

# **Návrh systému pro přenos a zobrazení videa z bezpečnostních IP kamer na webovém portálu**

Dan Jarkovský



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2014/2015

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: Dan Jarkovský  
Osobní číslo: A12096  
Studijní program: B3902 Inženýrská informatika  
Studijní obor: Bezpečnostní technologie, systémy a management  
Forma studia: prezenční

Téma práce: Návrh systému pro přenos a zobrazení videa z bezpečnostních IP kamer na webovém portálu

Téma anglicky: A Draft Design of a System for Video Transfer and Display from Security IP Cameras on a Web-portal

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma. Porovnejte a zhodnoťte současná řešení systémů pro streamování videa z IP kamer.
2. Popište jednotlivé prvky systému pro streamování videa z IP kamer včetně účelu jejich využití.
3. Navrhněte vlastní řešení systému. Popište instalaci a nastavení jednotlivých prvků systému od routeru přes streamovací server až po koncové IP kamery.
4. Vytvořte webový portál pro zobrazení videa z IP kamer.
5. Zhodnoťte souhrnně chod kompletně navrženého systému.

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. COAR, Ken a Richard Cooper BOWEN. Apache cookbook. Sebastopol, CA: O'Reilly, 2004. ISBN 05-960-0191-6.
2. SKLAR, David a Adam TRACHTENBERG. PHP cookbook. Farnham: O'Reilly, 2003. ISBN 15-659-2681-1.
3. WILLIAMS, Hugh E a David LANE. Web database applications with PHP and MySQL. 2nd ed. Sebastopol: O'Reilly, 2004. ISBN 05-960-0543-1.
4. BAUER, Michael D. Building secure servers with LINUX. Boston: O'Reilly, 2003. ISBN 05-960-0217-3.
5. KŘEČEK, Stanislav. Příručka zabezpečovací techniky. Vyd. 2. S.l.: Cricetus, 2003. ISBN 80-902-9382-4.
6. JANEČKOVÁ, Eva a Václav BARTÍK. Komerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti. Praha: Linde, 2011. ISBN 978-807-2018-505.
7. ONYXSERVERS, ?2013. How to stream your IP camera using Flash Media Live Encoder or any other live encoder. Onyxservers.com [online]. [cit. 2015-02-02]. Dostupné z: <http://www.onyxservers.com/guides/How-to-stream-your-IP-camera-using-Flash-Media-Live-Encoder-or-any-other-live-encoder.html>.

Vedoucí bakalářské práce:

**Ing. Bronislav Chramcov, Ph.D.**

Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce:

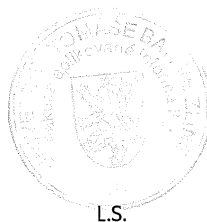
**6. února 2015**

Termín odevzdání bakalářské práce:

**3. června 2015**

Ve Zlíně dne 6. února 2015

doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



L.S.

Ing. Jan Valouch, Ph.D.  
*ředitel ústavu*

**Prohlašuji, že**

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s tím, že licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

## **ABSTRAKT**

Cílem této bakalářské práce je navrhnout systém, který by umožňoval uživatelům sledovat streamované video z IP kamer na webovém portálu. V teoretické části jsou popsány jednotlivé prvky systému a jejich účel v navržené struktuře. Dále se zabývá alternativními řešeními streamování videa z IP kamer. V praktické části je důkladně popsána instalace a nastavení jednotlivých prvků systému od routeru přes streamovací server až po koncové IP kamery. V závěru práce je popsán celkový chod navrženého systému.

Klíčová slova: IP kamery, stream server, webový portál

## **ABSTRACT**

The goal of this thesis is to design a system that would allow users to watch streaming video from IP cameras on the web portal. The theoretical part specify the various elements of the system and their purpose in the proposed structure. It also depicts alternative solutions to streaming video from IP cameras. The practical part is focused on installation and setup of the elements of the system from the router through streaming server to end IP cameras. The conclusion describes the overall functionality of the drafted system.

Keywords: IP cameras, stream server, web portal

Rád bych tímto poděkoval Ing. Bc. Bronislavu Chramcovi, Ph.D. za cenné připomínky, rady a jeho odborné vedení při zpracovávání mé bakalářské práce. Dále bych chtěl poděkovat své rodině a přátelům za jejich podporu a trpělivost.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

## OBSAH

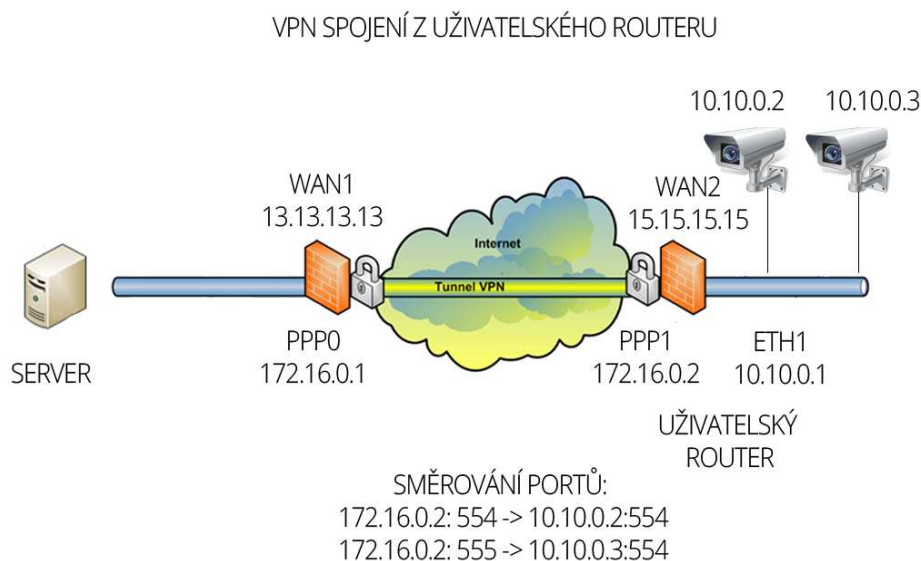
<b>ÚVOD.....</b>	<b>8</b>
<b>I TEORETICKÁ ČÁST.....</b>	<b>10</b>
<b>1 LITERÁRNÍ REŠERŠE WEBOVÝCH STREAMOVACÍCH SLUŽEB.....</b>	<b>11</b>
<b>2 SERVER.....</b>	<b>13</b>
2.1 LINUX.....	14
2.2 UBUNTU .....	15
2.2.1 Apache.....	16
2.2.2 MySQL.....	17
2.2.3 PHP .....	18
2.2.4 VPN Server .....	20
2.2.5 VLC Player.....	21
2.3 ROUTER.....	21
2.4 IP KAMERA .....	22
<b>II PRAKTICKÁ ČÁST .....</b>	<b>24</b>
<b>3 ÚVOD DO PRAKTICKÉ ČÁSTI.....</b>	<b>25</b>
<b>4 INSTALACE SERVERU.....</b>	<b>26</b>
4.1 ISPCONFIG.....	26
4.2 VLC .....	31
4.3 VPN.....	32
4.3.1 Server .....	32
4.3.2 Klient.....	33
<b>5 WEBOVÁ APLIKACE.....</b>	<b>34</b>
5.1 STRUKTURA DATABÁZE.....	35
5.2 ÚVODNÍ STRANA .....	36
5.3 PŘIHLÁŠENÍ / REGISTRACE A PROFIL .....	37
5.4 STRÁNKA UŽIVATELE .....	40
5.5 NASTAVENÍ SKUPINY .....	45
<b>ZÁVĚR .....</b>	<b>47</b>
<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>48</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>50</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>52</b>
<b>SEZNAM TABULEK.....</b>	<b>53</b>
<b>SEZNAM PŘÍLOH.....</b>	<b>54</b>

## ÚVOD

Tento projekt řeší problematiku přístupu ke streamovanému videu z IP kamer odkudkoliv a kdykoliv. Bylo navrženo řešení jak pro běžné uživatele, tak pro firmy. Při běžném použití IP kamer např. v podnikové síti každý zájemce o připojení ke kameře musí použít webové rozhraní nabízené IP kamerou, nebo použít přehrávač streamovaného videa (např. VLC player). V závislosti na kvalitě a typu IP kamer je schopna obsloužit pouze omezený počet takto připojených uživatelů. Je to dáno výkonem použitého hardwaru a kvalitou obslužného softwaru. To vede k určitým omezením, které navrhované řešení odstraňuje. Nutnost předání přístupových údajů (jméno, heslo) všem uživatelům vede k bezpečnostní slabině.

Tento nedostatek systém obchází tím, že uživatel (Administrátor) navrhované webové aplikace zadává přístupové údaje ke kameře do registračního formuláře a koncoví uživatelé nemají k těmto údajům přístup, pouze se registrují k přístupu do aplikace a k samotnému nahlížení na video stream. Tím se omezuje možnost zneužití přístupových údajů a útoku na IP kamery. Jelikož aplikace přistupuje na IP kameru jako jediná a server sám poskytuje video stream ostatním uživatelům, omezuje samotný datový tok nutný pro streamování na minimum. Šetří tak výkon kamery a vytížení síťové linky. Dalším nedostatkem při zobrazování streamovaného videa je nutnost přímého přístupu k IP adrese kamery, což znamená mít IP kameru dostupnou z umístění v síti (může být i routovaná síť, klient nesmí být za routerem provádějící NAT). Poslední nedostatek, a to přístup ke kamerám, omezený např. podnikovou sítí je řešen pomocí směrování portů nebo vytvořením VPN spojení z webové aplikace (serveru) na hraniční router poskytující NAT, nebo přímo na VPN router uvnitř sítě, kde se nachází sledované IP kamery. Toto řešení je vyobrazeno na obrázku 1.





Obrázek 1 VPN spojení s uživatelským routerem.

Na externím serveru s veřejnou IP adresou byla vytvořena webová aplikace umožňující uživateli zaregistrovat své IP kamery, na které se vzdáleně připojuje pomocí výše uvedených metod. Pomocí multimediálního přehrávače VLC použitého jako streamovací server se aplikace připojí na vzdálené IP kamery a v závislosti na nastavených parametrech pro zobrazení ve webovém prohlížeči se tento video stream zobrazí. Aplikace se snaží řešit umístění více kamer pod jedním uživatelským účtem například ve firmách. Vystává potřeba rozdělit kamery do několika skupin (okruhů) a k nim přiřadit jednotlivé uživatele oprávněné tyto kamery sledovat. Administrátor má možnost vytvořit zájmové skupiny kamer (např. kamery ve výrobní hale, kamery zabírající exteriér budovy apod.) a k těmto skupinám povolit přístup dalším uživatelům. Samotná aplikace po uživatelském pokynu spustí na serveru pomocí PHP příkazu streamovací server VLC, který použije přístupové údaje a jednotlivé konfigurační parametry uložené v databázi k připojení se k vzdálené kameře. Tento vstupní stream je převzorkován na výstupní proud požadované kvality a velikosti. Ten si uživatel zobrazí v náhledovém okně vytvořené aplikace.

Pro tento projekt byl navržen systém pro streamování a zobrazování videa z IP kamer na webovém portálu. Skládá se z video serveru, routeru a samotné IP kamery. Video server hostuje služby jako webový server Apache, databázový systém MySQL, skriptovací jazyk PHP, multimediální přehrávač VLC a VPN server. Router propojuje video server se sítí IP kamer, které streamují živý video záznam.

## **I. TEORETICKÁ ČÁST**

## 1 LITERÁRNÍ REŠERŠE WEBOVÝCH STREAMOVACÍCH SLUŽEB

Webové streamovací služby jsou velmi rozsáhlé a rozmanité svým zaměřením. Na trhu existují služby jako youtube, twitch nebo internetová rádia, které poskytují streamování video a audio médií přímo na internet. Výše zmiňované služby se ovšem liší od navrhovaného systému svou strukturou a způsobem vytvoření spojení mezi koncovým zařízením, které poskytuje streamovaná data a webovým serverem, na kterém je streamované video prohlíženo. Tyto služby jsou zaměřeny spíše na komerční obsah, na rozdíl od navrhovaného systému zaměřeného na praktické využití video záznamu.

