zmogljive delovne postaje Hewlett-Packard (v nadaljevanju: HP) za potrebe videonadzora in sledenja vozil, dva tanka klienta³² HP za komunikacijo s PE, dva 22-palčna LCD monitorja HP, štiri 27-palčne LCD monitorje Eizo, štiri 60-palčne LCD monitorje Sharp za potrebe videostene, dva IP telefona Cisco, tri 3D Connexion miške Space Navigator, dvakrat po dve miški in tipkovnici HP in Logitech, dvojne slušalke Jabra in tiskalnik Lexmark.

Na spodnji Sliki 3 sta prikazani delovni mesti operaterjev in videostena v NC-ju Pošte.



Slika 3: Nadzorni center Pošte Slovenije d.o.o.

Vir: Lasten

³¹ Videostena (angl. Video wall) je sestavljena iz več računalniških monitorjev, projektorjev ali televizijskih sprejemnikov, spojenih tako, da tvorijo en velik zaslon.

³² Tanki klient (angl. Thin client) je računalnik, narejen samo za dostop in uporabo aplikacij oz. programov na strežniku, v oblaku itd.

3.2.2 Delo operaterjev v Nadzornem centru Pošte Slovenije d.o.o.

V NC-ju delajo trije operaterji v triizmenskem 20-urnem delovniku. V jutranji izmeni jim pomaga tudi vodja NC-ja. Primarni nalogi operaterjev sta sledenje poštnih vozil in nadzor poštnih poslovalnic preko videonadzornega sistema. Načeloma pa lahko delo operaterjev v NC-ju Pošte razdelimo na operativno delo, administrativno delo in telefonske komunikacije.

Operativna dela:

- nadzor sprejema alarmnih in drugih (testnih) signalov videonadzornega sistema,
- sprejem obvestil o ponarejenih bankovcih v poštnih poslovalnicah in obveščanje policije,
- konfiguracija videonadzornega sistema,
- izdelava videoposnetkov,
- nadzor sprejema alarmnih in drugih signalov sistema za spremljanje vozil,
- konfiguracija sistema za spremljanje vozil,
- sprejem in obdelava informacij o delovanju sistemov tehničnega varovanja,
- posredovanje podatkov vodji NC-ja.

Administrativna dela:

- zbiranje, posredovanje in arhiviranje elektronskih in telefaks sporočil, poročil o delu drugih služb ipd.,
- pisanje in arhiviranje poročil, dopisov in drugih strokovnih pisnih izdelkov,
- pisanje poročila o delu NC-ja,
- vodenje evidence priklopov, odklopov, testiranj in sprememb delovanja naprav v varovanih objektih Pošte,
- druga administrativna dela po naročilu vodje NC-ja.

Telefonska komunikacija:

- obveščanje uporabnikov tehničnega varovanja na poštnih poslovalnicah in v vozilih Pošte,
- podajanje informacij o videonadzornem sistemu Pošte,
- komunikacija s predstavniki policije oz. Ministrstva za notranje zadeve Republike Slovenije in drugih pristojnih organov v primeru izrednih dogodkov,
- komunikacija s pogodbenimi izvajalci pri testiranju in vzdrževanju sistemov tehničnega varovanja (Navodilo za delo in organizacijo Nadzornega centra Pošte Slovenije d.o.o., 2013).

Operaterji v primeru alarma na vozilu aktivno sodelujejo z vozniki in voznimi parki vseh PE Pošte preko računalniškega programa CVS-Mobile, namenjenega sledenju vozil, ki omogoča sledenje vozil v realnem času, analize voženj in postankov vozil ter v primeru aktiviranega alarma v vozilu prenos alarma v NC, kjer operaterji preko monitorjev spremljajo vozilo na določeni lokaciji in postopajo po določenem protokolu.

Operaterji pri izvajanju videonadzora poštnih lokacij uporabljajo program MxControlCenter (v nadaljevanju: MxCC) podjetja Mobotix, ki omogoča upravljanje s kamerami videonadzornega sistema Pošte in z videoposnetki. MxCC je eden najsodobnejših in najstabilnejših na svetu, kar se dosega z rednimi programskimi posodobitvami. Program je bil izbran zaradi kompatibilnosti z Mobotixovimi kamerami in zaradi optimalnega delovanja samega videonadzornega sistema. Program ni testiran po standardu SIST EN 50132, vendar pa izpolnjuje večino njegovih določil in ga v tujini uporabljajo različne varnostne službe.

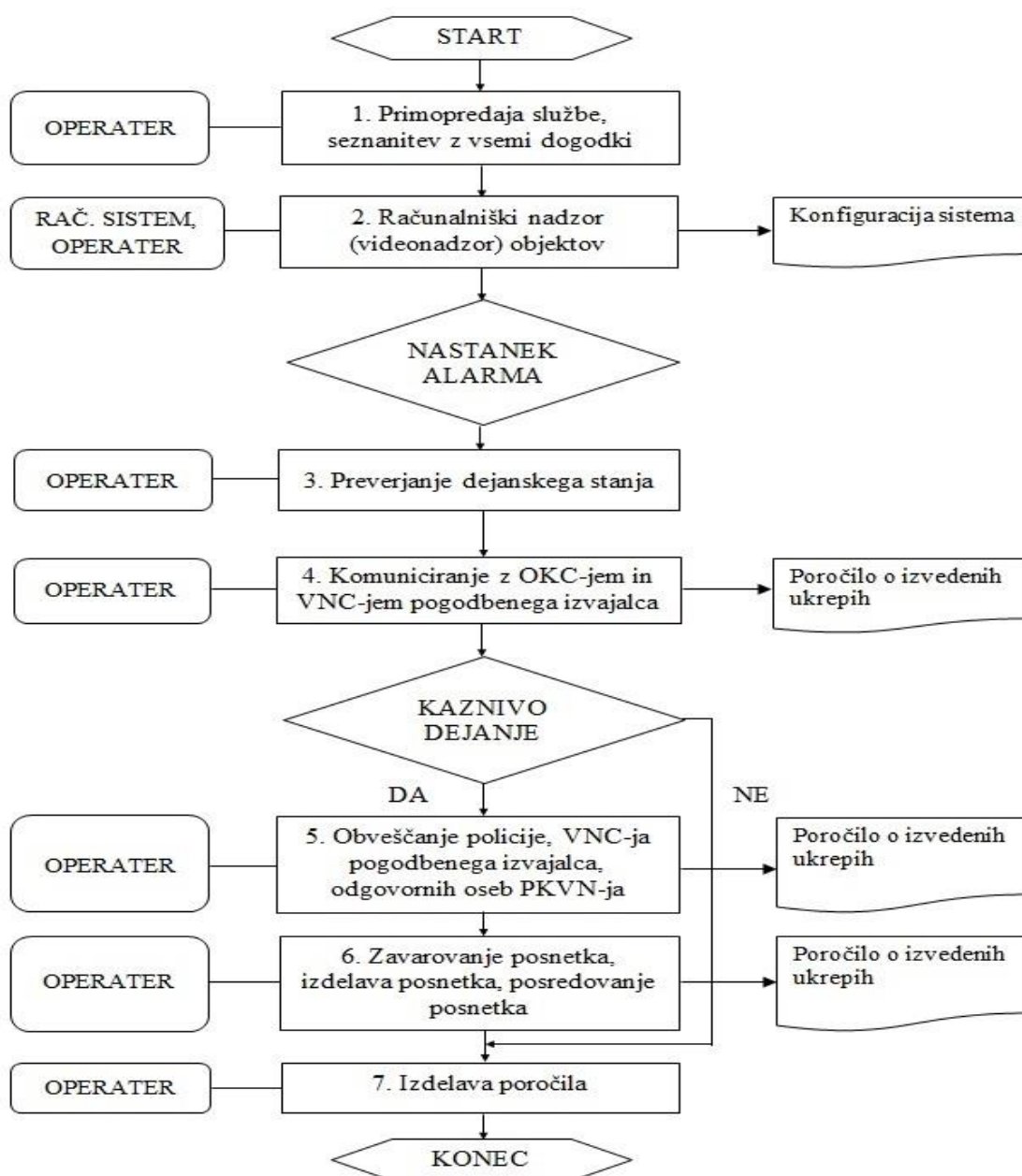


Slika 4: Program MxCC

Vir: <http://www.mobotix.si/produkti/mxcontrolcenter/>

Program omogoča izbiro dvojnega zaslona, na katerem je lahko prikazan načrt objekta in hkrati tudi lokacije kamer na objektu, iskanje dogodkov, procesiranje slik, odpravljanje popačenosti leč in PTZ podpora, seznam alarmov, avtomatični detektor kamere, avtomatični preklop med kamerami ali med načrti, integriran videoarhiv s podatkovnimi strežniki in upravljanje s podatki oz. z videoposnetki, konfiguriranje kamer in nadgradenj, čarovnik za avtomatično konfiguracijo in namestitvev številnih profilov kamere (<http://www.mobotix.si/produkti/mxcontrolcenter/>).

Operaterji preko monitorjev spremljajo dogajanje na določeni lokaciji in v primeru izrednih dogodkov (npr. aktivirani alarmi, tatvine trgovskega blaga, okvare varnostnega sistema itd.) postopajo po določenih protokolih, ki so odvisni od vrste dogodka. Tako se najprej poskuša ugotoviti vzrok izrednega dogodka, temu pa nato po potrebi sledi obveščanje pristojnih služb (policija, pogodbene varnostne službe, vzdrževalne službe, nadrejeni, gasilci, reševalne službe itd.). Operaterji nato shranijo posnetke, napišejo in shranijo poročilo o dogodku, obveščajo osebe po protokolu ter izpolnijo in hranijo predpisane evidence. Postopke oz. potek dela operaterjev NC-ja v primeru sprožitve alarma v poštni poslovalnici prikazuje Slika 5.



Slika 5: Diagram poteka dela operaterja v NC-ju ob sprožitvi alarma v poštni poslovalnici

Vir: Navodilo za delo in organizacijo Nadzornega centra Pošte Slovenije d.o.o.

Posebno pozornost operaterji posvečajo ravnanju s shranjenimi videoposnetki, na katerih se največkrat nahajajo osebni podatki različnih oseb oz. zbirki osebnih podatkov, ki so nastali z izvajanjem videonadzora. Pri tem morajo operaterji upoštevati predpise iz Odločbe o izvajanju videonadzora (zadnja je bila v skladu s 27. členom Akta o ustanovitvi in 75. členom ZVOP-1 izdana februarja 2014). Le-ta med drugim predpisuje, da se zavarovani oz. shranjeni videoposnetki lahko hranijo največ 60 dni ter kdo ima pravice do pregledovanja, shranjevanja, upravljanja in izvoza videoposnetkov na prenosne medije (samo pooblaščen osebe, v večini primerov to opravljajo operaterji in vodja NC-ja). Vsa omenjena dejanja je možno storiti samo v NC-ju.

V primeru zahtevka policije, ki mora temeljiti na podlagi 115. člena ZNPPol (obveznost posredovanja podatkov), kadar policija izvaja naloge po 148. členu Zakona o kazenskem postopku (Uradni list RS, št. 32/12 – UPB8) in so podani razlogi za sum, da je bilo storjeno kaznivo dejanje, za katero se storilec preganja po uradni dolžnosti (Informacijski pooblaščenec, 2013, str. 1), za posredovanje dokaznega gradiva oz. videoposnetkov iz zbirke osebnih podatkov, se le-ti posnamejo na prenosni snemalni medij v NC-ju ter pošljejo s priporočeno pošto pošiljko policiji ali pa jih pridejo zaseči v PLC Maribor, kjer se jim izroči fizično (v zadnjem obdobju se uvaja odlaganje videoposnetkov preko varne internetne povezave na sinhroniziran strežnik, vendar več o tem v nadaljevanju diplomskega dela).

Operaterji beležijo vsak shranjen videoposnetek iz določene kamere, ki je bil shranjen na računalnik v NC-ju ter kasneje posnet na prenosni snemalni medij. Iz teh podatkov je možno razbrati vse potrebne informacije o dostopanju in ravnanju z videopodatki iz določene kamere.

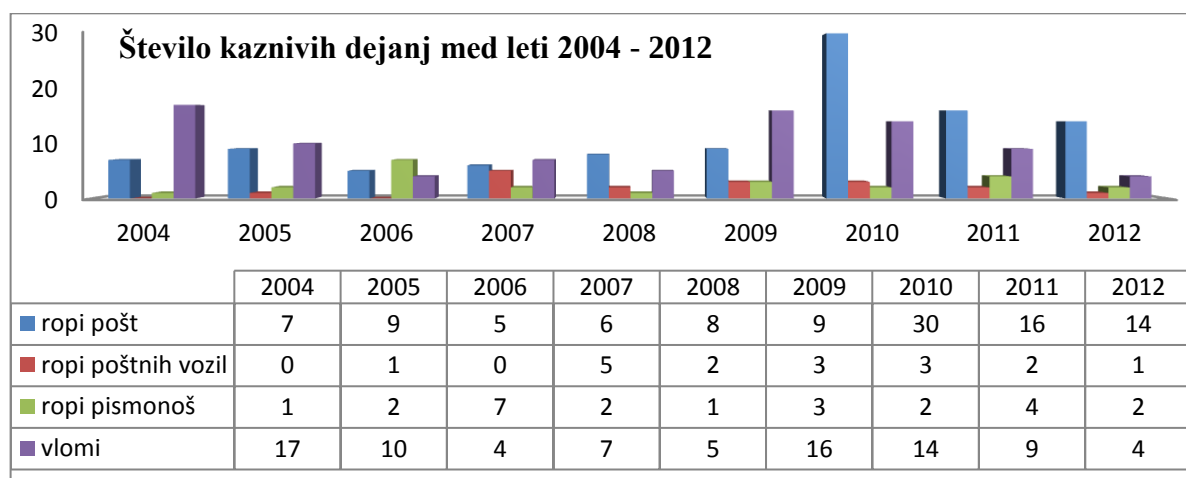
4 VIDEONADZORNI SISTEM POŠTE SLOVENIJE D.O.O.

