

Informačný systém ICM²

Opis technického vybavenia

1 ICM² – TECHNICKÝ OPIS SYSTÉMU

ICM² spoločnosti Positive s.r.o. je informačný systém, určený pre **finančných poradcov a sprostredkovateľov poistenia – poisťovacích maklérov a agentov**, na správu poisťných zmlúv, kontrolu a rozdeľovanie prichádzajúcich provízií a podporu vybraných biznis procesov.

1.1 CHARAKTERISTIKA INFORMAČNÉHO SYSTÉMU ICM²

Internetová verzia ICM² je klient-server aplikácia a funguje na princípe tzv. *tenkého klienta*. Aplikácia je ihneď po nainštalovaní na server prístupná prostredníctvom internetového prehliadača, čo umožňuje používateľovi využívať aplikáciu aj prostredníctvom internetu.

Systém ICM² je aplikácia, postavená na webovej technológii, s využitím skriptovacieho jazyka PHP a databázy MySQL. Celý systém je zhotovený vo frameworku WebDoors spoločnosti Positive s.r.o..

1.2 BEZPEČNOSŤ A OCHRANA OSOBNÝCH ÚDAJOV

1.2.1 Fyzická bezpečnosť

Servery, na ktorých je aplikácia hostovaná sú umiestnené:

- priamo u klienta – v tomto prípade za fyzickú ochranu serverov zodpovedá samotný klient, resp. ním poverená organizácia; alebo
- v hostingovom centre spoločnosti Positive s.r.o. – serverhousing VNET a.s.

Hostingové centrum spoločnosti Positive s.r.o. je okrem iného vybavené aj nasledovnými bezpečnostnými opatreniami:

- elektronický zabezpečovací systém
- kamerový systém
- 24/7/365 dohľad operačného centra
- bezpečnostné dvere so vstupom s kontrolou biometrických údajov
- redundantné klimatizačné jednotky napojené na záložné zdroje energie
- dvojité antistatická podlaha
- fyzicky nezávislé dva prívody elektrickej energie

- diesel generátor ako záložný zdroj elektrickej energie

1.2.2 Riadenie logického prístupu v rámci aplikácie

Aplikácia umožňuje riadenie logického prístupu na základe rolí jednotlivých používateľov. Systém umožňuje definovať používateľské práva pre jednotlivých používateľov, ktorí sú zaradení do skupín. Všetci používatelia v rovnakej skupine majú rovnaké oprávnenia.

Oprávnenia sú definované aj pre jednotlivé moduly. Tým je možné zabezpečiť a určiť, aké moduly môže ktorá skupina používateľov vidieť, prípadne, kto môže s akými modulmi pracovať.

Jednotlivé typy rolí a možnosti nastavenia ich oprávnení sú popísané v používateľskej dokumentácii k aplikácii. Riadenie prístupu v rámci aplikácie je plne v zodpovednosti klienta.

Aplikácia má implementovanú funkcionálnu správu hesiel, ktorá umožňuje vynútiť zmenu hesla používateľa na základe vopred definovaných parametrov (doba expirácie hesla, sila hesla a pod.).

1.2.3 Riadenie logického prístupu v rámci administrácie aplikácie

Administrácia aplikácie závisí od modelu implementácie. V prípade správy dodávateľom (Positive s.r.o.) sa pridelovanie administrátorského prístupu riadi internými smernicami dodávateľa. Ďalšie okolnosti sú predmetom dohody medzi dodávateľom a klientom.

1.2.4 Zaistenie bezpečnosti na úrovni infraštruktúry

Aplikácia (webservice) je dostupná pomocou internetového prehliadača. Na zaistenie dôvernosti prenášaných údajov je využitý protokol SSL verzia 3.0. Ak je to možné (pevná IP adresa, resp. rozsah IP adres klienta), prístup na aplikačný webservice je na sieťovej úrovni obmedzený len pre definovaných klientov.

Certifikát servera, resp. jeho odtlačok je bezpečným spôsobom doručený klientovi, s možnosťou overenia si autenticity servera, na ktorý prístupuje. Aplikácia nevyužíva overovanie klienta pomocou certifikátov – využíva sa riadenie prístupu pomocou prístupových práv popísaných vyššie.

Komunikácia webservice s databázou nie je šifrovaná, avšak databáza je hostovaná na izolovanom sieťovom segmente dostupnom len administrátorom systému.

Nakoľko je aplikácia dostupná z internetu, bola podrobená penetračným testom.

1.2.5 Logovanie a audit

Aplikácia umožňuje logovanie vybraných činností používateľov na základe predošlého nastavenia. Logy aplikácie sú chránené tak, aby nemohlo dôjsť k ich neautorizovanej zmene a čítaniu (okrem poverených administrátorov systému).

Za monitoring logov na technologickej úrovni je zodpovedný administrátor systému (poverený pracovník spoločnosti Positive s.r.o.), za monitoring logov používateľov je zodpovedný poverený pracovník klienta.

Osobné údaje sú v aplikácií spracovávané v súlade so zákonom č. 428/2002 Z. z. o ochrane osobných údajov, v znení neskorších predpisov.

1.2.6 Zálohovanie databázy

Zálohovanie celej databázy systému sa uskutočňuje pravidelne každý deň, pričom štandardne sú k dispozícii zálohy databázy systému za posledných 12 dní. Zálohy sú umiestnené na samostatnom záložnom serveri (nie produkčnom), na samostatnom fyzickom disku (nie disku, na ktorom beží záložný server). Podobne ako produkčný server, aj záložný server je umiestnený vo vyššie spomínanom serverhousingovom centre spoločnosti VNET a.s.

Prístup k vytvoreným zálohám databázy majú len administrátori systému spoločnosti Positive s.r.o.

Požiadavky na fyzickú a logickú ochranu záloh databázy sú rovnaké ako požiadavky na samotnú aplikáciu ICM² a jej databázu. Správa záloh a archivácia berie do úvahy požiadavky zákona č. 428/2002 Z. z. o ochrane osobných údajov, v znení neskorších predpisov.