V této rešerši byly porovnány dvě webové streamovací služby, jmenovitě Icecast a IPCamLive. Rešerše byla hlavně zaměřena na komunikaci mezi streamovaným médiem a koncovým uživatelem.

### **Icecast**

Oficiální dokumentace popisuje Icecast jako streamovací media server, který v současné době podporuje Ogg Vorbis a zvukové streamy ve formátu MP3. Může být použit k vytvoření internetového rádia nebo soukromého jukeboxu a mnoha věcí mezi tím. Je velmi univerzální v tom, že nové formáty mohou být přidány poměrně snadno a podporuje otevřené standardy pro komunikaci a interakce. [1]

Icecast využívá dvou hlavních prvků streamovacího serveru a zdrojového klienta. Server je umístěn například na webové stránce, kde se k němu připojí posluchači. Zdrojový klient je poté spuštěn a skrze něj jsou zasílána streamovaná audio data na server. Oproti tomuto systému, Icecast využívá techniky server-klient, kde roli klienta hraje klientský software poskytující zdrojové streamy ve formě mp3 a ogg souborů, které následně odesílá na serverovou část. Koncový uživatel pak přes webové rozhraní spouští jednotlivé poskytované streamy na svém prohlížeči. Systém je koncipovaný spíše pro audio streamy, techniku ovšem lze využít i okrajově pro stream videa. Oproti tomuto systému Icecast využívá speciální klientskou část, která odesílá stream na server a vytváří spojení z vnitřní sítě bez nutnosti řešení směrování portů, firewallu a jiných síťových překážek.

## IPCamLive

IPCamLive je řešení pro streamování IP kamer založené na cloud technologii. [2]

IPCamLive poskytuje řešení pro přehrávání videa (na základě Flash / HTML5), které umožňuje zobrazení živého video obrazu na všech hlavních platformách (PC, Mac, mobilní, tablety, atd.). Nabízí snadné připojení IP kamery k IPCamLive systému přes HTTP / RTSP streamovací protokol bez potřeby dalšího PC nebo softwaru. IPCamLive dovoluje přijímat a zobrazovat formáty video streamu jako MJPEG, MPEG4 a H.264. Zvládne zobrazit HD rozlišení video streamů a obsloužit neomezený počet uživatelů.

IPCamLive se nejvíce přiblížil tomuto systému tím, že je svým nastavením a přidáním kamer podobně přímý a jednoduchý. Na připojení kamer do vnitřní sítě používá směrování portů na routeru a na kamery se přihlašuje pomocí jména, hesla a URL adresy kamery.

IPCamLive nevyužívá jiné nebo dodatečné bezpečnostní prvky jako například šifrování a zabezpečení přenosu dat.

Streamovací služba je většinou nabízena jako komerční produkt, proto jejich know-how je chráněno a není možno detailně prozkoumat pozadí služeb. Tato rešerše čerpala ze zdrojů, které byly uvedenými společnostmi volně publikovány na internetu.

## 2 SERVER

Prvním a nejdůležitějším prvkem celého systému je webový server, na kterém je nainstalovaná volně šiřitelná distribuce operačního systému Linux, Ubuntu 14.10, balíček ISPConfig, VPN server a multimediální přehrávač VLC.

ISPConfig je open source software pro Linux schopný správy více serverů z jednoho řídicího panelu vytvořený společností ISPConfig UG. Balíček obsahuje sadu softwaru, který slouží jako platforma pro tvorbu a správu dynamických webových stránek. [3]

Podporovaný software:

- HTTP: Apache2 and nginx.
- SMTP: Postfix.
- POP3/IMAP: Courier and Dovecot.
- FTP: PureFTPd.
- DNS: BIND and MyDNS.
- Database: MySQL.
- Statistics: Webalizer and AWStats.
- Virtualization: OpenVZ. [3]

Server v tomto projektu slouží jako host pro webové stránky, správu, konverzi a streamování videa z IP kamer a jako VPN server pro propojení webového serveru s IP kamerami ve vzdálených sítích.

### Webové stránky

Pro tento projekt byly navrženy a vytvořeny webové stránky, které zprostředkují uživateli live stream z jeho zaregistrovaných IP kamer. Uživatel se musí nejprve na stránkách zaregistrovat vyplněním emailu, uživatelského jména a hesla do formuláře. Registrací uživatel souhlasí se smluvními podmínkami uvedenými v příloze PI. Poté se mu zpřístupní funkce jako registrace kamer, vytváření a správa skupin a prohlížení streamu ze svých IP kamer. IP kamery musí být zaregistrovány do systému, toho se opět dosáhne vyplněním údajů o kameře (IP adresa, MAC adresa, URL, přihlašovací údaje ke kameře atd.) do formuláře. V uživatelském rozhraní lze také vytvářet skupiny, do kterých může jejich správce vkládat svoje IP kamery a poskytnout k nim tak přístup dalším uživatelům ve skupině. Tím se otvírají možnosti např. pro firmy a podniky, kde zaměstnavatel chce zpřístupnit určité IP kamery některým svým zaměstnancům. Správa skupin obsahuje

přidání/odebrání kamer, úpravu informací, které uživatel vyplnil při jejich registraci a povolení/zákaz přístupu uživatelů do skupiny. Webová stránka samozřejmě obsahuje také základní informace o aplikaci, možnost kontaktovat administrátora pomocí emailu a informace o firmě, která tento projekt zaštiťuje.

Jak už bylo stanoveno, server je hlavní komponent tohoto systému, který prostřednictvím webové aplikace přináší uživateli streamovaná data z IP kamer kdekoliv a kdykoliv.

## 2.1 Linux

Linux je open source operační systém vyvinut finským programátorem Linusem Torvaldsem v roce 1991.

Na začátku devadesátých let byly stolní počítače dostatečně výkonné, aby dokázaly zprovoznit operační systém UNIX, který v tehdejší době byl spíše alternativa namísto MS DOS a Windows 3.1. Linusovým cílem bylo vynaleznout volně šiřitelný operační systém, který by byl kompatibilní s originálním UNIXovým jádrem. [4]

Plug-and-play v té době nebyl stále vynalezen, ale mnoho lidí mělo zájem o UNIXOVÝ systém, tak Linuxová komunita začala vyvíjet ovladače pro co nejširší okruh zařízení. V průběhu několika let byly všechny funkce UNIXU za dodržení standardu POSIX přidány a Linux dospěl do stádia jak ho známe i dnes. [4]

V dnešní době slouží Linux jako operační systém jak pro stolní počítače, servery a mobilní telefony, tak pro domácí spotřebiče a armádní techniku. Jeho hlavní výhodou je stabilita, spolehlivost a výkonnost. Díky těmto vlastnostem je hojně využíván ve vysoce zatížených systémech. K dalším jeho kladům patří možnost konfigurovat všechny serverové aplikace editací textových souborů bez nutnosti grafické nadstavby nutné například u operačního systému Windows. Plně tak můžeme využít výkonu serveru, který pak u zpracování videa je velmi potřebný. Díky těmto vlastnostem se stává ideální volbou pro tento projekt. [4]

## Bezpečnost

Byla zmíněna spolehlivost a výkon operačního systému Linux a tak je nutné připomenout také bezpečnost. Níže jsou uvedeny tři základní pilíře, na kterých stojí bezpečnost Linuxu.

1. Práva - Jeden ze zásadních rozdílů mezi OS Windows a Linuxem je v defaultním nastavení práv uživatelů. Pro uživatele na operačním systému Windows jsou ve většině případů nastaveny administrátorská práva automaticky po přidání nového uživatele. To znamená, že mají přístup prakticky ke všem funkcím systému. Naopak u uživatelů Linuxu jsou práva přiřazena tak, aby i při narušení integrity systému nedošlo k poškození celku.
2. Open source - Mnozí odborníci tvrdí, že otevřený model je bezpečnější z jednoho prostého důvodu, a to že ho může kdokoliv vidět a vylepšit. Všechny nové distribuce Linuxu a software, který na ně vyjde, prochází pod přísným okem tisíců uživatelů Linuxu, kteří ji začnou testovat, prověřovat a používat se svými reálnými aplikacemi. Takto široké testování je nemožné u uzavřených vlastnických programů.
3. 8 zdí, které chrání jádro Linuxu - Jádro Operačního systému Linux je obklopeno osmi bezpečnostními moduly. Každá z distribucí Linuxu používá jinou kombinaci těchto modulů čímž drasticky sníží šanci útočníka nabourat se do systému Linux. [5,6,7]

Ačkoliv má Linux své výhody, pro tento projekt byla vybrána distribuce s názvem Ubuntu, která se více specializuje na serverové aplikace. Ubuntu obsahuje veškeré bezpečnostní prvky linuxu a k tomu navíc přináší i spoustu dalších utilit, které zjednodušují instalaci a konfiguraci systému.

## 2.2 Ubuntu

Ubuntu je distribuce Linuxu neboli verze operačního systému, který obsahuje linuxové jádro (Kernel). Ubuntu je skvěle připraveno i pro náročné podnikové prostředí díky podpoře společnosti Canonical. Ubuntu server je postaven na kvalitních základech Debianu, který se vyznačuje robustní serverovou instalací a spolehlivým výkonem. Nejdůležitější vlastnost, která byla převzata z Debianu je bezpečnost výchozí instalace. Ubuntu server obsahuje pouze nejnutnější software a po instalaci nenechá otevřený jediný síťový port. Další volitelné aplikace pro Ubuntu server lze doinstalovat prostřednictvím internetu. Existují do-

slova stovky různých distribucí Linuxu. Mnohé z nich jsou zdarma a mají obrovskou komunitu uživatelů. [8]

Ubuntu server byl zvolen pro tento projekt především pro širokou podporu a dokumentaci, kterou nabízí administrátorovi, ale také pro svou robustnost a bezpečnost. V případě jakýchkoliv problémů při instalaci nebo konfiguraci se lze obrátit na rozlehlou škálu návodů, tipů a rad, které poskytují komunitní fóra. Ubuntu server využívá pro práci příkazovou řádku, což znamená, že výkon nezatěžuje jakékoliv grafické rozhraní jako je tomu u Windows serverů. Chybějící grafické rozhraní dále přispívá k celkové stabilitě celého systému. Ubuntu je dostupný zdarma na oficiálních stránkách, což je velkou výhodou v případě, že se v systému vyskytne více serverů a bylo by potřeba zakoupit licenci pro každý server zvlášť. Cena za hardware se také značně sníží díky faktu, že Ubuntu server je odlehčený, rychlejší a nároky na hardware jsou mnohem menší než u jiných operačních systémů.

Pro administraci Ubuntu serveru existuje několik nadstaveb, jako například webmin, kterých ale v tomto projektu nebylo využito. Více se zde hodí konfigurace pomocí editace konfiguračních souborů. Administrátor má tak větší kontrolu nad celým systémem. Níže jsou uvedeny hardwarové nároky na Ubuntu server. [8]

- 300 MHz x86 procesor.
- 192 MiB paměti (RAM).
- 1 GB volného místa na disku.
- Grafická karta a monitor, který je schopný rozlišení 640x480 px.

Je zde patrné, že náročnost na hardwarovou stránku serveru je minimální. Podobná sestava by bez problémů dokázala např. hostovat nenáročné webové stránky nebo mail server.

### 2.2.1 Apache

Apache HTTP Server je open source webová aplikace, která je zodpovědná za chod webové stránky a poskytnutí webových služeb uživateli.

Mezi tyto služby patří:

- HTML Dokumenty.
- Multimediální služby.
- Kaskádové styly.
- Skripty na straně uživatele.