4.1 Odločitev za vzpostavitev videonadzora

Potreba po videonadzoru v poštnih poslovalnicah se je začela pojavljati zaradi vedno večjega števila ropov in vlomov, ki so od leta 2009 naprej strmo naraščali in dosegli svoj vrhunec z umorom uslužbenke leta 2011 v Kresnicah. Pošta je na podlagi ocene stopnje tveganja, v kateri je izstopalo naraščanje ropov in vlomov v poštno poslovalnice, ter zaradi pritiska zunanje javnosti (mediji, stranke), notranje javnosti (sindikati, zaposleni), zahtev nadzornih organov (Banka Slovenije) in zavarovalnic, pri katerih ima Pošta zavarovano odgovornost (prenos tveganj – npr. v primeru roba ali kraje se povrne škoda) začela iskati rešitve, ki bi pripomogle k večji varnosti ljudi in premoženja. Odločitev je bila, da se izvedejo naslednji ukrepi (Pošta Slovenije d.o.o., 2014):

- dodatno fizično varovanje v poštnih poslovalnicah z varnostniki pogodbenega izvajalca varnostnih storitev, ki pa je bil le začasen ukrep in se lahko uporabi kadarkoli,
- pospešena postavitve dodatne mehanske zaščite delovnega mesta,
- uvedba sistema za obarvanje gotovine (dimni bankovci),
- postavitve videonadzornega sistema v vseh poštnih poslovalnicah.

Grafikon 1 prikazuje število kaznivih dejanj na Pošti med leti 2004 in 2012 oz. do vzpostavitve videonadzornega sistema. V statistiko pa niso zajete tatvine prodajnih artiklov v poštnih poslovalnicah, saj jih je brez videonadzora praktično nemogoče dokazati.



Grafikon 1: Število kaznivih dejanj na Pošti med leti 2004 in 2012

Vir: Prirejeno po: internem viru Pošte Slovenije d.o.o.

Odločitev o vzpostavitvi videonadzornega sistema je bila sprejeta leta 2011, s testiranjem kamer in s prvimi namestitvami pa so začeli leta 2012. Zadnje kamere so bile v poštne poslovalnice in druge lokacije Pošte nameščene maja 2014, s čimer se je zaključil proces dodatnih varnostnih ukrepov, načrtovanih s strani PKVN-ja.

4.2 Zahteve Pošte Slovenije d.o.o. za videonadzorni sistem

Pošta ima visoko razvito in napredno informacijsko infrastrukturo oz. globalno komunikacijsko omrežje (v nadaljevanju: GKO³³), zato so iskali rešitev, da bi takšno infrastrukturo tudi maksimalno izkoristili. Zaradi velikosti in prostorske razširjenosti načrtovanega videonadzornega sistema je bila že v osnovi predvidena postavitve t. i. decentraliziranega³⁴ videonadzornega sistema z možnostjo centralnega upravljanja, ki mora omogočati varnost podatkov oz. videoposnetkov (možnost vdora, tatvina podatkov itd.), nizko obremenitev GKO-ja in majhno porabo električne energije (predvideno je bilo čez 1.200 kamer). Z razpisom so začeli iskati ustreznega ponudnika visoko zmogljivih IP megapiksel kamer s pripadajočo tehnologijo in podporno programsko opremo, ki bi jim omogočil uresničitev in izpeljavo tako zahtevnega projekta.

Pošta je za svoj videonadzorni sistem postavila minimalne zahteve, objavljene v razpisu (Pošta Slovenije d.o.o., 2011):

- slike se morajo generirati in snemati z minimalno ločljivostjo 3 megapiksle na sliko na kamero, da bi zagotovili identifikacijo oseb in objektov na slikah v »živo« in na videoposnetkih,
- omogočen mora biti simultan pogled in snemanje slike v »živo« ter ogled posnetih slik in videosekvenc brez rizika za izgubo podatkov,

³³ GKO je globalno komunikacijsko omrežje Pošte Slovenije d.o.o.; več o GKO v poglavju 4.5 Globalno komunikacijsko omrežje Pošte Slovenije d.o.o.

³⁴ Posebnost le-teh je, da kamera ni samo zajemalec slike, temveč postane računalnik s potrebno umetno inteligenco ter nosilec podatkov (strežnik). Takšni sistemi ne potrebujejo več visoko zmogljivih strežnikov za nadzor in shranjevanje podatkov, temveč lahko shranjujejo posnetke na lastne pomnilniške medije – največkrat so to razne SD (Secure Digital) kartice – ki so vgrajene v kamere, ali pa že obdelane posnetke pošiljajo na centralni strežnik in tako odpade potreba po lokalnem strežniku (v primeru Pošte bi teh takrat bilo približno 500).

- za zmanjšanje stroškov mora omogočati napajanje kamer preko omrežnega kabla (PoE³⁵) ter ne sme vsebovati lokalnih strežnikov na samih objektih,
- sistem mora biti sposoben delovati pri temperaturi od –30 °C do +60 °C brez dodatnega gretja ali hlajenja kamer,
- kamere morajo omogočati premostitev izpada podatkovne povezave do centralnega sistema snemanja pri polni resoluciji³⁶ vsaj za 48 ur ter v primeru lokalnega snemanja omogočati možnost nastavljanja časovnega intervala prenosa videopodatkov s kamere na centralni shranjevalni strežnik,
- omogočeno mora biti delovanje in konfiguracija z uporabo SIP³⁷ IP videotelefona in nadzorne programske opreme, omogočena pa mora biti tudi napredna konfiguracija kamere preko spletnega brskalnika,
- zahteva po IP megapiksel kamerah brez gibljivih delov,
- videonadzorni sistem mora omogočati sprejemanje in oddajanje signalov obstoječim alarmnim centralam, ki so že nameščene v poštnih poslovalnicah (v primeru zaznanega dogodka na kameri se pošlje signal alarmni centrali, v primeru zaznanega dogodka alarmne centrale se pošlje signal kameri),
- vsa programska oprema za kamere in NC, kakor tudi njene posodobitve na novejšo verzijo, mora biti naročniku na voljo brezplačno v času življenjske dobe videonadzornega sistema oz. mora biti ta strošek vključen v nabavno ceno opreme,
- možnost priključitve kamer različnih proizvajalcev brez dodatnega nakupa licenc programske opreme za nadzor kamer,
- centralna administracija in nadzor celotnega videonadzornega sistema, sistem pa mora tudi omogočati večnivojske pravice upravljanja s kamero in z videonadzornim sistemom,
- kamere morajo omogočati upravljanje z videopodatki glede na časovno omejitev in/ali prostorsko omejitev (količina podatkov),
- za potrebe prenosa videopodatkov na centralno lokacijo in delovanje NC-ja se uporablja obstoječe omrežje Pošte (GKO),

³⁵ PoE (angl. Power over Ethernet) – omogoča električno napajanje v lokalnem omrežju oz. LAN omrežju (angl. Local Area Network).

³⁶ Resolucija oz. ločljivost slike se nanaša na število pik na sliki in nam pove, koliko pikslov (piksel je najmanjša enota slike, ki se jo lahko prebere ali nariše) je zapisanih na neki razdalji.

³⁷ SIP (angl. Session Initiation Protocol) zagotavlja vzpostavitev govornih in videokomunikacij, ugotavljanje prisotnosti, prenos hipnih sporočil itd.

- shranjevanje videopodatkov na centralni shranjevalni strežnik (preko TCP in SMB³⁸ programskega protokola z uporabo ustreznega uporabniškega imena in gesla za pridobitev pravic shranjevanja oz. snemanja), ki je del namenskega optičnega omrežja z zagotovljeno zadostno količino fizičnega diskovnega prostora kot del informacijske strukture in je nameščen v varnih sistemskih sobah PLC-ja Maribor.

Izbira najustreznejšega ponudnika

Testiranih je bilo več vrst IP megapiksel kamer in ostale opreme za videonadzor različnih ponudnikov. Velik problem je predstavljala integrirana programska oprema IP megapiksel kamer, ki je omogočala dokaj enostaven vdor in s tem zlorabo videopodatkov. Takšni sistemi niso ustrezali pogojem in posledično niso bili primerni za vgradnjo in za uporabo v GKO-ju Pošte. Ker je bil videonadzorni sistem predviden za lastne potrebe Pošte, ni bilo potrebe za doseganje standardov v zasebnem varovanju, zato je bil ves poudarek na doseganju varnosti, ki jo ima GKO Pošte. Po zelo natančnih testiranjih predvsem varnostne plati kamer ter same obremenitve GKO-ja s prenosom podatkov so se na koncu odločili za videonadzorni sistem, ki ga proizvaja nemško podjetje Mobotix.

4.3 Tehnika videonadzornega sistema Pošte Slovenije d.o.o.

Podjetje Mobotix je ponudilo celovito rešitev v obliki popolnoma decentraliziranega IP megapiksel videonadzornega sistema s centralnim upravljanjem, ki ne potrebuje lokalnih ali centralnega snemalnega strežnika, temveč shranjuje videopodatke na snemalni medij v kameri. Omogoča pa tudi shranjevanje videopodatkov na centralni snemalni strežnik ali drug snemalni medij na drugi lokaciji, odvisno od želja in potreb upravitelja ali lastnika videonadzornega sistema. Glede varnosti podatkov pa velja še omeniti, da je podjetje ponudilo oz. omogočilo brezplačno namestitvev digitalnega potrdila Microsoft CA³⁹, ki nepooblaščenim osebam onemogoča dostop do podatkov na spominskih medijih.

³⁸SMB (angl. Server Message Block) – programski protokol.

³⁹CA (angl. Certification Authority) – organ za potrdila, ki je podoben notarju, izdaja digitalna potrdila, preveri njihovo veljavnost in spremlja certifikat ter ga razveljavi, če je potekel. Nepooblaščenim osebam preprečuje dostop do podatkov.

Ostale lastnosti ponujenega videonadzornega sistema so še IP megapiksel kamere s CMOS⁴⁰ senzorjem s 3 in 5 megapiksli ločljivosti, z vgrajenim zvočnikom in mikrofonom, brez gibljivih delov, posledično minimalnim vzdrževanjem, PoE napajanjem, porabo približno 3 W električne energije na posamezno kamero, brez plačljive programske opreme in licenc, neomejeno nadgrajevanje programske opreme in videonadzornega sistema, možnost povezave lokacij brez večjih dodatnih stroškov, priklop kamer na obstoječe omrežje Pošte (tj. GKO), zelo hitra in enostavna postavitve.

Pri konfiguraciji kamer je preko programa MxCC omogočena možnost nastavitve zaznavanja gibanja s pomočjo načina videogibanja (angl. Video motion), pri katerem se preko sprožilcev oz. aktivatorjev (angl. Trigger) nastavlja področja, kjer želimo, da kamera zazna gibanje in začne s snemanjem, ali z novejšim aktivnim senzorjem gibanja (angl. MxActivitySensor), ki prične s snemanjem, če se pomemben dogodek dejansko zgodi. Razne motnje (gibanje dreves v vetru, sence, dež ali sneženje) enostavno prezre in ne snema. S pametno nastavitvijo teh dveh senzorjev, ki se največkrat nastavljata ročno v odvisnosti od specifik določene lokacije, lahko drastično zmanjšamo porabo prostora na spominskih medijih in povečamo arhiv posnetkov. Za določene potrebe marketinga se lahko nastavi tudi linije štetja (angl. Counting Line) in področja najpogostejšega gibanja na lokaciji⁴¹ (angl. Heatmap).

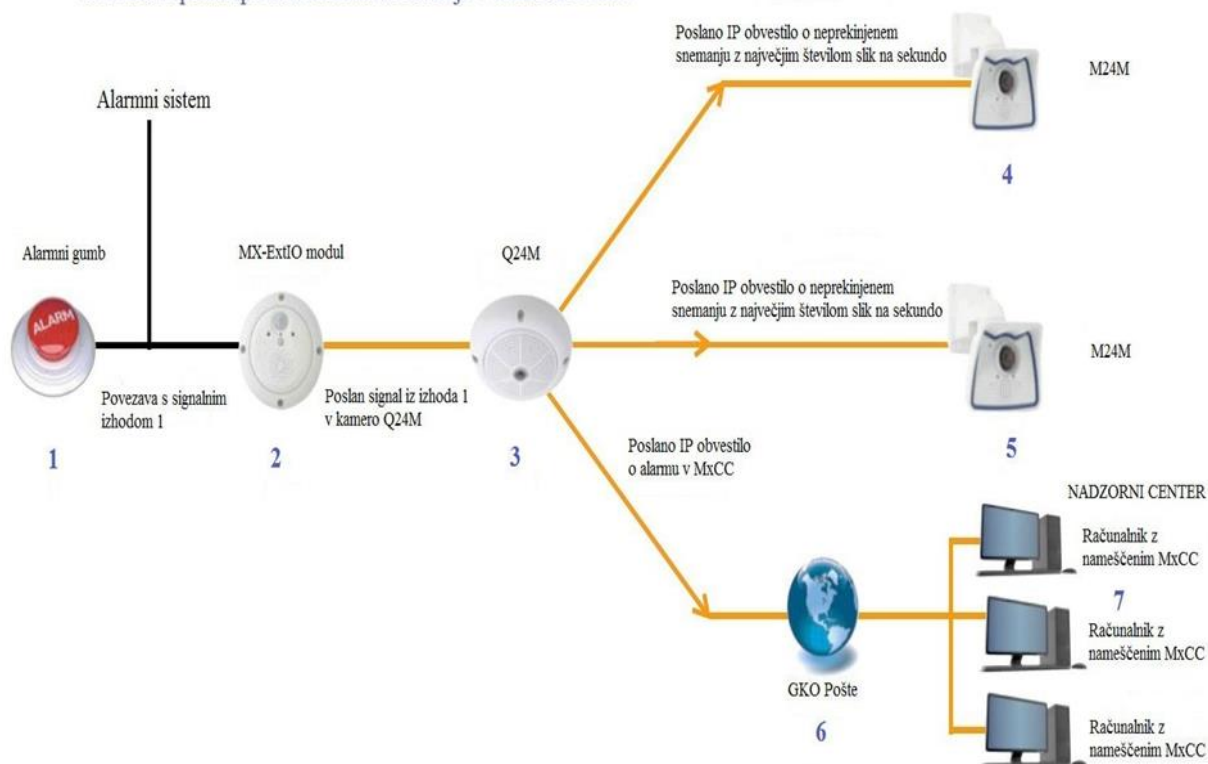
Te številne možnosti konfiguracij kamer s pomočjo programa MxCC omogočajo operaterjem v NC-ju enostavno upravljanje z videonadzornim sistemom Pošte in optimalno nastavitve kamer ter posledično slike na posamezni lokaciji. Omeniti še velja hiter in enostaven dostop do posnetkov in takojšen prikaz in vklop slike v »živo« iz lokacije, na kateri je bil aktiviran alarm. Operaterjem je to v veliko pomoč, saj jim ni potrebno iskati lokacije aktiviranega alarma in lahko takoj začnejo z ugotavljanjem vzroka nastanka alarma in nadaljnjimi postopki, s čimer se zelo zmanjša odzivni čas, ki je ključen v izrednih dogodkih.

Na Sliki 6 je prikazan shematski prenos alarma iz lokacije v NC-ju ter nato v Sliki 7 še prikaz lokacije alarma s sliko v »živo« v MxCC kot ga vidijo operaterji v Nadzornem centru.

⁴⁰ CMOS (angl. Complementary Metal Oxide Semiconductor) je komplementarni metal-oksidni polprevodnik. Eden glavnih sestavnih delov digitalnega fotoaparata je slikovni senzor. Sestavljen je iz majhnih svetlobnih senzorjev (1 svetlobni senzor predstavlja 1 piksel), ki so razporejeni v mrežo in nameščeni na mikročip skupaj z elektroniko za beleženje svetlobnih vrednosti. Svetlobni senzori zajamejo svetlobo in jo pretvorijo v električni naboj, nato pa se te podatke pošlje v procesor, ki določi vrednosti pikslov (<https://sites.google.com/site/tp4fotografija/e-skripta/slikovni-senzor>, dne 1. 6. 2014).

⁴¹ Več o tem v poglavju 5.5 Možnost uporabe videonadzornega sistema za marketing.

Shematski prikaz prenosa alarma iz lokacije v nadzorni center



Slika 6: Shematski prikaz prenosa alarma iz lokacije v NC

Vir: Prirejeno po: Project Slovenien V4 – Mobotix sheme sistema



Slika 7: Primer prikaza aktiviranega alarma v poštni poslovalnici v programu MxCC

Vir: Lasten

4.3.1 Videonadzorne kamere

Osnova videonadzornega sistema Pošte je pet različnih modelov Mobotixovih IP megapiksel kamer, ki imajo nekaj skupnih lastnosti (Mobotix, 2014):

- velika uporabnost, kar pomeni, da se lahko hitro in preprosto namestijo na strop, steno, steber ali tla ter se uporabljajo za snemanje v notranjih ali zunanjih prostorih podnevi in ponoči,
- imajo vgrajen snemalni medij z visoko resolucijskim (Hi-Res) DVR-jem,
- procesor lahko procesira ločljivost oz. resolucijo slike do velikost QXGA (2.048 x 1.536 pikslov), kar je 2,5 krat več kot FULL HD⁴² (1.920 x 1.080 pikslov) – navedeno teoretično pomeni, da lahko na sliki vidimo 2,5 krat več podrobnosti, kar je z varnostnega vidika zelo dobrodošlo,
- shranjevanje posnetkov s pomočjo različnih videokodekov⁴³ MxPEG, M-JPEG, JPG, H.264 (SIP samo video), kjer izstopa predvsem izredno zmogljiv MxPEG podjetja Mobotix,
- popolna sinhronizacija slike in zvoka (v »živo« in snemanje),
- CMOS senzorji brez zaslone z digitalnim povečanim kontrastom in s poljubno nastavljivim območjem merjenja osvetlitve zagotavljajo optimalen nadzor osvetlitve,
- vsaka kamera je IP videotelefon, ki je osnovana po SIP standardih z avtomatičnim alarmnim klicem in daljinskim upravljanjem,
- kamera sporočilo o alarmu pošlje preko elektronske pošte, SMS sporočila, telefonskega klica ali preko PDA⁴⁴,
- so brez internetne obremenitve, so robustne, preproste za vzdrževanje in odporne proti vremenskim razmeram, imajo nameščen digitalni PTZ⁴⁵ ter vgrajen mikrofoni in zvočnik,
- med snemanjem se lahko gleda slika v »živo« ali posnetki, kar je zelo pomembno v izrednih situacijah,

⁴² FULL HD ločljivost oz. resolucija pomeni, da lahko zaslon prikaže sliko v polni ločljivosti, to je 1.920 slikovnih točk po širini in 1.080 slikovnih točk po višini.

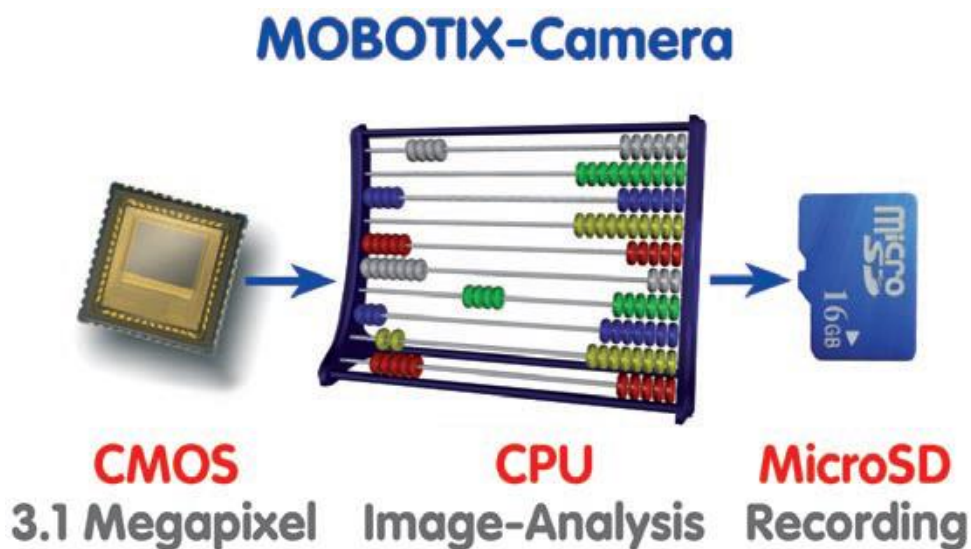
⁴³ Kodek je računalniški program za kodiranje in dekodiranje digitalnih podatkov ali znakov.

⁴⁴ PDA (angl. Personal Digital Asistent) je osebni digitalni pomočnik oz. prenosni računalnik manjše zmogljivosti, prilagojen za ročno uporabo (dlančniki, tablice, mobilni telefoni ipd.).

⁴⁵ PTZ (angl. Pan-Tilt-Zoom) je program v kameri, s katerim lahko sliko daljinsko usmerjamo in povečujemo.

- opremljene so s popolnim sistemom za pregledovanje slike v »živo« ali posnetkov v internetnem brskalniku, ki omogoča iskanje po dogodkih, previjanje dogodkov nazaj, signaliziranje alarma, alarmni seznam na prikazovalniku, četverkotni in večslikovni prikazovalnik (ni potrebe po programski opremi za dostop do videopodatkov, shranjenih na kamerah).

Na spodnji Sliki 8 je prikazan primer obdelave videopodatkov od zajema slike v »živo«, do kodiranja in hrambe podatkov na kameri podjetja Mobotix.



Slika 8: Primer obdelave slike od zajema do obdelave (kodiranja) in shranitve v Mobotixovi kameri

Vir: http://www.mobotix.si/fileadmin/dokumenti/navodila/15mx_MLq24m_en_090625.pdf

Za videonadzor v poštnih poslovalnicah se trenutno uporablja 1.282 naslednjih Mobotixovih IP megapiksel kamer:

- **Q24M in Q25M:** Q24M ima vgrajen CMOS 3 MP⁴⁶ slikovni senzor, njena izboljšana verzija Q25M pa CMOS 5 MP slikovni senzor in še nekatere druge izboljšave. Omogočata več vrst pogledov na prostor kot so normalni 360° pogled (zato sta največkrat nameščeni na strop, v izrednih primerih na steno), povečan pogled, popravljeni pogled, panoramski in dvojni panoramski pogled, panorama fokus pogled ter četverkotni pogled. Le-ta omogoča snemanje iz štirih različnih zornih kotov in s tem omogoča nadziranje celotne sobe ali prostora. Zato se lahko z eno takšno kamero nadomesti do štiri kamere, ki omogočajo samo enojen pogled na prostor. Omogočeno je snemanje v enem od pogledov, medtem ko se lahko za gledanje slike v »živo« ali

⁴⁶ MP – megapiksel.

posnetkov izbere drug pogled. Kameri imata vgrajen Hi-Res DVR za shranjevanje visoko resolucijskih posnetkov, alarmno funkcijo, zvočnik in mikrofona. Prav tako sta odporni proti vremenskim razmeram in sta brez gibljivih delov (<http://www.mobotix.si/produkti/q25/>).

V videonadzorni sistem Pošte je trenutno nameščenih 594 kamer Q24M in 13 kamer Q25M.



Slika 9: Mobotixovi kameri Q24M in Q25M

Vir: <http://www.mobotix.si/produkti/q25/>

- **M24M in M25M:** M24M ima vgrajen CMOS 3 MP slikovni senzor, njena izboljšana verzija M25M pa CMOS 5 MP slikovni senzor in še nekatere druge izboljšave. Omogočata zamenjavo in individualno izbiro leč (tele in širokokotna, dnevna in nočna) ter izbiro dveh načinov pogledov, normalni 180° pogled in povečani pogled, s katerim je mogoče upravljati preko integriranega digitalnega PTZ-ja. Zato lahko z njima nadomestimo do šest kamer, kar zmanjša stroške. Prav tako imata vgrajen Hi-Res DVR za shranjevanje visoko resolucijskih posnetkov, zvočnik in mikrofona. Sta brez gibljivih delov in vodoodporni ter omogočata preprosto in hitro namestitev na steno, steber ali zid. Primerni sta tako za zunanjo kot notranjo uporabo (<http://www.mobotix.si/produkti/m25m/>).

V videonadzorni sistem Pošte je trenutno nameščenih 549 kamer M24M in 44 kamer M25M ter dva starejša modela M14M (2 kameri) in M10M (5 kamer).



Slika 10: Mobotixovi kameri M24M in M25M

Vir: <http://www.mobotix.si/produkti/m25m/>

- **D14D in D15D:** sta prvi dvojni kupolasti IP megapiksel kameri na novi procesorski platformi, ki imata dve medsebojno neodvisni leči s po dvema individualno nastavljivima slikovnim senzorjema (D14D – CMOS 3 MP in D15D – CMOS 5 MP). Možna je individualna izbira leč (tele in širokokotna, dnevna in nočna ter panorama 180°), kar omogoča nadzorovanje in varovanje dveh ločenih sob hkrati ali nadzorovanje prostora in hkrati iskanje detajlov v njem. Omogočata nočno snemanje oz. snemanje v temi. Vgrajen imata Hi-Res DVR za shranjevanje visoko resolucijskih posnetkov (do 6 megapikslov), mikrofona, zvočnika, PIR⁴⁷ senzor gibanja, digitalni PTZ in šok (angl. Shock) senzor proti kraji ter sta brez gibljivih delov. Ena lahko nadomesti do 6 kamer (<http://www.mobotix.si/produkti/d15d/>).

V videonadzorni sistem Pošte je trenutno nameščenih 34 kamer D14D in 26 kamer D15D.

⁴⁷ PIR (angl. Passive InfraRed sensor) je pasivni infrardeči senzor.