Apache Server od svého počátku v roce 1995 se stal hlavní technologií, díky které se rozrostl internet do dnešní podoby. Podle webových stránek [www.netcraft.com](http://www.netcraft.com) v únoru 2015 přes 38% webových stránek je provozováno na Apache serverech. Ty se vyznačují svou robustností, tudíž zvládá zatížení velkého množství uživatelů na jednom serveru. Díky možnosti přidání modulů s dalšími funkcemi se Apache hodí pro různá webová řešení. [9]

Každý modul poskytuje specifickou funkci jako například:

- Podporu pro Kryptografický protokol SSL.
- Skriptovací jazyk PHP.
- Vyvažování zátěže pro více serverové řešení. [9]

Pro tento projekt byl Apache zvolen především pro podporu výše zmiňovaného skriptovacího jazyku PHP, ale také pro jeho bohatou dokumentaci, jednoduchou správu a instalaci.

### 2.2.2 MySQL

MySQL je multiplatformní databázový systém, který komunikuje pomocí skriptovacího jazyka SQL, neboli Strukturovaný Dotazovací Jazyk (Structured Query Language). [10]

Databázový systém MySQL používá architekturu klient-server. Server manipuluje s databází, kdežto klientské programy předávají záměr uživatele k serveru prostřednictvím dotazů. [10]

Pro lepší pochopení byl uveden příklad dotazu:

```
SELECT * FROM db_firma.uzivatel
```

Tento dotaz vybere všechny údaje z tabulky "uzivatel" v databázi "db\_firma". Dále vysvětlení tohoto dotazu je uvedeno v tabulce 1.

Tabulka 1 Příklad SQL příkazu.

SQL Výraz	Funkce
SELECT	Slouží pro výběr dat z databáze.
*	Slouží pro vybrání všech záznamů.
FROM	Určuje, z jaké tabulky budou data vybrána.
db_firma	Název databáze, z které budou vybrána data.
uzivatel	Název tabulky, z které budou vybrána data.

Každá databáze se skládá z jedné či více tabulek. Řádky udávají jednotlivé záznamy a sloupce rozlišují data v záznamu. Názvy databází, tabulek a sloupců podléhají určitým pravidlům.

- Délka nesmí být větší jak 64 znaků.
- Může obsahovat jakýkoliv alfanumerický znak.
- Může obsahovat znaky '\_' a '\$'.
- Začátek názvu může být jakýkoliv povolený znak včetně čísla.
- Nemůže obsahovat pouze číslice.
- Pro názvy databází a tabulek jsou zakázány znaky '.' a '/' nebo '\\).
- Název databáze, tabulky a sloupce nesmí končit mezerou. [10]

Doporučuje se vyhnout se mezerám v názvech a také rezervovaným slovům jako například "select".

Každá tabulka musí obsahovat sloupec, který bude jednoznačně označovat záznamy v tabulce, většinou pojmenován "id". Tento sloupec obsahuje číslo, které se s každým záznamem zvětší. Pokud v tabulce tento sloupec chybí, není možné záznamy editovat či mazat.

Uživatelské programy jsou instalovány lokálně na počítači, ze kterého se přistupuje k MySQL, kdežto server může být nainstalován kdekoliv, pokud se k němu mohou uživatelé připojit.

Jednotlivé dotazy jsou psány k mnoha různým účelům, ale princip je pro všechny stejný. Po připojení k serveru se zašle daný dotaz, který dále server zpracuje a zašle výsledná data zpět uživateli, kde je zobrazí webová aplikace. [10]

Pro tento projekt je databázový systém nezbytný. Jsou v něm uloženy veškeré informace o uživateli, IP kamerách a probíhajících streamovaných datech.

### 2.2.3 PHP

PHP (PHP: Hypertext Preprocessor) je široce používaný open source skriptovací jazyk, který je obzvláště vhodný pro vývoj webových aplikací. Místo spousty příkazů pro zobrazení HTML (jak je vidět ve skriptovacích jazycích C nebo Perl), PHP stránky obsahují HTML s vloženým kódem, který vykonává danou funkci (sečtení dvou proměnných, vypsání zprávy na obrazovku). PHP kód je uzavřen ve speciálních procesních instrukcích, které určují začátek a konec PHP kódu "<?php" a ">". [11]

To, co odlišuje PHP od jiných skriptovacích jazyků, které pracují na straně uživatele (jako například JavaScript), je to, že kód a následné generování HTML je prováděno na serveru, který poté odešle data uživateli. Uživatel tak obdrží výsledky spuštěného skriptu, ale neví, co základní kód byl. Tento fakt přispívá k celkové bezpečnosti webových stránek.

### **Co umí PHP?**

Dá se říci, že cokoliv. PHP je především zaměřen na skriptování na straně serveru, takže zvládne vše, co jakýkoliv jiný CGI (Common Gateway Interface) program. Jako například práce s formuláři, generování dynamického obsahu stránky, nebo odesílání a přijímání souborů cookie. Ale PHP umí mnohem víc.

Zde jsou uvedeny 3 hlavní oblasti, ve kterých se používá PHP.

- Skriptování na straně serveru. Tradiční a hlavní cílová oblast pro PHP. Pro správnou funkci jsou potřeba 3 věci. PHP parser (CGI nebo modul serveru), webový server a webový prohlížeč.
- Skriptování pomocí příkazového řádku. Je možné vytvořit PHP skript, který funguje bez serveru nebo prohlížeče. Je potřeba pouze PHP parse. Tento typ použití je ideální pro skripty pravidelně prováděné pomocí cronu (na \* nix nebo Linux systémech). Tyto skripty mohou být také použity pro jednoduché úkoly zpracování textu.
- Psaní desktopových aplikací. PHP není nejlepší jazyk pro tvorbu desktopových aplikací s grafickým uživatelským rozhraním, ale pokud programátor zná PHP velmi dobře, a chce používat některé pokročilé funkce PHP ve svých aplikacích na straně klienta lze použít nadstavbu PHP-GTK. [11]

PHP lze použít na všech hlavních operačních systémech, včetně Linuxu, mnoho variant Unixu (HP-UX, Solaris a OpenBSD), Microsoft Windows, Mac OS X a RISC OS. PHP má také podporu pro většinu webových serverů. To zahrnuje Apache, IIS, a mnoho dalších. [12]

S PHP nejsme omezeni pouze na výstup HTML. Ke schopnostem PHP patří zobrazení obrázků, PDF souborů a dokonce Flash animací generovaných dynamicky. Také je možné snadno zobrazit libovolný text, jako je XHTML a jakýkoliv jiný XML soubor. PHP automaticky generuje tyto soubory a ukládá je do systémových souborů. Tvoří tak na straně serveru vyrovnávací paměť dynamického obsahu. [12]

Jedna z nejvýznamnějších vlastností PHP je jeho podpora pro širokou škálu databází. Propojení PHP skriptu a databáze je neuvěřitelně jednoduché za použití specifických rozšíření (např, MySQL), nebo po připojení k libovolné databázi podporované standardem Open Database Connection přes rozšíření ODBC. [12]

PHP má také podporu pro komunikaci s dalšími službami pomocí protokolů, jako je LDAP, IMAP, SNMP, NNTP, POP3, HTTP, COM (na Windows) a bezpočet dalších. PHP má podporu pro WDDX, což umožňuje komplexní výměnu dat prakticky mezi všemi webovými programovacími jazyky. [11]

#### 2.2.4 VPN Server

VPN je virtuální privátní síť, která je konstruována za použití veřejných sítí, jako je internet, pro připojení přímo k privátní síti, například interní síť firmy. Existuje celá řada systémů, které umožňují vytvářet virtuální privátní sítě s využitím internetu jako média pro přenos dat. V této práci je využito softwaru PPTP. Poskytuje plně vybavenou a zabezpečenou tunelovou síť. Tyto systémy používají šifrování a další bezpečnostní mechanismy, které zajistí, že pouze oprávnění uživatelé mohou přistupovat k síti a že údaje nemohou být zachyceny. [13]

Prvním krokem k bezpečnosti je obvykle firewall mezi klientem a hostitelským serverem. Šifrování je také důležitou součástí bezpečného VPN. PPTP využívá knihovny OpenSSL pro šifrování dat a řídicích kanálů. Ověřování klientů probíhá pomocí sdíleného klíče, certifikátu nebo uživatelského jména a hesla.

VPN server je navržen tak, aby poskytl zabezpečený šifrovaný síťový tunel, ve kterém dochází k přenosu dat mezi vzdálenými sítěmi. Informace předávané mezi dvěma místy přes šifrovaný tunel nemohou být odposlechnuty, protože systém obsahuje několik prvků pro zabezpečení, jak privátní virtuální síť, tak vnější síť, přes kterou se vzdálený uživatel připojuje. [13]

### 2.2.5 VLC Player

VLC Player je open source multiplatformní multimediální přehrávač, dekodér a streamovací server. VLC podporuje široké spektrum audio a video formátů a kodeků, stejně jako DVD, VCD, a streamovacích protokolů. Umožňuje streamování přes síť, převzorkování multimediálních souborů a uložení do různých formátů. VLC, jako většina multimediálních frameworků, má modulární design, který umožňuje jednoduché přidání potřebných funkcí. [14]

V tomto projektu je VLC využito pro nastolení komunikace s IP kamerou, převzorkování dat z IP kamer do správného formátu a zprostředkování streamu uživateli prostřednictvím webové aplikace. Na straně serveru je VLC spouštěno bez grafického uživatelského rozhraní, aby byl zajištěn nejlepší možný výkon systému.

## 2.3 Router

Router je zařízení, které spojuje alespoň dvě sítě a předává mezi nimi datové pakety. Ve většině případů jsou využity k propojení vnější sítě (internetu) se sítí vnitřní (firemní nebo domácí síť). Takový router se nazývá "edge router" nebo také "brána". Routery používají záhlaví a tzv. routovací tabulky k určení cesty pro směrování paketů a protokoly, jako například ICMP ke vzájemné komunikaci a konfiguraci trasy mezi dvěma hostiteli.

### Komunikace s IP kamerou

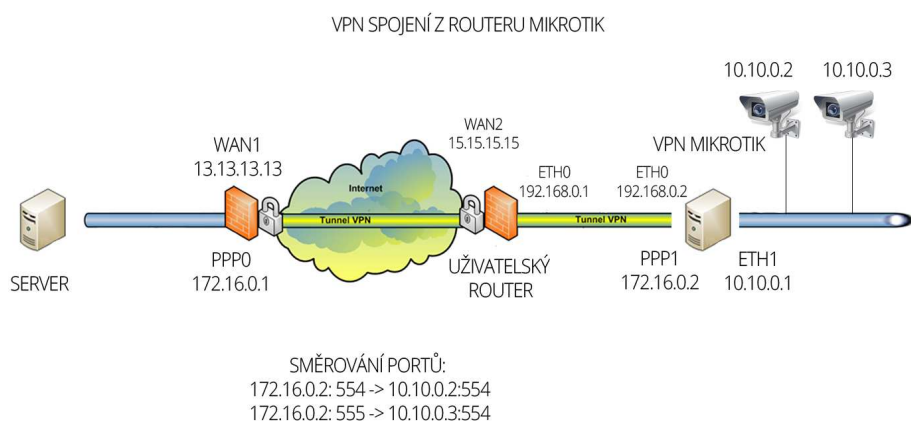
Nejdříve je nutné si uvědomit, že prvky, v tomto případě IP kamery, jsou umístěny ve vnitřní síti tudíž pro server neviditelné. Tento systém poskytuje dvě možnosti, jak tento problém obejít. Při registraci kamery uživatel má dvě možnosti způsobu připojení IP kamery k serveru.

### Směrování portů

První způsob využívá směrování portů. Uživatel ručně nastaví na svém routeru směrování příchozí relace s daným vstupním portem (vyplněným při registraci) do vnitřní sítě na IP adresu a port připojené kamery. Z hlediska bezpečnosti je tato metoda méně vhodná, protože na vstupním routeru otvírá porty, kterých může potenciální útočník využít k napadení sítě.

## VPN spojení

Druhá metoda vytvoří síťový tunel mezi serverem a routerem, který zajistí bezpečný šifrovaný přenos dat a přístup do vnitřní sítě s kamerami. Na video serveru je aktivní VPN server, který naslouchá žádostem o připojení ze strany uživatelských VPN klientů. Uživatel má na výběr ze dvou možností, jak vytvořit VPN klienta. A to buď nakonfigurováním vlastního routeru (uživatelské jméno, heslo, IP adresa), nebo zařazením speciálního VPN routeru (platformy Mikrotik) jak je uvedeno na obrázku 2. Tento router byl použit pro svou komplexnost, jednoduchost nastavení, cenovou dostupnost a bohatou podporu funkcí. Toto zařízení zprostředkovává připojení k VPN serveru a samotné směrování připojení na jednotlivé kamery v síti. Pro tento případ samotná aplikace vygeneruje část konfiguračního souboru pro Mikrotik, který uživatel zkopírováním do terminálu nahraje a zprovozní VPN připojení.



Obrázek 2 VPN spojení z routeru Mikrotik.

Router spojuje video server s IP kamerami uživatele jak pomocí směrování portů, tak přes VPN tunel.

## 2.4 IP kamera

IP kamera je koncový prvek systému. Kamery se obecně rozdělují do dvou kategorií, analogové kamery a IP kamery. Rozdíl, jak už z názvu vypovídá, je v typu komunikace. Analogové CCTV kamery vysílají analogové video přímo do DVR (Digital Video Recorder), který poté převede analogové video na digitální. Tato komunikace je jednosměrná a pro přenos je používán koaxiální kabel.

Na rozdíl od analogové kamery samotná IP kamera je schopná vysílat digitální video, tudíž není potřeba převodu z analogového signálu na digitální. Kamera je navíc síťový prvek připojený do sítě přes ethernet komunikující oboustranně mezi uživatelem a kamerou. Hlavní důvod proč jsou IP kamery populárnější než analogové, je jejich schopnost nahrát a poskytnout mnohem kvalitnější video a audio data s menší náročností na zátěž sítě.

Tento systém musí zvládat zpracovávat velký počet streamů zároveň, takže klade velký důraz na kompresi a odlehčení přenášených dat. Pro kompresi dat je využit open source Theora kodek vyvinutý organizací Xiph.org. Po technologické stránce je Theora navržena pro nenáročné streamy dat. Její in-loop deblokovací filtr je velice efektivní při prevenci rušivého členěného vzhledu komprimovaných dat, což je zásadní vlastností pro jakýkoliv video kodek cílený na webové aplikace.

Uživatel musí zaregistrovat kameru do systému pomocí formuláře. Je nutné vyplnit informace jako IP adresa, MAC adresa, URL, přihlašovací jméno a heslo pro přístup ke kameře. Podle typu připojení (směrování portů nebo VPN tunel) se dále vyplňuje port a v případě VPN tunelu je možno zvolit pro adresování kamery DHCP (anglicky Dynamic Host Configuration Protocol) protokol.

## **II. PRAKTICKÁ ČÁST**



### 3 ÚVOD DO PRAKTICKÉ ČÁSTI

V následujících kapitolách této práce bude popsán proces instalace a konfigurace jednotlivých prvků systému a to hlavně video serveru, VPN serveru a klienta, webové aplikace a mediálního přehrávače VLC, který v navrhovaném systému zprostředkovává stream z IP kamer na webový portál.

V prvním kroku bude popsána instalace operačního systému linux - distribuce Ubuntu. Dále instalace potřebných komponentů a balíčků nutných pro funkci webového serveru a dalších podpůrných programů (DNS, MySQL, Postfix - mail server, PHP), které jsou nezbytné pro instalaci webové nadstavby ISPConfig pro správu hostingového serveru. Na video serveru je dále nainstalován software VLC, který je spouštěn jako stream server. Pomocí něj se systém připojuje ke vzdáleným IP kamerám přes protokol RTSP a po změně parametrů přijatého streamovaného videa je upravený video signál streamován do webové aplikace. Následně je popsána metoda připojení kamer uvnitř sítě přes VPN spojení realizované buď na uživatelský router, nebo na speciální VPN router (Mikrotik) umístěný uvnitř sítě za firewallem.

V poslední kapitole praktické části je popsána webová aplikace, použité technologie, struktura databáze, jednotlivé sekce aplikace, jejich funkce a požadavky na uživatele systému.

V následujících kapitolách jsou uvedeny zdrojové části kódu označeny šedým zvýrazněním, psané kurzívou, fontem Courier velikosti 11 stejně jako v následujícím příkladu:

`apt-get upgrade`. Text psaný červeně označuje informace vložené uživatelem.

## 4 INSTALACE SERVERU

Z oficiálních stránek Ubuntu bylo staženo instalační CD, ze kterého byl nainstalován základní operační systém Linux. Celá instalace proběhla pomocí instalačního programu, kde byly vyplněny základní vlastnosti systému.

### 4.1 ISPConfig

Po instalaci operačního systému Ubuntu byl upraven konfigurační soubor pro repozitáře `/etc/apt/sources.list`.

Poté příkazem `apt-get update` aktualizována databáze apt balíčků a příkazem `apt-get upgrade` nainstalována aktuální verze balíčků ve zmiňované databázi. Pokud byl aktualizován i kernel, bylo potřeba restartovat server pomocí `reboot`.

Bylo nutné přenastavit výchozí shell, z `/bin/dash` na `/bin/bash`, příkazem `dpkg-reconfigure dash`

#### AppArmor

Dalším krokem bylo zakázat bezpečnostní rozšíření AppArmor. Tento program způsobuje řadu problémů a není vhodné ho používat. AppArmor byl zakázán příkazy:

```
service apparmor stop  
update-rc.d -f apparmor remove  
apt-get remove apparmor apparmor-utils
```

Je také vhodné aktualizovat systémové hodiny s NTP (Network Time Protocol) serverem. Toho bylo docíleno spuštěním příkazu `apt-get install ntp ntpdate`.

#### Postfix

Aby bylo možné nainstalovat postfix, bylo nutné nejprve odstranit sendmail. To bylo provedeno příkazem `service sendmail stop; update-rc.d -f sendmail remove`. Poté bylo možné nainstalovat Postfix, Dovecot, MySQL, rkhunter a binutils jediným příkazem:

```
apt-get install postfix postfix-mysql postfix-doc mariadb-client mariadb-  
server openssl getmail4 rkhunter binutils dovecot-imapd dovecot-pop3d dovecot-  
mysql dovecot-sieve sudo
```

Byly položeny následující otázky (vkládané informace jsou označeny červeně):

New password for the MySQL "root" user: *sqlrootheslo*

Repeat password for the MySQL "root" user: *sqlrootheslo*

Create a self-signed SSL certificate?: *Yes*

Host name: *video.3wpro.cz*

Local only: *OK*

General type of mail configuration: *Internet Site*

System mail name: *video.3wpro.cz*

Dále byly otevřeny TLS/SSL a submission porty pro mailový server Postfix.

### SpamAssassin a ClamAV

V následujícím kroku byly nainstalovány anti-spamové a anti-virové balíčky amavids-new, SpamAssassin a ClamAV příkazem:

```
apt-get install amavisd-new spamassassin clamav clamav-daemon zoo unzip bzip2  
arj nomarch lzop cabextract apt-listchanges libnet-ldap-perl libauthen-sasl-  
perl clamav-docs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-  
perl zip libnet-dns-perl
```

Jelikož služba SpamAssassin bude automaticky spouštěna jak při startu serveru, tak službou amavisd, bylo nutné službu zastavit a smazat ze zpouštěcích skriptů při startu Linuxu příkazem:

```
service spamassassin stop
```

```
update-rc.d -f spamassassin remove
```

poté byl spuštěn clamav příkazy *freshclam* a *service clamav-daemon start*

## Balíčky Apache, PHP a phpMyAdmin

Pro instalaci služeb Apache2, PHP5, phpMyAdmin, FCGI, suExec, Pear a mcrypt byl spuštěn příkaz `apt-get` ve tvaru:

```
apt-get install apache2 apache2-doc apache2-utils libapache2-mod-php5 php5-  
php5-common php5-gd php5-mysql php5-imap phpmyadmin php5-cli php5-cgi  
libapache2-mod-fcgid apache2-suexec php-pear php-auth php5-mcrypt mcrypt php5-  
imagick imagemagick libapache2-mod-suphp libruby libapache2-mod-python php5-  
curl php5-intl php5-memcache php5-memcached php5-ming php5-ps php5-pspell  
php5-recode php5-sqlite php5-tidy php5-xmlrpc php5-xsl memcached
```

Server vyžádal následující informace:

Web server to reconfigure automatically: **apache2**

Configure database for phpmyadmin with dbconfig-common? **No**

Bylo potřeba webovému serveru Apache povolit moduly suexec, rewrite, ssl, actions, include, dav, dav\_fs a auth\_digest. Vše bylo provedeno jedním příkazem `a2enmod suexec rewrite ssl actions include cgi dav_fs dav auth_digest`. Navíc bylo potřeba upravit soubor `/etc/apache2/mods-available/suphp.conf` odstraněním sekce `<FilesMatch "\.ph(p3?|tml)$">` a přidáním řádku "AddType application/x-httpd-suphp .php .php3 .php4 .php5 .phtml". Nakonec byl restartován Apache příkazem `service apache2 restart`.

Pro hostování frameworku ruby na serveru bylo nutné odstranit řádek `"application/x-ruby rb"` v souboru `/etc/mime.types`. Znovu byl restartován Apache stejným způsobem jako v předchozím případě.

Pro zrychlení PHP stránek byl nainstalován cache PHP opcode Xcache příkazem `apt-get install php5-xcache` a opět restartován Apache.

S příchodem ISPConfig verze 3.0.5 přibyl mód pro PHP, který umožňuje PHP spustit jako CGI (Common Gateway Interface). Byl nainstalován pomocí příkazu `apt-get install libapache2-mod-fastcgi php5-fpm`. Dále byl povolen modul a restartován Apache příkazy `a2enmod actions fastcgi alias` a `service apache2 restart`.

## FTP

Pro přenos souborů pomocí FTP (File Transfer Protocol) bylo využito služby PureFTP a Quota a ty byly nainstalovány příkazem `apt-get install pure-ftpd-common pure-ftpd-mysql quota quotatool`. Byl upraven soubor `/etc/default/pure-ftpd-common` tak, aby `start mode` byl nastaven na "standalone" a "VIRTUALCHROOT=true".

Bylo povoleno FTP a TLS sessions v PureFTPd. FTP není bezpečný protokol, protože veškerá hesla a data posílá jako čistý text. Použitím TLS byla zašifrována celá komunikace a zvýšena bezpečnost FTP. Pro povolení FTP a TLS sessions byl spuštěn příkaz `echo 1 > /etc/pure-ftpd/conf/TLS`. Pro použití TLS bylo potřeba vytvořit SSL certifikát. Nejdříve byla vytvořena složka `/etc/ssl/private/`. Poté vygenerován SSL certifikát příkazem `openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout /etc/ssl/private/pure-ftpd.pem -out /etc/ssl/private/pure-ftpd.pem`.

Bylo nutné vyplnit tyto informace:

Country Name (2 letter code) [AU]: **CZ**

State or Province Name (full name) [Some-State]: **Czech Republic**

Locality Name (eg, city) []: **Šumperk**

Organization Name (eg, company) [Internet Widgits Pty Ltd]: **poskytuj s.r.o.**

Organizational Unit Name (eg, section) []: **ispconfig4.poskytuj.cz,**  
**Poskytuj s.r.o.**

Common Name (eg, YOUR name) []: **ispconfig4.poskytuj.cz**

Email Address []: **jarkovsky.d@poskytuj.cz**

Nakonec byla změněna práva SSL certifikátu příkazem `chmod 600 /etc/ssl/private/pure-ftpd.pem` a restartován PureFTPd příkazem `service pure-ftpd-mysql restart`.