Slika 11: Mobotixovi kameri D14D in D15D

Vir: <http://www.mobotix.si/produkti/d15d/>

- **D24M in D25M** sta enojni kupolasti IP megapiksel kameri na novi procesorski platformi z enakimi karakteristikami kot D14D in D15D, vendar s to razliko, da imata vgrajeno samo eno lečo za zajem slike z vgrajenima slikovnima senzorjema D24M – CMOS 3 MP in D25M – CMOS 5 MP ter da se lahko pokriva samo en prostor. Ena lahko nadomesti do 6 kamer. S pomočjo MX-ExtIO modula se lahko nadgradi v interfon sistem (<http://www.mobotix.si/produkti/d25m/>).

V videonadzorni sistem Pošte je trenutno nameščenih 7 kamer D24M in 2 kameri D25M ter ena starejša D22M kamera.



Slika 12: Mobotixovi kameri D24M in D25M

Vir: <http://www.mobotix.si/produkti/d25m/>

- **T24M in T25M** sta IP megapiksel videodomofona oz. vratni postaji, ki omogočata enostavno namestitev, dvosmerni videoprenos po internetu, 360° pogled brez mrtvih kotov, omogočeno je snemanje zvoka, brezključni dostop (angl. keyless access) z možnostjo časovne nastavitve in poročanjem sporočil. T24M ima vgrajen CMOS 3 MP slikovni senzor, novejši T25M pa CMOS 5 MP slikovni senzor in Hi-Res DVR za shranjevanje visoko resolucijskih posnetkov (Mobotix, 2014).

V videonadzorni sistem Pošte je trenutno nameščen en domofon T24M na upravi Pošte in po eden T25M v PLC-ju Maribor in poštni poslovalnici v Piranu.



Slika 13: Mobotixova IP megapiksel videodomofona T24M in T25M

Vir: http://www.mobotix.com/eng_GB/Products/Cameras/IP-Video-Door-Station-T25?tab=225237#tab

V videonadzorni sistem Pošte sta nameščeni še dve starejši Mobotixovi kameri Generic.

Tabela 1 prikazuje vse modele in število kamer, ki se trenutno uporabljajo v videonadzornem sistemu Pošte.

Več podatkov o lastnostih kamer je navedeno na spletni strani podjetja Mobotix (<http://www.mobotix.si> ali <http://www.mobotix.com>).

Tabela 1: Modeli in število kamer v videonadzornem sistemu Pošte

Model kamere	Število kamer
MOBOTIX Q24M	594
MOBOTIX Q25M	13
MOBOTIX M24M	549
MOBOTIX M25M	44
MOBOTIX M14M	2
MOBOTIX M10M	5
MOBOTIX D14D	34
MOBOTIX D15D	26
MOBOTIX D24M	7
MOBOTIX D25M	2
MOBOTIX D22M	1
MOBOTIX T24M	1
MOBOTIX T25M	2
MOBOTIX GENERIC	2
SKUPAJ	1282

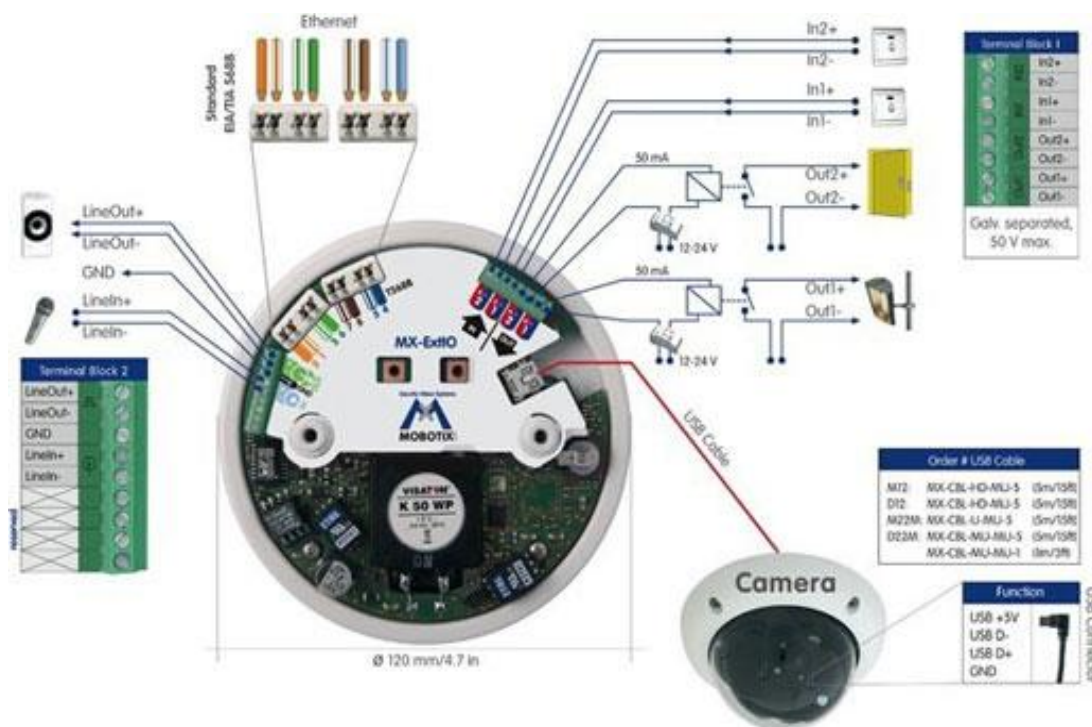
Vir: Lasten

4.3.2 Vmesnik oziroma MX-ExtIO modul

Vmesnik oz. v našem primeru MX-ExtIO modul je lahko s kamero priključen preko USB ključa ali direktno na internetno omrežje ter tako predstavlja izboljšano Mobotixovo kamero z zmogljivo avdioenoto z vgrajenim mikrofonom in zvočnikom, PIR-om in temperaturnim senzorjem ter z dodatnim zunanjim in notranjim stikalom. Zunanji in notranji interfon⁴⁸ se enostavno namesti na dva osvetljena gumba (<http://www.mobotix.si/produkti/extio/>).

V videonadzornem sistemu Pošte se MX-ExtIO modul uporablja za povezavo kamer z alarmnimi centralami tehničnega varovanja. S kamero je povezan preko IT tehnologije ter nam omogoča hkraten prenos različnih alarmov iz lokacije v NC in v pristojno varnostno službo, v katero prenos alarma poteka po telefonskih linijah.

⁴⁸ Interfon je naprava, ki jo uporabljamo za govorno komuniciranje znotraj določene organizacije.



Slika 14: Prikaz notranjosti MX-ExtIO modula

Vir: <http://www.mobotix.si/produkti/extio/>

4.4 Primer postavitve kamer (pokritost prostora z videonadzorom)

Sama namestitvev oz. montaža ter vključevanje kamer iz posameznih poštних poslovalnic v videonadzorni sistem je potekala brez večjih zapletov s hitrostjo od ene do treh poštних poslovalnic na dan, odvisno od velikosti poštних poslovalnic, v katere se je tisti dan nameščal videonadzor. Hitro nameščanje je bilo možno zaradi enostavne montaže, manjšega števila kamer na posamezni lokaciji (kar omogoča 360° pogled kamere), že nameščenega UPS-a⁴⁹, vzpostavljenega GKO-ja za potrebe poštних storitev v poštних poslovalnicah, PoE stikala za napajanje kamer in ker ni bilo potrebe po obstoječi ali novi računalniški infrastrukturi na lokaciji. Načrti za postavitve kamer na posamezni lokaciji so bili narejeni tako, da se je na posamezni lokaciji namestilo najmanjše možno število kamer glede na optimalno pokritost prostora z videonadzorom (Pošta Slovenije d.o.o., 2014).

Tako je za večino poštних poslovalnic, ki niso večje od 30 m², bilo za pokritost prostora pri videonadzoru dovolj namestiti le dve kameri. Večje poštne poslovalnice ali druge poštne lokacije pa so seveda pokrite z več kamerami v odvisnosti od velikosti in razporeditve

⁴⁹ UPS (angl. Uninterruptible Power Supply) je naprava za nemoteno napajanje različnih električnih porabnikov.

prostorov. Prioriteta je bila, da se z videonadzorom pokrijejo prostori za stranke ter službeni in glavni vhod. Zato so v večini poštних poslovalnic nameščene do štiri kamere. Najpogosteje uporabljena pokritost prostora v poštni poslovalnici z videonadzorom je prikazana na Sliki 15, kjer kameri Q24M pokrivata notranjost poštne poslovalnice, glavni in službeni vhod pa kameri M24M. Prav zaradi takšne postavitve videonadzora v poštних poslovalnicah število teh dveh modelov kamer tako izstopa.



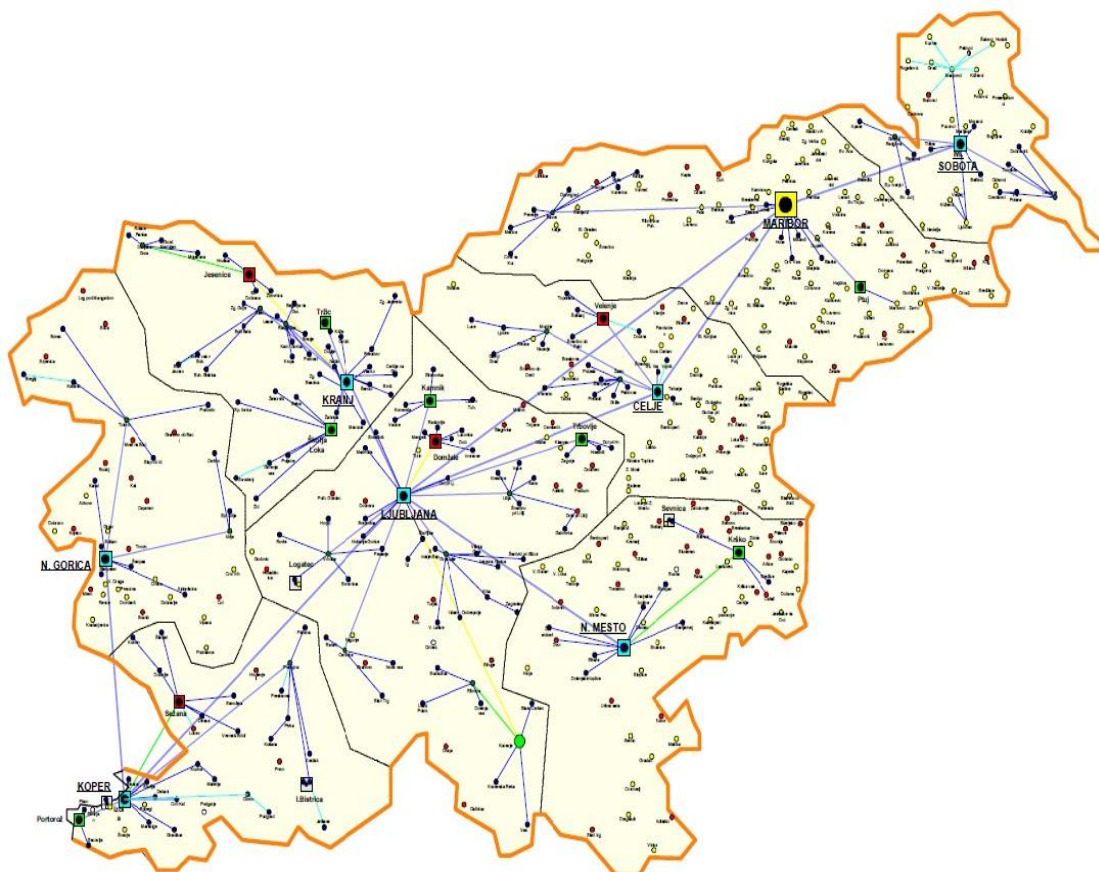
Slika 15: Primer pokritosti prostora poštne poslovalnice s štirimi kamerami

Vir: Lasten

4.5 Globalno komunikacijsko omrežje Pošte Slovenije d.o.o.

Pošta ima svoje poslovalnice in poslovne enote razporedene po vsej državi, zaradi nemotenega delovanja podjetja pa morajo biti med seboj informacijsko povezane. Zato so morali zagotoviti komunikacijske povezave z vsemi poštными enotami. Posledica tega je postavitve lastnega omrežja Pošte (tj. GKO).

Pošta je v preteklih letih izgradila in prenovila privatno omrežje, namenjeno prenosu podatkov, kateri so na prenosni poti oz. WAN⁵⁰ omrežju v celoti kodirani z naprednimi kodirnimi mehanizmi. S tem je zagotovljen varen prenos podatkov do vseh PE, PLC-ja in uprave. Hkrati pa to omogoča varno izvajanje storitev Pošte v poštnih poslovalnicah, zalednih delovnih mestih, interneta, intraneta, internetne pošte, videonadzora, registracije delovnega časa itd.



Slika 16: Globalno komunikacijsko omrežje Pošte Slovenije d.o.o.

Vir: Letno poročilo 2000 Pošte Slovenije d.o.o.

GKO informacijskega sistema Pošte je po arhitekturi razdeljeno na dva nivoja, in sicer na hrbtenično in pristopno komunikacijsko omrežje, ki v osnovi podpira IP komunikacijski protokol v vseh segmentih omrežja.