Dále byl editován `/etc/fstab` aby byly uplatněny quoty na File System. Následujícími třemi příkazy byly připojeny a povoleny quoty:

`mount -o remount /`

`quotacheck -avugm`

`quotaon -avug`

## DNS

Byl nainstalován DNS server BIND. Je to nejrozšířenější DNS server vhodný pro velmi zatížené systémy. Příkazem `apt-get install bind9 dnsutils` byl nainstalován BIND.

Pro zajištění statistik přístupu na web byl použit software Vlogger, Webalizer a AWstats. Příkazem `apt-get install vlogger webalizer awstats geoip-database libclass-dbi-mysql-perl` byly nainstalovány všechny tři zmíněné programy.

## Fail2ban

Fail2ban skenuje záznamy errorů a zakazuje přístup z IP adres, které se zdají být škodlivé (příliš mnoho pokusů zadat heslo, snaha o zneužití systému, atd.). Fail2ban aktualizuje pravidla firewallu a odmítá IP adresy po určitou dobu.

Pro jeho nainstalování byl použit příkaz `apt-get install fail2ban`. Poté byl nastaven Fail2ban tak, aby monitoroval PureFTPd a Dovecot.

## ISPConfig 3

Poslední verzi balíčku ISPConfig 3 byla nainstalována pomocí příkazu:

```
cd /tmp
```

```
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
```

```
tar xzf ISPConfig-3-stable.tar.gz
```

```
cd ispconfig3_install/install/
```

```
php -q install.php
```

Toto spustí ISPConfig 3 instalaci a automaticky nakonfiguruje všechny služby jako Postfix a Dovecot. Nakonec byly nastaveny informace jako uživatelská a root hesla pro MySQL, jméno databáze, která je dále využívána pro uchování dat z webové stránky a údaje o administrátorovi.

Tímto byla instalace softwaru ISPConfig a všech balíčků potřebných ke správnému chodu webové aplikace úspěšně dokončena.

## 4.2 VLC

Software VLC slouží ke streamování videa z připojených IP kamer. Pro jeho instalaci byl použit příkaz `apt-get install vlc vlc-nox libavcodec-extra-53`. Pro práci s VLC není použito GUI (Graphic User Interface), které je běžně využíváno v systémech Windows, ale je využit mód příkazové řádky (Command Line). Struktura parametrů v příkazové řádce určuje použití VLC. Příkaz pro spuštění streamu z IP kamery vypadá takto:

```
cvlc -I dummy rtsp://nick:heslo@ip/url  
  
--noaudio  
  
--sout '#transcode{vcodec=theo,vb=20,deinterlace=linear,width=350,height=200}  
:standard{access=http,mux=ogg,dst=:8888/name.ogg}' > /dev/null 2>&1 & echo $!
```

Zde jsou rozebrány použité parametry:

- `cvlc` - Nastartuje VLC.
- `-I dummy` - Je použito v případě, kdy je nevhodné výstup směřovat na konkrétní HW zařízení (např. monitor).
- `rtsp://nick:heslo@ip/url` - Vstupní stream do VLC poskytuje vzdálená IP kamera. V tomto případě je dán protokolem RTSP a vzdálenou *ip/url*. *Nick*, *heslo*, *ip* a *url* zadává uživatel při registraci IP kamery ve webové aplikaci. Výsledná adresa může mít například tvar "`rtsp://video:1234@192.168.1.200/live0`".
- `--noaudio` - V této verzi návrhu není zpracováván audio stream.
- `--sout` - Popisuje výstupní stream.
- `transcode` - Převzorkuje originální stream použitým kodekem (Theora), odstraní prokládání a nastaví `vb` (video bitrate).
- `:standard` - Výstup definuje modul standard, jehož volby jsou `access` - určuje způsob přenosu (HTTP), `mux` - určuje formát a `dst` - definuje adresu HTTP.
- `> /dev/null 2>&1` - Udává, že výstupy z předchozího příkazu jsou zahozeny a nezaznamenávány do logu.
- `&` - Přesune proceduru na pozadí.
- `echo $!` - Vráti hodnotu ID zpracovávaného procesu, která je poté použita pro ukončení streamování.

Pokud ve webové aplikaci uživatel vybere prohlížení své IP kamery, je spuštěn tento příkaz a jednotlivé parametry se přebírají z databáze registrovaných IP kamer.

## 4.3 VPN

Základní distribuce neobsahovala žádný před-instalovaný VPN server, a proto se musel pro potřeby aplikace doinstalovat pomocí příkazu `apt-get install pptpd`. Tím byla nainstaloována sada nástrojů a zbývalo pouze nakonfigurovat nastavení.

### 4.3.1 Server

Hlavním parametrem při konfiguraci VPN serveru bylo nastavení použitého šifrování, rozsahu poskytovaných IP adres pro klientskou část, definování přístupových údajů pro jednotlivá připojení. V konfiguračním souboru `/etc/pptpd.conf` byly v části věnované IP adresám nastaveny požadované rozsahy pro lokální adresu serveru a adresy klientských VPN rozhraní na routeru.

Příklad nastavení IP adres:

```
localip 172.16.0.1
```

```
remoteip 172.16.0.2-172.31.255.255
```

U ostatního nastavení pro PPTP byly nechány výchozí hodnoty. Zvláště pak nastavení pro šifrování, autentifikaci a autorizaci. Spojení PPTP jsou ověřována pomocí autentizačních metod Microsoft MSCHAP-v2. Přenos VPN je chráněn MPPE šifrováním (Microsoft Point-to-Point Encryption), které je popsáno pomocí standardu RFC 3078. [15]

Samotná část konfigurace uživatelských jmen a hesel definovaných ve vstupním formuláři pro VPN spojení je konfigurována v souboru `/etc/ppp/chap-secrets`. Ten je generován aplikací automaticky při každé změně nebo přidání nové IP kamery s metodou připojení přes VPN tunel.



#### 4.3.2 Klient

Pro připojení koncových IP kamer bylo využito, buď stávajících VPN routerů uživatelů, nebo byly konfigurovány v síti speciální VPN routery postavené na platformě Mikrotik.

##### **VPN na stávajícím routeru**

Uživatel musí nastavit VPN klienta na svém routeru dle informací zadaných při registraci IP kamery. Jsou to tyto hlavní parametry

- Veřejná IP adresa VPN serveru.
- Uživatelské jméno a heslo.
- Šifrovací metoda MPPE-128bit.
- Ověřovací protokol MS-CHAP v2.
- Nastavení směrování portů na jednotlivé kamery.

##### **VPN na routeru Mikrotik**

Pro uživatele, využívajícího router Mikrotik byl systémem vygenerován konfigurační soubor, který obsahuje nastavení všech IP kamer připojených, ke stejnému VPN spojení.

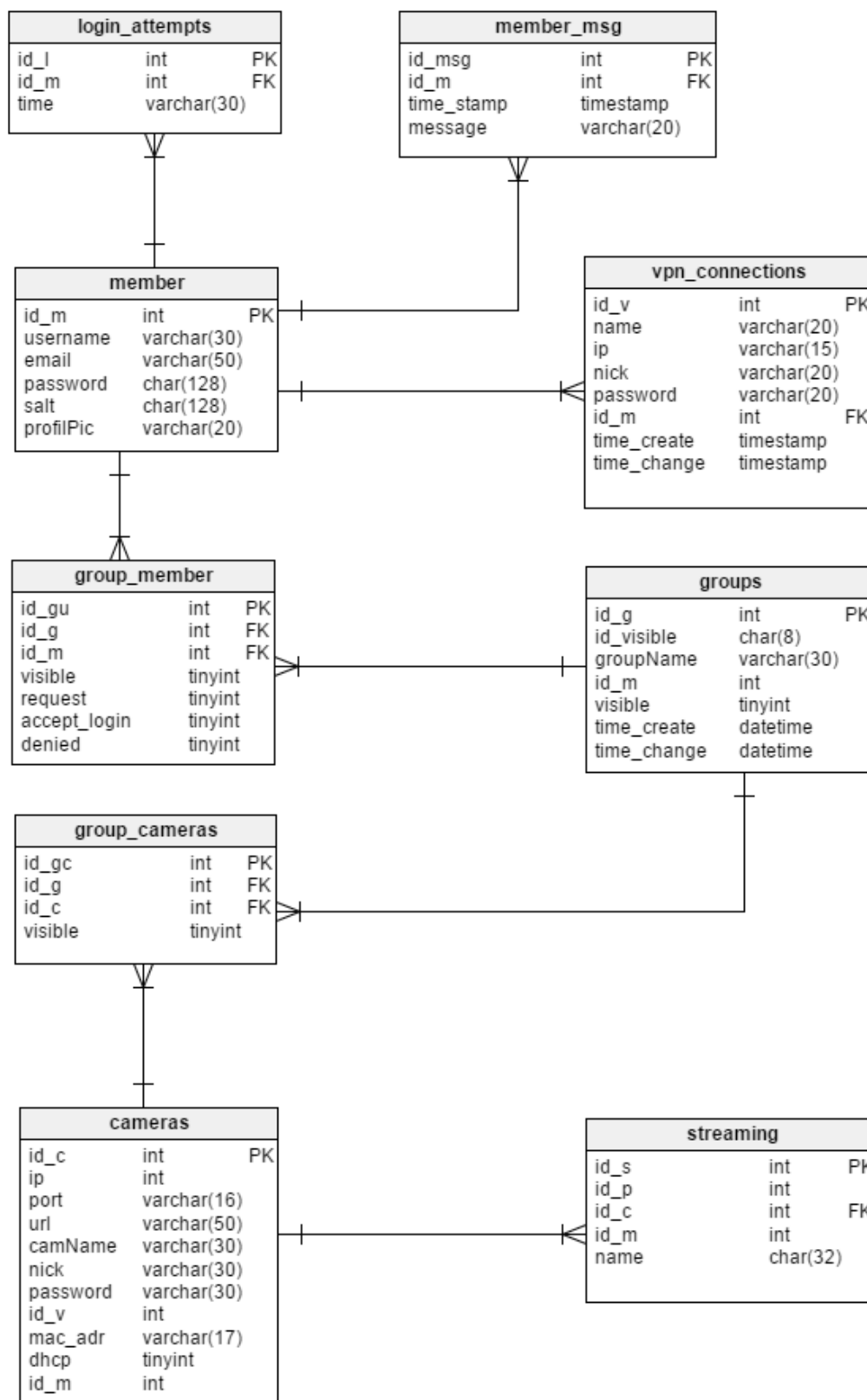
## 5 WEBOVÁ APLIKACE

Webová aplikace byla vyvíjena na platformě HTML5, PHP, CSS3, MySQL a javascript. Poskytování HTML stránek je zabezpečeno pomocí webového serveru Apache.

Při tvorbě webové aplikace bylo využito javascriptové knihovny jquery.js, díky které byly naprogramovány funkce systému jako funkce tlačítek, zobrazování videa z kamer na stránkách a další. Animace a přechody stránek zajišťují opět javascriptové knihovny jquery.fullpage.js a TweenMax.js. Jedná se pouze o grafickou část webové aplikace a na funkčnost nemají vliv. Ve webové aplikaci je využito open source fontů z databáze Google Fonts. Pro uvítací zprávu na úvodní stránce je využit webový font Pacifico, a pro zbývající text je využit font Open Sans, který je hojně využíván pro webové aplikace. Navíc se ve webové aplikaci vyskytují ikony, které jsou obsaženy v kaskádových stylech font-awesome.css.

Pro ukládání informací o uživateli, IP kamerách, uživatelských skupinách a probíhajících streamech videa bylo použito webové nadstavby pro správu MySQL databáze PHPMyAdmin. Struktura databáze a relace tabulek je vidět na obrázku 3.

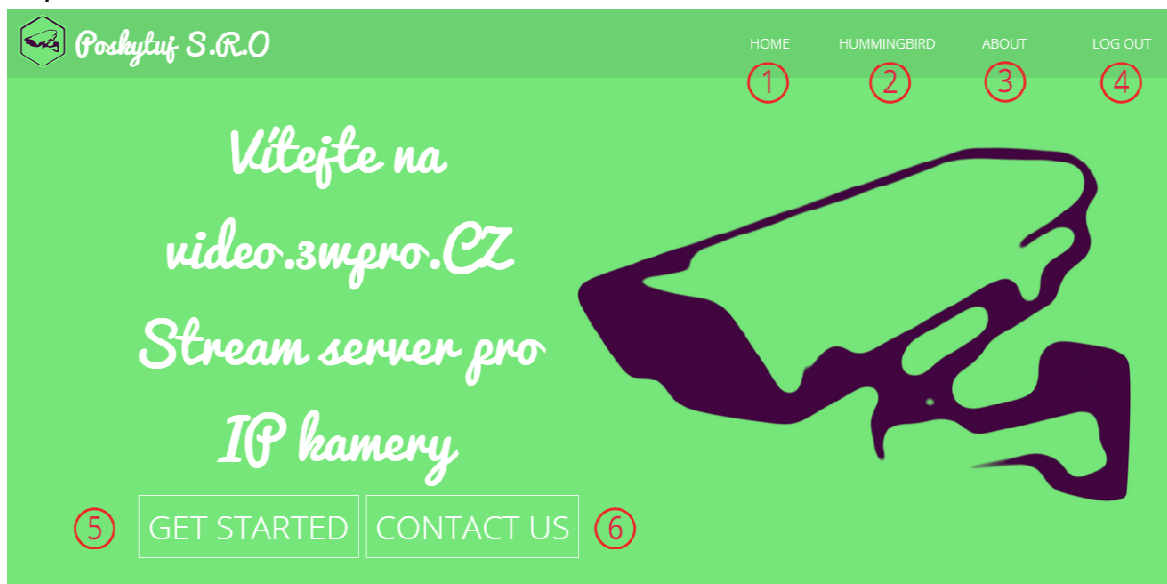
## 5.1 Struktura databáze



Obrázek 3 Relace mezi tabulkami v databázi.

## 5.2 Úvodní strana

Úvodní stránka obsahuje odkazy, které slouží k navigaci po webovém portále. Tyto odkazy jsou označeny body 1 - 6 na obrázku 4 a dále popsány v tabulce 2.



Obrázek 4 Rozvržení úvodní stránky.

Tabulka 2 Popis úvodní stránky.

Odkazy	Popisek	Cíl
1	Přechod na úvodní stranu.	/index.php#Uvod
2	Odkazuje na stránku s kamerami. Text se mění na jméno přihlášeného uživatele.	/users_home.php
3	Přechod na stranu O nás.	/index.php#Onas
4	Odhlásí uživatele, pokud byl přihlášen. Pokud ne, zobrazí přihlašovací obrazovku.	/index.php#Profil
5	Přechod na stranu profil.	/index.php#Profil
6	Přechod na stranu kontakt.	/index.php#Kontakt

Každá stránka obsahuje tzv. header, který slouží pro navigaci na webovém portále. Skládá se z loga a odkazů na jednotlivé části aplikace (body 1 - 4 na obrázku 4). Následuje krátký popisek, uvítání do aplikace a nabídka k registraci (bod 5 na obrázku 4) nebo kontaktování administrátora (bod 6 na obrázku 4). Při první návštěvě webové aplikace jsou některé elementy z designových důvodů animovány.

### 5.3 Přihlášení / registrace a profil

Webová stránka uvedená na obrázku 5 se mění v závislosti na přihlášeném uživateli. Pokud není uživatel přihlášen, neboli neexistuje session, zobrazí se nabídka přihlášení a registrace. Pokud je uživatel přihlášen a session existuje, zobrazí se profil uživatele. Dodatečné informace jsou uvedeny v tabulce 3.

#### Přihlášení / registrace

Obrázek 5 Rozvržení přihlašovací stránky.

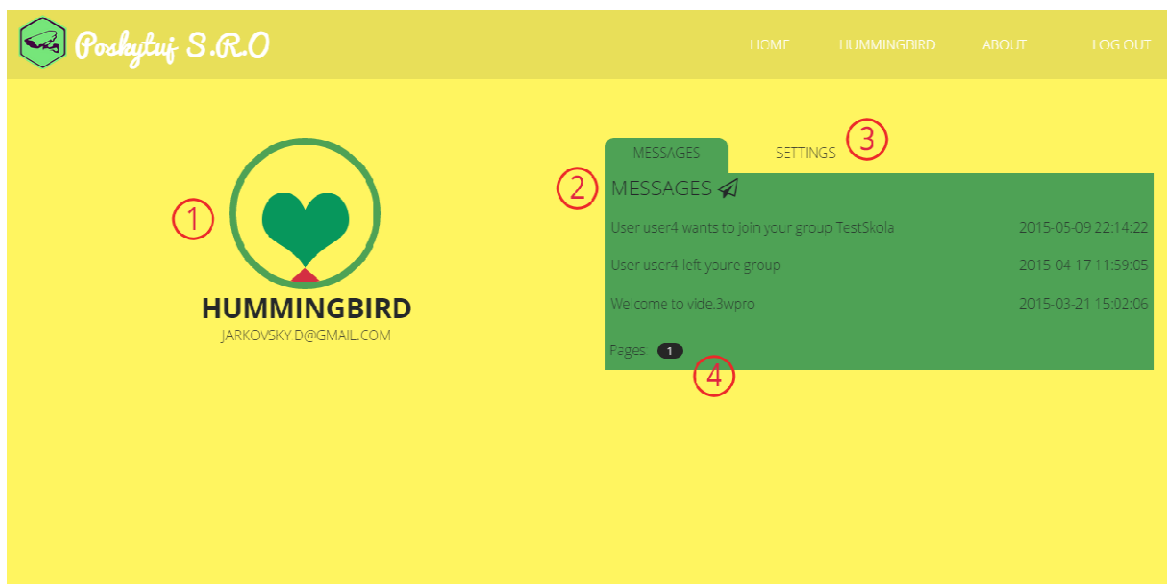
Tabulka 3 Popis přihlašovací stránky.

Odkazy	Popisek
1	Uživatel se přihlašuje E-mailem a heslem.
2	Po přihlášení se vytvoří session a zpřístupní se zabezpečené stránky.
3	Pro zašifrování hesla byla použita hashovací funkce sha-512.
4	Zadané údaje jsou vloženy do databáze a uživateli je vytvořen profil.

Pro přihlášení nebo registraci slouží tato stránka. Pro úspěšnou registraci je vyžadováno uživatelské jméno, E-mail a heslo. Formát těchto položek, stejně jako položek vyplňovaných při přihlášení, podléhá určitým pravidlům. Například E-mail musí být ve správném tvaru, heslo musí obsahovat alespoň jedno malé písmeno, jedno velké písmeno, číslo a délka nesmí být kratší než 8 znaků.

## Profil

Profil uživatele obsahuje jméno a email uživatele, který je vyznačen bodem 1 v obrázku 6. Dále obsahuje systémové zprávy a nastavení profilu. Jednotlivé body jsou popsány v tabulce 4.



Obrázek 6 Rozvržení profilové stránky.

Tabulka 4 Popis profilové stránky.

Odkazy	Popisek
1	Při registraci se uživateli automaticky přiřadí provizorní profilový obrázek.
2	Pravá část obsahuje systémové zprávy a nastavení profilu.
3	Uživatel má možnost změnit svoje uživatelské jméno a přihlašovací E-mail.
4	Zprávy jsou stránkovány po třech a řazeny od nejnovějších po nejstarší.

Systémové zprávy jsou zasílány v různých případech. V tabulce 5 byly vyznačeny možné systémové zprávy a akce, při kterých jsou zaslány.

Tabulka 5 Seznam systémových zpráv.

Znění anglicky	Kdy byla zpráva zaslána	Příjemce zprávy
Welcome <i>uživatelské_jméno</i> !	Po registraci uživatele.	Uživatel
Your request to join group <i>název_skupiny</i> was ACCEPTED.	Po přijetí žádosti na připojení se od skupiny.	Uživatel
Your request to join group <i>název_skupiny</i> was DENIED.	Po zamítnutí žádosti na připojení se od skupiny.	Uživatel
Your request to join group <i>název_skupiny</i> was DISMISED.	Po vyloučení žádosti na připojení se od skupiny.	Uživatel
User <i>uživatelské_jméno</i> wants to join your group <i>název_skupiny</i> .	Po zaslání požadavku na připojení se do skupiny	Administrátor skupiny
Group <i>název_skupiny(neupraveno)</i> has change its name to <i>název_skupiny(upraveno)</i> .	Po změně názvu skupiny.	Uživatelé skupiny
Group <i>název_skupiny</i> has been deleted.	Po smazání skupiny	Uživatelé skupiny

## 5.4 Stránka uživatele

Stránka uživatele obsahuje seznam jednotlivých IP kamer uživatele vyobrazených na obrázku 7 v bodě číslo 1. Další položky na obrázku 7 jsou popsány v tabulce 6.



Obrázek 7 Rozvržení stránky uživatele.

Tabulka 6 Popis stránky uživatele.

Odkazy	Popisek
1	Seznam registrovaných kamer.
2	Možnost registrace kamery a VPN spojení.
3	Uživatel má možnost vytvořit skupinu kamer za účelem sdílení, nebo pouze pro lepší organizaci.
4	Uživatel má také možnost požádat o připojení k existující skupině pomocí osmi místného identifikačního čísla.
5	Identifikační číslo skupiny je jedinečný osmimístný kód obsahující čísla a velká písmena.

Při prvním přihlášení má uživatel možnost zaregistrovat svoje IP kamery do systému. Tyto kamery se poté zobrazí v náhledu (obrázek 7 bod 1). Po kliknutí na jednu z kamer se naváže spojení a spustí se video stream.



The screenshot shows a web application interface for camera registration. The title bar at the top includes the logo 'Poskytující S.R.O.' and navigation links: HOME, HUMMINGBIRD, ABOUT, and LOG OUT. The main heading is 'CAMERA REGISTRATION'. The form is organized into several sections with labels on the left: 'CAMERA NAME' (with a red circle 1), 'Moje' (My), 'Test', 'Cizí' (Other), and 'group'. The input fields are: 'KameraDoma' (under CAMERA NAME), 'PORT' (dropdown), 'IP ADDRESS', 'PORT' (dropdown), 'URL', 'USERNAME', 'PASSWORD', 'CONFIRM PASSWORD', and 'MAC ADDRESS'. A 'REGISTER' button is located below the MAC ADDRESS field. On the right side, there is a settings panel with a red circle 5, containing 'SETTINGS', 'NEW', and 'DELETE GROUP' buttons. At the bottom, there are three buttons labeled 'Užname1', 'Užname2', and 'Užname3'.

Obrázek 8 Registrace kamery.

Pro registraci kamery je nutné vyplnit údaje jako přihlašovací jméno a heslo ke kameře, její IP a MAC adresu, URL kamery a port, na kterém kamera naslouchá. Formulář pro registraci kamery lze vidět na obrázku 8, kde jsou také vyobrazeny jednotlivé údaje, které je nutné vyplnit.

VPN REGISTRATION

VPN NAME

USERNAME

PASSWORD

CONFIRM PASSWORD

REGISTER

SETTINGS

HELP

DELETE GROUP

Cizí skupiny

ADD TO GROUP

group3

U3name1

U3name2

U3name3

Obrázek 9 Registrace VPN spojení.

V případě, když chce uživatel připojit kameru přes VPN tunel, je nutné jej vytvořit na routeru a zaregistrovat do systému pomocí formuláře vyobrazeného na obrázku číslo 9. Systém automaticky přidělí na straně VPN klienta jednoznačnou IP adresu z rozsahu 172.16.0.0/16. Tuto adresu poté využívá systém k přístupu ke kamerám prostřednictvím směrování portů na VPN routeru.