Hrbtenično omrežje je komunikacijsko omrežje visokih kapacitet, ki povezuje posamezne regionalne ali druge informacijske centre in mora zagotavljati delovanje vseh informacijskih

⁵⁰ WAN (angl. Wide Area Network) – široka omrežja, ki omogočajo priključitev na širokem geografskem področju, neomejeno število uporabnikov, omogočajo izmenjavo velikih količin informacij z visoko hitrostjo. WAN omrežja pogosto povezujejo več lokalnih oz. LAN omrežij v eno samo omrežje.

sistemov na Pošti. Poleg visokih kapacitet je za hrbtenično omrežje značilna zahteva po zelo veliki stabilnosti in razpoložljivosti omrežja. To dosega s pomočjo polne redundance naprav in povezav v tem segmentu omrežja. Hrbtenično omrežje je sestavljeno iz šestih regijskih vozlišč (PE Murska Sobota, PE Celje, PE Kranj, PE Nova Gorica, PE Koper, PE Novo mesto) ter štirih centralnih vozlišč (Uprava, PLC Maribor, PE Ljubljana, PE PLC Ljubljana).

Pristopno omrežje je komunikacijsko omrežje, razdeljeno na dostopovno in povezovalno omrežje, ki povezuje vse poštne poslovalnice do dveh centralnih vozlišč in je sestavljeno iz 520-ih vozlišč poštne poslovalnice, ki so neodvisno ena od druge povezane v posamezno centralno vozlišče. Vsaka poštna poslovalnica je dvojno vpeta v GKO Pošte, hkrati pa se ves promet kodira s pomočjo kodirnega algoritma.

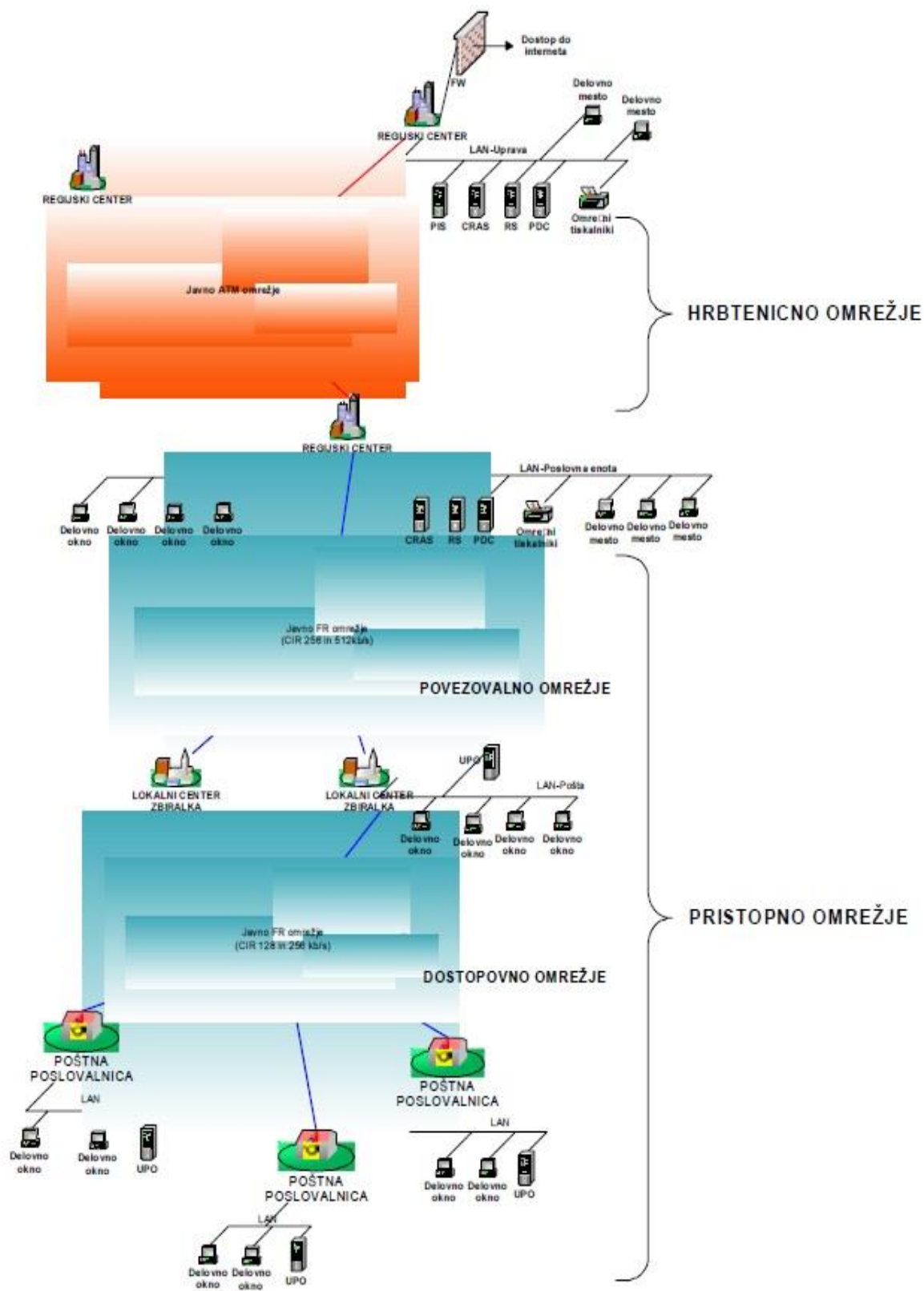
Primarne logične povezave za posamezne poštne poslovalnice za PE Kranj, PE Nova Gorica, PE Koper, PE Ljubljana in PE Novo mesto se zaključujejo v centralnem vozlišču na PE Ljubljana, medtem ko se primarne logične povezave za posamezne poštne poslovalnice za PE Maribor, PE Celje in PE Murska Sobota zaključujejo v centralnem vozlišču na PLC-ju Maribor. V kolikor pride do prekinitve primarne logične povezave, se avtomatsko aktivira sekundarna logična povezava, ki se zaključuje v drugi centralni točki.

Pristopno omrežje informacijskega sistema Pošte mora zagotavljati nemoteno delovanje informacijskih storitev, ki jih ponujajo na poštne okencu posamezne poštne poslovalnice.

LAN omrežja oz. lokalna omrežja so izgrajena na vseh lokacijah Pošte. Število aktivnih priključkov v lokalnih omrežjih sega od štiri pa do nekaj sto in celo tisoč. Lokalna omrežja na lokacijah Pošte se med seboj razlikujejo predvsem glede na velikost lokacije. Tako na večini lokacij oz. na vseh tistih lokacijah, kjer je manj kot 100 aktivnih priključkov, običajno nimajo ločenih hrbteničnih in pristopnih stikal. Kadar je aktivnih priključkov več kot 100, se ločujeta pristopno omrežje in hrbtenično omrežje.

Zagotovljen je visok nivo varnosti pri prenosu podatkov, kajti ves promet, ki se prenaša med vsako poštno poslovalnico in posamezno centralno točko, se kodira z dvema ključema, eden se uporablja za kodiranje prometa v smeri centralne točke Ljubljana, drugi pa za kodiranje prometa v smeri centralne točke Maribor (GKO Pošte Slovenije d.o.o., 2011, str. 10).

Za lažje razumevanje hrbteničnega in pristopnega omrežja je na Sliki 17 prikazan shematski prikaz omenjenih omrežij, ki skupaj tvorita GKO Pošte.



Slika 17: Shema hrbtničnega in pristopnega omrežja

Vir: Letno poročilo 2000 Pošte Slovenije d.o.o.

5 PREDNOSTI VIDEONADZORNEGA SISTEMA POŠTE SLOVENIJE D.O.O.

5.1 Prednosti pri obdelavi podatkov

Vsi podatki iz videonadzornega sistema se v NC prenašajo preko GKO-ja, ki omogoča izredno hiter prenos brez časovnega zamika, kar skupaj s centralnim dostopom in upravljanjem podatkov omogoča operaterjem v NC-ju celovit nadzor nad delovanjem in vzdrževanjem sistema, izdelavo posnetkov in obdelavo zbranih podatkov ter nadaljnje posredovanje obdelanih podatkov.

Operaterji iz videonadzornega sistema pridobivajo predvsem dve vrsti podatkov, ki jih je potrebno obdelati. To so podatki, ki jih pridobivamo s pomočjo zajemanja slike kamer (slika v »živo« ali posnetki), ter podatki o delovanju samega sistema. Pri obdelavi teh podatkov je potrebno upoštevati navodila ali zahteve, ki jih operaterji dobijo od nadrejenih iz PKVN-ja, policije, varnostnih služb, uslužbencev in strank. Od njih je odvisno, za katero časovno obdobje in iz katere lokacije se bodo zbrani podatki shranili za kasnejšo uporabo.

Prednosti pri obdelavi podatkov:

- centraliziran in hiter dostop do zbranih podatkov na različnih lokacijah iz NC-ja s pomočjo programa MxCC,
- Generalna policijska uprava (GPU) in Pošta imata preko varne internetne povezave vzpostavljeno sinhronizacijo strežnikov kamor NC odlaga videoposnetke, do katerih lahko dostopajo pooblašcene osebe iz Operativno-komunikacijskega centra (OKC) Generalne policijske uprave,
- nenehen nadzor nad morebitnimi okvarami na videonadzornem sistemu ter takojšnje obveščanje podizvajalcev o okvarah za čimprejšnjo odpravo okvar (naročila servisnih posegov, javljanje okvar na videonadzornem sistemu),
- obdelani podatki se hranijo na delovni postaji oz. računalniku v NC-ju in so tako vedno na razpolago za nadaljnje posredovanje ali analizo,
- obdelava in zbiranje podatkov preko slike v »živo« je pomembna pri izločanju morebitnih lažnih alarmov ter v primeru t. i. talske situacije,
- takojšnje posredovanje obdelanih podatkov preko interneta ali hitre pošte odgovornim osebam,

- vsaka obdelava zbranih podatkov se zabeleži v različne evidence, ki se hranijo v NC-ju,
- zapis obdelanih podatkov na različne prenosne snemalne medije (zgoščenke, USB ključi⁵¹, spominske kartice, trdi diski).

5.2 Centralizacija podatkov

Vsi obdelani podatki se hranijo in s tem centralizirajo na računalniku v NC-ju. Za centralizacijo podatkov iz varnostno najbolj pomembnih ali ogroženih lokacij je trenutno nastavljeno 317 kamer, da snemajo na centralni snemalni strežnik, kjer je nastavljena časovna omejitev na 12 dni s presnemavanjem podatkov. Na ta način se ohranja približno vedno enaka količina podatkov, ki se nahajajo na centralnem snemalnem strežniku. Omogočeno je spreminjanje števila kamer, ki snemajo na centralni snemalni strežnik, in spreminjanje časovnega obdobja snemanja. Vse nastavitve shranjevanja podatkov se usklajujejo s Področjem korporativne varnosti in nadzora, ki podaja navodila glede na varnostne razmere na Pošti, in s področjem informatike, ki vzdržuje in upravlja centralni snemalni strežnik. Trenutno so zgoraj navedene nastavitve dovolj za varnostne potrebe Pošte in ni potreb za njihovo povečanje. Vsako povečanje snemanja na centralni snemalni strežnik zahteva tudi povečanje kapacitet snemalnega strežnika in s tem večja stroške, saj je potrebno dokupiti snemalne medije oz. podatkovne diske.

Trenutno je na centralnem snemalnem strežniku za potrebe videonadzornega sistema rezerviranega prostora za 21 TB⁵² podatkov (za primerjavo: velikost snemalnega medija v eni kameri je v večini primerov 60 GB⁵³). Ta količina trenutno zadostuje za 3.804 dni shranjenih videoposnetkov, do katerih se lahko dostopa in se z njimi upravlja samo iz NC-ja.

Velikost obdelanih in shranjenih podatkov na računalniku v NC-ju se spreminja in je odvisna od zahtev po zavarovanju podatkov v določenem časovnem obdobju, saj se shranjeni podatki oz. videoposnetki po 60-ih dneh brišejo.

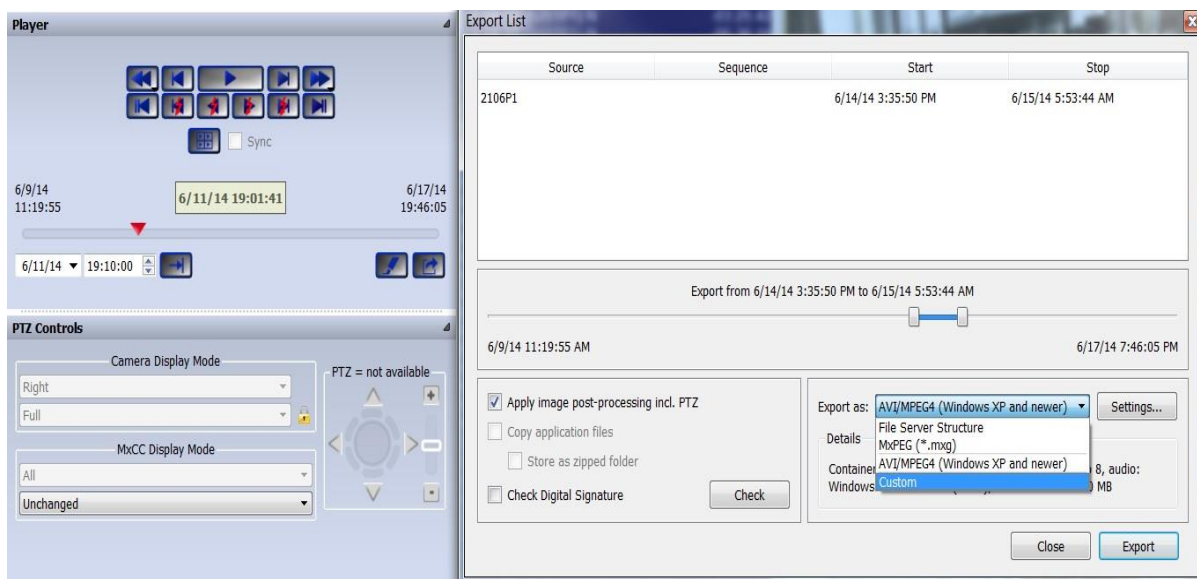
⁵¹ USB (angl. Universal Serial Bus) je univerzalno serijsko vodilo, ki je standardizirano in omogoča enostaven priklop na praktično vsako računalniško enoto. USB ključ je majhen zunanji pomnilnik, ki lahko ima do nekaj gigabajtov prostora za hrambo podatkov.

⁵² TB – terabajt (1 TB = 1.000 GB).

⁵³ GB – gigabajt (1 GB = 1.000 MB, 1 MB = 1.000 kB, 1 kB = 1.000 bajtov, 1 B = 8 bitov, 1bit – je osnovna in hkrati najmanjša enota informacije, ki se uporablja v računalništvu in teoriji informacij).

5.3 Hiter dostop do podatkov

Ne glede na to ali se podatki nahajajo na snemalnem mediju v kameri ali na centralnem snemalnem strežniku, operaterji do njih vedno dostopajo preko programa MxCC v »Player« načinu. Ta omogoča pregled posnetkov v poljubnih časovnih območjih, nastavljanje snemanja v različnih zapisih podatkov (kodeki) in izbiro lokacije, na katero se bodo presneli oz. shranili.



Slika 18: Prikaz »Player« načina v MxCC

Vir: Lasten

Omeniti velja, da je dostop do podatkov, ki se nahajajo na centralnem snemalnem strežniku nekoliko hitrejši, saj se do njih dostopa preko omrežne povezave GKO, ki je na voljo samo za potrebe NC-ja. Do podatkov na snemalnih medijih v kamerah pa se dostopa preko omrežnih povezav GKO-ja, ki jih uporabljajo tudi ostali uporabniki Pošte, zato je hitrost prenosa odvisna od zasedenosti omrežja. Vendar pa tudi v tem primeru pride do zakasnitve le za nekaj sekund, kar pa z varnostnega vidika ne igra pomembne vloge.

Lahko bi rekli, da je na ta način omogočen hipen dostop do podatkov oz. videoposnetkov ne glede na to, kam se hranijo. Za potrebe zavarovanja posnetkov kot dokaznega gradiva ali za potrebe različnih analiz je tako potrebno v programu MxCC samo izbrati želeno kamero, nastaviti snemalni način in v »Player« načinu določiti, kateri del posnetka se bo zavaroval oz. presnel in kam se bo shranil.

Takoj po zavarovanem oz. shranjenem posnetku se to zabeleži v evidence in shrani, kar omogoča večjo preglednost nad shranjenimi posnetki in hitrejšo kasnejšo uporabo.

5.4 Velikost zbranih podatkov

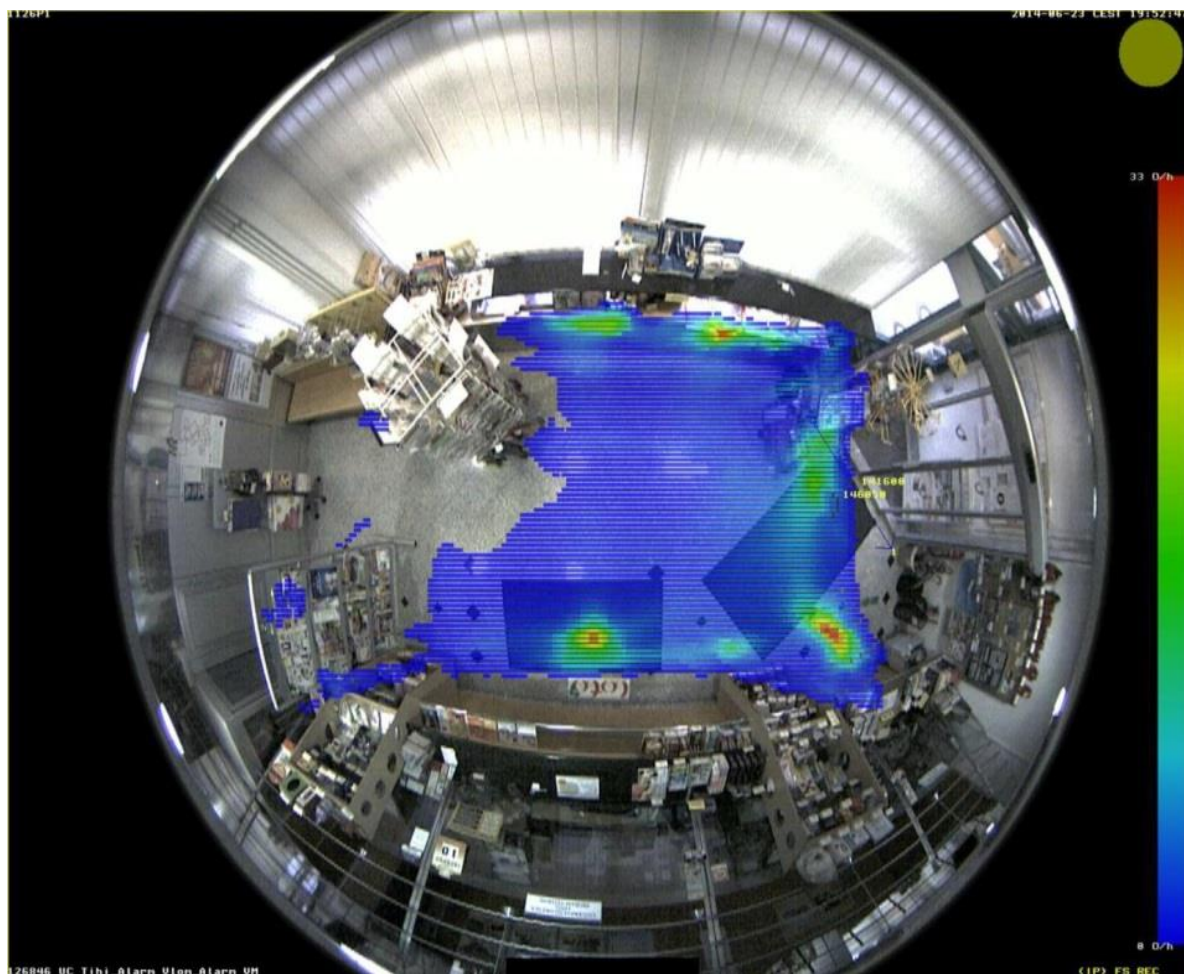
Trenutno je z videonadzorom opremljenih 438 poštnih poslovalnic z 1.282-imi kamerami, od katerih jih 317 snema na centralni snemalni strežnik, kjer zasedajo 21 TB oz. 21.000 GB podatkov. Ostalih 964 kamer snema na lasten snemalni medij, ki ima kapaciteto 60 GB na posamezno kamero in omejitev 60 dni s presnemavanjem, kar znese 57.840 GB podatkov. To skupaj znese 78.840 GB⁵⁴ podatkov (v maju 2014 je to pomenilo za 17.384 dni posnetkov ali povprečno 15 dni na posamezno kamero), ki so na razpolago za pregled ali obdelavo v vsakem trenutku.

5.5 Možnost uporabe videonadzornega sistema za marketing

Marketinški oddelek lahko sedaj dobi mesečno poročilo o številu in o lokacijah gibanja obiskovalcev v posamezni poštni poslovalnici. Funkciji »Counting Line« in »Heatmap« v programu MxCC namreč omogočata štetje obiskovalcev in analizo najpogostejše obiskanega prostora v poštni poslovalnici oz. pokaže območje, kjer se največkrat zadržujejo stranke. Ta analiza gibanja strank v poštni poslovalnici je v pomoč pospeševalcem prodaje v podjetju, ki s pomočjo pridobljenih podatkov iz analize na najbolj obiskana mesta v poštni poslovalnici postavijo police z artikli, ki so tržno najbolj zanimivi, ali pa ta mesta uporabijo za reklamiranje določenih izdelkov.

Slika 19 prikazuje funkciji »Counting Line« in »Heatmap«. V danem primeru je štetje obiskovalcev v poslovalnici nastavljeno pri vhodnih vratih prostora za stranke (modra puščica, ob kateri sta zapisani številki vhodov in izhodov iz poštnice poslovalnice). Območja, kjer so se obiskovalci oz. stranke največkrat zadrževali, so obarvana rdeče in rumeno.

⁵⁴ Za primerjavo nekaj podatkov v bolj poznanih enotah iz domače uporabe: to znese 112.628 zgoščenk s kapaciteto 700 MB na zgoščenko ali 16.774 DVD-jev s kapaciteto 4,7 GB na DVD.



Slika 19: Funkciji »Counting Line« in »Heatmap« v programu MxCC

Vir: Lasten

6 EKONOMSKI VIDIK IZBIRE VIDEONADZORNEGA SISTEMA POŠTE SLOVENIJE D.O.O.

Pri ekonomskem vidiku so bili upoštevani predvsem vidiki nabavne cene kamer, poraba električne energije, stroški v letih po postavitvi videonadzornega sistema, saj je le-ta izjemno velik, ter majhni stroški nadgradnje ali razširitve, če bi se pokazala potreba po večjem številu kamer v posamezni poslovalnici, ki se lahko dodajo v obstoječ videonadzorni sistem brez večjih stroškov (kamera in instalacije brez licenc).

Tako je bilo postavljenih šest osnovnih meril:

- merilo 1: Nabavna cena (utež v skupni oceni 60 %),
- merilo 2: Skupni stroški lastništva oz. TCO⁵⁵ v prvih treh letih po nabavi (utež k skupni oceni 15 %),
- merilo 3: Garancijska doba več kot 36 mesecev (utež k skupni oceni 10 %),
- merilo 4: Reference proizvajalca/ponudnika (utež k skupni oceni 5 %),
- merilo 5: Pospešena montaža – več kot 50 lokacij na mesec (utež k skupni oceni 5 %),
- merilo 6: Namestitev digitalnega potrdila Microsoft CA na kamere (utež k skupni oceni 5 %) (Oddaja javnega naročila po postopku s pogajanjem po predhodni objavi: Sistem video nadzora na poslovalnicah Pošte Slovenije, 2011, str. 6-7).

Pri testiranjih različnih sistemov in kamer različnih ponudnikov pa se je pokazalo, da ima zelo pomembno vlogo glede ekonomičnosti na dolgi rok poraba električne energije. Cena kamer je bila zaradi konkurenčnosti približno enaka pri vseh ponudnikih, zato je bil poseben poudarek pri analizah na ceni vzdrževanja in porabi električne energije v letih po postavitvi videonadzornega sistema.

Kljub dejstvu, da so bile Mobotixove kamere med dražjimi izmed ponujenih, se je izkazalo, da je zaradi manjšega števila potrebne strojne opreme (ni strežnikov in dodanih licenc) in posledično nižjih stroškov nakupa opreme, nižjih stroškov pri porabi energije in stroškov vzdrževanja videonadzornega sistema kot celota Mobotixov videonadzorni sistem za naročnika ekonomsko najugodnejši.

⁵⁵ TCO (angl. Total Cost of Ownership) oz. skupni stroški lastništva – je finančna ocena, namenjena za pomoč kupcem in lastnikom določiti neposredne in posredne stroške izdelka ali sistema.

Vrednost investicije v celotni videonadzorni sistem Pošte z montažo kamer in vzpostavitvijo lastnega NC-ja je bila manj kot 2.000.000 €. Tukaj je izjemno vlogo odigralo tudi stališče Pošte, da predstavljajo sredstva, namenjena za varnost, investicijo in ne strošek. Sredstva, ki jih namenijo za varnost, predstavljajo investicijo v ljudi, ugled podjetja in uspešnost celotnega poslovnega procesa.

Ekonomsko upravičenost gre iskati predvsem v zavarovanju odgovornosti oz. prenosu tveganj (v primeru ropa oz. kraje se povrne škoda), saj so zavarovalnice sklenitev zavarovanja pogojevale z vzpostavitvijo videonadzora, potencialnem trženju NC-ja ter pri razvijanju novih »storitev v oblaku«⁵⁶, pri čemer Pošta uporablja izkušnje, pridobljene z uporabo videonadzornega sistema, ki jih namerava tržiti v prihodnosti.

Za lažjo predstavo o pomembnosti stroškov delovanja tako obsežnega videonadzornega sistema sem na podlagi pridobljenih podatkov naredil analizo stroškov porabe električne energije v prvih 10-ih letih delovanja videonadzornega sistema od leta 2012. Pri analizi sem uporabil kameri dveh ponudnikov, ki sta bili v ožjem izboru, in sicer kamero podjetja Axis P1346-E (njihov sistem je takrat potreboval še dodatni DVR na vsaki lokaciji, le-ti pa so dodatni porabniki električne energije) ter kamero podjetja Mobotix M24M (v času izbire ustreznega ponudnika je bilo edino, ki je ponujalo kamere z vgrajenimi snemalnimi mediji). Za enostavnejši izračun sem uporabil samo ta modela kamer in en DVR na vsaki lokaciji videonadzora pri podjetju Axis ter upošteval takratno ceno električne energije, ki je znašala 0,12 €/kWh. Predvideno je bilo 1.200 kamer ter pri videonadzornem sistemu podjetja Axis še 500 DVR-jev (ker Axisov DVR zaradi premajhne kapacitete ni ustrezal pogojem Pošte je le-ta iskala primeren DVR pri drugih proizvajalcih). Poraba električne energije kamere M24M je 4 W/h, poraba električne energije kamere P1346-E je 13 W/h in poraba električne energije strežnika je 300 W/h (povprečna poraba električne energije DVR-ja s primerno kapaciteto in 1.000 W napajalnikom).