The screenshot shows a web application interface for camera registration. The main heading is 'CAMERA REGISTRATION'. Below it, there are several input fields: 'KameraDoma', 'VPN' (a dropdown menu), 'vpn1' (another dropdown menu), 'IP ADDRESS', 'DHCP' (a checkbox), 'PORT', 'URL', 'USERNAME', 'PASSWORD', 'CONFIRM PASSWORD', and 'MAC ADDRESS'. At the bottom of the form is a 'REGISTER' button. The form is set against a dark background with various icons and labels around it, including 'HOME', 'HUMMINGBIRD', 'ABOUT', 'LOG OUT', 'Moje', 'Test3', 'Cizis', and 'STOUK'. There are also red circles with numbers 1, 5, and 6 highlighting specific parts of the form.

Obrázek 10 Registrace kamery spojené přes VPN.

Po výběru VPN tunelu jako metody spojení přibude, do formuláře pro registraci IP kamer viditelného na obrázku 10, možnost zvolit DHCP jako metodu přidělení IP adresy kamery z VPN routeru. Systém automaticky přidělí kameře první volnou adresu z rozsahu 10.0.0.0/16. Pokud DHCP není zvoleno, uživatel vyplní přímo IP adresu kamery. Port pak slouží pro nastavení směrování na VPN serveru na standardní RTSP port kamery TCP/UDP 555. MAC adresa je použita mimo jiné pro přiřazení IP adresy DHCP serverem. Po dokončení registrace systém vytvoří konfigurační soubor pro router (mikrotik), který uživatel v případě potřeby přepokopíruje do svého routeru. Jde o jednoduchý textový soubor, který se v prostředí Winboxu nakopíruje přes terminál. Obsahuje nastavení DHCP serveru, IP adresy na interfacu do vnitřní sítě s kamerami, nastavení PPTP klienta pro připojení na VPN server, směrování portů v sekci firewall NAT a maškarádu vnitřní sítě.

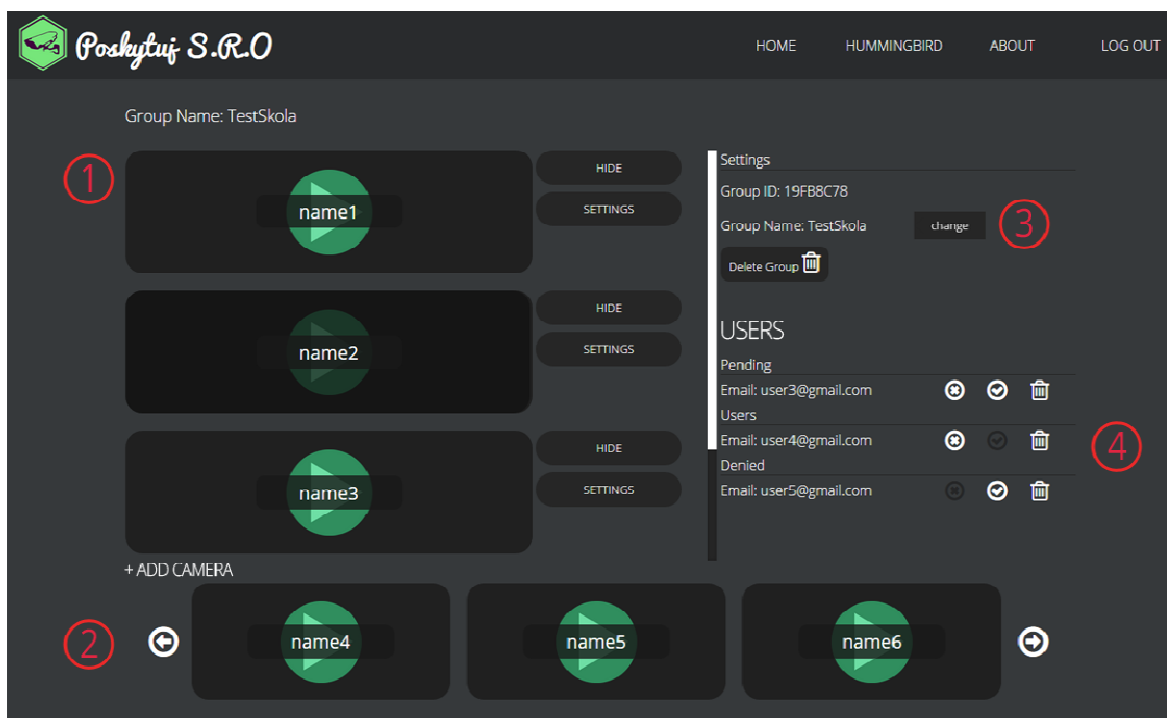
The screenshot shows a web interface for 'GROUP REGISTRATION'. At the top, there is a header with the logo 'Poskytující S.R.O.' and navigation links: HOME, HUMMINGBIRD, ABOUT, and LOG OUT. The main form area is titled 'GROUP REGISTRATION'. It contains a 'GROUP NAME' field with a red circle '1' around the label and a text input field containing 'GroupTest!'. Below this, there are two rows of checkboxes for selecting cameras and VPNs. The first row has 'name1' (checked) and 'name5' (checked), with buttons 'REGISTER CAMERA' and 'REGISTER VPN' respectively. The second row has 'name2' (unchecked) and 'name6' (unchecked). Below these, there are more checkboxes for 'name3' (checked) and 'name4' (checked), with buttons 'REGISTER SUP' and 'name7' (unchecked). A 'TestSkola' section follows. Then, there are three circular buttons labeled 'name1', 'name3', and 'Doma'. A large 'REGISTER' button is in the center. To the right, there is a 'SETTINGS' panel with 'BACK' and 'DELETE GROUP' buttons. At the bottom, there is an 'ADD TO GROUP' button and a 'groups' section with three circular buttons labeled 'U3name1', 'U3name2', and 'U3name3'. A red circle '4' is around the 'ADD TO GROUP' button. A red circle '5' is around the 'SETTINGS' panel.

Obrázek 11 Registrace skupiny.

Skupiny slouží pro sdílení přístupu ke kamerám nebo pouze pro lepší organizaci. Pro vytvoření skupiny stačí vyplnit pouze jméno skupiny ve formuláři viditelného na obrázku 11. Je nabídnut navíc seznam kamer, avšak pro vytvoření skupiny není nutné přiřadit kamery ihned. Vložení dodatečných kamer do skupiny lze provést přes nastavení skupiny.

## 5.5 Nastavení skupiny

Pro přidání kamer do skupiny, správa jejich parametrů a obecné nastavení skupiny se provádí na stránce vyobrazené na obrázku 12. Například IP kamery již ve skupině přidané jsou obsaženy pod bodem 1 na obrázku 12. Všechny body obsažené v obrázku 12 jsou popsány v tabulce 7.



Obrázek 12 Nastavení skupiny.

Tabulka 7 Popis nastavení skupiny.

Odkazy	Popisek
1	Seznam kamer ve skupině.
2	Seznam kamer uživatele.
3	Základní informace o skupině (ID a jméno skupiny) a možnost skupinu přejmenovat nebo smazat.
4	Správa uživatelů skupiny.

V levé části jsou zobrazeny IP kamery přidělené do skupiny (obrázek 12 bod 1). K zašedlým kamerám uživatelé skupiny nemají přístup. Administrátor skupiny má možnost změnit nastavení kamer pomocí tlačítka SETTINGS a znepřístupnit kameru tlačítkem HIDE. Pro přidání dodatečných kamer do skupiny slouží seznam kamer, umístěný ve spodní části (obrázek 12 bod 2). Kliknutím na kameru ve spodní části, kterou uživatel již

přidal, systém přiřadí kameru do skupiny v levé části. Důležitým údajem je Group ID v části settings (obrázek 12 bod 3). Tento osmimístný kód jednoznačně identifikuje zaregistrované skupiny v celém systému a uživatel jej zadává při požadavku na registrování do cizí skupiny.

Uživatel má možnost zažádat o přidání se do skupiny kamer jiného administrátora skupiny přes požadavek na stránce s přehledem kamer. Pak je tento uživatel zařazen do seznamu Pending, odkud administrátor skupiny buď zamítne, vyloučí nebo přijme požadavek. Ve stavu Pending požadavek čeká na vyřízení administrátorem. Ten jej může přijmout (symbol "fajfky"), tím se dostane mezi uživatele, kteří mají povoleno sledovat kamery ve skupině (uživateli je odeslána zpráva o povolení přístupu do skupiny). Zvolením symbolu "křížek" systém požadavek zamítne a vymaže (uživateli je odeslána zpráva o zamítnutí přístupu do skupiny a uživatel již nemá možnost zažádat o účast ve skupině). Volba "odpadkového koše" zamítne požadavek, ale umožní uživateli znovu o účast požádat (opět se odešle zpráva uživateli).

## ZÁVĚR

Tato práce řešila problematiku streamování z IP video kamer. Měla za úkol navrhnout systém, který zpřístupní video záznam z IP kamer přes webový video server. Zároveň dbala na zachování bezpečnosti při přístupu k datům a snažila se o maximální jednoduchost navrhovaného řešení. Při navrhování bylo použito prostředků šířených pod licencí GNU GPL. Projekt byl řešen na platformě systému OS Linux. Byla zpracována webová aplikace, která uživateli po přihlášení poskytne možnost zobrazení registrované IP kamery a sledování online streamu. Na pozadí aplikace se spouští VLC server, zabezpečující připojení RTSP streamu kamery, jeho převzorkování na požadovanou kvalitu a velikost a zobrazení výsledného streamu ve formátu ogg v klientském rozhraní. Samotné připojení ke kameře využívá několika způsobů založených na směrování portů a VPN spojení. Veškerá instalace serveru a komponentů na serveru použitých proběhla přes příkazovou řádku v prostředí Linux. Pro hosting webové aplikace byl použit webový server Apache s podporou PHP skriptovacího jazyka a databázového systému MySQL. Uvedené technologie spojuje do jednoho celku hostingová aplikace IPSConfig v3. Jelikož aplikace poskytuje citlivá obrazová data, byl kladen důraz na zabezpečení uživatelských přístupů pro přihlášení do aplikace a zároveň možnost sdílení kamer mezi jednotlivými uživateli definovaných skupin. Ty má možnost administrátor tvořit a spravovat. K jedné kameře má tak přístup více uživatelů (i několik desítek), přičemž vlastní kamera je zatížena pouze jedním video streamem vysílaným na server. Využitím skupin má uživatel možnost lépe zorganizovat své kamery, rozdělovat práva na jejich sledování mezi další uživatele. Systém byl navržen, zpracován a vytvořen pro praktické využití uživateli. Teprve větší počet uživatelů a připojených kamer prověří zatížení serveru a dimenzování hardwaru. Ve zkušebních podmínkách při testování pěti IP kamer se systém choval stabilně. Tento systém řešil pouze základní problémy týkající se připojení kamer, zobrazení streamu na webovém portále a základního uživatelského rozhraní.

Další fáze vývoje tohoto systému bude zaměřena na rozšíření možností zobrazení videa v různých kvalitách obrazu, možnosti záznamu video streamu, uchování a následné přehrávání z video archivu, možnosti sledovat více kamer najednou a vytvoření mobilní aplikace.