⁵⁶ Storitve v oblaku (angl. Cloud Computing) so storitve, ki se izvajajo v porazdeljenem okolju omrežno tesno povezanih navideznih računalnikov. Storitve v oblaku so vam dosegljive od koder koli v spletu z zanesljivostjo delovanja 24 ur na teden in temeljijo na najsodobnejših varnostnih in zasebnostih rešitvah. Med priljubljene storitve v oblaku sodijo varnostno in arhivsko shranjevanje podatkov (e-hramba), uporaba pisarniških in računovodskih orodij, spletne aplikacije za vodenje projektov in nadzor stroškov del (http://www.sontius.si/storitve/storitve_v_oblaku/, pridobljeno dne 28. 6. 2014). Primeri storitev v oblaku: YouTube, Google Picasa, Google Docs, iCloud, DropBox itd.

Izračun stroškov porabe električne energije za prvo leto uporabe:

- Mobotix: letni strošek porabe električne energije delovanja kamer je 5.046 €
 $1.200 \text{ kamer} * 4 \text{ W/h} * 24 \text{ h} * 365 \text{ dni} * 0,12 \text{ €/kWh} / 1.000 = 5.045,76 \text{ €}$
- Axis: letni strošek porabe električne energije delovanja kamer in DVR-jev je 174.079 €

$$(1.200 \text{ kamer} * 13 \text{ W/h} * 24 \text{ h} * 365 \text{ dni} * 0,12 \text{ €/kWh} + 500 \text{ DVR} * 300 \text{ W/h} * 24 \text{ h} * 365 \text{ dni} * 0,12 \text{ €/kWh}) / 1.000 = 174.078,72 \text{ €}$$

V spodnji tabeli so predstavljeni skupni predvideni stroški porabe električne energije med primerljivima sistemoma v prvih 10-ih letih delovanja videonadzornega sistema Pošte.

Tabela 2: Energetski izračun porabe električne energije med primerljivima videonadzornima sistemoma v prvih 10-ih letih delovanja

Energetski izračun v €		
Leto	AXIS	MOBOTIX
1	174.079 €	5.046 €
2	348.157 €	10.092 €
3	522.236 €	15.137 €
4	696.315 €	20.183 €
5	870.394 €	25.229 €
6	1.044.472 €	30.275 €
7	1.218.551 €	35.320 €
8	1.392.630 €	40.366 €
9	1.566.708 €	45.412 €
10	1.740.787 €	50.458 €

Vir: Lasten

Analiza pokaže ogromno razliko pri porabi električne energije in posledično veliko večjih stroškov sistema Axis predvsem na račun dodatnih DVR-snemalnikov, ki so veliki porabniki električne energije. Razlika pri stroških v prvih desetih letih obratovanja bi tako znašala nekaj manj kot 1.700.000 €, kar predstavlja skorajda vrednost celotnega videonadzornega sistema Pošte.

7 UGOTOVITVE IN SKLEPI

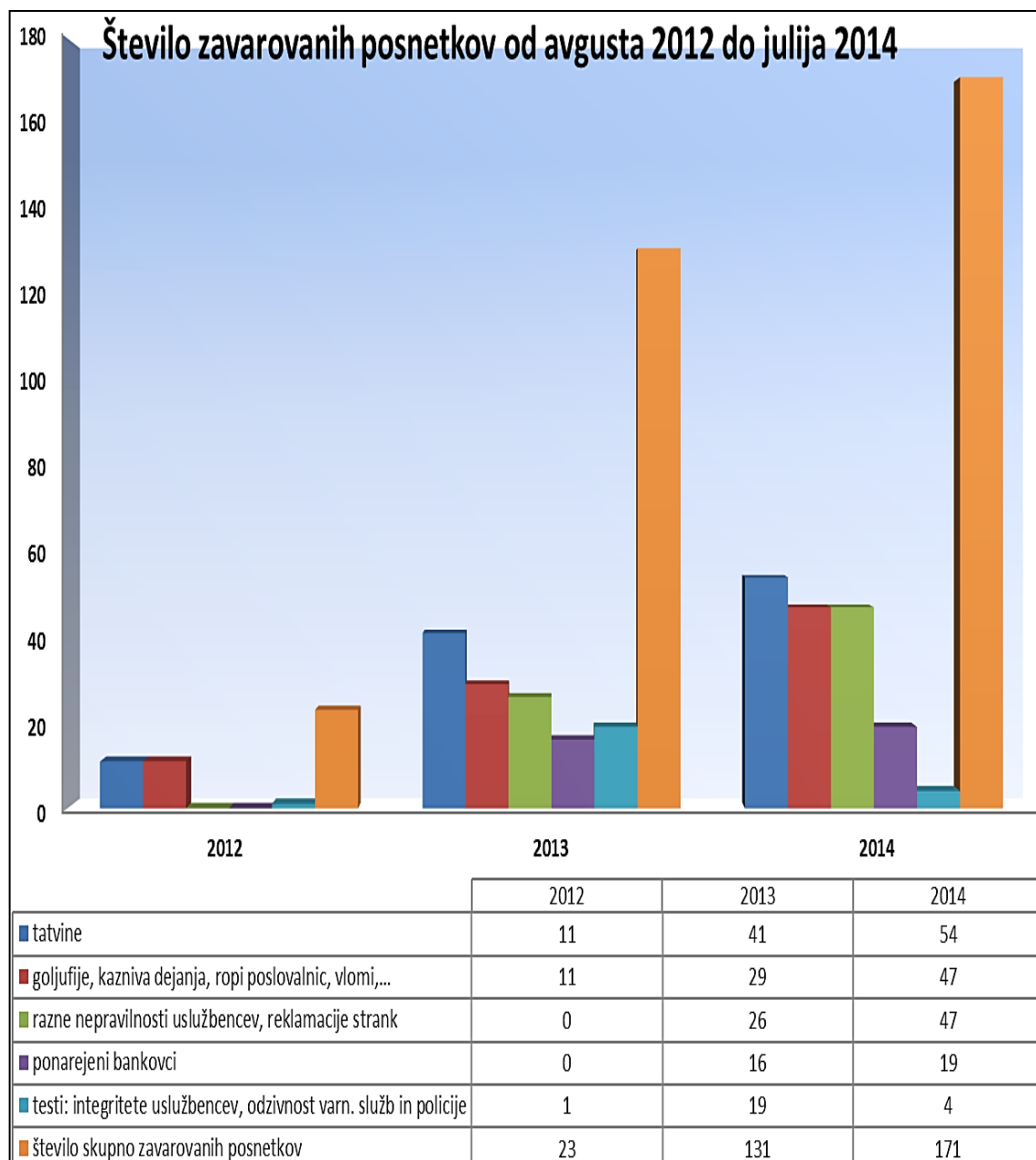
Videonadzorni sistem Pošte s svojim centraliziranim upravljanem iz NC-ja, ki je lociran v PLC-ju Maribor, omogoča neposreden nadzor nad dogajanjem na lokacijah Pošte, kjer je nameščen videonadzor, ter celovit nadzor nad delovanjem in vzdrževanjem sistema. Zelo pomembno je, da je omogočeno dokumentiranje dogodkov in pojavov, obdelava videopodatkov in hramba le-teh ter končna uporaba videoposnetkov za potrebe dokazovanj v primeru izvršenih kriminalnih ravnanj. NC je namreč centralna točka, kamor se preko GKO-ja stekajo videopodatki videonadzornega sistema, ki obsega 438 različnih lokacij Pošte, opremljenih z 1.282-imi kamerami. NC z lastnimi operaterji upravlja z videonadzornim sistemom. Operaterji imajo v vsakem trenutku možnost spremljanja dogajanja v »živo« ali pregledovanja posnetkov iz katerekoli lokacije, ki je opremljena z videonadzorom.

Videonadzorni sistem je dobro programsko podprt s programom MxCC in v kombinaciji z že vgrajenimi varnostnimi sistemi na lokacijah omogoča detekcijo izrednih dogodkov in učinkovito alarmiranje pristojnih organov. Na vsaki lokaciji, kjer je nameščen videonadzor, je ena od kamer preko vmesnika (MX-ExtIO modula) povezana tudi s protitropnim in protivlomnim alarmnim sistemom, kar v primeru aktiviranja alarmnega oz. panik stikala ali protivlomnih senzorjev omogoča takojšen prenos slike v »živo« v NC in s tem obveščanje operaterjev o izrednem dogodku. Tako lahko operater takoj oceni, ali gre za izredni dogodek ali ne in po potrebi obvesti pristojne organe (policijo, varnostne službe, nadrejene itd.).

Vsi obdelani videoposnetki se hranijo na računalniku v NC-ju Pošte, od koder se lahko s pomočjo najnovejših tehnologij nemudoma posredujejo pristojnim organom, ki bodo zato o dogodku, storilcu in posebnostih obveščeni takoj. Za različne varnostne potrebe je bilo od začetka delovanja NC-ja, to je od avgusta 2012, pa vse do julija 2014 obdelanih in shranjenih 325 videoposnetkov, kar znese 14,77 posnetkov na mesec, pri čemer je potrebno poudariti, da je bilo na začetku delovanja NC-ja z videonadzorom opremljenih samo 152 poštnih lokacij. Število lokacij, opremljenih z videonadzorom, se je nato večalo vse do marca 2014, ko je bila z videonadzorom opremljena zadnja 438. lokacija in s tem končana še zadnja faza postavitve videonadzornega sistema Pošte.

Kot je razvidno iz grafikona spodaj, se število obdelanih posnetkov povečuje, kar je deloma posledica opremljenosti vseh predvidenih lokacij z videonadzorom ter posledično večjega števila kamer, predvsem pa uporabnosti posnetkov kot dokaznega gradiva v posameznih

kriminalnih dejanjih in dejstva, da vodstvo PKVN-ja zahteva, da se o vseh pomembnih varnostnih informacijah glede Pošte obvešča NC. Tako je povprečno število obdelanih posnetkov iz 5,75 na mesec v letu 2012 naraslo na 10,91 na mesec, v letu 2013 in v prvi polovici leta 2014 pa že na 28,5 posnetka na mesec.



Grafikon 2: Število obdelanih in shranjenih posnetkov od avgusta 2012 do julija 2014

Vir: Lasten

Iz podatkov lahko razberemo, da je največ videoposnetkov zavarovanih zaradi tatvin v poštah, sledijo razne goljufije ter druga kazniva dejanja, ki niso neposredno povezana s Pošto (npr. goljufije s plačilnimi karticami, kraje avtomobilov in koles itd.), pri

čemer je potrebno poudariti, da v teh primerih zahtevo za zavarovanje posnetkov posreduje policija. Nato sledi še zavarovanje posnetkov pri poskusu unovčitve ponarejenih ali obarvanih bankovcev, kjer se posnetki shranijo za primer, če oseba, ki je hotela unovčiti ponarejeni bankovec ne bi hotela sodelovati s policijo.

S pomočjo videonadzora se je izboljšal tudi segment preiskovanja kaznivih dejanj zaposlenih, predvsem v primerih tatvin in poneverb, kjer beleži Pošta v zadnjem obdobju velik porast. To se odraža tudi v večanju števila zavarovanih videoposnetkov, ki so v veliko pomoč PKVN-ju pri odkrivanju notranjih nepravilnosti na Pošti.

Videonadzorni sistem se s pomočjo analitskega orodja, ki ga sam ponuja preko programa MxCC, uporablja tudi za druge namene, npr. ugotavljanje števila oz. štetje obiskovalcev v posamezni poslovalnici in kje se ti najpogosteje zadržujejo.

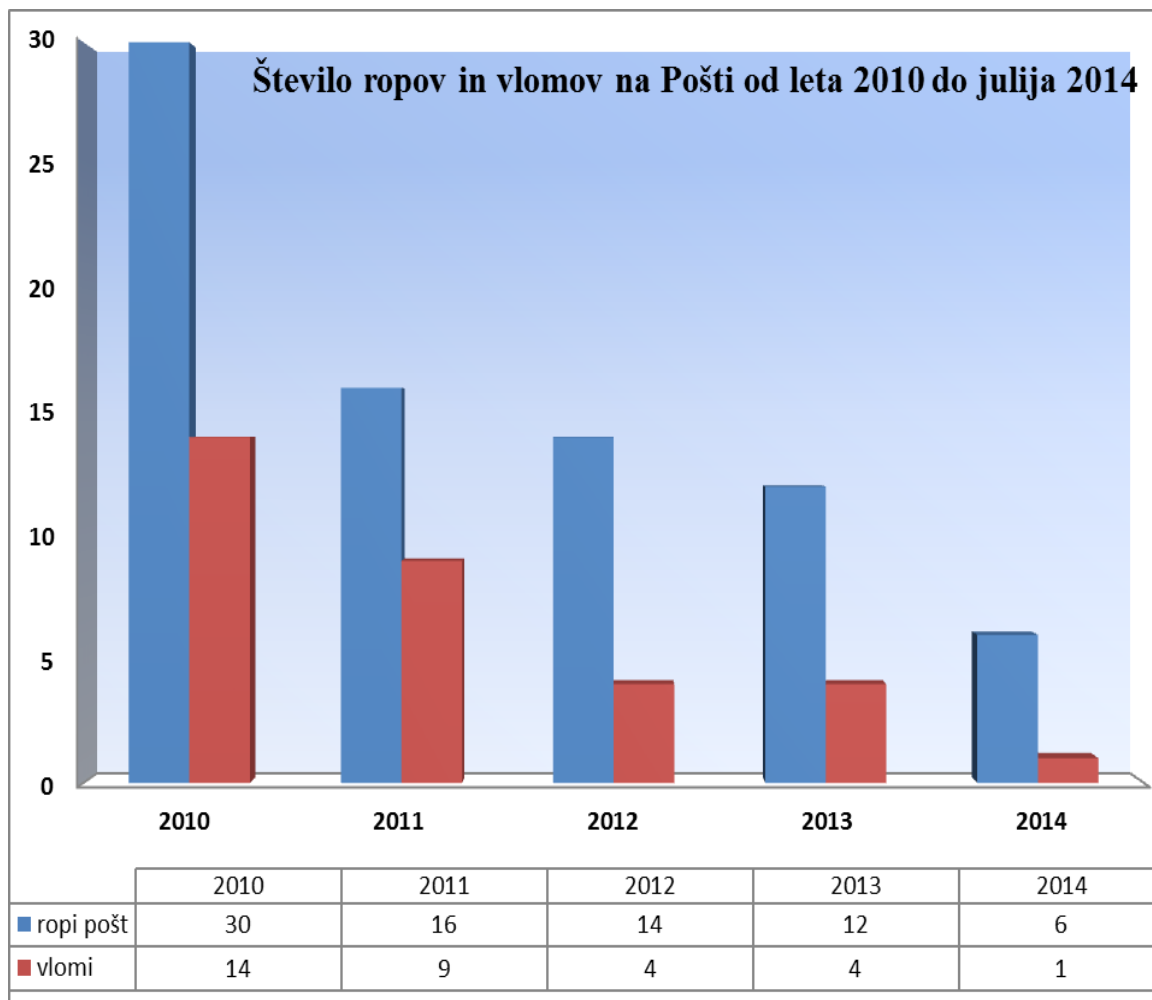
Področje videonadzora je ne glede na obseg izvajanja eno tistih, na katerem se najpogosteje naleti na kršitve zakonodaje. Na Pošti so tako že pred uvedbo videonadzornega sistema upoštevali veljavno zakonodajo na področju varstva osebnih podatkov ter kasneje z njegovo uvedbo izdali še lastno Odločbo o izvajanju videonadzora, ki natančno ureja pravila ravnanja z osebnimi podatki pri uporabi videonadzornega sistema Pošte. Izredna inšpekcijska nadzora Inšpektorata Ministrstva za notranje zadeve in Informacijskega pooblaščenca leta 2012 sta potrdila ustreznost in pravilnost izvajanja in upravljanja z videonadzorom in NC-jem.

V začetku leta 2014 je bila dokončana postavitve videonadzornega sistema Pošte, ki je največji takšen sistem v tem delu Evrope in predstavlja investicijo v varnost ljudi in premoženja, ugled podjetja in uspeh celotnega poslovnega procesa. Uporabnost in prepoznavnost videonadzornega sistema Pošte se odraža s krepitvijo sodelovanja med pristojnimi organi Ministrstva za notranje zadeve in pogodbenimi varnostnimi službami ter NC-jem.

Po slabih dveh letih se je izkazalo, da je bila odločitev za vzpostavitev videonadzornega sistema Pošte pravilna. V tem času so videoposnetki, pridobljeni iz videonadzornega sistema, pomagali pri razjasnitvi nastalih okoliščin v več kot 300 različnih primerih. To je zelo povečalo učinkovitost PKVN-ja pri odkrivanju nepravilnosti in tatvin pri zaposlenih, policije pri ropih, vlomih (v primerih dokazovanja) in testih odzivnosti na izredne situacije (videoposnetki koristijo analizi odziva policistov in varnostnih služb).

Prav tako se kaže trend upadanja števila ropov in vlomov v poštne poslovalnice od leta 2010 naprej, ko sta ti dve vrsti kaznivih dejanj na Pošti dosegli svoj vrhunec. V letu 2011 je delno k

temu pripomoglo tudi veliko medijsko oglaševanje o vzpostavitvi videonadzornega sistema na Pošti. Od leta 2012, ko je začel delovati videonadzorni sistem, pa se že kaže efekt odvritve predvsem pri vlomih v poštne poslovalnice, saj je bilo v prvi polovici leta 2014 izvršeno samo eno takšno kaznivo dejanje.



Grafikon 3: Prikaz števila ropov in vlomov na Pošti od leta 2010 do julija 2014

Vir: Lasten

Na koncu bi podal še nekaj lastnih misli o prednostnih in slabostih videonadzora. Kot glavno prednost videonadzora bi izpostavil takojšen pregled in analizo zbranih podatkov iz lokacije izrednega dogodka ter takojšnje obveščanje in podajanje podatkov o stanju na lokaciji interventom ali raznim drugim pristojnim službam. Dobra informiranost o stanju na lokaciji pripomore k ustreznejši pripravljenosti in boljši odzivnosti na izredni dogodek. Med prednosti lahko štejemo tudi uporabo zbranih podatkov, pridobljenih s pomočjo videonadzora, kot dokazno gradivo v kazenski postopkih ter kot pomoč pri razjasnitvi okoliščin pri različnih izrednih dogodkih. Med tehnološkimi prednostmi je potrebno omeniti, da imajo sodobne IP

videonadzorne kamere že vgrajene senzorje (infrardeči in toplotni), s čimer odpade potreba po dodatni namestitvi le-teh in posledično nižanje stroškov namenjenih varovanju. S psihološkega vidika pa lahko prisotnost videonadzora odigra tudi pomembno vlogo pri odvrnitvi povzročitve kaznivega dejanja.

Kot slabost bi poudaril predvsem visoko nabavno ceno videonadzora, ki pa je razumljiva in pričakovana, saj mora vsa tehnika ustrezati standardom na področju zasebnega varovanja, da se lahko zagotavlja varnost podatkov in brezhibno delovanje. Vendar pa si v današnjem času kvalitetnega varovanja ni možno predstavljati brez videonadzora, zato ga podjetja za zasebno varovanje, razen pri varovanju pravnih oseb, vedno pogosteje vključujejo v ponudbe pri varovanju fizičnih oseb in njihove lastnine.

Kljub vsej sodobni tehnologiji na področju zasebnega varovanja pa je pogosto še vedno najšibkejši člen v varnostni verigi prav človek. Zato je potrebno na tem področju poleg zagotavljanja ustreznih delovnih pogojev, prijetne delovne klime in ustreznega plačila za opravljeno delo v podjetjih za zasebno varovanje predvsem skrbeti za ustrezna izobraževanja in usposabljanja varnostnega osebja. Pri izvajanju testa odzivnosti varnostnih služb in policije na izredne dogodke na Pošti je bilo tudi s pomočjo analiz podatkov, pridobljenih iz videonadzora, ugotovljeno, da je potrebno predvsem več praktičnega usposabljanja. Tako je bila odzivnost na prvem testu slaba, z večkratnim ponavljanjem testov pa je bil dosežen želeni nivo odzivnosti. Takšni testi in praktična usposabljanja lahko bistveno pripomorejo k učinkovitejšemu in posledično uspešnejšemu varovanju. Storilci kaznivih dejanj so namreč vedno bolj predrzni, organizirani in oboroženi, zato je lahko nestrokovno posredovanje in podcenjevanje izrednega dogodka tudi nevarno za varnostno osebje in ostale udeležence pri izrednem dogodku.

8 UPORABLJENA LITERATURA IN VIRI

8.1 Literatura

1. Mobotix, (2012). *Project Slovenien V4 - Mobotix sheme sistema.PDF*. Langmeil: Mobotix.
2. Potokar, M. (2012). *Dileme učinkovitega video nadzora in varovanje zasebnosti.PDF*. Ljubljana: Inštitut za korporativne varnostne študije ICS.

8.2 Viri

1. GKO Pošte Slovenije d.o.o., Pošta Slovenije d.o.o., julij 2011.
2. Interni viri in brošure, Mobotix, 2014.
3. Interni viri, Pošta Slovenije d.o.o., 2014.
4. Letno poročilo 2000, Pošta Slovenije d.o.o., maj 2002.
5. Letno poročilo 2012, Pošta Slovenije d.o.o., avgust 2013.
6. Navodilo za delo in organizacijo Nadzornega centra Pošte Slovenije d.o.o., Pošta Slovenije d.o.o., februar 2013.
7. Oddaja javnega naročila po postopku s pogajANJI po predhodni objavi; Sistem video nadzora na poslovalnicah Pošte Slovenije, Pošta Slovenije d.o.o., avgust 2011.
8. Odločba o izvajanju video nadzora, Pošta Slovenije d.o.o., februar 2014.
9. Odredba o določitvi standardov, ki so obvezni na področju zasebnega varovanja. Ur. l. RS, št. 24/2012 z dne 30. 3. 2012.
10. Odredba o notranji organiziranosti Pošte Slovenije d.o.o. Okrožnica št. 44/T, Pošta Slovenije d.o.o., april 2014.
11. Uredba o obveznem organiziranju varovanja. Ur. l. RS, št. 80/2012 z dne 26. 10. 2012.
12. Zakon o kazenskem postopku (uradno prečiščeno besedilo) (ZKP-UPB8). Ur. l. RS, št. 32/2012 z dne 4. 5. 2012.
13. Zakon o nalogah in pooblastilih policije (ZNPPol). Ur. l. RS, št. 15/2013 z dne 18. 2. 2013.

14. Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo) (ZVOP-1-UPB1). Ur. l. RS, št. 94/2007 z dne 16. 10. 2007.
15. Zakon o zasebnem varovanju (ZZasV-1). Ur. l. RS, št. 17/2011 z dne 11. 3. 2011.

8.3 Spletni viri

1. <http://www.intranet.si/predstavitev-sektorjev/23570/Podrocje-korporativne-varnosti-in-nadzora>, dne 13. 4. 2014.
2. http://www.mobotix.com/eng_GB/Products/Cameras/IP-Video-Door-Station-T25?tab=225237#tab, dne 4. 6. 2014.
3. <http://www.mobotix.com/region/index?URL=&COOKIETEST=1>, dne 21. 4. 2014.
4. <http://www.mobotix.si/>, dne 21. 4. 2014.
5. <http://www.mobotix.si/produkti/d15d/>, dne 1. 6. 2014.
6. <http://www.mobotix.si/produkti/d25m/>, dne 4. 6. 2014.
7. <http://www.mobotix.si/produkti/extio/>, dne 1. 6. 2014.
8. <http://www.mobotix.si/produkti/m25m/>, dne 1. 6. 2014.
9. <http://www.mobotix.si/produkti/q25/>, dne 1. 6. 2014.
10. <http://www.posta.si/opis-storitve/551/Poslanstvo-in-vizija>, dne 9. 5. 2014.
11. http://www.sontius.si/storitve/storitve_v_oblaku/, dne 28. 6. 2014.
12. <http://www.technoriya.in/ipcctv.php>, dne 23. 5. 2014.
13. http://www.varnost.si/videonadzorni_sistem, dne 23. 4. 2014.
14. <https://sites.google.com/site/tp4fotografija/e-skripta/slikovni-senzor>, dne 1. 6. 2014.
15. [https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1\[showUid\]=2284&cHash=41132d8c071533595f3745f6268bba6c](https://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=2284&cHash=41132d8c071533595f3745f6268bba6c), dne 1. 7. 2014.
16. Informacijski pooblaščenec (2008). Smernice za izvajanje videonadzora. Pridobljeno 24. 4. 2014 s spletne strani https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_videonadzor2.pdf.

17. Informacijski pooblaščenec (2014). Videonadzor. Pridobljeno 17. 4. 2014 s spletne strani <https://www.ip-rs.si/varstvo-osebni-podatkov/informacijske-tehnologije-in-osebni-podatki/videonadzor/>.
18. Mobotix (2011). Q24M: Camera Manual. Pridobljeno 3. 6. 2014 s spletne strani http://www.mobotix.si/fileadmin/dokumenti/navodila/15mx_MLq24m_en_090625.pdf.
19. Petek, S. (2011). Kriminalna ogroženost Pošte Slovenije d.o.o. in ukrepi za odkrivanje, preiskovanje in preprečevanje njene ogroženosti. Pridobljeno 23. 4. 2014 s spletne strani <http://dkum.uni-mb.si/IzpisGradiva.php?id=19548>.
20. Pošta Slovenije d.o.o. (2012). Poštni Razgledi, september/oktober 2012, št. 5, glasilo Pošte Slovenije. Pridobljeno 28. 4. 2014 s spletne strani <http://www.posta.si/seznam-dokumentov/556/Interno-glasilo-Poste-Slovenije>.
21. Potokar, M., Welzer Družovec, T. (2013). Video nadzor z vidika varstva osebnih podatkov. Pridobljeno 20. 4. 2014 s spletne strani http://www.fvv.uni-mb.si/DV2013/zbornik/splosna_sekcija/potokar_welzer.pdf.