## SEZNAM POUŽITÉ LITERATURY

- [1] ICECAST. Introduction. *Icecast.org* [online]. ©2004-2014 [cit. 2015-03-16]. Dostupné z: <http://www.icecast.org/docs/icecast-2.4.1/introduction.html>
- [2] IPCAMLIVE. How does it work? *Ipcamlive.com* [online]. ©2015 [cit. 2015-03-18]. Dostupné z: <http://ipcamlive.com/howdoesitwork>
- [3] ISPCONFIG. Services and Functions. *Ispconfig.org* [online]. ©2015 [cit. 2015-03-21]. Dostupné z: <http://www.ispconfig.org/page/en/ispconfig/services-and-functions.html>
- [4] GARRELS, Machtelt, 2008. *Introduction to Linux: A Hands on Guide* [online]. [cit. 2015-04-01]. Dostupné z: <http://www.tldp.org/LDP/intro-linux/intro-linux.pdf>
- [5] SCAMBRAY, Joel a Stuart McCLURE a George KURTZ, 2002. *Hacking bez tajemství*. Vyd. 2. aktualizované. Praha: Computer Press. ISBN: 80-7226-644-6.
- [6] NOYES, Katherine, 2010. *Why Linux Is More Secure Than Windows* [online]. ©2010 [cit. 2015-04-06]. Dostupné z: [http://www.pcworld.com/article/202452/why\\_linux\\_is\\_more\\_secure\\_than\\_windows.html](http://www.pcworld.com/article/202452/why_linux_is_more_secure_than_windows.html)
- [7] HATCH, Brian a James LEE a George KURTZ, 2002. *Linux - Hackerské útoky*. Praha: SoftPress. ISBN: 80-86497-17-8.
- [8] HELMKE, M., E. K. JOSEPH, J. A. REY a P. BALLEW, 2014. *The Official Ubuntu Book*. Vyd. 8. New Jersey: Prentice Hall. ISBN: 0-13-390539-X.
- [9] BOWEN, Rich a Ken COAR, 2003. *Apache Cookbook*. Sebastopol: O'Reilly. ISBN: 0-596-00191-6.
- [10] DuBOIS, Paul, 2002. *MySQL Cookbook*. Sebastopol: O'Reilly. ISBN: 978-0-596-00145-2.
- [11] SKLAR, David a Adam TRACHTENBERG 2002. *PHP Cookbook*. Sebastopol: O'Reilly. ISBN: 1-56592-681-1.
- [12] LANE, David a Hugh E. Williams 2004. *Web Database Application with PHP and MySQL*. Vyd. 2. Sebastopol: O'Reilly. ISBN: 0-596-00543-1.
- [13] YUAN, Ruixi a W. Timothy STRAYER 2001. *Virtual private networks: technologies and solutions*. Boston: Addison-Wesley. ISBN: 0201702096.



- [14] VIDEO LAN. Videolan.org [online]. ©2015 [cit. 2015-05-02]. Dostupné z: <https://www.videolan.org/>
- [15] MICROSOFT. Implementace ověřování PEAP-MS-CHAP v2 pro síť Microsoft PPTP VPN. *support.microsoft.com* [online]. ©2015 [cit. 2015-05-06]. Dostupné z: <https://support.microsoft.com/en-us/kb/2744850/cs>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

CCTV	Closed Circuit Television.
CGI	Common Gateway Interface.
CSS3	Cascading Style Sheets.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System.
DVR	Digital video recorder.
FCGI	FastCGI.
FTP	File Transfer Protocol.
GNU GPL	GNU General Public License.
HD	High-definition.
HTML5	HyperText Markup Language.
HTTP	Hypertext Transfer Protocol.
ICMP	Internet Control Message Protocol.
ID	Identification.
IMAP	Internet Message Access Protocol.
LDAP	Lightweight Directory Access Protocol.
MAC	Media Access Control.
MPPE	Microsoft Point-to-Point Encryption.
NAT	Network address translation.
NNTP	Network News Transfer Protocol.
NTP	Network Time Protocol.
ODBC	Open Database Connectivity.
OS	Operation system
PC	Personal computer.

---

PHP	Hypertext Preprocessor.
POP3	Post Office Protocol 3.
PPTP	Point-to-Point Tunneling Protocol.
RAM	Random-access memory.
RTSP	Real Time Streaming Protocol.
SMTP	Simple Mail Transfer Protocol.
SNMP	Simple Network Management Protocol.
SQL	Structured Query Language.
SSL	Secure Sockets Layer.
TCP	Transmission Control Protocol.
TLS	Transport Layer Security.
UDP	User Datagram Protocol.
URL	Uniform Resource Locator.
VCD	Video CD.
VPN	Virtual private network.
WDDX	Web Distributed Data Exchange.
XML	Extensible Markup Language.

**SEZNAM OBRÁZKŮ**

Obrázek 1 VPN spojení s uživatelským routerem. ....	9
Obrázek 2 VPN spojení z routeru Mikrotik. ....	22
Obrázek 3 Relace mezi tabulkami v databázi. ....	35
Obrázek 4 Rozvržení úvodní stránky. ....	36
Obrázek 5 Rozvržení přihlašovací stránky. ....	37
Obrázek 6 Rozvržení profilové stránky. ....	38
Obrázek 7 Rozvržení stránky uživatele. ....	40
Obrázek 8 Registrace kamery. ....	41
Obrázek 9 Registrace VPN spojení. ....	42
Obrázek 10 Registrace kamery spojené přes VPN. ....	43
Obrázek 11 Registrace skupiny. ....	44
Obrázek 12 Nastavení skupiny. ....	45

**SEZNAM TABULEK**

Tabulka 1 Příklad SQL příkazu. ....	17
Tabulka 2 Popis úvodní stránky.....	36
Tabulka 3 Popis přihlašovací stránky. ....	37
Tabulka 4 Popis profilové stránky. ....	38
Tabulka 5 Seznam systémových zpráv. ....	39
Tabulka 6 Popis stránky uživatele. ....	40
Tabulka 7 Popis nastavení skupiny.....	45

## **SEZNAM PŘÍLOH**

- P I            Smluvní podmínky
- P II           Webová aplikace [video.3wpro.cz](https://video.3wpro.cz)

## **PŘÍLOHA P I: SMLUVNÍ PODMÍNKY**

Smluvní podmínky užívání služeb serveru dostupném z internetové adresy <http://www.video.3wpro.cz>

### **Úvod**

Společnost XYZ s.r.o., se sídlem na adrese Hálkova 5 Praha, PSČ: 150 00, IČ: 29587071, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 6493 (dále jen „Provozovatel“), je provozovatelem internetového serveru video.3wpro.cz, dostupného z internetové adresy (URL) <http://www.video.3wpro.cz>. Služba video.3wpro.cz umožňuje Klientům prostřednictvím Provozovatele registrovat, sledovat a sdílet své IP kamery.

### **1. Používání a přístup ke službě video.3wpro.cz**

1.1. Přístup ke službě video.3wpro.cz mají pouze registrovaní zákazníci na tomto video serveru. Zákazníkem se pro účely těchto podmínek rozumí jakákoli osoba, která si u Provozovatele zaregistrovala účet.

1.2. V současné době se za používání služby video.3wpro.cz neplatí žádný poplatek. Provozovatel však může kdykoli dle svého výhradního uvážení zavést poplatek, předplatné nebo jiný poplatek či podmínku týkající se používání služby video.3wpro.cz poté, co o tom informuje zákazníka

1.3. Provozovatel si vyhrazuje právo dle svého výhradního uvážení, a bez předchozího informování zákazníka, odepřít přístup nebo ukončit přístup ke službě video.3wpro.cz či tuto službu upravit, zastavit nebo přerušit. Změny veškerého obsahu naplánovaného ve službě video.3wpro.cz jsou vyhrazeny a Provozovatel může změnit, zastavit, nahradit nebo stáhnout obsah ve službě video.3wpro.cz dle svého absolutního uvážení, a aniž o tom informuje zákazníka.

1.4. Vstupem do služby video.3wpro.cz zákazník přijímá zde uvedené podmínky.

### **2. Možné časové zpoždění**

2.1. Provozovatel upozorňuje, že navzdory skutečnosti, že je služba video.3wpro.cz propagována jako „live“ (přímý přenos), může při vysílání docházet ke zpoždění, které

může trvat několik sekund. Podrobné údaje o přesné délce zpoždění nelze poskytnout. Provozovatel odmítá přijmout jakoukoli odpovědnost za jakoukoli ztrátu, která byla způsobena tímto zpožděním, protože zákazník službě video.3wpro.cz důvěřuje.

### 3. Vyloučení odpovědnosti

3.1. Provozovatel výslovně odmítá přijmout jakoukoli odpovědnost za to, že služba video.3wpro.cz bude přerušena, bude poruchová nebo nebude zákazníkům dostupná během oznámených hodin. Provozovatel dále odmítá přijmout jakoukoli odpovědnost za to, že video.3wpro.cz nesplňuje technické požadavky zákazníka a že nebude fungovat ve spojení s jakýmkoli konkrétním softwarem nebo hardwarem.

3.2. Provozovatel nezaručuje určitou video kvalitu služby video.3wpro.cz, protože vysílání závisí na internetovém připojení uživatele, na něž nemá Provozovatel vliv. U jednotlivých událostí se také může lišit nabízená kvalita a velikost obrazu.

3.3. Provozovatel nenese odpovědnost za žádnou přímou či nepřímou ztrátu, včetně mimo jiné ztráty zisku, dat, podnikání či obchodních hodnot, které zákazník utrpí, protože důvěřuje službě video.3wpro.cz.

### 4. Práva duševního vlastnictví

4.1. Všechny nabízené video obsahy jsou chráněny právy duševního vlastnictví. Právo využívat službu video.3wpro.cz je nevýhradní, nepřevoditelné a odvolatelné a uděluje se pouze pro osobní, soukromé, nekomerční účely. Autorská práva, ochranná známka a další vlastnická oznámení nejsou používáním ze strany zákazníka narušena. Jinak může Provozovatel právo na používání služby video.3wpro.cz příslušnému zákazníkovi odebrat.

4.2. Užívání služby video.3wpro.cz nesmí být v rozporu s právním řádem České republiky, zejména nesmí docházet k porušování práv duševního vlastnictví -autorských práv a práv souvisejících s právem autorským nebo průmyslových práv, k předpisům upravujícím nekalou soutěž a trestním předpisům.

4.3. Uživatel služby video.3wpro.cz ručí za dodržení zákona 101/2000 Sb., o ochraně osobních údajů při instalaci IP kamer. Zároveň bere ohled při monitorování prostor na práva na ochranu soukromí na pracovišti §316 zákoníku práce, zák. č. 262/2006 Sb.



4.4. Zákazníci nesmějí kopírovat, ukládat ani upravovat či distribuovat obsah služby video.3wpro.cz, ani v těchto činnostech podporovat třetí osoby.

4.5. Obsah služby video.3wpro.cz nesmí zákazník vysílat na veřejnosti, ani v případě, že se za něj neplatí žádný poplatek, a nesmí v této činnosti podporovat ani jinou osobu.

4.6. Kterýkoli zákazník, který poruší ustanovení těchto podmínek, může být zažalován o náhradu škody. Patří sem i porušení práv třetích osob, které mohou zákazníka rovněž zažalovat.

## 5. Obecná ustanovení

5.1. Provozovatel může tyto podmínky kdykoli změnit. Pokud provede významné změny, bude o tom informovat zákazníka. Navzdory těmto informacím zůstává odpovědností každého zákazníka, aby si podmínky čas od času zkontroloval. Pokud zákazník pokračuje ve využívání služby video.3wpro.cz poté, co byly podmínky změněny, má se za to, že tyto změněné podmínky přijal.

5.2. IP kamery a IP kamerové systémy musí splňovat veškeré podmínky Zákona o ochraně osobních údajů, dodrženy všechny stanovené principy a zároveň splněna přiměřenost a úměrnost zásahu do osobnostních práv subjektů údajů. Přiměřenost a úměrnost zásahu do osobnostních práv subjektů údajů je podle § 5 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, určena deklarovaným účelem a dále zvolenými prostředky.

5.3. Služba video.3wpro.cz neprovádí záznam z kamerových systémů, proto nepodléhá oznamovací povinnosti vůči Úřadu pro ochranu osobních údajů.

## **PŘÍLOHA P II: WEBOVÁ APLIKACE VIDEO.3WPRO.CZ**

Přiložena na CD ve složce video.3wpro.